UNIVERSITY OF PIRAEUS
DEPARTMENT OF
DIGITAL SYSTEMS

DIGITAL SYSTEMS
SECURITY DIRECTION

Risk Analysis and Risk Management in Critical Infrastructures

Master Thesis

By Motaki Katerina

Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in the Department of Digital Systems at University of Piraeus

PIRAEUS, DECEMBER 2016

Abstract

Cyber Physical Systems (CPS) are evolutionary development of embedded systems, into interconnected systems, taking advantage of network technologies to enhance systems' functionality and efficiency. They are considered as Systems of systems. They are used in different industrial sectors and Critical Infrastructures (CI), energy sector, extensively applied in Smart Grids, water supply systems and hazardous environments. They provide effective system management and enhanced accuracy. However, they inherit both vulnerabilities of IP technology and physical systems and they are characterized by increased risk due to complexity, nature and their critical importance.

During design phase, but also periodically during CPS lifetime, Risk Analysis (RA) is conducted in order to achieve and maintain a high security level. Such a security level is achieved by utilizing effective countermeasures or through adaptation in accordance to specific conditions, system changes and new threat discovery. RA aims at identifying what can go wrong, its causes, relevant probabilities, assets affected, consequences, estimate risks and set priorities for the protection of valuable assets, while setting guidelines for proper policies and countermeasures' selection.

Risk assessment involves the integration of threat, vulnerability, and consequence information. Risk management (RM) involves deciding which protective measures to take, based on an agreed risk reduction strategy. Many models/methodologies have been developed by which threats, vulnerabilities, and risks are integrated and then used to inform the allocation of resources to reduce those risks.

The current thesis presents a survey of RA and RM methods and methodologies applied in CPS domain. Some have already been widely applied, trusted and accepted, while some theoretical propositions are presented too. Most of existing techniques have not been developed with CPS characteristics in mind, though they are considered suitable or suggested for such usage. A set of criteria is developed for RA and RM methodologies comparison and evaluation. Advantages and disadvantages of each one are presented. Furthermore, an overall comparative presentation is attempted and general conclusions are made. Moreover, some frameworks and standards are presented in order to provide an overview of some of the most common conceptualizations of Risk.

More specifically, RA and RM methodologies will be evaluated in order to decide which one is more suitable for Critical Infrastructures. Current thesis presents methods advantages and disadvantages and evaluates them against a detailed set of comparison and evaluation criteria. In conclusion estimation about appropriateness for appliance in CPS environment is made, while in parallel specifications for relevant methodologies development, fulfilling special requirements is set. Criteria used not only apply to traditional RA methodologies stages like asset, threat and vulnerability identification but are oriented to requirements arising from CPS character and consider special CPS characteristics like dependencies, robustness, resilience and criticality.

Finally, in the conclusion of the thesis a comparison between two methodologies of risk management take place. More specifically, these methodologies will be examined in a general hospital use case. The point in this comparison is to decide which one is the most appropriate for Critical Infrastructures, such as a hospital.

Acknowledgements

I want to thank my parents for their patience, understanding and support during my postgraduate studies and the development of my master thesis. Furthermore, I want to thank the supervising professor, Dr. Konstantinos Lambrinoudakis from University of Piraeus, for help, advice, inspiration and guidance.

December 2016

Katerina Motaki

Table of Contents

Table of figures

List of tables

Acronyms

AMI	Advanced Metering Infrastructures
AT	Attack Tree
CAP	Cyber Access Point
CCI	Cyber Critical Infrastructures
CI	Critical Infrastructures
CPS	Cyberphysical Systems
CRAMM	CCTA Risk Analysis and Management Methodology
DOE	Department Of Energy
DDOS	Distributed Denial Of Service
DHS	Department of Homeland Security
DOS	Denial Of Service
EPCIP	European Programme for Critical Infrastructures Protection
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
EURAM	European Risk Assessment Methodology
FMEA	Failure Mode
FMECA	Failure Mode Critical
FTA	Fault Tree Analysis
HAZOP	HAZard and Operability analysis
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
INFOSEC	Information Security
IP	Internet Protocol
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
IT	Information Technology
MITM	Man In The Middle attack
MHA	Major Hazards Analysis
OAM	Operational Architectures Model
OCTAVE	Operational Critical Threats Assets Vulnerabilities Evaluation

PHA	Process Hazard Analysis
PN	Petri Net
PV	Photovoltaics
RA	Risk Analysis
RMG-DOE	Risk Management Guide – Department Of Energy
RVA	Risk and Vulnerability Assessment
SCADA	Supervisory Control And Data Acquisition
SNRA	Strategic National Risk Assessment
SVA	Security Vulnerability Assessment
THIRA	Threats Hazards Identification and Risk Assessment
VSAT	Vulnerability Self-Assessment Tool

Introduction

Cyber physical systems (CPS) are evolutionary development of embedded systems to interconnected systems. Embedded systems are computational units with dedicated functions built in mechanical / electrical systems, controlling, monitoring and recording electric/ mechanic devices function. CPSs extend the concept of embedded systems to wide interconnected systems using network technology, for system remote control, feedback, providing efficient, low cost communications. CPSs can be considered as interconnected systems of systems. They are collaborating computational elements controlling physical entities. However, the integration of this technology poses risks related to the inherent weaknesses of network technologies. Intruders may attempt to exploit these vulnerabilities and gain access to system resources or disrupt their operation.

CPSs are extensively used in critical infrastructures (CI), i.e. state and private infrastructures which support smooth operation of state critical functions. Their disruption may cause serious consequences in state function and citizens' everyday life. CI include electrical power plants, electricity transfer and distribution networks, water supply system, oil and natural gas distribution networks, telecommunications, public transportation including air transportation and commercial shipping, taxis and banking systems as well as basic industrial units such as chemical industries and nuclear power plants.

CPSs are used for efficient management and control of CI services and systems operation, lower operational costs. All sectors of modern economies, public facilities, communications and social services heavily rely on IT and CPS. Their disturbance or disruption could severely impact national economy and population. They are highly probable to be targeted by cyber criminals, hostile national entities, cyber-terrorists in extortion or cyber-attack schemes as these systems relying on network technologies, inherit their vulnerabilities, becoming subject of potential cyber-attacks exploiting relevant security inefficiencies and vulnerabilities. Consequences may be fatal for population health, security and wellbeing, economy and state stability because of the tremendous magnitude of the potential effects.

System design stages involve appropriate RA processes to identify potential threats and hazards, likelihood of their occurrence, systems' vulnerabilities, damages they will suffer under a possible attack and restoration costs. RA aims at the optimal design integrating foreseen security aspects and adopting effective security preemptive mechanisms. Ultimately intends to model system infrastructures, identify threats and vulnerabilities, threats and risks that are not obvious and estimate criticalities. RA process should be repeated periodically during systems' and infrastructures lifecycle to recognize potential risks resulting from changes, emerging threats and discovery of new vulnerabilities. Then security policies and appropriate prioritized countermeasures' strategies should be implemented based on risk estimations for optimal countermeasure selections.

RM is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. RM's objective is to assure uncertainty does not deflect the endeavor from the business goals.

Risks can come from various sources: e.g., uncertainty in financial markets, threats from project failures (at any phase in design, development, production, or sustainment life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters as well as deliberate attack from an adversary, or events of uncertain or unpredictable root-cause. There are two types of events i.e. negative events can be classified as risks while positive events are classified as opportunities. Several risk management standards have been developed including the Project Management Institute, the National Institute of Standards and Technology, actuarial societies, and ISO standards. Methods, definitions and goals vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety.

Risk affects different levels, entities and stakeholders and it is estimated for all concerned entities involved. RA is to take place in lower cyber and physical level of infrastructures in order to identify all relevant factors shaping risks and adopt the appropriate protective measures. Risk should be communicated and estimated for higher layers, operational and strategic, for all interested parts and stakeholders to make the optimal security investments and adopt effective protection strategies.

Risk sources are more often identified and located not only in infrastructural or technological assets and tangible variables, but also in human factor variables, mental states and decision making. The interaction between human factors and tangible aspects of risk highlights the need to focus closely on human factors as one of the main drivers for risk management, a "change driver" that comes first of all from the need to know how humans perform in challenging environments and in face of risks (Daniele Trevisani, 2007). As many describe, «it is an extremely hard task to be able to apply an objective and systematic self-observation, and to make a clear and decisive step from the level of the mere "sensation" that something is going wrong, to the clear understanding of how, when and where to act. The truth of a problem or risk is often obfuscated by wrong or incomplete analyses, fake targets, perceptual illusions, unclear focusing, altered mental states, and lack of good communication and confrontation of risk management solutions with reliable partners. This makes the Human Factor aspect of Risk Management sometimes heavier than its tangible and technological counterpart».

During the last decade likelihood of cyber-attacks has increased. Cyber-attacks aim at destroying or downgrade CI functions, ICS and ICT systems, like electrical power generators, Smart Grids and water supply systems. Vulnerabilities rise because of extended use of ICT, particularly use of commercial products. In [1] 120 cyber incidents involving attacks against ICS and SCADA systems are presented. Worms and other malware have been developed to impact such systems and infrastructures, while DDOS and APT pose highly dangerous threats against CPS.

Study of such cases indicates that cyber-attacks have often political and religious motivation. In the case of Logan Energy, a fuel cell energy provider for residential, commercial and industrial systems, with customers like US Armed Forces Critical Facilities, attackers left

defacement indicating their religious beliefs in Islam. These facilities had been related to missile facilities, aircraft communication and air traffic control. No just defacement had been achieved but also lists with operators and customers' personal data had been accessed during SQL injection attacks. In turn these data could be used for targeted phishing attacks against systems operators and social engineering in order to gather critical information for gaining access to critical systems. In 2007 the Aurora test at Idaho National Laboratories, showed that a power generator could be accessed remotely by hackers over the internet and destroyed [2]. Another example is the development and attack of the Stuxnet worm, which attacked the Iranian nuclear infrastructures. Stuxnet has been primarily written to target Industrial Control Systems (ICS). Its goal has been to reprogram ICS by modifying code on Programmable Logic Controllers (PLC) to make them work in a way the attacker wanted and hide those changes from the operators of the equipment [3]. In January 2003 a worm attack against the networks of Davis-Besse nuclear power plant in Ohio, USA disabled its safety monitoring system for almost five hours. The Maroochy water SCADA breach in Australia attacked and disabled the wastewater treatment systems for two months and leaked hundreds of thousands of gallons of putrid sludge into parks, lakes, rivers and private properties and caused the death of marine life, pollution of creek waters and an unbearable stench in the surrounding areas [4]. During the period 2007-2009 one in five CI entities reported being victim to extortion through cyber-attacks or threatened cyber-attacks. Most of the victims belonged to the power, oil and gas industry according to McAfee global report on key industries [2]. In November 2009 there had been reports about two power outages in Brasil, in 2005 and 2007, caused by hackers perhaps as part of an extortion scheme [2]. In September 2009 Pacific Energy Resources Exploration Company had been under cyber-attack. Company's IT consultants had been found guilty for tampering SCADA systems designed to alert operators of leaks or other damage to the miles-long undersea company's pipelines [2]. During the period 6th to 12th May 2001 California experienced two days rolling blackouts affecting 400,000 customers, caused by cyber-attacks originating from China, focused on May 7th , the day for the anniversary of Chinese embassy in Kosovo accidental bombing, while initial access in systems' servers estimated on April 25th 2001. It was characterized as a catastrophic breach [5]. On December 26th 2006 a Turkish hacker hacked the website of Tascomp company in UK. This company had been developing industrial SCADA software. That hacker stole a customer list including well known trends and industries as well as infrastructures and operators personal information [80]. National Science Foundation Amundsen Scott South Pole Station science research facilities were penetrated and hackers gained access to servers controlling station radio telescope [5]. In 2000 according to Russia's Interior Ministry Turkish hackers collaborated with Gazprom insider used Trojans to attack the central switchboard which controls gas flow in pipelines, although Gasprom gas provider refused the existence of such incident. In May 23rd of 2008 hackers attacked nuclear power related websites that provided information about radiation levels, while they spread false rumors about a nuclear accident in St. Peteburg. Hackers had brought down for several hours all webpages providing access to Automatic Radiation Environment Control System according to officials of the Rosatom Nuclear Energy State Corporation. In October 2009 hackers gained control over computers controlling critical watering systems in Harrisburg, while WATERISAC declared that there had been four similar

attacks in the last four years. In January of 2003 operations in the nuclear power plant Davis Besse in Ohio had been interrupted because of the attack of the Slammer Worm [5]. A quite recent incident is presented in [6]. Adversaries showed knowledge of ICS and were able to cause multiple system failures, impacting critical process components resulting in massive physical damages using APT tactics and tools. Using social engineering techniques attackers send malware implanted in attached to emails pdf files and then worked their way in the production line through the local network, opening network connections and infecting ICSs. Controlling components failed causing furnace malfunctions, leading to unexpected conditions and physical damages, because of furnace explosion.

Many other occasions have been set under investigation because incident conditions have been unclear. In many cases, incidents are supposed not being successful or it had not been possible to be identified as cyber-attacks. So, no safe conclusions have been made or incase conclusions are extracted they may have not been made known in public. Because of the Critical character of such infrastructures events and investigations in many occasions are kept secret by national authorities, in order to avoid spreading panic and terror.

The current thesis is a survey of CPS and CI RA and RM methods and methodologies. It presents methods advantages and disadvantages and evaluates them against a detailed set of comparison and evaluation criteria. In conclusion estimation about appropriateness for appliance in CPS environment is made, while in parallel specifications for relevant methodologies development, fulfilling special requirements is set. Criteria used not only apply to traditional RA and RM methodologies stages like asset, threat and vulnerability identification but are oriented to requirements arising from CPS and CI character and consider special CPS and CI characteristics like dependencies, robustness, resilience and criticality. Criticality is expanded to a set of criteria, more than consequence magnitude. Consequences and measurement is difficult in traditional methodologies; this difficulty not only remains in the case of CPS but even gets even more difficult as consequences get even higher complexity and extension.

Additionally, in the conclusion of the thesis a comparison between two methodologies of risk management take place. More specifically, the methodologies are CRAMM and MAGERIT in a general hospital use case. The point in this comparison is to decide which one is the most appropriate for Critical Infrastructures, such as a hospital.

1 Chapter 1 – Cyber Physical Systems and Critical Infrastructures

1.1 Definitions

1.1.1 Cyber Physical Systems

CPS technology is based on embedded systems technology. Actually CPS are evolutionary development of embedded systems and can be considered as interconnected embedded systems. Embedded systems are computational units which are embedded to electromechanical systems. Both, they function as a unified system, hardware and software. They use their dedicated functions for system overall function controlling. So, they are unified systems of computational and physical processes, where the first provide control over the hardware part functions and physical processes. CPS extends the concept of embedded systems to wide interconnected systems using network technology, for the purpose of systems' remote control, feedback reception to the controller station, and low cost effective communications. CPS can be considered as systems of systems using interconnections. They are collaborating computational elements controlling physical entities. They are using computer power to provide surveillance, command and control to a wide range of applications from everyday life like traffic control systems and smart home functions, to high level industrial functions and processes, controlled by ICS and SCADA systems. They guarantee effectiveness and accuracy in the controlled processes, ensuring that controlled devices function according to predefined standards, providing accurate and standardized results, possibly characterized by criticality, strict specification and high requirements of quality, regularly in hazardous environment where man is impossible to work.

"A system is a combination of interacting elements organized to achieve one or more stated purposes. Systems of systems apply to systems-of-interest, whose systems' elements themselves are systems; typically these entail large scale inter-disciplinary problems with multiple, heterogeneous, distributed systems." [7, 8]

"Cyber Physical Systems term refers to the tight conjoining of and coordination between computational and physical resources. We envision that the cyber-physical systems of tomorrow will far exceed those of today in terms of adaptability, autonomy, efficiency, functionality, reliability, safety, and usability. Research advances in cyber-physical systems promise to transform our world with systems that respond more quickly (e.g., autonomous collision avoidance), are more precise (e.g., robotic surgery and nano-tolerance manufacturing), work in dangerous or inaccessible environments (e.g., autonomous systems for search and rescue, firefighting, and exploration), provide large-scale, distributed coordination (e.g., automated traffic control), are highly efficient (e.g., zero-net energy buildings),

augment human capabilities, and enhance societal wellbeing (e.g. assistive technologies and ubiquitous healthcare monitoring and delivery).”[7, 9]

CPS is a set of systems that uses computational processes to control physical processes; they use interconnections, networking and cooperation relationships between them. They satisfy the necessity of physical processes to be controlled through feedback loops. Interconnected embedded systems then affect these physical processes and vice versa. CPS is designed as a network of interacting computational and physical devices. Opposite to traditional embedded systems, typical CPS are designed and implemented as a network of elements which function with interactions between them using physical input and providing physical outputs, and they do not function as completely autonomous devices. Individual interconnected elements are subsystems belonging to one of following categories:

a. Activators and encoders
b. Systems of adaptive and predictive control
c. Systems of intelligent control
d. Real time control systems
e. Systems with human controllers on feedback loops.

CPS functionality is based on techniques of conceptualization and physical processes modeling. The first ones describe physical processes progress while the others are related to transformation of analogue signals to digital data and digital data to analogue commands as well as processing of digital information.
Large scale CPS interconnections and the ability to dynamically change the system structure during processes raise CPS complexity to extremely high levels. Modeling of network, interconnection and communications taking into account time delays, packet dropping and communication constraints requires effective and efficient management and the use of advanced non-conventional control techniques regardless the level of complexity. CPS design needs the use of improved design tools. That means high cost of CPS having a direct impact to cost of maintenance and repair on the event of faults and physical or cyber-attacks. Therefore there is imperative need to discover and use security mechanisms and services for error and attack detection, threat and relative risk identification and estimation to handle risks and mitigate or limit their impacts and consequences. So cyber security strategies are implemented on CPS to protect them from disturbances due to endogenous systemic factors or exogenous influences and guarantee their proper function in complex environment.

1.1.2 Critical Infrastructures

The dynamics of CPS are showed today to be much greater than it was originally estimated. The decreasing computational cost and the need of finding new ways of producing, managing and saving energy, while the energy costs and energy demands

present increasing rates and in the opposite gradually reduced quantity of produced energy led to the development and use of CPS in energy sector. Health, water supply in urban environment and public transportation are areas where incentives for improvement, economic and social require more investments for the development of such technology. CPS are applied to numerous technological applications related to areas such as transportation, communications, urban water supply and distribution, medicine, robotics, defense, energy production and distribution including gas, petroleum and electricity. Particularly the application of CPS to electricity energy sector spearheaded development of smart grids.
Therefore, CPS are directly related to Critical Infrastructures (CI) command and control. CI is defined as "*an asset, system or part thereof located in Member States which is essential for maintenance of vital societal functions, health, safety, security, economic or social well – being of people and the disruption of which would have a significant impact in a Members State as a result of the failure to maintain those functions*". So, disrupted or destroyed CI provoke serious consequences to citizens, society and the state as a whole.

Moreover, we can determine that "Critical Infrastructures is large-scale infrastructures, whose degradation or destruction would have a serious impact on health, safety or well-being of citizens or the effective functioning of governments and / or the economy.

Typical examples of such infrastructures are the sectors of telecommunications, Electricity, Natural Gas and Petroleum, Banking and Financial System, Transportation, Water supply Systems, Government services, Emergency services, Food / Agriculture (production, storage, distribution), Health, Education and numerous goods (iron, steel, aluminum)".

Figure 1: *Generic production model*

Noticing that CIs are divided into **four** levels:

a. **business / strategic**, which includes the central business process
b. **organizational**, concerning the structure, processes and human behavior
c. **cyber**, which is associated with data, communication and information systems, including the management systems for the physical layer (e.g. SCADA)
d. **physical**, in which we meet the physical devices of the respective infrastructures (e.g. in electricity infrastructures meet indicative generators, switches, cables)

1.1.3 Criticality

Criticality can be expressed as the extreme importance of consequence caused by the destruction or unavailability, permanent or temporal, of an asset or a service. Critical events present consequences with vast magnitude and affect seriously economy, population safety and health, population well-being, and may cause mass psychological effects. Fatalities and health problems, financial effects, environmental damage, population everyday life disturbance, impacts to public vital services and trust to government and state, sorrow and hurts, downgrading or denial of services may be caused because of attacks against critical assets.

This type of consequence is referred as Critical Consequence and relevant assets are characterized as Critical Assets. Correspondingly vulnerabilities which when exploited may lead to critical effects can characterized as Critical Vulnerabilities and impacts as Critical Impacts.

Estimation of time for unavailable critical service or asset to become available again partially or completely restored, before serious consequences start appearing is needed to define criticality. If unavailability cannot be tolerated over some time period this fact results to relevant asset receiving characterization of critical asset. Criticality is also related to the availability of back up services and alternative assets, when major assets and services are brought down by attacks or damages. If there is not any other alternative solution when assets or services are impacted then this fact amplifies critical asset characterization of assets and services. Additionally, when recovery of an asset to its initial state after being impacted is not feasible in reasonable time and with reasonable restoration costs and there are no alternatives and unavailability is not tolerated, then these facts amplify critical characterization. Finally, apart the asset and services criticality the entire criticality of the infrastructures should be taken into consideration.

An asset may be characterized critical in two different aspects:

a. The first one relates criticality to operation, so asset is considered critical for the organization operation. When it becomes unavailable or being impacted it affects organization operations and consequences interest only the organization.

b. The second aspect is related to consequences to the interested parts: stakeholders, population, customers and State. Consequences apply not only inside the organization but spread over a wide area affecting more interested parts.

For example, cyber-attack against the SCADA system controlling the waste treatment of a chemical industry may not impact its production processes, so it is not critical for the organization operation, but on the contrary such impact would cause extremely severe environmental consequences affecting nearby population, so being critical in this aspect. In the other hand, cyber-attacks against a main power

generation plant for 24 hours, causing critical damages would not influence residential areas severely, although it could be an inconvenience, but it could be critical for industry where financial losses would be high or for other involved market stakeholders.

1.1.4 Risk Assessment

"The process of determining the likelihood that a specified negative event will occur. Investors and business managers use risk assessments to determine things like whether to undertake a particular venture, what rate of return they require to make a particular investment and how to mitigate an activity's potential losses".

More specific, Risk Assessment can be determined as "*the determination of quantitative or qualitative estimate of risk related to a concrete situation and a recognized threat. Quantitative risk assessment requires calculations of two components of risk (R): the magnitude of the potential loss (L), and the probability (p) that the loss will occur."*

***"Acceptable risk** is a risk that is understood and tolerated usually because the cost or difficulty of implementing an effective countermeasure for the associated vulnerability exceeds the expectation of loss*. For example, *"Health risk assessment" includes variations, such as risk as the type and severity of response, with or without a probabilistic context.*

In all types of engineering of complex systems sophisticated risk assessments are often made within Safety engineering and Reliability engineering when it concerns threats to life, environment or machine functioning. The nuclear, aerospace, oil, rail and military industries have a long history of dealing with risk assessment. Also, medical, hospital, social service and food industries control risks and perform risk assessments on a continual basis. Methods for assessment of risk may differ between industries and whether it pertains to general financial decisions or environmental, ecological, or public health risk assessment."

1.1.5 CI characteristics

The spatial and geographical scale is a key feature of a CI, because in case of a security incident event on a single gas compressor the risk analysis will be limited to system level and down (subsystem, unit, part), as opposed to a national level electricity infrastructures, where the analysis will take place at national or international level, but also in infrastructures or interdependent infrastructures.

A second characteristic is the time scale, which indicates the time that an action lasts, such as the operation of an energy system which contributes to the evaluation of interdependence.

Directly linked to the above temporal component is loose or no connections, as a loose interdependence, the effects of an infrastructures do not affect in a short time-dependent infrastructures.

Subsequently, operational factors such as Backup and redundant systems, security policies, contingency plans, education and training affect the way a CI will react to an event.

Finally, organizational factors, such as the government as opposed to private ownership of an infrastructures impact in their own way in dependencies between infrastructures.

1.1.6 CI toughness

The dependence of the critical infrastructures of the achievements of technology has made the availability factor in determining their smooth operation. However, the variable nature of technology has affected the reliability of the CI. Thus, the creation of resistant CI (CIR) is a challenge. Resilience focuses on preventing occurrence of critical failures or minimize their impact if ultimately occur. It is the ability of infrastructures to resist the impact of a threat (external or internal) and maintain their core functionality.

"Resilience is the ability to absorb, recover or adapt successfully to adversity or change of circumstances."

Similar approaches is that which provides resilience with terms such as "absorptive" through "robustness" and "redundancy", "adaptive" which means the extent to which the system is capable in itself for a recovery through "substitutability" and "restorative", which means the ability of the system to be corrected quickly.

Furthermore, another approach is that used terms such as, "robustness", "restorative", that are the management of an incident during evolution, "rapid recovery" and "adaptability", which are the ability to learn from a new incident.

Finally, it is said that resistance is determined by two parameters, ***performance*** and ***recovery time*** under normal conditions.

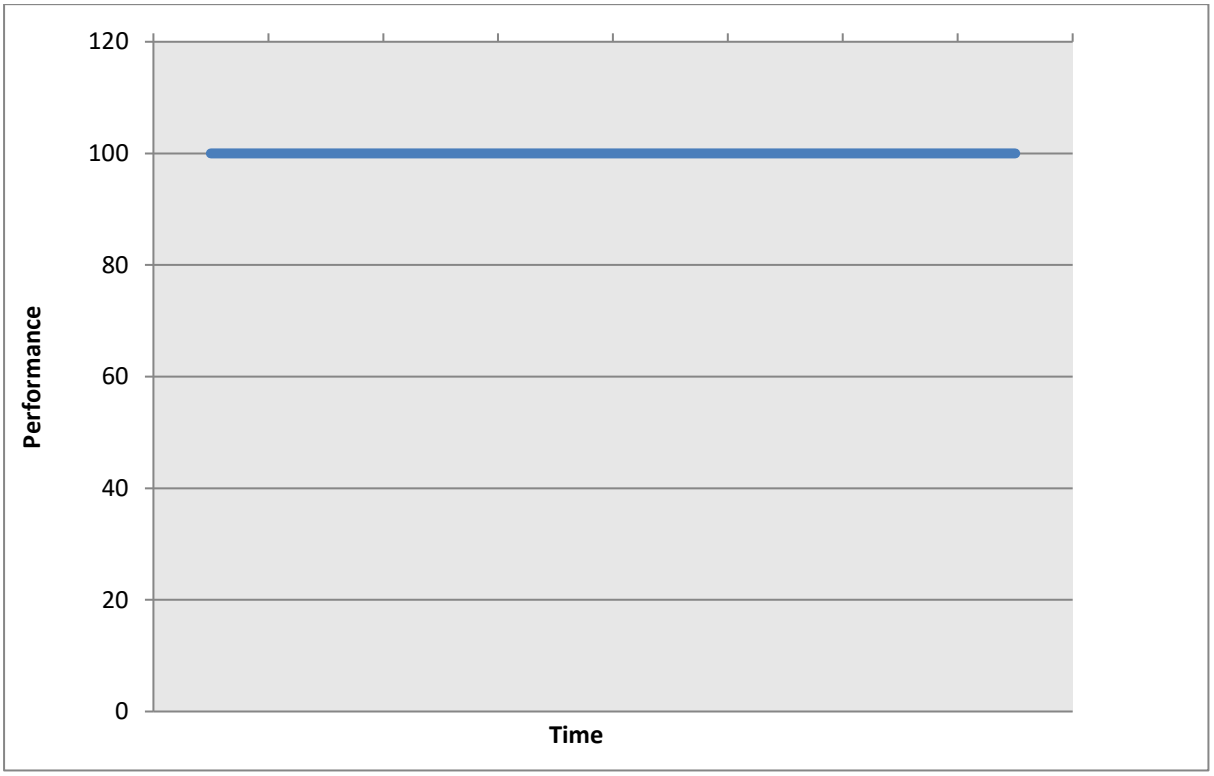


Figure 2: *Parameters of resilience under normal conditions*

In an event of a failure or in non-normal situation as shown above change and as a consequence we lose the service provided. But after the end of that period the yield are reset (normal mode).

2 Chapter 2 – Cyber Physical Systems' Security and Risk

2.1 Cyber Physical Systems' Security

The top three objectives concerning cyber physical systems are availability, integrity and confidentiality. Security significance objectives according to NIST [12, 15] are:

a. **Availability:** Timely and reliable access of information is of the most importance in CPS. Loss of information may disrupt and undermine services delivery. For example, in Smart Grid case availability loss is translated to electrical power unavailability.

b. **Integrity:** Guarding against improper information modification or destruction to ensure non repudiation and authenticity. Power grid components are controlled with SCADA systems and other ICS which communicate with distant controlling modules and exchange sensitive information. Latency in these systems is important as well as controlling messages and commands; power grid's physical safety and functionality depends on accurate information exchange inside strict time frames. Improper handling, message delays or modification of control messages and commands could be disastrous for electrical network and interconnected electrical devices safety as sudden electrical network anomalies would not be detected and reported directly, activating feedback and protective / controlling mechanisms.

c. **Confidentiality** is significant mostly in operational and strategic layers; information related to smart grid structure, protocols, access mechanisms, encryption methods and keys, operators personal information, organization strategy, customers' personal and economic data, key design properties of power grid and important security aspects need to remain confidential and be accessed only by authorized personnel. This information could be used for attack plan preparation exploiting sensitive aspects if it was accessed by hackers.

In contrast with classical legacy power systems, Smart Grids feature a rather open and widespread communication network. So, it is considered impossible that none of the nodes or parts of the Smart Grid system will be invulnerable to attacks. The same vulnerability applies to any other widespread CPS like water supply and distribution system, natural gas distribution systems, traffic control and telecommunications. Continue network monitoring is needed to ensure that abnormal states due to attacks will be detected and identified. Resilience and robustness are high critical properties of the Smart Grid. Resilience refers to the system attribute or ability to withstand an attack and return to its initial state, while robustness express how hard is to take down such a system.

Identification, authentication and access control are important security aspects in CPS. Strict access control and authentication mechanisms should be applied in order to ensure that only authorized persons may have access to control critical infrastructures, access sensitive

information and resources or are legitimate users of power grid services and connecting to the Smart Grid.

Cyber threats in Smart Grids are related to gaining root / administrative access in SCADA systems and then sending improper controlling commands to the controlled systems. Or even gaining access to rooms where relevant infrastructures is installed and physically destroying, making related services unavailable. This could set services and systems completely unavailable or in undesirable conditions which could expose the grid and the connected devices to danger of destruction. DOS attacks against availability may attempt also to delay, block or corrupt Smart Grid communications. Integrity attacks may modify or disrupt data exchange. Generally DOS, DDOS are considered the most dangerous attacks. DOS may be performed:

a. On physical layer for channel jamming, particularly effective against wireless networks. This is the primary attack as hackers do not have to be authenticated in the network and such jamming attacks may lead to wide range of damages to power station network performance, in local areas, causing delaying or complete Denial of Service for critical delivery messages.

b. MAC layer misbehavior by modifying malicious users MAC parameters may lead to weak versions of DOS attacks. Or even an attacker by executing masquerade attacks exploiting open MAC address gain access to power stations and command IEDs to shut down.

c. Attacks at network and transport layers can severely degrade end to end communications while recent buffer overflow attacks against SCADA systems have proven high vulnerability against this type of attacks.

d. Attacks on application layer target bandwidth and consumption of computational resources intending for example to exhaust CPU or I/O bandwidth.

As already said, Smart Grids networks are delay-constrained. So, hackers do not have to shut down access to networks and use extreme attack techniques, but rather it is enough to cause delays to high critical messages and violate strict timing requirements. Synchrophasors (PMUs) use precise GPS signals for time synchronization. GPS spoofing techniques (jamming GPS receivers) could cause severe impacts to network elements controlled by desynchronized PMUs controllers.

ElectroMagnetic Pulse (EMP) threat is extremely rare and hard to deploy, while restricted entities afford such capability, but such an attack could completely destroy all electronic circuits and devices within the attack range severely impacting a large part of the Smart Grid, while chained dominos effects could spread in the entire network.

Physical attacks are easy to deploy against poorly protected system elements. Physical destruction may cause definite unavailability of the attacked assets as well as any other

dependent asset and system function. Dependencies are always to be taken into account to identify total impacts and attack surface.

Recently privacy has been proven to be a matter in Smart Grid Security. Adversaries can make hypothesis on customer habits by intercepting and analyzing energy consuming behavior by attacking smart meters data confidentiality.

In addition, by attacking smart meters integrity and changing feedback data about energy consumption or even establishing a botnet that simulates commercial, residential or industrial customers and sending malformed data about energy consumption, attackers can disrupt energy generation causing financial damage as more energy is produced than quantity of energy is needed in reality forcing use of extra generator plants or alternative generators leading topic energy generation. On the other hand, by attacking integrity of smart meters transmitted data or gaining access to service provider or distribution center, attackers could create the impression that less energy is need to be generated, making energy assets unavailable to consumption demands.

DDOS attacks performed against service providers or other smart meter data receivers downgrading or eliminating services for long periods would have a serious impact on economic and effective power production and distribution in the way that has already been explained in the previous paragraphs. Integrity attacks against Advanced Metering Infrastructures (AMI) is considered as more critical as time delays in this area can vary from minutes to hours. Attackers can set private data or consumption data as their target attempting to modify this type of data prior being sent to the service provider. Alternative attack is eavesdropping customers' communications with the service provider attacking user privacy.

Most probable/ possible way of achieving such attacks is considered the use of botnets as they attack directly the users exploiting client-side vulnerabilities and they are out of the reach of CPS defensive mechanisms and unaffected by their security policies.

According to [16] ICS implementation should include the following security principles:

a. Capability of restoring systems after an incident which implies resilience property.

b. Maintaining system functionality during adverse conditions. ICSs should be designed so every part has an uncertain counterpart. If any part fails it should not affect other system parts.

c. Protecting individual ICS parts from exploitation.

d. Restricting physical access to ICS network and devices.

e. Restricting logical access to ICS network and devices by using Demilitarized Zones (DMZ) architectures, firewalls and layered defense applying in depth strategies.

Since ICS and SCADA systems are not isolated any more from the environment and use internet technology for control because of low cost and applicability they appear to be accessible and vulnerable against hacking attacks

2.2 Risk definitions

Information security is defined as the protection of the properties of availability, confidentiality and integrity. It can also be defined as protection of property (assets), i.e. material, equipment, communication equipment, controlling equipment, environment of CPS, documentation, personnel, software and data.

Risk is defined as the product of the likelihood of an attack or a hazardous state occurrence and the damage expressed as financial losses, restoration costs or other kind of damage like reputational damage, health losses and fatalities, legal and regulation related consequences caused by disturbance or attack against an information system. In the last case, risk and damage cannot be quantitatively expressed, but rather qualitatively described, most usually with the help of risk matrices. The probability of occurrence of security incident is a function of the probability of occurrence of a threat, which will attempt to exploit system vulnerabilities and the probability of successful vulnerability exploit.

Risk has two dimensions, probabilities and consequences. Risk is therefore a function of the value of assets usually measured by the potential consequences caused by an attack against it, the system components that are of value and are necessary to protect, the nature and level of vulnerabilities, the nature and likelihood of threats against the system and the nature and intensity of impact would have if these threats are carried out successfully.

$$\boldsymbol{Risk = f\ (asset,\quad vulnerabilities,\quad threats,\quad probability)}$$

Threat is defined as any act or fact which could have harmful effects on an information system state or function. Vulnerability is defined as the potentiality that a system suffers some consequences when attacked or simply a weakness that should be exploited to bring system to an undesirable state. Impact is defined as the result of failure to maintain the security of information system. There are four types of effects:

a. Disclosure

b. Denial/ unavailability

c. Destruction

d. Modification

All these effects lead to consequences. So, combination of likelihood of appearance and act of threats and vulnerabilities of assets lead to events which cause consequences.

2.3 Risk Methodologies Types

There are three (3) types of RA methodologies:

a. Qualitative
b. Semi qualitative
c. Quantitative

The difference is in the way that consequences and impact probabilities occurrence and assessed and measured.

2.3.1 Qualitative Risk Analysis

Qualitative RA methods provide comprehensive understanding of risk and guidance for risk handling strategies and countermeasures prioritization. Risk and probability are usually expressed in generalized, typical terms or empirical risk/ probabilities ranges using qualitative, descriptive formulation to declare relative importance and prioritization. It does not allow determination of probabilities and risk results in accurate numerical form. Qualitative RA attempts to adequately characterize risk in words and enable development of the appropriate risk handling strategy. Assigning risk rating allows risk grouping processes. Deterministic impacts may not be accurately correlated to qualitative RA typical metric scales. Qualitative RA may be the foundation for initiating quantitative RA and provides inexpensive results quickly.

Qualitative analysis encounters some restrictions regarding selection of the most suitable risk measuring scale. Impacts against CPS cause different consequence type, side effects, chained effects, differentiating across the state. Designing the most suitable scale and metrics for measuring consequences severeness and prioritizing threat scenarios is challenging as different natures of effects should be made efficiently comparable, while it should be possible to add them and estimate total losses. For example, hygiene problems, psychological effects, financial damage, political stability, should be measured, compare one to each other and add their severeness to estimate the total consequences severeness of attacks against CPS.

2.3.2 Quantitative Risk Analysis

Estimating probabilities of threats' appearance, impacts occurrence, successful attacks, vulnerabilities and countermeasures' effectiveness is vital for risk level estimation.

There is **no natural mathematical logic** to transform human experience and intuition into numerical data. Estimation is based on intuitive mental process. Apart from that, estimation accuracy depends on sufficiency of background knowledge about all factors that influence events occurrence probabilities and possible outcomes.

Moreover, there is **no mathematical form** to directly connect knowledge and probability and quantify them. But knowledge intuitively affects accuracy of

probability estimation. Past experience and statistical data enhance accuracy of estimation. Bayes theorem and Markov analysis enhance this mental procedure. Bayes' Theorem connects past and new knowledge to make probability estimation more accurate. But, black swans and zero-days problems, practical approach become problematic. Black swans and 0-days are extremely rare and hard or even impossible to predict, because occurrences of such events historically have not been met before. In these cases, there is lack of past knowledge, so theoretically events cannot be efficiently predicted and probabilities of their occurrence estimated. But they can still appear. The World Trade Center attack was a terrorist attack without precedent in Human History. There has not existed historical or statistical data about similar events. Although this attack seemed impossible to happen, it did happen and had extremely severe consequences with 20,000 life casualties and very high economic damage. It had an extremely high impact on mass psychology and shaped the State's external affairs and Security Policy in the decades to come. But risk analysis process should be able to deal with such cases; even if probability may be extremely low, risk remains extremely high, having vast consequences magnitude, affecting the entire state population, industry or even the whole state. Chained effects, cascading effects, due to presence of dependencies presence makes risk quantification very difficult if not impossible. Dependency elements expand over the limits of infrastructures components to different sectors.

Regarding quantitative RA method appliance, it is assumed to be difficult in cases of CPS, particularly CI related CPS, because relevant impacts may cause chained effects and side effects resulting to widespread casualties to multiple different domains. For example an impact to a Smart electricity Grid would cause unavailability of electricity; but electrical power unavailability would affect public transportation. Affected public transportation in turn would affect goods and resources distribution across the state. Public, political, psychological environmental effects and financial consequences, organization reputational damages may be caused. Urban population well-being can be affected. Lack of energy affects industry and corporate functions; in turn these functions would have financial impacts to state economy. Different types of consequences like financial, fatalities, reputation damages have to be compared each against others after being quantified which is a difficult if not impossible task.

Risk estimation for other involving entities may not be as simple, because chain, escalating and cascading effects take place. Moreover, impacts severeness varies across different regions inside the State. Industrial areas would suffer more severe consequences, having critical losses, when Smart Grids is attacked and electrical power made unavailable in comparison residential areas. Consequences of energy unavailability vary with duration across different geographical areas and production sectors. Short times of blackout are insignificant for population, but extended blackouts start affecting population well-being. Additionally, chained and side effects may recursively affect supply chain and the power grid industry.

Attacks against water distribution and health systems could affect mass health/ hygiene problems and cause deaths. Sizes in such case scenarios cannot be effectively measured. Quantitative analysis could use historical data of energy consumption and pricing per time unit and per area, based on AMI past information, then use this information to calculate future losses. In this case industrial consumption, population energy consumption habits and energy pricing should be presumed remaining constant. But in reality energy demands continuously raise and are balanced with the markets prices, sufficiency of resources, costs in the supply chain, demands and business fluctuations. So, adopting such perception would lead to important errors.

2.3.3 Semi qualitative Risk Analysis

Semi-quantitative analysis stands in the middle distance between quantitative and qualitative analysis. While in quantitative analysis risk is expressed in terms of costs and qualitative analysis use risk matrix of abstract descriptive probability and consequences' level, semi-qualitative methods expresses both probability and consequences in numerical form. It is much more accurate than qualitative analysis, but less than quantitative. It uses weight factors or suitable system values and probabilities to express risk in numerical form, presenting risk declinations not possible for qualitative methods. But since scaling or weight factors are based on operator's subjectivity and not on real or statistical data it cannot be as accurate and objective as quantitative methods are.

3 Chapter 3 – Risk Analysis

Each system has three basic security attributes:

a. Confidentiality of information

b. Data and functions integrity

c. Functions and services availability to persons who are authorized to use or access them at any time it is necessary.

Privacy is violated by loss of confidentiality of economic data by intercepting private billing information or data exchanged between SCADA and smart meters or by monitoring, recording and analyzing consumer behavior pattern and energy consuming habits.

Apart from the availability of information, availability extends to energy sector. Energy services must be available to companies and individuals 24/7 as well as other critical assets and services like fresh water supply and distribution.

A customer related management process is relatively more tolerant of risks associated with loss of availability and integrity, but much less tolerant of risks associated with loss of confidentiality: unauthorized disclosure of personal identifiable information (PII) can have a high financial and reputation impact. On the other hand, processes associated with the reliable transmission and distribution of electric power in the energy market and everyday life are relatively more tolerant of risks associated with loss of confidentiality and less tolerant of risks associated with availability and integrity: inability to complete an operation in real time may result in loss of life or substantial damage to the electric infrastructures.

Integrity extends to non-authorized modification of functionality of SCADA and physical systems and exchanged data between sensors and controlling units preventing or detecting malfunctions and anomalies either to the cyber infrastructures or the physical informational or electrical networks, which could cause various impacts and consequences to industry, environment, population, connected electrical devices and manufactures.

A common characteristic of CPS that should be considered in every RA procedure is the presence of dependencies and interdependencies between system parts or between system and its environment. Attacks against one part cause effects to another part.

Physical security must be added to the above concerns. Attacks against CI regularly aim at their physical destruction by efforts of compromising ICS and SCADA systems and setting them to anomalous states through improper manipulation. Both cyber and physical security are concerns in CPS and CI. Cyber and physical assets must be protected against cyber and physical attacks or attack combinations.

Risk analysis process aims at identifying valuable assets, threats, vulnerabilities, estimating probability of threat appearance and attack, identify impacts and potentially caused damage and measure its consequences. Consequences' severeness and magnitude combined with probability of attack or other threatening event occurrence express system risk depended on

the factors of threat, vulnerability, value and probability. Then priorities are set in protection of relevant assets and vulnerability reduction because of the usually limited budget and resources. Risk analysis first takes place without any countermeasures implemented setting an initial reference baseline for future implemented countermeasures effectiveness comparison and repeated regularly, whenever new countermeasures are applied, when new threats emerge, when new vulnerabilities or exploits are discovered or whenever major or important system changes happen. Risk analysis results in residual risk level and residual vulnerabilities which have not been treated. If risk level or vulnerability level is not accepted and there are not sufficient or effective protective measures, services and mechanisms to reduce vulnerability or risk level, then the risk analysis procedure should be iterated adopting proper system and countermeasures implementation or work on hypothesis level prior implementation, until an acceptable residual risk level and residual vulnerability is left and no major assets of interest are left unprotected. So, the goal of RA and RM process should be after risk components identification, defining relevant risks, which threaten systems and infrastructures and apply proper protective mechanisms to limit risk in acceptable level, providing a basic security design and analysis tool.

RA process in wide area CPS and critical infrastructures differentiate from classic risk analysis methods on that criticality of systems is what should additionally be examined, while much more complex assets multiple vulnerabilities and potential attackers should be identified and system specific properties like resilience, robustness and dependencies should be taken into account. Such processes should be able to address those systems' high level of complexity, magnitude and severity of effects, often extremely low probabilities, unpredictable situations that may arise, 0-day attacks, special or composite attacks and presenting system, infrastructures and cross-sector dependencies and interdependencies. The scope or spatial distribution should be taken into account in CPS analysis cases; it concerns the geographical areas that may be affected by the loss or destruction of a system or infrastructures.

Because of the high complexity of CPS, their vast size, often expanding to the entire state and the presence of strong relationships and dependencies, it is difficult even to identify assets and vulnerabilities in the entire infrastructures; critical assets are of much more importance since being impacted by attacks or hazards bring severe consequences, which are difficult to be quantified in the analysis procedure. Vulnerabilities in CPS adopt many forms in accordance with the nature of assets: physical, technical, cyber and composite vulnerabilities while physical attacks, cyber-attacks and combinative attacks can take place, while multiple vulnerabilities not easily discovered may exist. Lack of proper defined standards and methods do not ease these cases.

Because of CPS complexity and their involvement in CI, relevant RA methodologies should be able to examine the entire scope (business scope), functions and layers of infrastructures: strategic dealing with top management and decision making, operational referring to structure, management and business actions, cyber concerning data, informational and communication systems and the physical layer concerning the physical infrastructures including the whole infrastructures and hardware.

3.1 Presentation and Evaluation of Methods and Methodologies

In the need of comparing CPS RA methods and methodologies appropriate criteria should be developed and used. Using such criteria it would be possible to examine these methodologies, their special characteristics and effectiveness on a common basis. Moreover, these criteria not only serve comparison and evaluation needs, but make up specifications for developing appropriate methodologies for analyzing CPS risk, according to CPS special characteristics and properties. Following criteria are proposed:

a. Ability to identify assets in the entire range of CPS. Meaning that it should be able to **recognize assets and measure** their **value**. CPSs particularly when associated with the critical infrastructures are characterized by high complexity and include multiple functional and physical components. An effective method of RA should be able to analyze these different components or related parts, informational facilities or manpower in order to **identify all assets** need to be protected, especially **critical** ones.
b. **Criticality.** Criticality has been described in previous chapter. Analysis methods should consider criticality and should be able to identify Critical Assets and Vulnerabilities and assess Critical Consequences.
c. Ability to **identify threats** and estimate the likelihood of threat occurrence and attack success. Many times combined threats with composite attack plans may appear, therefore requiring appropriate screening. Threats can take the form of natural phenomenon, equipment failure, hazards, human errors and handling operations, sabotage and cyber resources being exploited from remote access points in the Internet or after gaining access local computer systems. Examinations should be able to answer what can happen, when it may happen, how it can happen and where it will happen. Disperse over wide area CPS present huge attack surface, where attackers have a wide selection of targets. As CPSs are resilient systems attackers may follow complicated attack paths and attack multiple targets to take down the whole system and overcome control mechanisms and system resiliency. Dual nature of CPS, consisting of both cyber and physical domains, invoke different attack types to take place in these domains, adopting the forms of cyber and physical attacks or combinative multi stepped attacks, where each step open way for another attack method to take place, e.g. monitoring system neutralization, permits physical intrusion and local ICS exploitation.
d. Existence of appropriate **scales** for risk measurement and risk quantification methods. Risk quantification is the most important element of any methodology, allowing self-expression, analysis of results and their exploitation. Particularly accuracy of results in risk quantification is important as precision errors may lead to mistaken decision making and unsuitable risk mitigation strategies planning, ineffective security investments and ineffective cost/ benefit evaluation of countermeasures to be applied. Severity of consequences taking into account cascading and escalating effects, presence of dependencies and interdependencies

should be examined and taken into account during risk estimation identifying aggregated damages in different assets or even locations.

When different types of effects and consequences appear it is necessary to make it possible to compare them. Defend natures of consequences have to be compared: financial damage, fatalities, trust, societal and political stability. Expressing these consequences in appropriate is important for risks comparison and risks prioritization.

e. **Practical and intuitive implementation**. In a complex environment such as CI / CPS identification and RA can be complex and time consuming processes with a requirement to screen a large number of parameters and in-depth study and analysis of existing systems and situations. A **holistic** approach [18] is the examination of individual components and different hazards arising in unitary manner expected to simplify the process of RA in complex and different systems/ sectors and in all layers.

This criterion may include the application of RA method by specialized personnel or specialized team members, time required to draw accurate results, even the availability of automated tools to simplify and accelerate work, the need or ability to provide specialized training. Another aspect is ability of assessing effects and costs, economic concerns, sociopolitical or measurable elements. This criterion is in direct correlation with risk expression and measurement. **Holistic** approach makes methods applicable to all different layers and sectors, but sometimes details may be left and not examined, exposing systems to dangers not analyzed. **Applicability** of methods for RA in strategic and operational level and at lower levels in order to recognize the risks, threats, vulnerabilities and assets in each of these levels, as well identification of risk owners in order to be taken appropriate action depending on the type and extent of damage and the way corresponding to each of them. It is important to be possible to properly present results of the proceeding lower level analysis to higher levels of management and decision-making [18].

f. Ability to estimate the **probability of occurrence** of attack scenarios with **accuracy and objectivity**. Ability to estimate composite probabilities on composite attack scenarios taking into account feasibility and discrimination of complex attack scenarios into elementary parts and breakdown probability to achieve realistic, complete and accurate analysis. But in a lot of cases no historical and statistical data are available, while cyber incidents might have not appeared in the past to provide safe probability indicators. More over 0-day attacks exploiting new vulnerabilities are not easy to be predicted. Black Swans, incidents that today knowledge and experience consider that are impossible to happen may happen in a future time period. Even if probability of such events may be extremely low or zero, risk and criticality are retained in high levels because of the consequences magnitude and severeness. So, they are not allowed to be ignored neither be accepted as residual risks; that would be a difficult political decision. Probability accuracy and objectivity are important factors as objective and accurate estimation is translated in accurate

and objective risk assessment. Attack against world trade center had been unpredictable. Though it did happen and its consequences were critical.

Many methods can be used in to support probability estimation like Monte Carlo simulation or other stochastic and deterministic methods applied in quantitative assessments. ISO 27005:2011 provides guidance for conducting risk analysis and uses rather abstract and qualitative approach on likelihood of occurrence estimation using a three level qualitative estimation scale. In the other hand NIST SP 800-30 provides a more detailed method. It distinguishes probability of a threat appearance (threat initiation), scale for likelihood of event occurrence, scale for event resulting in adverse impacts and overall likelihood scale. It uses a five level scale both qualitative and semi-quantitative/ quantitative in ranges 1 to 10 and 1 to 100; ranging from very low (0-4, 0), low (5-20, 2), moderate (21-79, 5), high (85-95, 8) and very high (96-100, 10). It also provides more accurate criteria for all circumstances quantification, for example if an incident has happened once in the last ten years is considered to have very low probability to happen again or probability is maximum 4% according to the semi quantitative scaling. Historical data may give a more trusted probability; stochastic methods requiring complex calculations may offer accurate results but in the other hand may be less cost/ effective and become complex, impractical and time consuming since they produce a vast volume of calculations for all possible input parameters. Uncertainties in estimation and inutility are factors that should be limited during probability and risk estimation in order to succeed accurate and reliable results.

g. **Adaptability**: May be independent on the **technical nature** / **wide application** and be able to be applied to all different sectors and layers. CPSs are used in a wide application range. Critical infrastructures include many services of different nature e.g. water supply, energy supply, banking system, public transportation and traffic control, which use completely different technologies. Analysis methods should be able to examine and identify all different technological components of a system or infrastructures. In the other hand specialized methodologies would give better results, succeeding accurate asset identification and risk estimation.
h. **Reliability**. Extensive use, experience and trust indicate methods reliability. Practical assessment and existing experience on method application, acceptance, trusted tools and theoretical bases enhance credibility. Agreement with valid existing standards and providing results compatible with results of valid and reliable methodologies indicate methods' reliability.
i. Consideration of **dependencies and interdependencies** should be taken into account. Dependency is a unidirectional relationship, where the state of one asset/ infrastructures depends on another asset's/ infrastructure's state. Interdependency is defined as a bidirectional relationship where the state of one asset/ infrastructures depends on the state of another asset/ infrastructures and vice versa. In system theory a dependency exists when a change to the state of one system induces a change in the state of another system. Dependencies and interdependencies are characterized as:

(1) **Physical,** where the output of a system is required as an input for another system and vice versa or loss of a physical asset affects function of another.

(2) **Cyber**, where the state of a system depends on the information transmitted from an information infrastructures.

(3) **Geographic,** where two systems/ infrastructures are affected by the same local event, in other words they are spatially proximate.

(4) **Logical.** In this category are included all other cases which do not fit to the previous categories.

Attacks against an asset may affect functionality of another or create dangerous hazardous conditions. This is a common fact in CPS where subsystems are interconnected and interacting to each other and these interactions may take place in different locations. Dependencies and interdependencies may be present in relationships of different mechanisms or even between different operational sectors. So, these factors do not apply just between system's components. They are possible to apply between different systems of the same or different infrastructures e.g. between energy infrastructures and communications or transportations. Different layers are interrelated.

So dependencies and interdependencies may apply in and between all layers:

(1) **Strategic layer**: Top management processes and decisions take place in this layer.

(2) **Operational layer** where Organization structure, functions, finance and management take place.

(3) **Informational (Cyber) layer** which is related with data, informational and communication systems and SCADA controlling systems.

(4) **Physical layer** related to generators, physical infrastructures, cables, lines, hardware etc.

So factors of dependencies and interdependencies should be possible to be detected and identified during risk analysis.

j. **RA originating point**. RA methodologies may be asset, impact, threat oriented or vulnerability oriented. The difference between these categories is the RA starting point. In the first case initially assets identification come first, then analysis is built on identified assets. In the second case possible impacts and losses related to them are firstly estimated and then follows risk management without, usually, interrelating assets and vulnerabilities. In the third case threats identification comes first and then risk analysis takes place for each threat considering capabilities of

each. In the final case vulnerabilities is the methodology's starting point, threat capable to exploit them and probabilities of vulnerabilities being exploited are analyzed and relevant risks estimated.

There is some danger that some risks may not be recognized in threats, impact and vulnerability assessment orientations [19]. Additionally there are two more deficiencies to threat oriented approaches: black-swans and insufficient historical data. "Black swan" is a high impact, large magnitude attack, which is rare and hard to predict statistically. So, such kind of approaches which are based in past knowledge may fail to predict never seen before attacks. Moreover 0-days attacks may happen and until that day could be unpredictable, so no preventive or protective measures might have been taken against it and there would be no risk assessment for that case. In such occasion vulnerability oriented methods would be ineffective. Additionally, during threat oriented analysis system is examined iteratively against each threat capabilities, being time consuming. Some vulnerabilities and assets may never be examined and omitted during risk management because of poorly identified threat factors. The same applies to impact oriented analysis, but in this case no threat indication is used so specific countermeasures may be not taken into consideration. Vulnerability analysis takes place only for known vulnerabilities so unknown vulnerabilities and many threats and 0-days cases will not be examined. Asset oriented analysis may fail recognizing multiple threats against the same asset/ vulnerabilities, but it is considered as the most complete method and most of existing methodologies tend to this orientation.

k. **Scope.** To whom analysis results are addressed is of importance. RA methods may apply in different levels from strategic decision making to operational and technical. Who is affected, stakeholders and population and the geographical extend of consequences are included in the scope. Scope has also another notion; geographic factor has to be examined during analysis process to identify different locations threatened and relevant risks.

l. **System behavior and performance identification:** In order to understand vulnerabilities and identify assets, threats and their course of action, systems' behavior and performance and provided services should be identified, during asset identification stage, since CPS are dynamic systems, meaning their status changes with time and inputs in opposition with traditional information systems which only store and manage information. Systems' responses and reaction time should be taken into consideration as they influence not just risk but also CPS key attributes like **resilience** and **robustness**. Resilience refers to the system property to recover and return to its initial state after being impacted, while robustness express system's strengths and ability to withstand against attacks. These attributes obviously affect risk significantly. Time is an important part of risk assessment. It refers to:

(1) Duration of effects, where unavailability of service defines the severeness of the consequences.

(2) Detection of attacks, Alert and Reaction time in combination with attacks duration indicating system capability to react and overcome threats.

(3) Expected time of attacks or threat appearance. If attack will occur directly or in short time criticality and risk raises as preparation and reaction time shortens.

So time factor should be taken into consideration during risk measurement and directly related to the resilience attribute.

m. **Objectives:** Objectives determine the particular character and purposes set for the risk assessment methodology. Objective selection affects entire methodology design and scope.
n. **Method orientation/ risk assessing:** Alternative approaches for risk estimation and/ or quantification may exist like Time To Exploit and alternative semi-quantification methods.

Following there are RA methods and methodologies applied to CPS and CI. Designating methods and methodologies, the former concern a set of steps used to accomplish a task, while the latter is a set of tools or research methods translating theory to practice.

3.1.1 Critical Infrastructures Modeling Simulation (CIMS)

CIMS [20, 21, 22] had been developed in 2005 by the Idaho University and Idaho National Laboratory supported by the US Department of Energy during research for protection of CI.

CIMS provides the capability of simulating CPS particularly the element of dependencies and interdependencies between systems parts and their results in this complex environment. It uses the graph theory for system representation. CPSs are graphically represented as a network of nodes and edges with these two elements having specific meaning. It can also represent other factors not having a physical form but which can impact physical infrastructures, like political factors and influences. Respectively, an edge is defined as an entity which acts as a physical or virtual entity that acts as a conduit for flow of a physical quantity, influence or information [21].

More specifically, in CIMS, infrastructures is represented with a set of parallel lines. Each line represents an individual sector inside the infrastructures (Figure 3). Nodes represent key infrastructures components within the individual sector. Relationships and dependencies are developed between the nodes within common sectors of the infrastructures, but also between different sectors, even between nodes in different infrastructures. Solid lines represent these relationships and dependencies inside the same sectors while infrastructures interdependencies are represented with dashed lines. Methodology uses mathematical formalization to describe dependencies and interdependencies using graph theory. According to used mathematic formalism, a set of nodes related to each other composite an

infrastructures network I, which can be disjoint or connected. It can be directional unidirectional or having elements of both. Internal interdependencies are represented by an edge (a, b). Edges represent system dependencies or interdependencies. CIMS describes all kinds of interdependencies with mathematic formalism.

CIMS generally examines dependencies and interdependencies of chains of influences crossing multiple sectors. The **main advantage** CIMS offers, is the simulation of interdependencies that exist between different infrastructures, for example between transportation and smart grids. It can also provide individual sector analysis with desired detail and describe system in terms of system mechanics/ physics in correspondence with the degree of conceptualization. It can also address to high management level to model systems without the need of using low-level technical / engineering analysis. So it provides a holistic view and examination towards the systems of interest at any level of consideration.

Analysts can use "What – If" methods changing system states or nodes states and observe the caused behaviors. In this way, Critical assets and vulnerabilities can be identified as well as means to protect them. CIMS uses graphical visualization tools to represent/ visualize examined infrastructures.

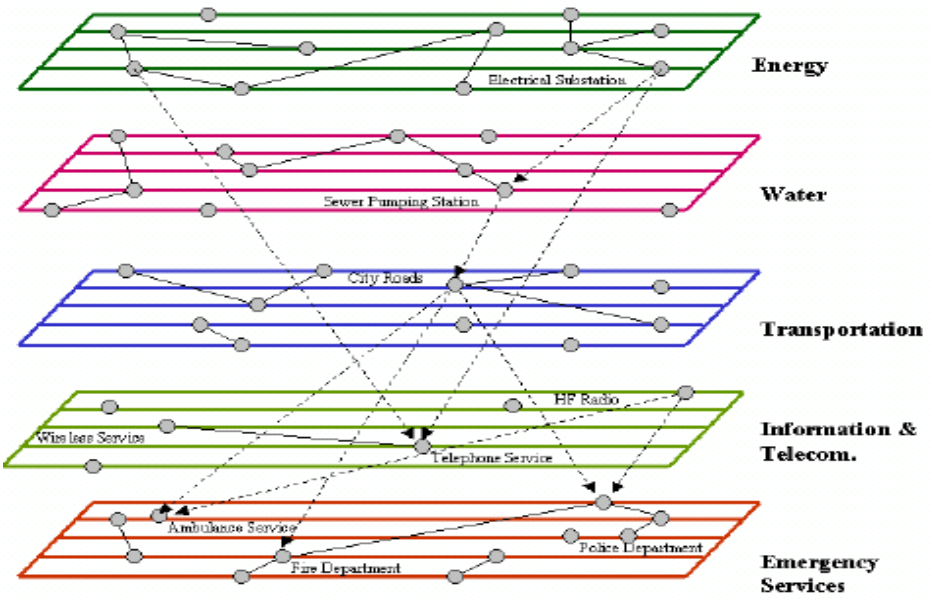


Figure 3: *CIMS, infrastructures interdependencies*

Modeling capability permits simulating systems but does not include any special framework providing capability of accurate system identification. It quickly constructs infrastructures models using map, images, photos and other electronic images. It has the ability to drill down and extract/ change properties of individual infrastructures elements. Also, it is able to link active information to simulated

entities. Method can simulate specific threats or rather events that could lead system to a defined end state. As far as criticality concern, method uses lists of critical assets, relative importance information of each infrastructures asset, cost to destroy the individual assets, cost of asset repair and time to destroy or repair the individual assets.

Since no risk assessment takes place no appropriate scaling is needed. But this does not mean that method does not consider impacts and consequences, in the contrary it does, but simulates them in order to examine the best countermeasures practices through simulated processes. Time factor has critical importance in this simulation method; duration of effects, time to destroy assets and time to restore them is used to examine severeness of impacts and estimate criticality.

Furthermore, it is not considered intuitive and easy applicable method as it requires special knowledge about graph theory and modeling. In the other hand, it uses graphical tool offering high capability 3D assets representation and model building, while still being lightweight and it is characterized by mobility, being used in a lot of different platforms. CIMS tool is highly visual and interactive for observing the cascading effects and consequences.

The method with varying degree of abstract approach can simulate all layers from higher (strategic) to lower layers (cyber and physical), but can also be applied in different infrastructures or even sectors. As already stated it CIMS is able to be applied in all different types of infrastructures and address different systems. This method is based on proved theoretic methods of graph theory and uses strong simulation tool.

Using graph theory method is capable of modeling and representing graphically examined systems. It had been designed on this specific purpose to model wide area critical CPS. It extends dependency/ interdependency factors not just to system components but between different infrastructures, allowing visualizing all different layers and energy sectors. Additionally, it simulates and visualizes interdependencies without physical form e.g. societal and interdependencies. Generally it is a methodology accompanied with a specialized tool designed to simulate infrastructures and dependencies/ interdependencies elements in all their different forms and layers.

Method and supporting graphical tool is used to simulate assets, impacts and threats (indirectly) selected from lists. This method simulates impacts and system elements on all layers of interest across the entire system and infrastructures considering geographical dispersion and related sectors.

CIMS has the ability to tie node behavior directly to live sensor inputs, simulate different transition states and examine interdependencies even if they do not have any physical form. Impacts can be simulated visually with the use of graphical tool. Enhanced edition uses genetic algorithms apart from automated or not “what if - procedure” to analyze and optimize different threat scenarios. Vulnerabilities can be identified through simulation of assets and threat scenarios. Moreover, resilience is

not directly examined. But possibly can be simulated too in accordance with defined end states. Time to destroy provides a measure of robustness.

Finally, method addresses the task of Critical Infrastructures Protection preparedness and recovery. On that purpose it uses asset and infrastructures simulation, giving emphasis on dependence and interdependence element, analyze different threat scenarios, estimate criticality and propose effective countermeasure strategies based on pre-installed information in its highly interactive graphical tool.

3.1.2 Catastrophe Modeling

In [43] a generic model of RA focused on natural disasters and terrorist acts is presented. Specific guidance on matters relating to natural disasters is provided, but this model can be used in any other case, leaving freedom to users, but also the responsibility of adapting analysis to requirements to them. It is the basic model for the development of the CRAMM method.

It first focuses on three levels of risk, depending on the interest, investment and auditing bodies of critical infrastructures under the listed threats. So, risk is addressed at the strategic level, i.e. to government agencies, at operational level, i.e. the local audit and private bodies and also in investment and finally refers to consumer level.

Figure 4 shows the mechanism of this RA model. The methodology starts with the identification and description of threats (Hazard Module). Basics constitute any threat to the place of event, occurrence, origin of the threat, helping predictions of future occurrences. The forecasts are based on statistical data, historical information and scientific data based on the presence of physical signs that indicate the likelihood of catastrophic phenomena.

Then trace the valuation of property and belonging assets (Inventory Module). Includes the number of property / buildings, economic value, the formula as to their use (residential premises, commercial premises, industrial premises), technical characteristics which will help defining losses that may occur during action of a natural phenomenon. Indicate the contents of the installation, the use, the activities carried out in them and estimated recovery time measured in man hours and loss, costs of repairmen and quality of work-based infrastructures and duration of unavailability in case of severe damage.

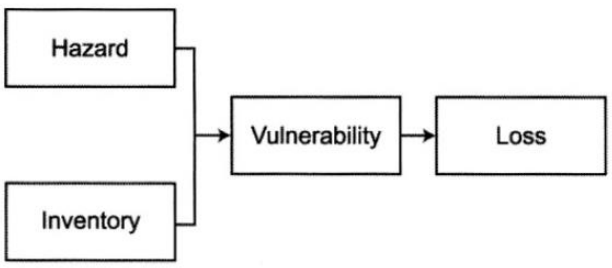


Figure 4: *Catastrophe model RA*

Based on information already gathered infrastructures vulnerabilities (vulnerability module) are identified. Damage level estimation depending on the type and phenomenon intensity takes place. Estimates are made for different intensities / severity of events based on estimates of specialized technical / engineering, statistics, recorded data, specifications and strengths already studied, findings from a study and simulation models. To facilitate the study of assets they are usually grouped by standard generic criteria.

The next step is assessment of the financial cost of the damage. This cost corresponds to the cost of repair or total replacement, although in some cases it can be expressed as the ratio of these two quantities.

Using of this data, diagram of exceedance probability curve is determined, which expresses the probability of losses exceeding a certain value. Based on the amount of damage which is considered the maximum acceptable the maximum acceptable risk is defined.

So probability of appearance of event $\mathbf{E_i}$ with cost $\mathbf{L_i}$ is:

$$\boldsymbol{P(\ E_i\ appearance) = p_i}$$

In the other hand the probability of $\mathbf{E_i}$ not occurrence is:

$$\boldsymbol{P(\ E_i\ not\ appearance) = 1 - p_i}$$

The expected cost in this last occasion is obviously 0.

Number of possible events in one year duration cost is:

$$\boldsymbol{AAL = \sum p_i \times L_i}$$

Probability of costs exceeding a certain level for the occurrence of an event once a year is:

$$\boldsymbol{EP(L_i) = P(L > L_i) = 1 - P(L \leq L_i)}$$

As already indicated this is a very basic and generic framework for risk examination. Though specific guidance for structures is provided it can be used in cybersecurity sector, but it is on user responsibility to gather all necessary information and prepare a more specific and detailed risk analysis plan. As other methods provide more specific guidelines it is rather impractical to use such methodology, but it gives good advice on estimating financial losses.

Catastrophe modeling has been designed to address disasters and massive damages

caused by physical phenomenon, affecting cities and populations, having great cost to risk stakeholders, including government and major market investors. It does not provide any mechanism for characterizing critical assets and generally defining criticality. Moreover, catastrophe modeling is a generic model for asset identification and risk estimation. It provides general guidelines and then it is up to the risk analysts' to identify any particularities. It does not provide any specific guideline or framework for examining dependencies or interdependencies.

Generally, method uses historical and statistical data and experts' knowledge and experience to estimate probabilities. Additionally probability of losses exceeding certain levels annually is estimated. Catastrophe modeling is a quantitative method. It uses quantified probabilities taken from historical and statistical data and financial values and provides expected losses to express risk and give a complete picture of the costs of necessary countermeasures strategies that will be necessary to be implemented. It expresses damage in form of financial losses which indicate the cost for damaged systems repair or replacement, in accordance with what is considered more cost effective.

Since method has been developed with physical phenomenon disasters in mind it takes into consideration geographic factor, as different areas are threatened by different threat sources and phenomenon, earthquakes, floods etc. Catastrophe modeling also considers terrorism as a threat source, but not cyber-terrorism. Since method is generic and provides financial results referring to massive disasters caused from major phenomenon it is suitable for use by operational and strategic layers and any interested market stakeholders. Method has been designed for use in the insurance field. Because of the generic aspect it cannot be easily used in any low layer, physical, and cyber. Mathematical models and historical / statistical data are used for probability estimation. Costs and financial losses are used to express damage, since method has been initially addressed for use in the insurance industry. So, risk is estimated accurately in quantitative risk approach. Probabilities of losses exceeding certain loss levels are calculated, so providing an accepted risk level and countermeasure effectiveness index.

Catastrophe modeling is primarily an elementary asset oriented method, but it can be considered as threat or impact oriented method too. Since method is executed by experts of different sectors, considers vital the use of detailed and precise information and provides a basis for the development for many other risk assessment methods like CRAMM, it is considered as a quite reliable method.

As said Catastrophe modeling provides only a very generic guidance framework since asset, threat and vulnerability identification and risk estimation are based on experts' judgment. It is not considered as an easily implemented method. In fact it needs the facilitation of many different experts for use in complex CPS systems. Catastrophe modeling requires a lot of information to be used. The more detailed the planning is, the more precise results are given. It requires different experts' facilitation for each different sector involved, so, it is unavoidable that method appliance is supposed to be costly. In particular CPS environment characterized by

high complexity and different technologies co-existence, it is supposed to be extremely time consuming and costly to apply such a method, because, as said, it provides only a very generic framework, not specific guidelines and requires a group of expert to work for the analysis.

Method has been developed for addressing physical catastrophes caused by physical phenomenon, and later had been adapted to address terrorism and related impacts and damages. Because of its generic character it can be used to address CPS systems, but it is entirely up to user responsibility and capabilities to make it feasible and efficient. Finally we should note that catastrophe modeling is a totally holistic approach and method provides a very generic framework for calculating risk expressed as financial losses regarding physical disaster for use by the insurance industry.

3.1.3 RA – Cyber Attacks and hybrid Attacks

Most of RA methods examine physical and cyber security independently, not taking into consideration combined operations in physical and cyber space. In [44] attacks are distinguished in physical attacks, cyber-attacks and combined physical and cyber-attacks: hybrid attacks.

Physical attacks take place in the physical environment of CPS including intrusion to spaces where they are installed, physical force and destruction. For example, commandos infiltrate to an industrial control station violating security mechanisms, breaking safety locks or killing guards and destroy CPS using explosive mechanisms or by causing malfunctions with improper local system operations impacting infrastructures. These impacts cause direct consequences to production or provided services.

Cyber-attacks may cause system malfunctions and downgrade critical systems functionality without the need of having direct physical access to CPS and control-unit rooms. Such an attack would be feasible if targeted systems use network technologies to be controlled like CPS cases permitting their remote exploitation and access. In this case, hackers could exploit systems vulnerabilities and gain access to CPS and ICS infrastructures having direct control over industrial systems and lead them to undesirable states attacking software and transmitted commands integrity.

Hybrid attacks occur in two stages: physical intrusion and cyber-attacks. The first stage permits or eases the access to spaces where CPS or ICS/ ICT systems are located in order to gain direct access or exploit. Depending on the sequence of actions these attacks are distinguished to:

a. Cyber-attacks taking place after physical intrusion or physical enabled cyber-attacks.

b. Physical intrusion and attacks taking place after cyber-attacks easing physical access or cyber enabled physical attacks.

In the first type of hybrid attacks physical intrusion to workspace of interest proceeds of cyber-attacks in order to gain physical access to CPS in this space and used as a CAP to attack different interconnected systems or be directly exploited.

In second type of hybrid attacks, cyber-attacks proceeding physical attacks intent to create favorable conditions for successful intrusion to guarded workspaces by deactivating network controlled protection mechanisms after attacking them through cyberspace using appropriate CAPs.

So, most usually an attacker will attempt to either gain direct control over an asset state or try to reduce the effectiveness of a physical protective measure, like a sensor or an alarm.

This method estimates a risk level for each of the assets that may require improved protection and provides a relative risk ranking between them, in order to provide guidance for spending limited capital on security investments. This RA method takes into account the Critical Consequences or differently Consequences of Concern caused by acting against CPS. For example, fresh water supplied to a city is corrupted after attacking against mechanisms controlling drinkable water quality and clearance at water cleaning facilities. This is the first step of this RA method. Next these consequences are correlated to undesirable system states controlled by CPS that may cause them. An Engineering Process Model is suggested for this purpose or experts' opinions. Then vulnerability assessment takes place. Invulnerability is defined as the ability of an asset to withstand an attack without suffering CoC on failure. It comprises of the following steps:

a. Definition of appropriate cyber and physical protective measures for each asset.

b. Define the appropriate threat model, i.e. define the capabilities of a specific adversary, both cyber and physical capabilities and quantify them. Physical capabilities empirically have been quantified in acceptable level, but cyber capabilities have not. Several parameters are related to adversaries' capabilities like funding, strength, commitment intensity, cyber skills, physical strength and access possibilities, while qualitative scaling is used to describe them.

c. Comparing the protective measures, asset susceptibility and threat characteristics generate the Probability of Success Given an Attack (PSIA) for each scenario/ undesirable system state that can cause a CoC.

This method defines two factors: probability of neutralization P_n and probability of interruption P_i of attack. The first is related with the probability of the defender to interrupt the attack sequence before completes it; while the second is the likelihood that defender stops the adversary from proceeding on with the attack sequence. The effectiveness of the physical protective measures is defined:

$$\boldsymbol{P_E = P_i * P_n}.$$

The effectiveness of protective measures against cyber-attacks is denoted as P_{Ec}. So, the likelihood that cyber-attack succeeds is: $1 - P_{Ec}$, while the likelihood that

physical attacks succeed is:$\mathbf{1} - \boldsymbol{P_{Epz}}$. The likelihood that the system is effective against combined cyber enabled physical or physical enabled cyber-attacks is:

$$\boldsymbol{P_{Ecp}} = \mathbf{1} - (\mathbf{1} - \boldsymbol{P_{Ec}})*(\mathbf{1} - \boldsymbol{P_{Epz}}).$$

The overall effectiveness of the system is the lower between effectiveness of physical attacks and effectiveness of combined attacks. In case of cyber enabled physical attacks or cyber-attacks the effectiveness of the system is the lower value that is calculated for different CAPs.

The method also considers the values of time to mitigate T_m i.e time needed to apply countermeasures and T_{me} which corresponds to the time from threat detection to time that CoC happen. Their ratio $\frac{\boldsymbol{T_m}}{\boldsymbol{T_{me}}}$ being small means that there is sufficient time to detect and mitigate threats, while if it is large it means that there is insufficient time to detect threat and apply countermeasures on time to avoid CoC. This methodology help identify vulnerabilities as well as what causes them, using as proposed quantifying method Monte Carlo Simulation.

This method initially considers risk as

$$\boldsymbol{R} = \boldsymbol{P_A} * \boldsymbol{P_{S|A}} * \boldsymbol{C}$$

But because P_A meaning the probability of attack is usually unknown or sensitive data conditional risk is defined where attack is supposed to occur, i.e $\boldsymbol{P_A} = \mathbf{1}$ and

$$\boldsymbol{R_c} = \boldsymbol{P_{S|A}} * \boldsymbol{C}$$

Where C is the consequence and $P_{S|A}$ is the vulnerability estimation.

Consequences are quantified using pairwise comparison for every pair of CoC and CoC outcomes using weight factors for each CoC and CoC possible outcomes representing subjective relative importance.

This method is considered as a semi-quantitative approach as it has the ability to express risk in numerical form based on probabilities and quantified CoC weight factors, providing prioritization capabilities. It supports CPS major characteristics like dual physical and cyber character, cyber and physical attacks against components and combined attacks. Dependencies and interdependencies are taken into account. Monte Carlo simulation used for quantification for each possible parameter is considered as an effective but extremely time consuming method and there is the need to distinguish realistic, useful results from mass of extracted results, otherwise precise realistically data are needed. Work has to be done in order to establish a risk index for examining in holistic way different nature CoCs. Considering attacks certain to happen and obtaining conditional risk may be logical for CI but in the other hand is not so useful, as capital is not limitless and must be effectively distributed to cover different security demands. Amplified criteria and motivation examination could make better estimations about adversaries' capabilities, probability of appearance and intentions. Estimation of time to mitigate is an amplifying factor for better effectiveness and probability of attack estimations.

Method does not directly consider dependencies and interdependencies, but rather considers attacks as multi-stages procedures, decomposing them to successive steps and assuming relevant probabilities for each stage. Success of proceeding step is necessary for next stage. Different attack steps cyber and physical can be combined; each is perquisite for the next. Certain impacts are considered to lead to undesirable system states that may cause certain consequences. Logical, physical and informational dependencies are examined by current method. By applying physical attacks geographic dependencies of assets located in the same space and threatened by common attackers may be present.

As said method decomposes attacks to successive attack steps and estimates the probability of success for each one of these steps, while the total success probability is expressed as the product of all individual substages probabilities. Attack decomposition to attack steps and relevant step probability estimation leads to more accurate probability estimation especially considering relevant conditions and perquisites for each step. Monte Carlo simulation can provide further more accurate and complete results. Method examines attackers' motivation and capabilities in order to achieve more realistic and accurate estimations. When probabilities are not easy to be estimated or they are unknown method uses conditional probability, where event occurrence is considered certain.

Method is a semi-quantitative approach using probability and effectiveness indicators as measures of risk. Moreover, method consider locational factor in risk assessment as it considers combinations of physical and cyber-attacks against physical and cyber assets. Method considers consequences of concern; these consequence interest many parts like population affected by attacks against critical infrastructures, although analysis remains in lower cyber and physical layers.

Probability assessing has already been discussed in previous character. Method provides one additional indicator for risk, assuming time needed to apply protective mechanisms when attack occurs and overall time from threat detection to consequences occurrence. The highest the ratio, the higher is the risk estimation. There is no particular method to quantify consequences. As they may relate to financial damage, fatalities, health impacts and population well-being, consequences of different natures, difficult to be measured and compared amongst them, Analytic Hierarchy Process or Vital Issues Process are proposed for a semi-quantification approach creating weighting factors for each one of them.

This methodology is a threat oriented one approach. But can also use as initiating point the identified of Consequences of Concern, so considered as an impact oriented methodology. In the second case after identifying CoC, it successively identifies undesirable system states and impacts that may lead to such consequences. Then attack methods are decomposed and analyzed. Method although is a theoretical one, presents clear and easily implemented tools and steps, while proposal of Vital Issues Process or Analytic Hierarchy Process which are trustworthy methods make this one, quite reliable.

As already stated it is easily implemented and supported by graphical and computational tools. Methodology is quite generic, and it is assumed that can be used to assess risk in different sectors and systems. As a consequence, it makes a holistic approach, being quite generic. There is no special guidance on asset identification. It is assumed to be used on consequences related assets, which should be identified during method evolution and attack plan analysis.

Threats corresponding to certain impacts and consequences are analyzed and scaled in three level simple qualitative scaling in order to help estimating probabilities more accurately. Attacks are considered to happen in multi-stepped procedures including cyber-attacks and physical intrusions. Furthermore, vulnerabilities whose exploitation may lead to the undesirable state are to be examined. Prevention and protection measures aiming at stopping adversaries' prior taking over attacks or interrupting attacks, as well as their effectiveness are proposed to be examined; no other specific guidance for vulnerability identification is given, while specialized software or experts' knowledge is significant on that purpose.

Three level typical qualitative scaling is used to assess attackers' characteristics like cyber capabilities, funding, stealth etc. in order to help making more optimal probability estimations. System behavior and performance are taken into consideration, since method identifies consequences of concern, then undesirable systems states that may cause these consequences, then identifies impacts that would cause system undesirable states leading to CoC. Method examines robustness as system effectives against cyber-attacks by estimating probability of asset failure prevention or asset failure mitigation.

Method examines Critical Consequences or Consequences of Concern as consequences having significant impacts. No special guidance is given. Also, method provides semi-quantifying risk approach for estimating risks related to critical consequences and setting priorities for budget optimal allocation in order to apply protective mechanisms. Method provides a framework for attackers' identification and identification of their course of action.

3.1.4 European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks – EURAM

EURAM method [47, 48] had been developed by the European Team for Critical Infrastructures Protection under the EU aegis inside relative EPCIP framework. The RA method had been developed by Thales and extended by TNO. Its purpose is provide a holistic methodology for analyzing and managing risks that should cover all areas of CI related to production, distribution and consumption of energy as well as any involving shareholders.

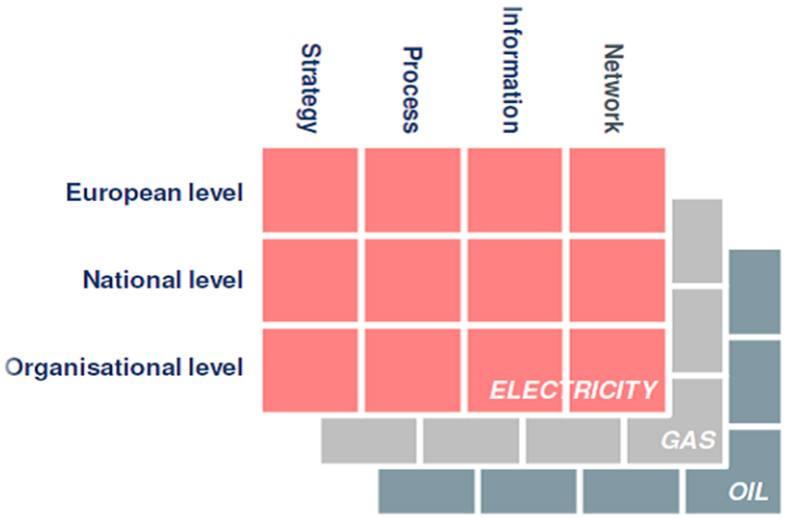


Figure 5: *EURACOM, application framework*

This methodology addresses to electricity, oil and gas energy sectors in different management levels (national, European, operational, strategic) and different functional or responsibility levels like energy distribution networks, infrastructures, information level that includes relevant ICT and information exchanges, strategic level where strategies and policies are set (Figure 5) and operational level. All these levels are in continuous interaction (figure 6). It was necessary that this RA methodology could be applied in all above mentioned levels. It is a holistic approach at different levels of abstraction from business level to European multi-national level. It is holistic in terms of infrastructures coverage. That means method should cover all operation sectors, like IT departments, physical infrastructures, organization including links to external stakeholders, human factor and human resources. It also makes a combined approach in the sense that Risk Assessment and Contingency Planning processes need to be closely integrated with clear linkages between one another. It also makes an all-hazards approach, in the sense it will cover the two main categories of accidental (human or technical, natural causes, or linked to external dependencies), and deliberate (human caused). It accommodates the outcomes of previous RA conducted at lower levels of abstractions. These outcomes may are based on different RA methods.

It uses a uniform approach with a single list or potential threats in order to permit multiple teams of organizations working in parallel and identifying risks based on experts' knowledge.

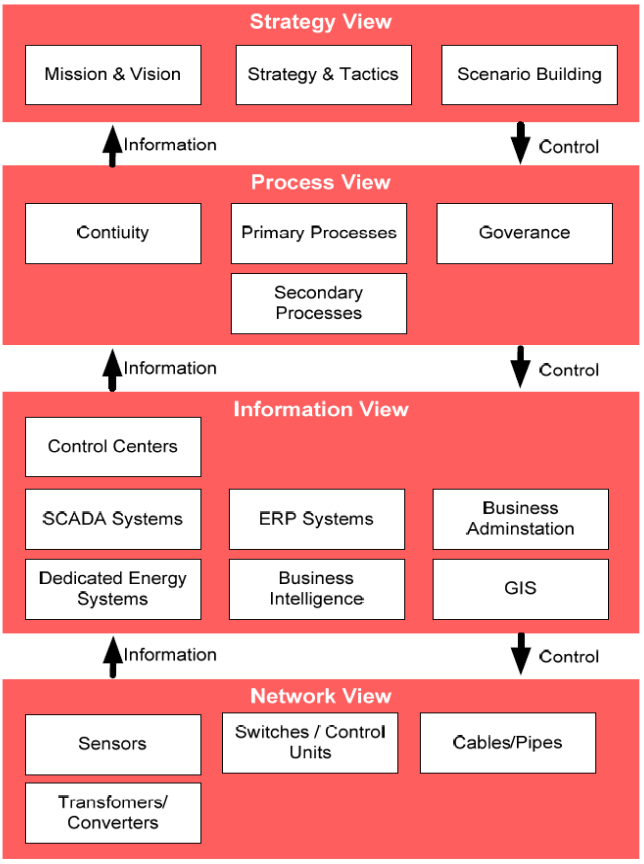


Figure 6: *EURACOM, application framework*

Holistic RA method means that risks in ICT systems, networks, human action or interference, physical or operational risk are examined in common ways. At the first phase of methodology each level related infrastructures and threats against energy communication networks, information system and other relative infrastructures are identified. Interconnections between energy transmission and distribution networks and control mechanisms where system response time is less than 15 minutes for every geographical scale are to be examined. If attacks or bad management occur it is possible that critical malfunctions may be caused and propagated in short time. In addition ICT systems are used in information exchange and command between decision and control centers and operation centers.

ICS include:

a. Sensors, metering devices and control units: They are used for supervising energy grids, monitoring functional situation, confirming proper function and monitoring system measurements ensuring they remain under allowed limits.

b. SCADA systems which monitor processes in industrial modules.

c. Specialized systems for monitoring integrity and availability of transmission and distribution of networks, fault detection or network management.

d. Networks and facilities central control stations.

Remote control of SCADA systems as well as other systems and control units because of wide geographical dispersion of energy networks and other CPS and networks with low cost and high efficiency, enforce the use of IP technology. But using this technology CPS and rest infrastructures are exposed to exogenous threats and attackers and oblige taking additional protection measures.

EURAM uses dependency theory according to which risk in CI is affected by different CI and the need of raw materials supply and service support. Dependence is defined as the relationship between two assets or services where one's presence is necessary for other's creation, while in occasion of bidirectional relationships between them interdependencies are defined [48]. So infrastructures faults may cause more faults in different part of infrastructures or in completely different infrastructures when dependencies or interdependences appear between them, for example between production and consumption. The method takes into consideration second level dependencies which become critical when a primary dependency fails.

When moving through levels of abstraction each level can treat certain risk levels. When identified risks exceed thresholds the risk that could not be handled is conveyed to the next level. This tactic permits communication of risk, while risk categories become of no importance while new risk categories and scorings are appearing at each next level transferring catastrophic risks to higher levels to be treated.

EURAM methodology consists of **seven** steps:

a. In the first step the operational holistic risk assessment team is constituted. It consists of the team leader and personnel of different expertize covering all dimensions of the analysis.

b. At the second step the scope of the analysis is defined with the desirable level of detail. It should have a physical perimeter including the physical assets, be composed of defined systems and networks and it should have boundaries with identification of the various job functions involved. Elements outside the scope can be examined as dependencies or interdependencies.

c. At the third step scales for risk measurement are developed. Risk is a function of probability of events occurrence and their severity. Typical scales ranging 1 to 5 are used. Probability scales developed fit to two main categories: accidents and untargeted attacks using historical data to develop probability scales and targeted or intentional attacks. In the second event category statistical or historical data is not an appropriate source for probability estimation. Rather targets' attractiveness, attack feasibility, motivation, adversaries' strengths, skills and resources and targets' level of protection should be examined for attack probability estimation. Information exchange between different organization and INTELLIGENCE is necessary to achieve this kind of estimations. There should exist a common base between different scales in order to have accurate risk measurement results and enable analysis of dependencies and interdependencies in CI.

d. The objective of the fourth step is to provide an understanding of CI delivery of services and products i.e. operations and processes.

e. Step 5 examines threats to the infrastructures. Generic threat classification is used for each one of the energy or other operational domain. Common threats or interdomain threats are examined; terrorism level in countries and past incidents and intelligence are taken into consideration. Detailed threat profiles are produced for specific threats.

f. In step 6 security controls that are implemented or missing are examined in order to identify the protection level, review security and the vulnerabilities that are present in the infrastructures. Security standards and actual vulnerability information sources should be taken into account on that purpose. Industry associations and national government can provide threat updates and best practices for vulnerability identification and treatment. In this step dependencies and interdependencies are taken into account, both internal and external to examine systems and infrastructures resilience, identify risk factors and provide more detailed view to the vulnerabilities.

g. In the final step associated risks are identified. An incident scenario is developed for each of the vulnerabilities identified and probabilities/ severities are estimated using the previously developed risk measurement scales. Dependencies and interdependencies provide useful information for incident scenario development. They are examined over an entire sector or following a cross-sectorial approach. Stakeholders and authorities involved in the RA process are identified in this step.

Risk assessment is repeated in case of organizational evolution, infrastructures changes, new threats and vulnerabilities identification and new security controls implementation.

Concluding, EURAM allows risk scoring on the axis for seriousness of the effects for all fields of impact; economical damages, political, health and psychological effects and environmental damage. The EURAM method is one between few methods both holistic, all-hazard and generically applicable to all CI sectors, being applicable to all CI operational layers and different energy sectors. EURAM method provides a mechanism to spread responsibilities for risk management over all levels while assuring all risk factors are addressed. Additionally, this is facilitated by a non-prescriptive mechanism. EURAM method is still rather conceptual and has few supporting tools including questionnaires and checklists. It complies with the common good practice approaches. EURAM is a qualitative approach, while its vulnerability driven approach, even though it uses a complete informational basis may not be able to identify zero days attacks, leaving infrastructures unprotected against this type of attack. Special care given to scales development and different impacts measuring scaling interrelation gives a rather accurate semi-quantitative risk expression. Probability estimation approach gives the best estimation capabilities; although subjectivity cannot be omitted. But experience

and expertise of involved personnel in the holistic operational risk assessment team and the use of enriched information collections, trustworthy information sources and national/ industrial intelligence may restrict probability estimation declination from possible realistic outcomes. EURAM method is suitable for application in CPS, covering their individual characteristics such as complexity, criticality and presence of dependencies and interdependencies in all levels, e.g. strategic, operational, technical, and covers internal and organizational external relationships.

EURAM makes distinction of internal and external dependencies and interdependencies meaning between same systems components, but also between different infrastructures and sectors, and looks up for dependencies between systems and resources/ raw materials as well as between consumption and energy production fields. It is known that EURAM provides a qualitative risk analysis approach. EURAM considers geographical dispersion of cyber physical systems. It assesses risk for all interest stakeholders in national/ multinational, strategic and operational layers. So, it is considered a high level RA methodology. As methods documentation states different expertizes are needed to analyze widespread and complex CPS.

EURAM makes an all-hazards approach covering domains of accidental or linked to external dependencies and deliberate events. Risk thresholds are defined and when risks exceed these thresholds so they cannot be managed at the current layer/ level they are transferred to the direct higher levels/ layers so catastrophic risks may be managed more efficiently in higher layers. Statistical or historical data is not an appropriate source for probability estimation. Rather targets' attractiveness, attack feasibility, motivation, adversaries' strengths, skills and resources and targets' level of protection should be examined for attack probability estimation. Moreover, EURAM is an asset oriented method as it begins with infrastructures identification in each layer of interest. Initially operational concept is described in detail and then operational concept and organization function decomposition takes place.

Generally, EURAM had been developed by Thales under the aegis of European Union to be applied in European Critical Infrastructures and particularly in the Energy Sectors. EURAM addresses all different energy sectors and different management levels such as multi-national, national, operational, strategic and layers, energy distribution networks and relevant infrastructures, cyber and physical infrastructures and all these levels are in continuous interaction, Furthermore, EURAM is a holistic approach for all different layers to multinational layer to national and business, applied to all different energy sectors, production and distribution as well as other CI. All risks related to ICT systems, energy distribution networks, physical and operational risks are examined in common way.

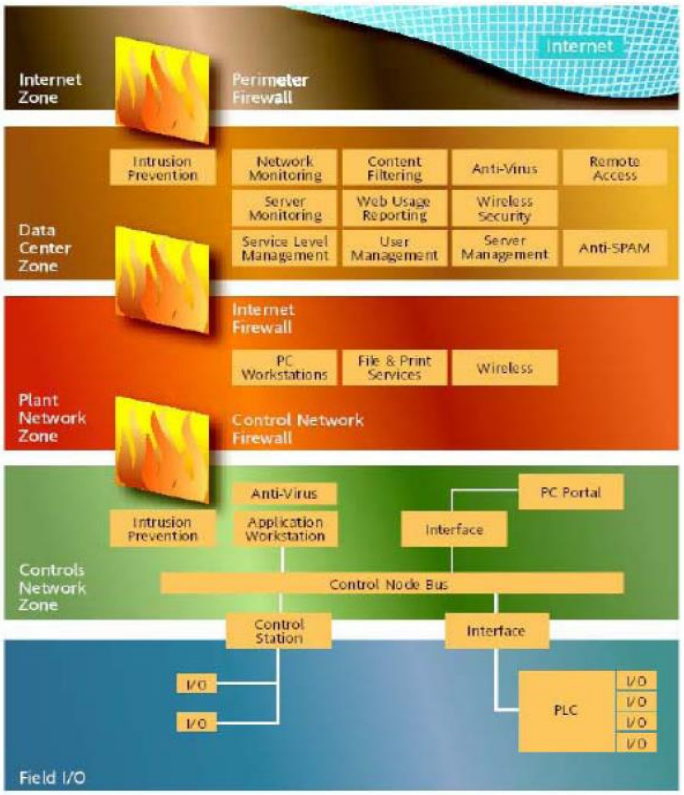


Figure 7: *SCADA systems and security mechanisms*

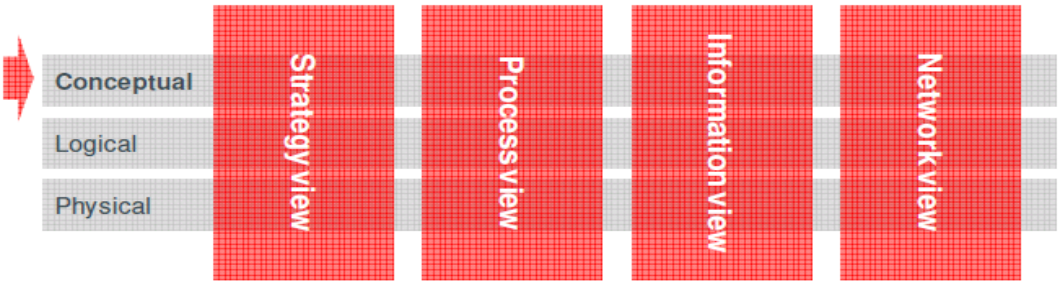


Figure 8: *EURAM applicability and scope*

Asset identification is based primarily on operational concept and operational function disassembly and then matching with physical infrastructures. Threat is primarily identified using as basis national intelligence information. Also, scales for risk measurement are developed. Risk is a function of probability of events occurrence and their severity. Typical scales ranging 1 to 5 are used. Probability scales developed fit in two main categories: accidents and untargeted attacks using historical data to develop probability scales and targeted or intentional attacks.

EURAM examines interconnections between distribution and transmission networks and respond delays when a command is transmitted or an attack occurs. Management errors and caused malfunctions and their propagation in short time periods are examined during risk examination to determine different system states and reactions. Method considers power grids as CI, no other criteria and procedures are used to identify critical assets and vulnerabilities. Finally, its purpose is provide a holistic methodology for analyzing and managing risks that should cover all areas of CI related to production, distribution and consumption of energy addressing related shareholders' interests, providing a common and holistic approach for end-to-end energy chain risk assessment and management solutions.

3.1.5 Baseline Protection Concept for CI

The Baseline protection concept for Critical infrastructures [18, 20, 49, 50] was developed under the authority of the German Federal Office for Civil Protection and Disaster Response and the Centre for the Protection of Critical Infrastructures having being issued in 2005.

The aim of this baseline concept is reduction of the level of vulnerability of Critical Infrastructures. As starting point different threats are identified and categorized including physical phenomenon, human errors, criminal and terrorists acts, environmental, epidemics, organizational and cyber-attacks. This concept focuses on averting physical dangers and does not cover cyber threats. IT and cyber threats subjects follow ISO 17799 standard and IT baseline protection manual [50].

Special questionnaires and checklists are in use to help initiate a discussion process within the companies in order to help and guide users through detection and recognition of threats and assets stages and setting security priorities. Questionnaires and checklists are samples and not definite guides for the enterprises.

Next protection level is defined, then damage and threat scenarios described and vulnerabilities analyzed. Geographic location as CI are usually geographically dispersed, company symbolic character prescribed by its high importance and societal effects, importance of facilities and interdependencies are taken into account. This method considers dependencies and interdependencies. Failure or attack to one asset that is related with dependency or interdependency character to another asset, function or service may lead to domino effects affecting these different functions, services and assets. Or attacking an asset may affect assets located in different places.

Risk sources are considered human factors related to behavior and human caused errors on purpose or not, attacks, organization factors related to sources concentration and outsourcing, environmental factors (physical phenomenon and hazards) and IT.

During asset and risk recognition this methods considers particularly

endangered assets and areas in companies. These areas refer to high risk areas exposed to extreme weather conditions, earthquakes, epidemics, areas endangered through human and technical failure, hazardous substances, explosions, terrorism and criminal acts. Risk assessment is applied regarding potential dangers involving threat scenarios and repeated in order to define accepted level of security and proper security measures. In order to define possibilities of attack, historical and statistical data is used as well as criminality or terrorist attacks information and indication acts.

So, during the analysis procedure firstly the location of the CI is to be examined taking into account above mentioned risk factors. Systematic danger analysis[1] is undertaken in order to establish whether critical areas may constitute possible critical targets. Then impact consequences are analyzed and whether they might lead to a serious danger (hazard analysis).

Special consideration has been taken for cases of terrorism or unauthorized human access and interference. Additional hazard and danger analysis is performed to ascertain the possibility or probability of such threats. Attractively of targets is examined using criteria of general risk assessment, geographic location of the operational area and facilities, importance of facilities and symbolic character, interdependencies between the infrastructures, structural nature of the cooperation between public facilities and the operators, type, topology and cooperation relation of the risk management structures implemented by the operator.

After requirements are assessed for protection against human attacks, human caused errors, technical failures and natural hazards. Danger and hazard analysis have equal priority and should be decided which one of them should be examined first at each RA procedure. It is generally suggested to start with danger analysis, and then determine consequences. RA and results are documented. RA is repeated regularly in order to identify new dangers and carry out reassessment to adapt security requirements properly. It should always be taken in consideration the possibility of domino effects in order to apply the proper protective measures in the proper places.

This baseline protection concept may be considered as a try-and-succeed analysis, where thorough extensive repeated analysis in theoretical framework, using threat scenarios; most affordable countermeasures are chosen to be applied to reduce systems' level of vulnerability. As it is referred it does not focus on IT systems but it can cover this area in a generic way. In [50] is provided a very general guideline and definition about RA procedure and task and method refers to ISO 17799 for further instruction. It is considered as too cost-intensive for small and medium size enterprises.

[1] Method of identifying regions, infrastructures, facilities and installations which might be at risk as result of possible incidents. Danger refers to possibility of an incident which may lead to injury or cause damage to material assets and the environment or result in social and economic disturbances.

As already mentioned dependencies are examined in the form of the so-called domino effects which appear when external events affect the facilities. These events may occur in the same or different places within a short time of each other. More over secondary damage should be taken, for example traffic problems, supply bottlenecks and shortages linked to transport systems disruptions due to power failures. BCI is a qualitative method and address risk assessment for protection of CI and population from different types of threats and hazards focusing on safety and protection against natural phenomenon, not focusing on IT, ICS and CPS. Rather it covers these aspects strategically.

This baseline uses a general security situation, indicators based on statistic and historical data, regional data and previous recorded offenses in order to provide indication of level of dangers. It keeps a history data set of five years on this purpose. Furthermore, risk is estimated using a three level typical scale. To determine risk category and evaluate probability of attack analysts consider several factor like attackers intentions, motivation, preparatory acts and resources needed for the attack and attack types.

BCI is a threat oriented method, starting by identifying threats of different nature, like physical phenomenon, human errors, technical faults, attacks and cyber-attacks against CI. Also, BCI has been developed for use by Germany national authorities and it is constant with International Risk Assessment Standards like ISO 17799 and adopting best practices from BCI security manual. Brainstorming techniques and supporting methods are used in BCI framework requiring participation of different expertized personnel. Finally, BCI assess risks related to CI. Identifying or selecting CI is operators' responsibility and method does not include any characterization criteria.

3.1.6 Risk and Decision System for Critical Infrastructures – DECRIS

DECRIS [20, 52] had been developed in Norway. This approach does not cover interdependencies issues effectively. RVA is conducted in two phases. In the first phase, the most severe threat scenarios are screened for detailed analysis. This phase resembles the basic concept of PHA procedure, during which consequences of an undesirable event are assessed. DECRIS usually refers to worst case scenarios consequences, because it is used for emergency preparedness planning. So, the whole procedure and incident frequencies refer to such cases. To overcome this problem, "average" scenarios and worst case scenarios are examined separately. But this fact presents unrealistic incident probabilities as just one case, that of the worst case scenario is examined and leaving outside of the examination the mass of incidents. In DECRIS several impact areas are examined, like economic losses, safety, loss of services etc., so probability of incident occurrence estimation is more difficult.

DECRIS approach to RVA uses the following steps:

a. Taxonomy of undesirable events is established. Undesirable events

are categorized as natural events, technical/ human caused (accidents/ errors) and malicious (cyber-attacks/ sabotage).

b. Decision about the consequences dimensions used to analyze the undesirable events. DECRIS uses the following categories: Life and health, environment, economy, manageability, political trust, availability of the supply of the infrastructures.

c. Risk matrices calibration. The undesirable events are described with a probability category for each consequence category.

d. Perform a standard PHA/ RVA analysis. All hazardous events are identified. The risks related to each undesirable event are assessed. In simple analysis undesirable events categories of infrastructures supply availability, life and health losses are considered. Main events are used to link the undesirable events on which PHA focus with the infrastructures.

e. Selection of events for further analysis. Candidates for further analysis are usually high risk events. Specific criteria are also used for event selection, like the presence of dependencies/ interdependencies, if events have gross accidental potential and if there are communication challenges related to the event.

f. Perform detailed analysis of the event. Course and various consequences of selected events are examined in more detail. Analysis should include:

(1) Evaluation of interactions and other couplings in between infrastructures, and how consequences of the undesirable events are affected.

(2) Evaluation of vulnerabilities.

(3) Suggesting and evaluating risk and vulnerability reduction measures.

During the detailed analysis FTA and event tree analysis (ETA), flow line networks techniques etc. are used in order analyst to gain an insight to systems' interdependencies.

During DECRIS application in case studies need of infrastructures owners to gain knowledge about each other's systems had been revealed. It needs a more structured and systematic procedure in order to facilitate system decomposition and analysis during RVA procedure. As it declared by its own designers it is not effective on taking into account systems interdependencies.

It utilizes experience from RA in different sectors of CI in order to satisfy one of its main objectives to provide a generic, all hazards RVA methodology suitable for CI cross sector RA. It covers subjects of safety like accidents and failures and security e.g. malicious cyber-attacks. Furthermore, it examines how media and public opinion affects decision process and how different opinions can be combined to provide a more effective decision making across CI. DECRIS involve electrical power and water

distribution, transportation and ICT. It is based on worst case scenarios examination.

Dependencies are considered during risk analysis, although there is no particular process to detect and analyze them, not only between the same system parts but also between different infrastructures. FTA and event trees support dependency identification. DECRIS is a qualitative approach to RA methodologies. Moreover, DECRIS considers two scenario cases: average scenario case and worst case scenario. It uses the worst case scenario because it is used for preparedness. Risk is expressed qualitatively with the use of risk matrixes. So, other scenarios are left not being analyzed. During analysis main scenarios are examined. The undesirable events are described with a probability category for each consequence category. After initial risk estimation, higher risks are selected for further analysis. DECRIS is an impact oriented method addressing defined events affecting specific categories of critical assets, like human life, political states, etc. finally, by definition DECRIS examines risks related to critical assets, but no critical asset identification process is included. Asset selection and analysis is operator's responsibility.

3.1.7 Electricity Sector Information Sharing Analysis Center - ES-ISAC

ES-ISAC [18, 53] provides general guidelines for vulnerability and risk assessment to help identify critical facilities and their vulnerabilities while recommending "best practices" for facilities and functions considered critical. It can also help in identifying countermeasures to mitigate threats. It provides a method of setting priorities for critical assets, threats and countermeasure strategies. It takes into account both physical and cyber domains to contribute to critical systems security. It uses a structured methodology with checklists and questionnaires, used by expertized personnel and it is applied in successive steps. The outline of this method is described by a four steps process:

a. Identification of assets, impacts and loss caused by impacts. In this step critical assets requiring protection are determined. Then undesirable events and their impacts with respect to critical assets are defined and then priority of assets is set based on impact consequences and loss.

b. The second step deals with identification and analysis of vulnerabilities. Potential vulnerabilities are recognized related to specific assets or undesirable events. Also the degree of vulnerability related to each asset is defined. Then existing countermeasures are identified as well as their level of effectiveness in reducing vulnerabilities.

c. Assessment of Risk and the determination of priorities for the protection of critical assets. The degree of impact related to each critical asset and the likelihood of attack against it by a potential adversary, are estimated. The likelihood that a specific vulnerability will be exploited relative to specific asset is estimated. Statistical and historical data and expert's opinion weights during these estimations. Risk prioritization follows based on integrated estimations.

d. The final step has to do with risk management and proper countermeasures detection and application.

The method advices considering interdependencies among assets and functions during asset and impacts identification step as impact at specific infrastructures may affect a different infrastructures on both physical and cyber domain. It is based on NERC standard for establishing security in energy domains. This method is quite generic, approaching its subject in a holistic way. Method examines dependencies/ interdependencies abstractly. ES ISAC is a qualitative approach to risk analysis setting asset protection priorities. ES ISAC is used for critical asset protection.

After assets, threats and vulnerabilities have been identified, considering dependencies the possibility of attack to each asset is estimated. Based on these estimations a ranking of threat scenarios is set in order to prioritize assets for being protected. So, in fact no risk assessment takes place, but rather only threat analysis is done and priorities are set based on threat analysis results. ES ISAC is an asset oriented methodology focusing on critical assets.

Although, this method is based in US national standards it is considered unreliable since prioritization not based on risk is estimated inefficient as assets and countermeasures will not be managed with the most cost effective way. Method is very generic so it can be considered as holistic approach. Finally, it provides general guidelines for vulnerability and risk assessment to help identify critical facilities, vulnerabilities and recommends best practices for critical facilities and functions.

3.1.8 Risk and Vulnerability Analysis – RVA

RVA presented in [18, 54] had been developed by Danish Emergency Management Agency and released in 2006. It is designed for use by government authorities in other words it is used in strategic level. It is used by Danish ministries for planning maintenance and continuation of societal functions, in case of major events including war case.

It is presented as a simple and functional tool consisting of four parts and it is supported by interactive docx documents. It uses well-structured guidelines including standardized questionnaires the interactive documents.

In the first part the scope of the analysis, its purpose and the participants are written down. RVA starts with identification of assets considered critical for the organization function.

In the second part users generate threat scenarios based on what is most relevant to them. Threat scenarios are described thoroughly with the help of complete and detailed questionnaire.

At the third part users assess risk based on the previously generated risk scenarios. The consequences are defined in accordance with a set of pre-defined sets of impact areas. Incident consequences level and probability of occurrence are estimated.

Both probability and consequences level are expressed in numerical range 1 to 5. Consequences are related to overall organizational and societal damage and describe a variety of system defined consequences. The product of consequences level and incident probability defines the risk level.

Finally it aggregates provided data and estimation in standardized worksheet format in which the analyzed scenarios are presented and compared graphically in risk and vulnerability profile for critical functions.

Since it is used in strategic level it is characterized by generic character. It is very easy in use and provides general results for strategic planning in short time. It provides a simple and effective tool. So these characteristics make it feasible to apply this method without the need of specialized training and skills in risk analysis methodologies.

Probabilities of impacts are based on historical and statistical data indicating relative frequency of appearance, if such data is available. User's experience, knowledge and qualified guess substitute historical and statistical data if such data is not available. Vulnerabilities are not considered directly. Just countermeasure used to mitigate or limit impacts effects and consequences are taken into account during risk analysis procedure.

Method presents results for critical functions. It is considered possible that some threats, assets and related vulnerabilities might remain unnoticed and not be analyzed. Method provides guidelines for countermeasure and mitigating/ limiting strategies accompanied with risk level implementation. Risk metrics are mainly qualitative making it difficult to make comparisons among assessments. It is on user's hand, knowledge and abilities to apply this method in certain domains like cyber domain in order to estimate risks on information and CPS as no specific guidance is provided. Possibly it can be used for more assets other than critical assets. http://www.brs.dk provides the tool, supporting documentation and a case study example. So strong points are simplicity, user friendly tool interface and implementation.

Probability estimation is based on historical and statistical data describing frequency of occurrence and formulated in qualitative scale ranging 1 to 5. Qualitative method cannot distinguish small risk variations. RVA is a qualitative assessment method. Moreover, both probability and consequences level are expressed in numerical range 1 to 5. Consequences are related to overall organizational and societal damage and describe a variety of system defined consequences. The product of consequences level and incident probability defines the risk level.

RVA is threat oriented methodology and focuses in specific threats considered relevant by the operators, although specific scenarios are examined thoroughly. Use of standardized questionnaires make procedure easy in implementation, but fail to assess rare attacks, zero days and black swans or other unconventional and non-predictable actions, particularly when available guidelines are not revised regularly. This makes method unsuitable for use in wide area dispersed and complex cyber

physical systems, where variable threats are posed against numerous systems and systems components. Furthermore, by using simple interactive docx document format tool it is made user friendly and low cost and easy to learn and apply. It uses well-structured guidelines including standardized questionnaires the interactive documents, presents analysis results graphically and it is supported by sufficient documentation.

Being a strategic tool it assess risks in holistic approach being appropriate for use in all different sectors. The drawback of the method is that it cannot address assets, threats and vulnerabilities in detail and depth being inappropriate for usage in lower layers especially low level cyber and physical layers and may omit significant detail and risks. Also, detailed questionnaires are used for specific threats and threats scenarios identification. This practice drawback is discussed in previous paragraph.

Since assessment is executed in high strategic level not considering technical specificities and system particularities, but risk components are examined from a general aspect. So, there is no need for interdisciplinary application with participation of different expertizes analysts. Departmental and system risks and consequences assessments are communicated from lower levels to the higher management level for overall assessing. Moreover, it is supposed that RVA is used for CI risk assessment, so critical assets are imported in the risk process; there is no other method or criteria to identify criticality during the risk assessment process. Finally, it is designed for use by government authorities in other words for use in strategic level. It is used by Danish ministries for planning maintenance and continuation of societal functions, in case of major events including war case.

3.1.9 Risk Management Guide (RMG) - Department of Energy (DOE)

The Risk Management Guide presented in [17, 18] had been issued by Department of Energy in 2011 for projects in the energy sector risk analysis and management.

The RMG – DOE consist of the following processes:

a. Risk identification

b. Assignment of the risk owner,

c. Assignment of the probabilities and consequences,

d. Assignment of risk trigger metrics,

e. Risk register,

f. Risk analysis

g. And finally risk handling and monitoring throughout project lifecycle.

Risk assessment identifies, analyzes and quantifies programs and projects risks in terms or probabilities and consequences. RA examines risks, identifies assumptions regarding these risks, and discovers risk causes and relationships with other

identified risks. RA is irritated throughout project lifecycle.

Risk identification is the first step of the RA procedure. Beginning with this step the project is broken down in the breakdown structure (Figure 9), that is the hierarchical structuring of risks. The upper levels of this structure represent project technical, internal and external risks while the lower levels are set to cost and schedule risks. It demonstrates risks in a methodical and structural way permitting indication of likely risk sources and a better understanding of these risks. Each tier can be broken down for further analysis.

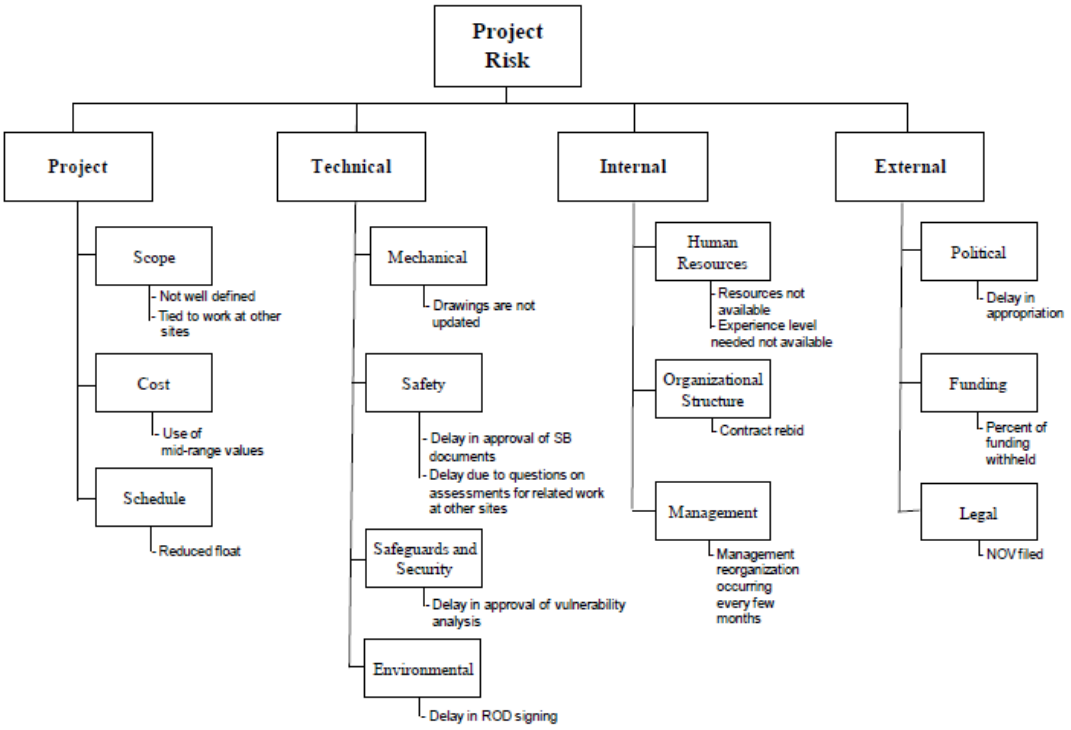


Figure 9: *Breakdown structure*

At the next step the risk owner is identified. The risk owner is the person or team responsible for managing the risks and validating qualitative and quantitative assessment.

As said consequence is the outcome of an event and probability is the likelihood of this event occurring. During qualitative analysis categorical scales are used for probabilities and outcomes, however many times it is useful to use quantitative metrics to ensure consistent assignments of probabilities and outcomes.

Next risk triggers and interdependencies are identified. Risk triggers are events or sequences of events indicating that risks are initiating. Trigger monitoring permits preparation for initiation of risk handling strategies.

Risk register is a uniform format for presenting each identified risk in much detail, possibly integrating appropriate risk handling strategies.

At the RA step all costs and impact consequences and calculated, presented and compared between them for risk prioritization. It sets risk priorities by setting a rating to each identified and analyzed risk. RA is performed as qualitative and as quantitative analysis. Purpose of each kind of analysis had been described in previous paragraph.

Qualitative RA is initially processed without any mitigation strategy applied or already countermeasures applied to recognize initial risks, then repeated after countermeasures to identify best risk handling strategy including potential measures and risk handling strategies. Qualitative RA uses qualitative RA matrix or differently, probability impact diagram or matrix (Figure 10). The matrix combines probability and consequence of a risk to identify risk rating for each individual risk. One common practice is to search for common risk causes or other similarities in risk registers so to adopt shared risk handling strategies to deal with these risks.

Quantitative RA uses mainly Monte Carlo Simulation statistical modeling to estimate the cost to projects and schedules by applying a numerical analysis including all possible outcomes and all possible probability values. It provides a Probability Distribution Function for a range of possible project outcomes and a Cumulative Distribution Function representing the likelihood that for a given probability the project cost will be at or below a given value. Quantitative RA could provide a view for risks that require the most focused attention. Quantitative RA could be restricted just to the results of qualitative RA with top ratings. To quantify risks a percentage distribution is assigned to each probability. Economic values are assigned to impact costs and duration is assigned to affected activity impacts in schedule. Then Expected Value (EV) of cost impact or duration impact for all risks is calculated[2]:

$$\boldsymbol{EV = \sum P_{Ri} \times CI_{Ri}\,(or\ SI_{Ri})}$$

Where,

$EV = Expected\ Value\ of\ cost\ impact\ or\ duration\ impact\ for\ all\ risks$

$P_{Ri} = Probability\ Distribution\ function\ of\ risk\ occuring$

$CI_{Ri} = Cost\ Impact\ Distribution\ function\ of\ a\ risk\ occurence$

$SI_{Ri} = Schedule\ Impact\ Distribution\ function\ of\ a\ risk\ occurence$

Quantitative analysis normally uses continuous probability distribution, but can also function in discrete mode when user wants distinct values to be examined. The most common practice is to use a range of values representing the most likely view or expressing optimistic and pessimistic views.

Quantitative RA further extends using more analysis models:

a. Planning assumption validation analysis. Reviews the assumption

[2] In this occasion $\sum$ operator does not mean summation of individual expected values for each risk but represents a stochastic process (Monte Carlo Simulation) using the collective probabilities and cost/ schedules impacts for all identified events.

made and used as a base for planning the project budget.

b. Cost and schedule quantification range assumption data – gathering process and validation analysis.

c. Sensitivity analysis. Targeted Monte Carlos Simulations or specific risks or key risks are executed in order to examine their effect on various activities.

d. Project learning analysis. Method uses older data from past Monte Carlo simulations to control current results accuracy.

e. Error and variance analysis. Older valid data is used to indicate the range of analysis results that should be expected and limit them inside a valid range.

f. Contingency ad equation evaluation. Used to analyze the adequacy of the contingency valuation that has resulted from the quantitative analysis of the risks.

Consequence						
		Negligible	Marginal	Significant	Critical	Crisis
	Cost	Minimal or no consequence. No impact to Project cost.	Small increase in meeting objectives. Marginally increases costs.	Significant degradation in meeting objectives significantly increases cost; fee is at risk.	Goals and objectives are not achievable. Additional funding may be required; loss of fee and/or fines and penalties imposed.	Project stopped. Funding withdrawal; withdrawal of scope, or severe contractor cost performance issues.
	Schedule	Minimal or no consequence. No impact to Project schedule.	Small increase in meeting objectives. Marginally impacts schedule.	Significant degradation in meeting objectives, significantly impacts schedule.	Goals and objectives are not achievable. Additional time may need to be allocated. Missed incentivized and/or regulatory milestones.	Project stopped. Withdrawal of scope or severe contractor schedule performance issues.
Probability	Very High >90%	Low	Moderate	High	High	High
	High 75% to 90%	Low	Moderate	Moderate	High	High
	Moderate 26% to 74%	Low	Low	Moderate	Moderate	High
	Low 10% to 25%	Low	Low	Low	Moderate	Moderate
	Very Low <10%	Low	Low	Low	Low	Moderate

Figure 10: *Probability impact diagram*

RMG-DOE addresses physical, oorganization and personnel assets. The method focuses on technical and human failure. The method offers extensive checklists for determining threats and effects but cyber security is referred just as a risk factor. The method provides metrics for probability and effects, which makes comparisons between projects possible. It is an impact oriented RA method and that means that in some cases some assets and threat scenarios may go unnoticed. Strong points of RMG-DOE are the rigorous metrics and the extensive glossary of terms, which enables a consistent understanding of the terms used. The quantitative analysis with the use of extensive Monte Carlo simulation and further error detection analysis methods provides accurate risk estimation for a range of possible outcomes as well

as it is possible to make a more deterministic approach to estimate discrete outcomes and risks. It can be used in different levels, technical and particularly operational and strategic, as quantitative RA provides much cost and economic information for decision makers and persons responsible for budget planning.

Risk Management Guide of US department of energy examines any dependencies through process although there is no particular guidance on that purpose. RMG is both qualitative and quantitative method; according to each user needs the appropriate expression is selected. RMG is used for risk analysis and management for projects in the energy sector.

Method uses risk triggers; risk triggers are events or sequences of events indicating that risks are initiating. Trigger monitoring permits preparation for initiation of risk handling strategies. Expected values are used to quantify risk. Monte Carlo simulation is used to examine all possible outcomes, permitting accurate risk calculation. Though this method may prove to be time consuming and may be impractical when a lot of probabilities are to be examined. Contingency analysis, project learning analysis methods are using older extracted data from previous Monte Carlo simulation and valid data during Error and variance analysis to control correctness of generated results. Method uses expected values to calculate quantified risks. Total risk is acquired by summing all individual risks expressed as expected losses. Moreover, RMG-DOE addresses physical, oorganization and personnel assets. The method focuses on technical and human failure. It analyzes them to subcategories to identify relevant risk using risk breakdown diagrams, describing risk related to every organization element.

Use of strong mathematical models like Monte Carlo Simulation, Contingency analysis, project learning analysis and error/ variance analysis produce accurate and consistent results. This method particularly requires the participation of expertized personnel because of the advanced mathematical models it uses, requiring specialized knowledge about these modeling and analysis techniques. Additionally these methods although they are able to produce accurate and consistent results they may prove to be extremely time consuming and impractical, while generated data may not all be usable. The method offers extensive checklists for determining threats and effects, but cyber security is a referred just a risk factor viewed from operational or strategic level. By using risk breakdown structure methodology is able to identify every different organization part, systems, subsystems and function category defining relevant risks

Method cannot be characterized as holistic since combination of qualitative and quantitative risk estimation approaches and risk breakdown structure permit identification and treatment of many different risks but it remains quite generic and it is considered that cannot address low layer, cyber and physical risk, concerning for example SCADA and ICS systems. It is rather considered appropriate for operational and strategic layers risk analysis. In qualitative approach probability impact diagram or matrixes are used, which combines probability and consequence of a risk for each

individual risk. Criticality is assumed through qualitative scaling where critical impacts and consequences are imprinted in appropriate scales in risk matrix.

3.1.10 Vulnerability Assessment using Attack Tress

In [55] a method for Vulnerability Assessment of Cybersecurity for SCADA Systems that uses attack trees is presented. Attack tree is a methodology used to examine the security of a system based on varying attacks against it. It uses a tree structure to model attacks against it. The root (top) of the tree represents the attack goal and the leaf nodes represent the various ways to achieve it. Each node in the attack tree represents a subgoal while children of this subnode represent ways of achieving this subgoal.

At each node values of impossible or possible can be assigned. There are logical (Boolean) AND nodes and logical (Boolean) OR nodes. In the first occasion all related nodes should come TRUE in order the attack achieves its goal. Nodes represent different steps until succeeding of the attack goal. That means that each subnode should be achieved in order to achieve the attack goal. AND node succeeds its goal if all of its children succeeds its goal and fails if one or more of its children fail. In the other occasion one or more leaf nodes from a set of leaf nodes, in the same level of the tree, come true. OR nodes are alternatives of succeeding the attack goal. So, OR node succeeds its goal if any of each children succeeds its subgoal and fail if all children's fail, too.

After structuring the attack tree and simulating all possible attacks against a specific goal and assigning values to each subnode, the effective ways of action are determined. Moreover the method indicates the points which should be protected in order to prevent adversaries succeed their goals. Any Boolean value can be assigned at each node [56]. Also, the value of probability of success for each given attack can be assigned at each node, thus permitting to calculate the total probability of attack of succeeding the root goal.

To create attack trees, first all possible goals should be identified. For each one of these goals, an attack tree will be structured. Then all possible attacks against each goal should be added to the attack tree and then this procedure will be repeated for each subnode of each attack tree. So, working in reverse, nodes representing attack goals are researched; attack methods capable to exploit these nodes are looked for. When attack against a node is successful, preconditions to attack next higher level node or parent node are met. So creating a complete attack tree requires experience, knowledge of all system vulnerabilities, attack skills and knowledge and of course it is considered as a time consuming process. There is always the risk of some cases not being included into the attack tree. However, different factors integration to the attack tree, like cost, vulnerability, countermeasures etc. offers a much integrated picture of the system, describing both defensive and attacking capabilities. Attack trees are useful tools because by using and testing different types of values each time in the tree nodes may provide conclusions about difficulty

of attacks, attack requirements, attack costing, damages and impacts for alternation of system parameters, even select most affordable or promising attack method. Also, different attack methods may be integrated into the attack tree structure in accordance with potential adversaries' capabilities and strength and target types, vulnerabilities and countermeasures.

[55] make use of cybersecurity vulnerability index that is a measure of probability that an attack tree or an attack leaf of being compromised. Its value ranges between 0 and 1, where 0 represents an invulnerable system and 1 a vulnerable one. Different indexes are assigned to different leafs. Total attack tree vulnerability index is calculated based on individual leafs vulnerability indexes.

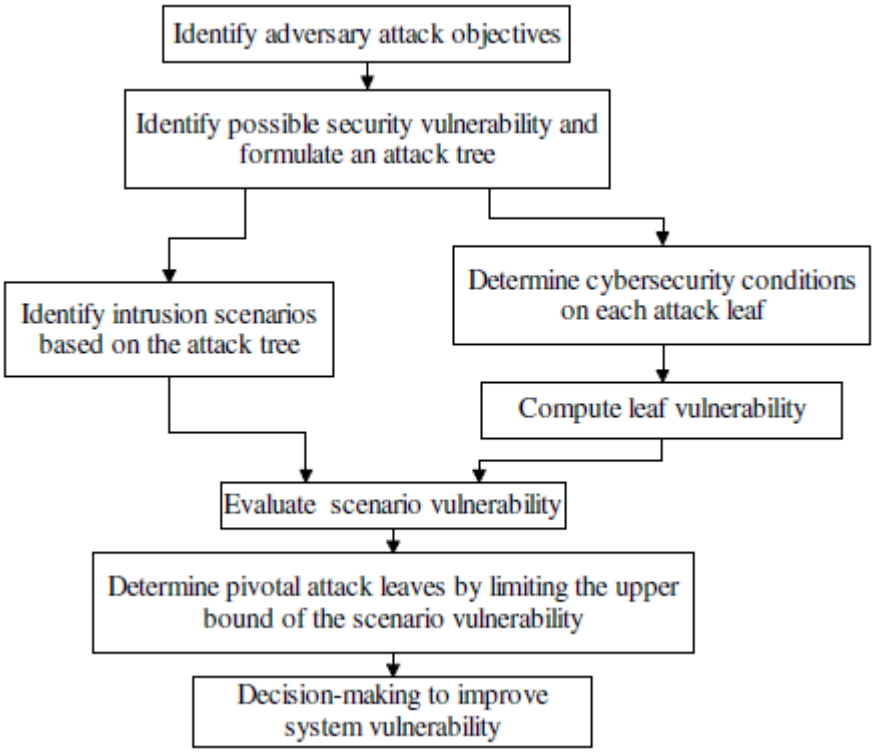


Figure 11: *Vulnerability index evaluation*

Figure 11 describes the process of evaluating vulnerability index. Vulnerability index assessment is based on technological countermeasures and security policies. Before vulnerability indexes evaluation takes place, a set of user defined cybersecurity conditions is determined. Preliminary these conditions are assigned values 0, 0.5 and 1 whether they are met or not. Again value 0 represents an invulnerable system and value 1 represents a vulnerable one. After that vulnerability index evaluation for the attack tree takes place using four steps:

a. Intrusion scenarios identification and possible attack tree scenarios enumeration. Each of the attack scenarios is formed as a combination of attack trees AND, OR leafs.

b. System, scenarios and attack leaf index evaluation. Leafs vulnerability index $\boldsymbol{v(G_k)}$ is calculated. The overlall scenario vulnerability index equals the the composing leafs indexes indexes product. The system's vulnerability index $\boldsymbol{V_s}$ is defined as the maximum attack tree vulnerability in other words the maximum scenario vulnerability index:

$\boldsymbol{V_s = max\{V(i_1), V(i_2), V(i_3), \dots V(i_k)\} = max\big(V(I)\big)}$, **k** the total number of the intrusion scenarios and

$\boldsymbol{I = \{i_1, i_2, \dots i_k\}}$, intrusion scenarios set

$\boldsymbol{V(I) = [V(i_1)\ V(i_2) \dots V(i_k)\ ]^T}$, vector of scenarios vulnerabilities

$$\boldsymbol{V(I) = \begin{bmatrix} V(i_1) = \prod_{j \epsilon s_1} v(G_j) \\ V(i_2) = \prod_{j \epsilon s_2} v(G_j) \\ \vdots \\ V(i_k) = \prod_{j \epsilon s_k} v(G_j) \end{bmatrix}}$$, $\boldsymbol{s_1, s_2, \dots s_k \epsilon S}$, $\boldsymbol{S = \{1, 2, 3, \dots n\}}$, s is and index subset of S and n is the total number of the attack tree leafs.

So, system vulnerability is defined by the maximum scenario index value. To identify the strength of countermeasures, the ratio between number of technological countermeasures implemented against the attack $\boldsymbol{n_{c^T}}$ and the total number of technological countermeasures $\mathbf{n_c}$ designed is calculated. Then this ratio is deducted from 1 to convert it to the vulnerability ratio.

$$v(G_i) = \begin{cases} max\left\{\omega \cdot \left(1 - \left({}^{n_{c^T}}/_{n_c}\right)\right), \omega \cdot max\{\Theta(C^P)\}\right\}, & \omega > 0 \\ max\left\{\left(1 - \left({}^{n_{c^T}}/_{n_c}\right)\right), \quad max\{\Theta(C^P)\}\right\}/x\ , & \omega = 0 \end{cases}$$

C^P is the policy enforcement factor and x is the number of measures used for cybersecurity conditions. This notation represents the set of levels of security policy. When the strongest policy is implemented, then

$\boldsymbol{\Theta(C^P) = 0.00}$.

The final evaluation for upper bound of ω is based on the more vulnerable of the two measures, policies and technological countermeasures.

c. Evaluation of security improvements. Security improvement can be achieved by replacing countermeasures with more effective ones. The improvements for an attack leaf and intrusion scenario can be measured with the implementation of defense nodes denoted as $v'(G)$ and$V'(i)$. The degree of improvement for leaf vulnerability is given by $\left|\left(\left[\boldsymbol{v'^{(G)} - v(G)}\right]/_{\boldsymbol{v(G)}}\right) \times \mathbf{100}\right|$ and similarly for the scenario improvement.

d. Identification of the pivotal leafs. To identify the pivotal leafs an optimization problem solution is proposed by the writers, minimizing $\boldsymbol{V_s}$, and setting

upper bounds for $\boldsymbol{V(I)}$ and $\boldsymbol{V(G)}$, where $\boldsymbol{V(I) \leq 1}$ and $\boldsymbol{0 \leq V(G)}$. System's vulnerability is lowered by lowering upperbounds, so the pivotal leaf combination for system improvement is determined.

Purpose of this methodology is to primary to model the attack plan of the adversary and then identify the access points of power systems control networks and evaluate the network vulnerability. It can also be used to evaluate the improvements. Using the optimization problem exhaustive search on attack leafs can be avoided and the attack tree can be solved to determine pivotal leafs for security improvements. It can also help estimate the budget use for countermeasures optimization. The higher the vulnerability the higher security investment is.

Through development of possible action combination producing composite threat scenarios, dependencies may be indicated. Through overall attack breakdown to successive and/ or parallel attack stages, probability of success for each of them is estimated. As attack stages get shorter and simpler, probability may be estimated more efficiently for each individual attack stage. The overall probability of success for the entire attack equals to the product of probabilities for substages. When same level actions are related with AND logical operation, meaning that all conditions set must be successfully executed in order stage to be considered successful, then as probability for this level is defined the lowest of all. When there are multiple choices in the same level, connected with logical OR operation, meaning that attacker has multiple selection options, then level probability of success is of course the probability of the selection path. Particular approach using vulnerability index, simplifies procedure and indicates a relative vulnerability measure. Using number of implemented countermeasures instead of countermeasures' effectiveness provides an abstract indication of node effectiveness or robustness. Effectiveness of course is not easy to be measured; personal judgment and intuition are to be used. This can be considered as a semi-quantitative method, although it does not indicate risk but only efficiency and vulnerability measures.

During vulnerability/ attack trees scenarios process may become complex as possible outcomes and attack paths may be numerous and a lot of combinations (serials) may be presented. User has the option to examine countermeasures, robustness in each of the examined tree branches and estimate its effectiveness and probability of success, so compute the most optimal tree. In comparison to traditional risk assessment methodologies it cannot be considered as efficient as them, because it does not consider importance of every assets and damage costs. A highly vulnerable tree may correspond to a non-critical asset and in contrary some critical assets may have a lower vulnerability index. The same applies to individual nodes and assets examined in the same tree. Neither correlates vulnerability with attacker. So, vulnerability trees do not provide cost effective analysis for making optimal investments allocating available resources in the most optimal, cost effective way, which is achieved with risk methods. This method is impact/ vulnerability oriented; starting with attack goal possible threat scenarios ending with top event attack goal are developed, evaluating each of them with vulnerability

index. Method is based on a theoretical model that it is subject of many researches, supported by mathematical models and it is easily understood and applied. Its drawback as already said is that it is not easily managed. Vulnerability indexes, knowledge, experience and intuition restrict possible solutions to realistic and cost effectives.

So, analysis process sometimes may not be manageable, while being time consuming and not all results being useful or cost effective. User experience and knowledge is a critical factor to restrict planning to realistic frames, selecting empirically or intuitively the most optimal serials. Being generic it can be applied with the proper level of abstraction in all different layers and sectors.

Finally, user experience and intuition are used. Vulnerability index is used to express if systems are vulnerable or invulnerable. If vulnerability index takes the non-standard values of 0, 0.5 and 1 then it provides more accurate results, though more subjectivity is entered in the procedure. Generally subjectivity is considered unavoidable, but knowledge and experience restrict it.

3.1.11 Vulnerability Trees

Vulnerability Tree deployment addresses the problem of analyzing and examining vulnerabilities [57, 58] and different attack scenarios/ chained attack scenarios and their exploitation. Vulnerability definition applies to following types: human, hardware/ software, physical, natural, media and communication.

Vulnerability trees are hierarchy trees constructed as result of relationship between vulnerabilities that have to be exploited in the raw by a threat agent in order to reach to the top of the tree. The top of the tree represents the parent vulnerability which is the most critical of all and has to be exploited in order attacker's goals to be achieved. Multiple vulnerabilities at each level of the tree are related with Boolean operators.

Low level vulnerabilities (child vulnerabilities) sets, which have to be exploited, construct a tree branch. Each of the vulnerabilities from top to bottom of the tree can be broken down in similar way, being decomposed in child vulnerabilities. When decomposition reach the point where no more child vulnerabilities can be found and only non-exploiting actions fit there, then the step-only level of vulnerability tree has been reached and this is the lowest level of tree decomposition. Child vulnerabilities can be exploited by steps an attacker must make in order to reach to the parent vulnerability.

Vulnerabilities have attributes which can be manipulated by potential attackers. Vulnerabilities have the following attributes:

a. Vulnerability name and unique identifier

b. Type: whether nodes are steps or vulnerabilities

c. Categories which are already described: human, hardware/

software, physical, natural, media and communication.

d. Complexity Value (CV) which is defined as *"the smaller number of vulnerabilities/ steps that a threat agent has to exploit/ utilize in order to achieve his objective"* [57].

e. Additionally, Educational Complexity (EC) values are associated with each one of the vulnerabilities and this value is closely related with the educational level of the threat agents, meaning his capabilities and resources. This means that each adversary will follow a different attack path and different number of steps and different techniques in order to achieve its goal. So, Educational Complexity is defined as *"the educational qualifications that a threat agent has to acquire in order to exploit that vulnerability"* [57].

f. An additional characteristic of the vulnerability tree is the Time To Exploit (TTE). It directly depends on adversary capabilities and assets properties. TTE is defined as *"the time required for a threat agent type to exploit a certain vulnerability"*. If vulnerability exploitation needs more than one steps to be executed, then TTE is the sum of total steps duration. Assets are secure against attacks if it is possible to detect them and apply appropriate countermeasures for asset protection inside time window presented by TTE.

g. Family position meaning the level of node 0 which represents the parent or top vulnerability. Any other number indicates child vulnerabilities and their distance from parent vulnerability. The lower level i.e. step-only level refers to initiating events.

h. Head identifier of the head vulnerability used in simulating tools.

i. Asset ID which a unique asset identifier linking asset and vulnerability.

j. Tree ID which is a unique identifier linking tree with vulnerability.

k. Descriptions which include more details about the vulnerabilities.

Defenders identify the most optimal scenario for the attackers and deploy available countermeasures to effectively protect systems keeping in mind the optimal cost/ benefit ratio for countermeasures appliance.

Vulnerability Tree construction from defender's aspect consists of **five** stages:

a. Pre-analysis, where vulnerabilities are identified. Then assets related to specific vulnerability are identified and collected from a previously constructed asset table during asset identification phase. Vulnerabilities and assets are interrelated.

b. Structural Analysis: Trees are constructed from top to bottom until only-step levels are met, defining nodes and branches. Countermeasures are applied to the trees.

c. Node Analysis, where the trees are described with their attributes.

TTE, CV and EC are examined and they are assigned values for given adversaries. Threat identification should have already been done.

d. Value Analysis, where critical attack paths to the parent (top) vulnerability are identified based on previously assigned values.

e. Optimization Analysis: Vulnerabilities that are met more than once in the same or different trees are being identified and selected for minimizing the countermeasures costs. The more instances appear the most cost effective the applied countermeasures will be.

Vulnerability trees' development is based of course on attack tree design, but there are qualitative and structural differences between attack and vulnerability trees. Modern practices combine both attack and vulnerability trees by constructing attack trees enriched with different types of knowledge, offering complete modeling of attacks and complete view of systems and attacker specifications to bypass defenses or successfully overcome attacks from the defender view. Obviously vulnerability tree RA is a vulnerability-oriented method. This means that it is possible that some 0-days vulnerability may not be identified, so related assets may be left unprotected against threat scenarios exploiting these vulnerabilities. In the other hand, assets non related to vulnerabilities will be left out of examination too. This method uses objective criteria for defining vulnerabilities and threat scenarios. It follows a Boolean logic of vulnerabilities being exploited or not, leaving away relative probabilities. This is not considered as economical or cost effective practice. Risk and probability of attack success will not reflect to reality. It is best used for critical vulnerabilities and damage identification, where it is considered that optimal cost effective countermeasures and strategies for the specific asset, vulnerability and threat will be applied. This vulnerability tree method uses standardized symbolic language for construction and description of the trees on purpose to assist specialized graphical tools development.

Vulnerability trees do not discuss dependencies and interdependencies. Attack and Vulnerability Trees integration can enhance this ability. Many aspects have already been discussed in other paragraphs for vulnerability and attack trees advantages and disadvantages. This particular method defines potential adversary's background, necessary for exploiting vulnerabilities and shows the successive vulnerabilities to be exploited and actions to be taken in order attackers reach top vulnerability exploiting the system. Time is a factor that affects risk and especially Time To Exploit a system. The higher TTE is, the higher is risk for that system for a given adversary. Educational level required for vulnerability exploitation indicates both a risk level and adversary capability. High requirements indicate low risks because vulnerabilities can be exploited only by knowledgeable attackers. Method efficiency is based on the premise that all systems are eventually comprisable. But by another view, according to Murphy's Law, everything that can go wrong will go wrong. So, a vulnerable and attractive system eventually will be exploited. If Murphy's Law is considered, above premise gains weight.

As it is noticed this is a vulnerability oriented methodology. Overall vulnerability is identified by examining each vulnerability tree element/ branch, deciding individual vulnerabilities, TTE for each one, critical/ shortest attack paths and required knowledge for exploiting each tree node. Method provides a measure of difficulties posed to an attacker during vulnerabilities exploitation and attacking systems, associating it with system risk, detects possible attack paths and assess adversaries' capabilities attaining the necessary protection level to efficiently encounter them.

3.1.12 Threat Assessment Model – TAME

TAME [59] is a methodology based on organizational analysis using business modeling techniques. The methodology consists of four phases each one of them consisting of a number of processes:

a. Scope of Assessment is made based on gathered staff knowledge containing following five processes:

(1) First process is about Business analysis. Business goals, processes and environmental analysis takes place in this process.

(2) The second process has to do with stakeholders' identification where involved stakeholders and responsibilities are identified.

(3) In the third process system and its boundaries are identified as boundary control is ascertained.

(4) In forth process threat agents are identified and selected. So, threat agents' identification, selection and intentions are made.

(5) In the fifth process assets for the analysis and their value are identified.

b. The second phase is related to threat and vulnerability analysis including likelihood and importance analysis.

(1) Type of vulnerabilities are identified and selected for further analysis.

(2) Threat agents' capabilities, opportunities and motivation are estimated.

(3) The last process of this phase is vulnerability analysis, using the vulnerability tree method [63] that has already been analyzed in previous paragraph.

c. At the third phase threat scenarios are constructed and the system is modeled and analyzed using pre-analysis and structural analysis.

d. At the final phase impacts are identified. Tangible and intangible impacts are identified and analyzed across the impact field.

TAME is an asset oriented RA method. It is a structured method that can be used

across all levels of organization hierarchy. Using vulnerability tree inherit all of the specific method advantages, but since asset that are valued for organization are identified and selected for the scope of analysis, vulnerability orientation disadvantages of the tree method are not in place now. Asset identification is considered effective based on structural analysis and gathered knowledge by all personnel from all organization levels. Dependencies and interdependencies are not specially discussed even in the impact analysis. It is a holistic and easy implemented method. Examining capabilities and motivation of adversaries one can estimate probabilities of attack, hence vulnerability tree disadvantages related to only critical threat scenario identification are not applied, while strategies and budget distribution are deployed more effectively taking into account risk. So, there is one additional parameter used for selection between different attack trees or branches and this is estimated risk level. More over discussion of adversaries' opportunities may define more accurate estimation about threat appearance and acts.

This is a qualitative risk assessment approach. Method analyzes operational concept and operational functions to identify organization valuable assets. For each identified asset, a vulnerability tree is deployed and adversaries capable to exploit vulnerabilities are identified in turn. Method is considered to be a holistic approach providing only generic guidelines. Finally, potential threats are identified based on hypothesis of their abilities to exploit analyzed vulnerabilities and reciprocating to the education level needed.

3.1.13 Threat and Hazard Identification and Risk Assessment and Strategic National Risk Assessment – THIRA and SNRA

Threat and Hazard Identification and Risk Assessment (THIRA) presented in [60] had been designed for appliance in extended environments like cities, against a wide spectrum of threats and hazards. It expands on local, territorial and state risk assessments. It is described as a step-by-step method:

a. Assessing threats and hazards of concern, those a community, of any size faces. It uses past experience, forecasting, experts' judgments and available resources. It identifies natural, like physical phenomenon, technological like system failures and human caused and adversarial, like cyber-attacks.

b. Assesses the vulnerability of the community using varying season, time, locations and community factors. Using above threats and hazards list, it develops context showing threats' acts against the community. Inherent to this step is the understanding of the likelihood or probability of a threat affecting community. Estimation is based on experts' judgment or on statistical analysis. Conditions under which a threat or hazard could occur is briefly explained. Time and location data of threat possible occurrence is included in the analysis. Expected situations and impact areas are developed using varying condition parameters as these differences successively differentiate the way community is affected. Other factors like environment or demographics factors can be also taken into account.

c. Using context, estimate the consequences of those threats and hazards impacting the community and through the lens of core capabilities (table 1) establish capability targets. The impacts are paired with desired outcomes, and this permits having a first understanding of demands for managing risk in accordance with core capabilities, as seen in example table 2. An example of estimated impact for core capabilities and consequences appears in example table 3.

d. Set capability targets. Once impacts have been identified for each one of the core capabilities and desired outcomes have been defined it is turn of setting capability targets. The greatest impact coupled with the desired outcomes sets the target for each capability. This step uses information from previous steps combining impacts with desired outcomes to set capability targets.

e. The final step of THIRA is related to Risk Management. It sets foundation for prevention, protection, mitigation, response and recovery planning. THIRA is consistent with and expands on US nationally acceptable emergency management standards. Using capability targets appropriate resources to achieve desired outcomes are determined.

THIRA is complemented with Strategic National Risk Assessment (SNRA) in Support of Presidential Policy Directive 8 [61]. SNRA has been used to:

a. Identify high risk factors that supported development of core capabilities and core targets in the National Preparedness Goals.

b. Support the development of collaborative thinking about strategic needs across prevention, protection, mitigation response and recovery requirements.

c. Promote ability for all levels of Government to share common understanding and awareness of national threats and hazards and resulting risks, so they are ready and can do so independently but collaboratively.

Department of Homeland Security (DHS) has identified thresholds of consequences necessary to create a national-level event. Different types of consequence threshold have been used to define national-level events, like economic loss and casualties thresholds, but it no occasion these different types have been treated as equivalent to each other. Even in cases where no quantitated thresholds are set, no minimum threshold is meant to be used in relative descriptions (example table 4).

SNRA uses data from a variety of sources like government models and assessments, historical records, structured analysis and experts' judgments from different fields of expertize. SNRA concludes in that referred risks may appear perhaps more than once every ten years, and authorities should not rely on historical data as new threats and risks may come up with greater consequences, and they should be ready to deal with. Identified risk is assessed as a function of consequences and frequency of event occurrence and more specifically sets the questions:

a. With what frequency is estimated that an event will occur?

b. What are the consequences of the event on the hypothesis that it

will occur?

SNRA relies on the best quantitative estimation of both frequency of occurrence and consequences size by government experts. When such a quantitative estimation is not possible or there is not sufficient quantitative information, assessments are processed qualitatively. Uncertainty in estimation is represented with generic low and high bounds.

Moreover, this method examines definite threats and attacks. It is not possible to examine composite attacks and related probabilities, such as cyber-attacks, cyber and physical enabled attacks against complicated and widely dispersed CPS and SCADA systems neither can adapt to the special dynamics of the nature of these cases where attackers tactics changes in response to defenders' posture. It rather examines their critical impacts and consequences affecting mass population and industry if are of critical magnitude, from a strategic aspect of view.

As said it could address single events against single electrical grid units through examination on strategic or operational level. It is a well-structured method using guides and complete patterns through a step by step procedure to identify threats, impacts, risks and consequences but although its applicability it can be used just by government experts because of the background information and ability of estimation of probabilities about critical national concepts. But since it is not an asset oriented RA methodology many dangerous threats and threat scenarios may be missed and not be analyzed.

Core capability	Desired outcome
Screening, search and detection	Screen 100% of targeted cargo, conveyances, mail, baggage and people associated with an imminent terrorist threat or act using technical, nontechnical, intrusive, or non-intrusive means.
Access control and identity verification	Ensure 100% verification of identify to authorize, grant or deny physical and cyber access to specific locations, information and networks
Long term vulnerability reduction	Achieve a measurable decrease in the long term vulnerability of critical infrastructures and systems
Fatality management services	During the first 72 hours of an incident conduct operations to recover fatalities
Infrastructures systems	Within 15 days of an incident restore and sustain essential services (public and private) to maintain community functionality

Table 1: *THIRA example table of desired outcomes*

Prevention	Protection	Mitigation	Response	Recovery
Planning				
Public information and warning				
Operational coordination				
Forensics and attribution	Access control and identity verification	Community resilience	Critical transportation	Economic recovery
Intelligence and information sharing	Cybersecurity	Long term vulnerability reduction	Environmental	Health and social services
			Public health and medical services	
Interdiction and disruption	Intelligence and information sharing	Risk and disaster resilience assessment	Response/ health and safety	Housing
Screening, search and detection	Interdiction and disruption	Threat and hazard identification	Fatality management services	Infrastructures systems
	Physical protective measures		Infrastructures systems	Natural and cultural resources
	Risk management for protection programs and activities		Mass care services	
			Operational communications	
	Screening, search and detection		Mass search and rescue operations	
	Supply chain integrity and security		On scene security and protection	
			Public and private services and resources	
			Situational assessment	

Table 2: *THIRA, Core Capabilities*

	Prevention	Protection	Mitigation	Response		Recovery	
	Screening, search and detection	**Access control and identity verification**	**Long term vulnerability reduction**	**Fatality management services**	**Public health and medical services**	**Infrastructures system**	**Economic recovery**
Terrorist attack: A terrorist deploys a self-improvised explosive device (IED) inside a stadium during a sporting event	67500 spectators 2500 vendors and employees	2500 vendors and employees	Reinforce 500 concrete support columns in stadium	52 fatalities	350 casualties	N/A	$14 million of direct economic loss (tickets sales, hotel stays, parking, food and souvenirs)

Table 3: *THIRA example of estimated impact for core capabilities/ consequences*

No dependencies or interdependencies are taken into account, but rather simple scenarios are examined. Although, it could examine single events like physically attacking large power generators or other parts or electrical grid, examining the attack through the strategic or operational level. Analysts use historical and statistical data and expert's judgment to estimate probabilities of threats' appearance and action against the targeted environment. More over interrelate the conditions under the threat appears as well as time and season during which threats are expected to act and locational data. Where no historical records exist and there is no sufficient quantitative information, qualitative process is done and procedure/ results accuracy may be lower.

THIRA is a qualitative method, but sets risk thresholds to identify critical risks which are either expressed in numerical values, like financial losses, human life losses or more generic describing critical and severe impacts or threats like massive biochemical strikes. Method considers a set of factors affecting risk, like location where threat is expected to appear, time of appearance and specific conditions under which it is going to act and the way that will affect its target. This method is used in government level i.e. it is used in strategic level. Its generic character makes it inappropriate for use in lower than operational level, because in this occasion more detailed description and analysis is required. Because it is used on strategic level it does not present view to all risks community or systems face.

Method, as already said, sets risks thresholds to identify critical impacts and consequences. So, if expected risk level is higher than the one that has been set, then the threat/ impact is considered critical and should be properly treated. For example if cyber-attacks cause financial losses higher than a certain value this case must be considered critical. Method analyzes threats and impacts for extended environments, so by definition assets of interest are considered critical, like large parts of population, human life, etc. These thresholds can be also described qualitatively like nuclear/ biochemical threats which always have extremely severe consequences. This assessment had been designed to avoid false precision, given the uncertainty of inherent in assessing risks, in national level, and the inefficient information about some events.

THIRA is a threat oriented approach. By firstly identifying potential threats considering potential attackers capabilities, potential impacts are determined and then possible targets relevant to these threats and impacts and their consequences. Moreover, THIRA has been designed based on national US standards and policies for risk assessment and infrastructures protection on behalf of government services. Furthermore, THIRA is to be applied by top management or high hierarchy government officers dealing strategic and operational risks, but still need knowledge and judgment of departmental infrastructures specialized experts.

THIRA is a strategic method for analyzing critical risk for mass infrastructures and population. It does not focus on specificities but rather maintain a strategic object view, so it is inappropriate or rather incapable to deal with low level operational and cyber/ physical layer analysis. By definition method is used for extended environments like cities and relevant threats capable to impact them. That means that method analyzes critical scenarios for critical assets. Method sets consequences thresholds to identify criticality. Finally, this method analyzes multiple threats of different nature, technological, physical phenomenon, adversarial or not against extended environments like cities.

3.1.14 Cyber Attacks on SCADA Petri Net modeling and Risk Analysis

[62] presents an analytic technique for quantifying risk of cyber-attacks against SCADA systems using Petri Net (PN) state cover ability analysis and measuring risk in terms of the extent to which an attacker can manipulate process control elements, the vulnerability and the consequences of the attack to the system.

Addressing this problem this technique uses decomposition of the object system into analyzable subsystems. In particular it first identifies potential processes failure modes and then examines those failures operational consequences. PNs are is used to present industrial processes, SCADA operations, network resources and vulnerability topology. Risk measuring is achieved as a function of operational consequences of process failure and the propensity for process failure induction due to an attacker's assertion of control over network resources during the course of the

attack.

Resources in PN modeling are represented by places. Given the initial marking of the system finding all places that are marked at some time during the net's execution, shows the places/ resources an adversary can gain access to in reference with the initial state. This corresponds to system risk for the cyber-attacks. In other words the problem is solved in the domain of the reachability analysis and more specifically a cover ability problem is posed, i.e. whether there exists a reachable marking coming up from the initial system marking. This variation uses cover ability graphs. Cover ability graph comparing to reachability graph is always finite. The resources controlled by an adversary are identified in the cover ability graph, constitute preconditions for SCADA failure mode induction. Another PN is used to simulate the operation of the SCADA system. Via PN identification full set of SCADA failure modes is feasible. Network resources attacker needs to access in order to induce each failure mode, are identified meaning appropriate markings are searched for. Operational consequences are also identified by the PN process. So, to access risk, these cases of possible failure modes and consequences through whatever SCADA or network failure are quantified. Consequences metrics being meaningful for analyst are used. Two risk measurements are proposed; one is relative to worst case scenario while the other is related to above mention quantified failure modes outcomes. These outcomes are rank-ordered and the extreme value represents the worst case scenario.

The PN presents the advantage of examine attack as well as attack pre and post-conditions, representing system not just statically but also dynamically taking into account its different states. Using cover ability analysis all the resources an attacker can gain access and compromise can be determined and impacts are analyzed. But it is a rather complex methodology requiring help of graphical computer programs. Its complexity increases as complexity and size of the examined system increase making it impractical. Though it is assumed of being capable to examine composite and multi stage attacks. It requires system to be analyzed in prior and the use of FTA and AT may enhance its functionality and effectiveness. Because of its complexity this methodology can only implemented by specialized personnel having an in depth understanding of the supporting theory and methodology. Since it is asset and threat oriented, this model is assumed that can detect all possible threat again infrastructures as well as indicate hidden vulnerabilities. Severity metrics for comparing different impacts and consequences should be developed. Dependencies and interdependencies between different parts and subsystems are detected, identified, dynamically represented and simulated using PN representation.

As all methodologies based on system theoretic modeling and simulation, current method is able of identifying possible dependencies and interdependencies, analyzing system parts different states, responses and impulses. Though, method examines dependencies and interdependencies at cyber and physical layer only. Petri Net a modeling methodology while proposed risk analysis methodology in paper of reference is a qualitative approach.

Petri Net modeling permits industrial ICS and SCADA systems as any other cyber or physical system industrial or not dynamic simulation and structured view as well as simulation of attacks and their further analysis. NIST or ISO standards can be effectively used for risk qualitative expression and probability quantification. There are not particular risk and probability methods proposed. It is an asset oriented method, where structural system view and system states emerging from initiating events like system malfunctions or attacks are simulated, so initial and ending systems states can be viewed and examined.

Although this assessment is somewhat theoretical and complex, overall research view shows that Petri Nets theory and generally system theory are a new trend in CPS identification in risk analysis methodologies, providing structured system view, but more important simulating system functioning and response to environment or system stimulating actions and attacks, offering a deeper and more complete analysis capability than traditional risk assessment methodologies.

Petri Net methodologies are quite complex and not easily understood and applied and require its appliance by experienced and knowledgeable expertized personnel. As systems complexity and size grow difficulty in applying specific method raises and may become impractical. Being able to model any type of system Petri Net can be applied in all sectors. But because of its complexity and not easy appliance it must be supported by specialized tools and applied in rather simple systems or systems with a certain degree of abstraction.

Method proposes decomposition of system into examinable subsystems. It first identifies potential processes failure modes and then examines those failures operational consequences. For each process failure SCADA failure modes that have the potential to induce the corresponding process consequences are identified. More over any process failures may be induced via more than one SCADA failures and any SCADA failure may cause multiple process failures. Finally, for each SCADA failure network resources attacker could attack, compromise and gain control over the SCADA system in order to induce the corresponding SCADA failure are identified. Given an initial network attack state, network resources which could be attacked given network and host vulnerabilities are identified.

Attack is modeled through places describing pre-conditions and post-condition of the attack execution using PN modeling. Attack exploits are represented by the firing of corresponding transitions. The preconditions and post conditions for each exploit are represented using an input function and an output function using corresponding markings. Method aims at simulating system and attackers, behavior/ responses, different system states, corresponding consequences to induced anomalous states and qualitatively estimating relevant risk.

3.1.15 Process Hazard Analysis – PHA

Process Hazard Analysis (PHA) is an organized and systematic assessment of the potential hazards associated with industrial processes. It provides information to

assist decision making for improving safety and reducing consequences of fire, explosions, release of toxic or flammable chemicals and major spills of hazardous chemicals. PHAworks [63] is a specialized tool used to conduct PHA studies, such as **HAZOP, FMEA and What If studies**, making them quicker, easier and more cost effective. It has been developed by Primatech Company. This tool is widely used and trusted throughout the world and thousands of studies have been completed with it. It is suggested for use in companies managing liquid hazard materials and chemical industry.

PHA sets the foundation for process safety and risk management in companies. It helps in identification of hazard scenarios for processes which may affect personnel, environment and properties; that means it identifies situations with the potential to create harm. Hazard scenarios identification is PHA principal objective. They are identified as a combination of their starting and ending points, i.e cause and consequences. Hazard is considered a situation or intrinsic property with the potential to cause harm. In process safety it means a potential for an accident with undesirable consequences. It focuses on equipment, instrumentation, utilities, human actions and external events that may impact processes.

It uses techniques like HAZOP, FMEA, Major Hazard Analysis (MHA) and What If scenarios. In general PHA is a set of organized and systematic assessments of the potential hazards associated with industrial processes. It provides information for improving safety and reducing the consequences of unwanted or unplanned release of chemicals. It is directed to analyzing potential causes and consequences of chemical releases, fires, explosions, toxic and flammable materials. FTA can also be used if PHA team will not conclude in risk estimation using default methods.

During PHA scenarios caused by equipment failure, human errors and external events are considered. Safeguards are taken into account which detect, prevent or mitigate events in the hazard scenario and impacts on safety are identified. The first event of a hazard scenario is called initiating event. It may be equipment failure or external event. Intermediate events follow. These are personnel and equipment response to initiating events. Enabling conditions and events are also involved. They do not directly cause the hazard scenario but must be present in order to make possible another event to occur and cause the hazard scenario. Combination of those events causes the consequences which are the impacts of hazard scenarios on personnel, property and environment. Consequences are characterized by type and severity with the last appropriately measured. Measures are the units used to describe severity. PHA is usually used to identify safeguards that are in place. Safeguards are systems, devices or actions intended to interrupt the chain of events following initiating events to avoid or mitigate consequences identifying risk controls that have already been taken, but also additional measures need to be taken.

During PHA study very basic causes are identified in order to provide the best recommendations for risk reduction. For example pump fail that causes an impact is not the basic cause; the basic cause is considered as a power loss that caused the

pump fail and successively hazards and impacts. PHA can divide process so individual parts can be analyzed.

PHA and PHAworks do not pay independent attention to CPS, ICS and ICT systems; cyber-attacks against them are considered as initiating events and vulnerabilities as enabling conditions. Relative impacts are user defined in a much generic way. PHAworks tool leaves the impression that it is a complex and not friendly/ low level of usability tool. Special training for using method and tool is required and provided by the primatech company. Conducting PHA demands the cooperation of a team leader and a group of people familiar with the PHA and uses brainstorming to detect possible causes and consequences of accidents as well as appropriate corrective measures. Given the complexity of examined systems, the assistance of expert specialists is required in order to complete PHA study. According to the view of Primatech and PHA study is considered as a tedious and time consuming procedure.

Method does not consider dependencies, but freedom provided to users and available tools negate this disadvantage. PHA – MHA constitute primary qualitative methodologies although it is possible their consequences to be expressed quantitatively in many occasions.

PHA and MHA examine industrial processes and hazardous states that may arise because of human errors and technical faults. They focus on infrastructures and human safety, considering cyber-attacks, if examined, as initiating events. Moreover, there is no proposal for risk assessment methodology. Many supporting methods and methodologies can be used in PHA examination framework. PHA – MHA are threat oriented methodologies, beginning with identification of possible initiating events that could result in hazardous impacts.

PHA and MHA are trusted methodologies having been applied for long time in industrial environments and they are generally acceptable for use in hazardous situations and relevant risk estimation. Relevant international standards to the use of PHA have been developed. Although PHA is a relative simple procedure and it is supported by specialized tools, it requires appliance by expertize personnel specialized in the field of the examined environment and systems.

Although it provides a systematic and structured view and identification of threats and hazards and it is well supported with tools, methodologies and documentation, it relies most in operators' knowledge and experience. Finally, there are not criteria to identify any system assets and vulnerabilities as critical. Rather this method addresses assets and systems are already considered critical as they are related with severe impacts to human, industrial and environmental safety; addressing and estimating critical assets and consequences is operators' only responsibility.

3.1.16 Viable System Model – VSM

Viable System Model (VSM) had been firstly introduced by professor Stafford Beer, who suggested depicting an organization, as a human body. It had been introduced for modeling an organization's viability. Method divides organizations in two fundamentals parts: the Operational part and the Management part. The operational part entails all operations taking part inside the organization. The management part controls the smooth operation of the system, ensuring its stability, and facilitating its adaptation to environment and organization policies.

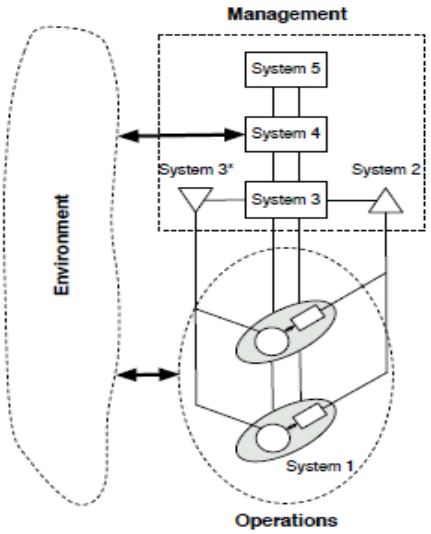


Figure 12: *Viable System Model*

In [65] VSM is proposed for use for risk assessment in ICSs. VSM makes a holistic approach to CPS risk management by being applied as a diagnostic tool to identify threats against the system, assets, interaction between system internal parts as well as between system and the environment. Most RA methodologies applied in CPS and CI follow sectorial approach; but VSM considers these systems as interconnected network systems taking into account resilience. So, it is a system behavioral approach and can be applied to model all system's levels, from top organization strategic levels to bottom hardware level. It can also provide a structural view of the modeled system (architecture). So, model is used for system characterization or identification that encompasses the process of gathering system information and for threat and vulnerabilities identification. Threat identification includes source of threat, motivation and various acts that may take place. System's vulnerabilities that are possible to be exploited by identified threats are identified and listed. VSM consists of six different systems with a different role assigned to each one of them (Figure 12):

a. System 1: Operational units within the organization.

b. System 2: Attenuation of oscillations and coordination of activities via information and communication.

c. System 3: Management of the primary units. Provision of synergies.

d. System 4: Investigation and validation of information flowing between Systems 1 – 3 and 1 – 2 – 3 via auditing/ monitoring activities.

e. System 5: Management of the development of the organization; dealing with the future and with the overall external environment.

f. System 6: Balancing future and present as well as internal and external perspectives; ascertaining the identity of the organization and its role in its environment; embodiment of supreme values, norms and rules of the system.

VSM has a recursive nature where each operation in system 1 can be considered as a lower level VSM model with its own management and operational parts.

VSM has been used in cyber security domain as a framework for detection of system weaknesses and attacking organizations. In the paper of reference threats are identified that:

a. Render the system unavailable to the rest of the systems or subsystems disruption the connection, to its external environment between them by means of DOS.

b. Corrupt the connection between the systems, subsystems or external environment by sending false data to them using MITM attacks.

c. Disclose or corrupt data transferred from the system to another system or its external environment or vice versa using data theft or data tampering techniques.

d. Render its subsystems or suprasystem unavailable.

e. Alter or disclose data transferred to its subsystems or suprasystems.

Then identified vulnerabilities are explored while part of RA is performed in traditional way. All procedures of VSM identification are repeated hierchically from top to bottom, for all systems and subsystems until the lower one referring to hardware executed operations. So, all possible assets and interactions are taken into account. Assets are identified and mapped as management and operational systems. Expertized personnel must be contacted to help in asset and interaction identification and mapping.

VSM helps in identification of all interactions between CPS's parts, control mechanisms, management mechanisms, identify all possible system vulnerabilities and possible system exploitation and attack types and successively potential threats. It provides a more thorough and structured view and analysis for the system in depth, being asset oriented procedure. This method has the ability to correlate different parts that belong to different hierarchical levels. By examining operating parts with management parts problematic relationships, command and control functions may be detected and identified. So dependencies and interdependencies between different system parts or between the system and its external environment can be identified and examined thoroughly.

System's modeling and analysis permits structured view of assets and different level of hierarchy relationships, while a set of standardized threats against assets and communications examines typical relationships and dependencies factors. This method's purpose is not Risk Assessment but only system modeling and analysis, proper for detecting and identifying assets, vulnerabilities, threats and interaction

amongst them. By default VSM models and analyses organizations in two parts: managerial and marketing sectors. In CPS case management and executive sectors are to be modeled and analyzed, i.e. strategic or operational and cyber physical layers or any controlling and executing parts by using the right degree of recursion from to top to bottom, examining all levels of organization and systems examining and correlating different units of different hierarchies. It enhances capabilities and results of classical RA methods by setting up and effective identification basis. In accordance with level of abstraction it can be applied separately in every organizational level, while RA elements are viewed and dealt in holistic way.

Method is based on a tested method proved to be effective, though examination of different objects in entirely different scientific and operational areas. As already seen this project is an interdisciplinary application of a structural modeling method used to model and analyze business related objects. Writers experimented with its basic theoretic framework and tried to apply it to a completely different study area. Since it is just a modeling method for complex systems it is considered that may be possible to be applied in all different study areas and levels, through the proper level of abstraction and recursion. Structured view and analysis of the system and its environment, using recursion from top to bottom permits identification of system elements, interrelationships, dependencies and interdependencies between different hierarchies

Finally, method has been applied mainly as a business model, but its usage extends to all organization having hierarchical structure; it researches relationships and communication between internal and external parts and estimates relevant risks when these elements are attacked.

3.1.17 SCADA Quantitative Risk Reduction Estimation Methodology

In [66] a methodology is proposed for estimating risk reduction for a small SCADA control system. The methodology is based on the assumption that risk is related to the elapsed time required for a successful attack. The methodology consists of the following steps:

a. Establishing system configuration. Primary targets are defined as any control system device which can directly trigger a physical event. A perimeter device is defined as any device that is both part of the control system and can be directly reached without routing, switching, forwarding or inspection. Primary goal of system configuration is identification of control system and perimeter devices.

b. Identification of the applicable portions of the quantitative risk model. Risk $\boldsymbol{R}$ for an undesired event is calculated as

$$\boldsymbol{R} = \boldsymbol{P} * \boldsymbol{C}$$

$\boldsymbol{P}$ and $\boldsymbol{C}$ are probability of occurrence of an undesired event and its consequences correspondingly. Probability $\boldsymbol{P}$ can be further decomposed to component probabilities:

$$\boldsymbol{P = P_t * P_a * P_b * P_s * P_c}$$

P_t is the probability of target being in adversaries' attack list, $\boldsymbol{P_a}$ is the probability of system being attacked given it is targeted, $\boldsymbol{P_b}$ is the probability of a perimeter breach given the system has been targeted, $\boldsymbol{P_s}$ is the probability of successful attack given that there had been a security breach before and $\boldsymbol{P_c}$ is the probability of damage given the attack had been successful.

a. Identification and prioritization of the security requirements for the primary targets. Integrity and availability are the most important requirements in CPSs and SCADA systems. Confidentiality is not so important. So, attacks of denial of service and replaying, unauthorized access and control are extremely dangerous.

b. Vulnerability identification. It is permitted through testing and existing vulnerability databases accessing.

c. Vulnerability categorization using criterion of each device compromise type. Then compromise graphs are constructed. Compromise graphs are directed graphs, where nodes represent a potential attack state. So, nodes are distinguished into:

(1) Start, where nothing yet is known about the system to be attacked. This is the single entry node of the graph.

(2) Launch, where enough data have been collected in order to develop or use an existing exploit. There is such a node for each potential attack entry point in the perimeter.

(3) User Privilege. This state applies to a particular machine. At this state the attacker has gained access to the specific machine with the user privileges. There is one such state for every machine in the system.

(4) Root Privilege. This state applies to a particular machine too and at this state attacker has gained root access to the specific machine. There is one such state in every machine in the targeted system.

(5) Target node, where at this state attack has succeeded.

The edges of the compromised directed graph represent transitions from one attack state to another and each transition represent a successful compromise. For each edge there is a corresponding value related to the time needed to make the transition, i.e. it express the difficulty of edge related vulnerability exploiting. Vulnerabilities are categorized in the following types:

- Reconnaissance
- Breach representing edges starting from launch

nodes.

- Penetrate, representing edges starting from a user or root permission node and end to the same type of node.
- Escalate representing an escalation of permissions in the same machine.
- Damage represents the transition to a target node.

d. Estimation of time to compromise each device. Time to compromise is defined as the time needed for an attacker to gain some level of privilege on the same system device and it depends on the attacker capabilities and the vulnerabilities of the system. Time to compromise is modeled as a random process including the following subprocesses:

(1) One at least vulnerability is known and there is at least one known exploit to attack it.

(2) One at least vulnerability is known by adversaries do not have exploit readily available to attack it.

(3) Identification of new vulnerabilities and exploits.

Time to compromise can be calculated using the following equation:

$$\boldsymbol{T = t_1 * P_1 + t_2 * (1 - P_1) * (1 - u) + t_3 * u * (1 - P_1)}$$

Where the time to compromise is T, t_1, t_2, t_3 are the expected values of the first, second and third subprocesses correspondingly.

$$\boldsymbol{t_3 = \left(\left(\frac{V}{AM}\right) - 0.5\right) * 30.42 + 5.8}$$

$\boldsymbol{u = (1 - \left(\frac{AM}{V}\right))^V}$ is the probability of the second subprocess to be unsuccessful and V is the number of vulnerabilities.

$\boldsymbol{P_1 = 1 - e^{-V*m/k}}$, m is the number of exploits readily available to the attacker and k the total number of vulnerabilities in the CVE database

$\boldsymbol{ET = \left(\frac{AM}{V}\right) * (1 + \sum_{tries=2}^{V-AM+1} \left[tries * \prod_{i=2}^{tries} \left(\frac{NM-i+2}{V-i+1}\right)\right])}$ is the expected number of tries, AM is the average number of vulnerabilities for which an exploit can be found or created by the attacker given their skill level. NM is the number of exploits attackers will not be able to use because of their skill level.

e. Generation of compromise graphs and attack paths.

f. Dominant attack path estimation. It is defined as the path across the directed compromised graph following which allows executing the attack in the minimum possible Time to compromise. Attack path begins at the start node and ends at the target node. So, minimum time to

compromise is translated to maximum risk. By comparing attack paths' values for the baseline system and the enhanced system is possible to estimate the risk reduction.

g. The third to eighth steps are repeated for baseline and enhanced systems.

h. Estimation of risk reduction.

It has been noticed by researchers that as Time to Compromise for a system raises security level raises too. So, time is considered by the researchers as a suitable metric for indicating security effectiveness and risk level. When there are many systems the procedure has to be repeated for each one of them, and as more complicated they are, the more time consuming is this methodology, making time consuming and perhaps impractical for large and disperse CPSs. It also considers only number of exploits and considering that they will be effective, setting security level as a function of just vulnerabilities numbers and exploits numbers. This method applies to SCADA systems and refers to dependencies where a physical act depends on a control system breach. By combining referred probability decomposition perhaps it can produce more objective probabilities. Though it expresses risk quantitatively it cannot provide indicators for mitigating strategies and resources distribution effectively. Also the ways that attacker skill level and vulnerabilities affect the time to compromise across each graph's end should be investigated in order to provide a more accurate estimation.

Attack trees can be used to indicate and analyze presence of dependencies between system elements, different systems. Methods subjects are control devices that can directly trigger physical events, so attacking controllers cause damage or malfunctions to physical devices. Moreover, method decomposes possible threat scenarios to successive attack stages including attacking control systems and breaking perimeter security mechanisms. Probabilities of successive attack substages are to estimate independently and this permits a more accurate approach, while simpler cases individual probabilities are estimated. Then the overall probability of success is expressed as the product of all individual probabilities.

This method provides a semi-quantified risk indication, or rather vulnerability level and not real risk. Using graphs (attack trees) possible attack scenarios and possible combinations can be visualized and analyzed extensively and in depth. Advantages and disadvantages of attack trees have already been discussed in previous paragraphs presenting vulnerability and attack trees. Time to compromise a system or device exploiting a vulnerability category type is used as a risk measurement criterion. This approach is not efficient because vulnerability, time to exploit and asset value are not always directly and easily interrelated and proportionate. Some users may prefer less vulnerable perimeters, while other may consider amplifying main assets protection. So, this approach may not make the most accurate estimation for cost effectiveness relating to countermeasure policies.

Method is an asset oriented approach where targets are identified as control system

devices directly triggering physical events. Additionally, perimeter devices are to identified; devices both part of the control system directly reached without routing, switching, forwarding or inspection. By indicating only vulnerability level and potential to attack, not using efficient cost effectiveness criteria, it is not considered as a reliable risk analysis method.

Method is considered applicable but requires participation of personnel specialized in SCADA systems and security experts to examine possible attack scenario and provide results. Moreover, this method by definition can be applied in small SCADA control systems. Specifically, method addresses to small SCADA control systems, using specific criteria for risk indication, so it cannot be considered holistic.

Finally, method suggests vulnerability identification using existing databases and penetration testing. This is a consummate solution because it uses already detected and identified vulnerabilities, but with continuous search and penetration testing, new vulnerabilities may be detected, that may be omitted from lists of vulnerabilities. Vulnerabilities are categorized as reconnaissance related, breach related, penetration related, privilege escalation related and damage related.

3.1.18 A RA Model for Cyber Attacks on Information Systems

In [67] a comprehensive mathematical risk assessment method for calculating financial losses caused by cyber attacks' impacts on SCADA systems in a wide range of industrial plants and organizations is presented. Attacks on these systems may cause direct and indirect losses. Direct losses for example are connected to the blackout power losses. The indirect losses are related to societal damage and instability because of the negative climate caused by long lasting or repeated blackouts impacting population well-being and economy. This method considers only short term financial losses resulting only from real time cyber-attacks. The method can be used for cost/ benefit analysis in order to conduct the most optimal resources allocation for being security hardware and software countermeasures.

Risk is estimated by assessing:

a. The probability of the occurrence of an event p.

b. The financial losses because of the occurrence of this event.

Risk is calculated as:

$$\boldsymbol{R_i = L_i p(L_i)}$$

For a set of undesirable events or multiple losses risk is calculated as:

$$\boldsymbol{R_{total} = \sum_i L_i p(L_i)}$$

Risk exceedance probability curves (EP) may be used on this purpose. Losses can be considered function of the type of cyber-attacks and other losses which value can be estimated by the plant managers and engineers. In the following table most common type of attacks according to the presented paper are described:

Type of attack	Description
Replay	Capture a message and resend it at a later point one or more times
Spoofing	Pretend to be a MTU or RTU
Denial Of Service	Send a very large number of spurious messages so that RTU is unable to fulfill a valid request
Control Message Modification	Capture a request, modify some of its parameters and send it to the RTU
Write to MTU	Add or modify files on the MTU
RTU response alteration	Capture a response, modify some of its parameters and send it to the MTU
Write to RTU	Add or modify values on the RTU

Table 4: *Most Common Attack Types*

Core of the proposed model consists of a set of revenue loss functions used for calculating the total loss. Figure 13 depicts the proposed model.

According to this method probabilities of occurrence are estimated using criteria of historical attack occurrences and each attack type is given a relative weight factor compared to other attack types for given damage. Each attack can cause more than one type of damage. Damages caused by different attacks are not mutually exclusive. This model associates each attack type with the revenue loss functions that correspond to kinds of damage caused by attacks' impacts on CPS systems. So, revenue-loss functions are functions that determine the values for the financial loss resulting from different types of attacks. The method uses quartile points for calculating number of systems being attacked.

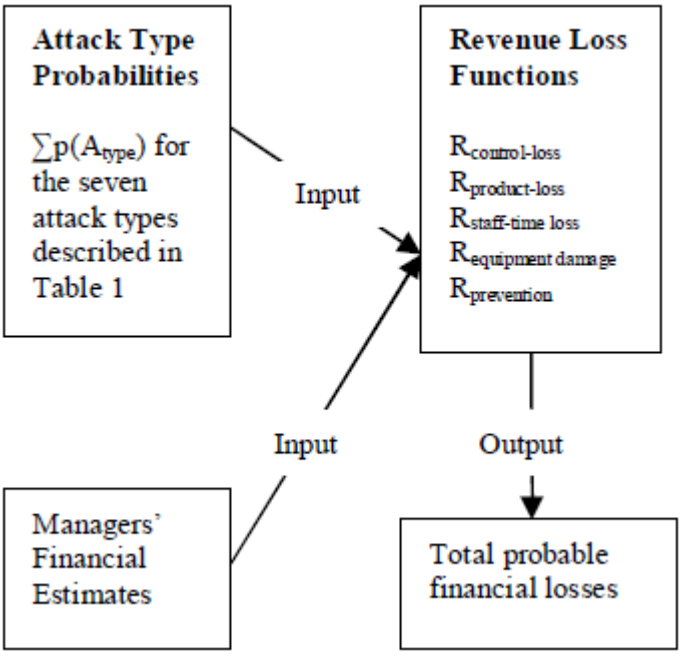


Figure 13: *Risk assessment model for cyber-attacks on information systems*

Types of damage taken described in this model are:

a. Control and monitoring loss: The loss of control or view is the financial damage caused while trying to run the process without the SCADA control. Attackers hamper plant operation by disabling monitor and control functions. So, functions that require constant monitoring should not anymore be executed. The loss is a function of the attack type A_{type}, revenues per day for normal plant operation R_{normal} and revenues per day for operation without SCADA control R_{manual}. Moreover, SCADA normal function permit automated decision based on gathered data. When systems are attack ed, decision making should be executed manually by managers and engineers with added probability of mistaken decision. According to some assumption losses and revenues are referenced on smaller time periods than days, like 8-hours periods. Revenues caused by control and monitoring losses are given from the equation:

$$\boldsymbol{R_{control-loss} = (R_{normal} - R_{manual}) * \sum p(A_{type})}$$

Where: $\sum p(A_{type})$ is the sum of all probabilities of all attack types that could cause damage.

b. Material loss: It is the loss caused by the bad product quality, because the products in the supply chain could not be used; or the material in stock became worthless because the raw materials were not used before their expiration dates. This loss is treated as a function of the number of the vulnerable machines. The revenue loss is $R_{\%\ machines\ down}$, for a given percentile point if vulnerable machines

are down. This loss is estimated by calculating the average for the revenue losses of the four quartile points of machines being attacked: $R_{25\%}$, $R_{50\%}$, $R_{75\%}$, $R_{100\%}$. So,

$$\boldsymbol{R_{product\ loss}} = \left(\frac{\boldsymbol{R_{25\%} + R_{50\%} + R_{75\%} + R_{100\%}}}{\boldsymbol{4}}\right) * \sum \boldsymbol{p(A_{type})}$$

c. Staff time loss: It is the revenue loss resulting from idle personnel. For example a company continues paying employees whether or not the plant is active or not because of damage. This value is calculated by multiplying the number of operators with their idle hours and their hourly pay-rate.

$$\boldsymbol{L} = (\boldsymbol{time\ taken\ to\ fix\ machines}) * (\boldsymbol{number\ of\ idle\ operators}) * (\boldsymbol{hourly\ pay - rate})$$

Losses are estimated for the four quartile points of machines taken down because of the attack. So, the revenue loss for staff time loss is:

$$\boldsymbol{R_{staff\ time\ loss}} = \left(\frac{\boldsymbol{L_{25\%} + L_{50\%} + L_{75\%} + L_{100\%}}}{\boldsymbol{4}}\right) * \sum \boldsymbol{p(A_{type})}$$

d. Equipment Damage: It is the amount of damage to the process equipment. This loss is treated as a function of total cost of the SCADA controlled equipment that could be permanently damaged and the total cost of SCADA controlled equipment that could be temporarily damaged. The cost of replacing equipment is estimated by taking each piece of equipment that may be damaged and its cost. The average loss $E_{quipment\ replace}$ would be:

$$\boldsymbol{L_{equipment\ replace}} = \left(\frac{\boldsymbol{total\ equipment\ cost}}{\boldsymbol{number\ of\ equipment}}\right)$$

Using historical data and statistical analysis managers and engineers can estimate the cost of fixing equipment:

$$\boldsymbol{L_{equipment\ fix}} = \left(\frac{\boldsymbol{total\ cost\ to\ fix\ equipment\ from\ past\ records}}{\boldsymbol{total\ number\ of\ problems\ in\ the\ past\ records}}\right)$$

$$\boldsymbol{R_{equipment\ damage}} = \left(\boldsymbol{L_{equipment\ replace} + L_{equipment\ fix}}\right) * \sum \boldsymbol{p(A_{type})}$$

e. Prevention Costs: Cost of intrusion prevention includes fixing software problems and updating/ replacing vulnerable software and hardware. This cost is treated as a function of protecting the damaged machines from similar attacks in the future. The cost can be calculated from the average cost of similar

repairs and upgrades in the past:

$$R_{prevention} = L_{prevention} * \left(\sum p(A_{type})\right)$$

This method is a very generic, quantitative approach, meaning it can provide a more accurate and useful to managerial personnel RA method. This method helps estimate financial losses by cyber-attacks. But these losses are restricted to the industrial or corporate environment not considering indirect and chained losses when attack occur against CI. In the first case method may provide relatively accurate results, while in the second case risk assessment is far away of being considered realistic. It is only a mathematical model to estimate financial losses caused by cyber-attacks on SCADA systems, so it cannot be used as a stand-alone method, but has to be combined with system modeling and vulnerability analysis to identify all assets and vulnerabilities. It does not consider cases of dependencies or interdependencies; but they can be empirically estimated during the assessment or after have used an asset and vulnerability identification method. Predicted average values may differentiate in a significant degree from reality and it is estimated that should be taken independently and examined in case scenarios based on historical data.

Methods estimates quantified risk based on calculation of expected financial losses due to cyber-attacks against SCADA systems. Moreover, probability of attacks is estimated based on availability of historical and statistical information of similar attacks. So, due to this fact, this method appears to be ineffective against zero-day attacks, for which there are not historical data, so investment for prevention losses may be insufficient against this scenario. This is a quantitative risk assessment method.

During risk analysis all potential damage due to cyber-attacks against SCADA systems are expressed and quantified as financial losses. Method does not consider societal and chained impacts, but only short term financial losses and imminent damages that can be directly expressed in the form of financial loss. Furthermore, this method provides a list of most common attacks and it is a threat oriented method. By estimating attack probabilities method determines risk quantified as financial loss for given assets.

Method is well structured and simple, providing an easily understandable mathematical model, based on prior trusted and acceptable knowledge and risk quantification base. This is not a holistic method. It addresses strictly SCADA systems and industrial environment, dealing only with short term impacts expressed as financial losses. It interrelate low level technical analysis with operational and strategic layer decision making since provides directly results expressed as financial losses. Being quantitative provides a rather accurate and practical measure for risk, although not considered multiple types of consequences. It is considered appropriate for analyzing corporate risk only.

There is no particular model to identify and analyze potential threats. Most probable threats are retrieved from a relevant threat list. So, this method will become ineffective against zero day or rare attacks since it cannot identify potential impacts. By combining it with a model like VSM or petri net would amplify risk estimation capability. Actually it is not its concern since it provides only a mathematical model to quantify risk. Consequences are quantified as expected losses but risk exceedance probability curves (EP) may be used on this purpose. Losses from different damages are added altogether to provide total expected loss. Each cyber-attack incident causes a series of damages and costs like equipment repair cost, prevention of future attacks taking into account appropriate countermeasure costs, staff time losses, material and production or outages losses etc. All these losses are quantified as financial losses and added altogether.

3.1.19 A graphical adversarial model for oil and gas drilling cybersecurity

The authors of [68] propose a model for cybersecurity risk decisions based on Adversarial Risk Analysis (ARA) that takes into account attacker's behavior. Additionally an application of the model in drilling cybersecurity is presented tailored to the needs of offshore rigs employing drilling control systems.

ARA is based on a subjective utility model of the attacker, treating attacker's decisions as uncertainties. Attacker is considered to be a utility maximizer i.e. intending to cause the maximum damage to the assets.

While traditional RA methods provide information for decision making, ARA integrates decision making with RA. ARA assesses extensively attacker's intentionality and decision making incorporating strong mathematical and statistical tools in RA procedure. It uses graphical representations to provide a better understanding for complex cases through visualizing the causal relations between system nodes. The main graphical tool is the Multi Agents Influence Diagrams, a generalization of Bayesian Networks. Method is structured from the following elements:

a. Decisions or actions characterized as decision nodes.
b. Uncertain states or uncontrollable scenarios representing possible outcomes, characterized as uncertainty nodes.
c. Utility and value, representing ways that previous elements would affect agents and characterized as value nodes.
d. Agent representing people related to decision making, possibly with opposed interests and represented with different colors.

The method assumes that adversaries pursue monetary gains. More assumptions are made:

a. Model is discrete.
b. Attackers are utility maximizers.
c. One defender is assumed. Attacker's nodes do not represent a

specific attacker, but a generalization of potential criminal organizations representing business-oriented Advanced Persistent Threats (APT) guided mostly by monetary incentives.

d. Detection related activities or uncertainties to simplify the model are avoided. Thus the attack is always detected and the defender is always able to respond.

e. An atomic attack i.e. attacker performs one action is assumed, with several consequences as well as several residual consequences once risk treatment strategy is selected.

f. Defender's and attacker's costs are deterministic nodes.

g. The scope of the model is assessment activity prior to attack supporting incident planning handling.

Defender nodes are:

a. Protect Decision node. Defender selects among different security measures portfolios to increase protection against the attack.

b. Forensic System Decision node, where defender selects among different security measures portfolios that may cause harm to the attacker.

c. Residual Risk Treatment Decision node modeling defender actions after the assessment of other decisions made by the attacker and the defender.

d. Respond and recovery decision nodes.

e. Defender cost deterministic nodes. The costs of the defender's actions are deterministic as well as the monetary consequences of the attack.

f. Value nodes. The defender evaluates the consequences and costs taking into account risk attributes.

g. Utility nodes which merge value nodes of the defender.

The attacker's nodes help characterizing the attacker taking into account uncertainties about the attacker probabilities and utilities that defender has for him:

a. Perpetrate decision node. The attacker decides to attack or not and adapt an attack option from a set of attack options.

b. Attacker cost deterministic cost.

c. Values nodes and finally

d. Utility nodes.

Uncertainty nodes are:

a. Contextual threats uncertainty node. These threats present during the attack.

b. Attack uncertainty node. It represents the likelihood of the attack event, given its conditioning nodes. It depends on the perpetrate and on the protect decision nodes.

c. Consequences uncertainty nodes. It represents the likelihood of different consequence levels a successful attack can lead to.

d. Residual consequences uncertainty nodes. It represents the

likelihood of different consequence levels after applying residual risk treatment options.

e. Counterattack uncertainty node representing the possibility that a forensic system attacks and harm the adversary.

This method proposes ARA method incorporating risk analysis with decision making based on adversary behavior examination. The main graphical tool is the Multi Agents Influence Diagrams, a generalization of Bayesian Networks, which represents and analyzes relationships between systems' different nodes. Method uses strong mathematical methods and Bayesian networks to estimate uncertainties which express potential adversaries' decisions. The proposed methodology is a qualitative approach to RA.

Although methodology has been applied for petroleum related infrastructures and offshore rigs employing natural gas and petroleum drilling operations, it can be considered quite generic or **holistic** to address different sectors and companies' risks. During risk assessment attackers are considered as utility maximizers, intending to cause maximum damage to the targeted assets.

This method proposes ARA model and it is a threat oriented method based on adversarial modeling treating attackers' decisions as uncertainties based on a subjective expected utility model of the attacker. Although this method seems complex it is supported by graphical tool and it is based on strong mathematical theories using Bayesian networks for probability and risk estimation.

Method uses graphical representation tool to simulate assets, threats and risks. This method is addressed to standard assets which are pre-selected for risk analysis. Method uses generations about threat models, but it can model and visualize complex scenarios, decisions and potential outcomes through the provided graphical system. Finally, system that is consisted by both asset and attacker is modeled and visualized as well as potential system states.

3.1.20 Safety and security framework for risk and vulnerability analysis

In [69] a framework that provides a holistic framework for both security and safety is presented. Starting point of the methodology is that system to be analyzed consists of one or more functions or tasks. Study has interest in systems that have special interest in society, in other words CI, which can be exposed to certain threats or hazard. These threats or hazards may lead to consequences quantified as financial losses, number of life losses, etc. They appear as observable quantities which express states of world, physical, economical or natural quantities that may become real when an impact occur.

Paper distinguishes sources, threats, hazards and opportunities. It also distinguishes security and safety; security refers to intentional events i.e. attacks, while safety relates to accidental situations.

Paper defines risk as combination of possible consequences and associated uncertainties. A source is an event or a situation with a potential of a certain consequence. Vulnerability is defined as possible consequences combined with associated uncertainties for a given source. Hence risk is defined as a combination of sources and vulnerabilities. Taking above mentioned into consideration risk analysis comprises of sources identification, vulnerabilities identification, uncertainties estimation and finally risk compiling.

Probabilities and statistically expected values are used to quantify uncertainties. The same logic applies to vulnerabilities and risk. Common vulnerability measures are the probability a system is impaired and the expected loss given a certain threat. So if X is an observable quantity, the statistical expected value EX is defined as the center of gravity of the uncertainty distribution of X. For example if X takes values of 0, 5,100 for probabilities 0.89, 0.1 and 0.01 correspondingly, then expected value equals: $\boldsymbol{EX = 0 * 0.89 + 5 * 0.1 + 100 * 0.01 = 1.5}$

In case of repeatable experiments the expected value equals to the long time run average value of observations X, provided that limiting probability distribution function is used to determine the expected value.

Probability is defined as a measure of uncertainty with reference to a certain standard. Probabilities are conditioned to background information and knowledge. Analysis provides assignments of probabilities and expected values of selected observable quantities in the form of $P(A|X)$ and$\boldsymbol{E[X|K]}$. $P, A, X, E, K,$ represent probability function, event of interest, observable quantity, expected value (EX) and background knowledge correspondingly. So, there is one level of uncertainty representing assessor's lack of knowledge at the time of the assessment in contrast to probability to frequency approach where two levels of uncertainty appear.

The risk and vulnerability analysis consists of eight steps:

a. Functions and subfunctions of the system to be analyzed and relative performance measures (observable quantities). For instance, electrical power delivery to consumers, in case of Smart Grids. Relevant performance measures are:

(1) Damage level scaled 0 to 5 where:

(a) Level 0 corresponds to no damage state.

(b) Level 1 corresponds to transient outage (0-24h) to a network.

(c) Level 2 corresponds to transient outage to region and a network.

(d) Level 3 corresponds to long term outage to a network (more than 24h).

(e) Level 4 corresponds to long term outage a network and transient outage to the region.

(f) Level 5 corresponds to long term outage to region.

(2) Numbers of attacks.

(3) Proportion of attacks being successful.

b. Definition of systems that are to meet these functions. Understanding of system functionality is provided in order to identify declination from normal system operation when an attack or accidental situations occur.

c. Sources identification. Brainstorming analysis and tools like HAZoP, FMEA, FMECA, past attack experiences and analysis scope provide possible sources.

d. Performing uncertainty analysis of the sources. This step can be subdivided to the following substeps:

(1) Information gathering.

(2) Scenario identification. Using event trees and FTA possible scenario can be identified.

(3) Uncertainty assessments.

(4) Probability assessments.

Then resource attack analysis is performed examining attacker's resources and capabilities, possible attackers and their motivation. Knowledge, target vulnerabilities, access and ability to assess attack success on behalf of the adversary.

e. Performing consequence analysis addressing uncertainties. This step can also be subdivided to the following substeps:

(1) Information gathering.

(2) Identification of scenarios. Event trees and FTA or other brainstorming techniques are used to identify possible scenarios and consequences given that an initiating scenario has occurred.

(3) Uncertainties assessment. Likelihoods are estimated based on previous substep methods.

(4) Probabilities assessment

f. Describe risk and vulnerabilities. To describe vulnerabilities comprehensive taxonomies and checklists are usually used; systemic analysis can be also used including examination of architectural and behavioral design attributes and other general criteria. By systematic review of these attributes, vulnerabilities beyond the standard well known cases can be identified. For performance measures observable quantities may be used, but also CIA[3] model for information systems can be used too.

Risk is categorized according to the following eight consequences characteristics:

(1) Potential consequences represented by observable quantities.

(2) Ubiquity, describing the geographical dispersion of potential

[3] Confidentiality, Integrity, Availability security principles

damages.

(3) Persistency, describing temporal extensions of potential damage.

(4) Delay effect, describing the latency between initiating event and main impact.

(5) Reversibility, describing the possibility of restoring system to previous state before impact and damage occur.

(6) Violation of equity, describing discrepancy between those who enjoy benefits and those who bear the risks.

(7) Potential of mobilization, meaning violation of individual, social and cultural interests and values causing conflicts.

(8) Difficulty in establishing an appropriate measurement system.

Similar matters to those related to uncertainty analysis of sources exist here.

Returning to Smart Grid example, where unavailability of services is the main concern, consequence is expressed as outage time C_i for a given period of time. By relating it to relevant initiating events, $\boldsymbol{C_i} = \sum_j \boldsymbol{C_i} \times \boldsymbol{I}(\boldsymbol{A_j})$, where A_j denotes the source j and $I(A_j)$ is the indicator function which equal 1 if A_j occurs and 0 otherwise. By $\boldsymbol{C_i} \times \boldsymbol{I}(\boldsymbol{A_j})$ outage as a result of source j is expressed. The expected value corresponds to$\boldsymbol{EC_i} = \sum_j \boldsymbol{E}[\boldsymbol{C_i}|\boldsymbol{A_j}] \times \boldsymbol{P}(\boldsymbol{A_j})$**.** So the expected value of outage time equals probability of event j multiplied by the expected outage time given this event, summed all events$j$.

g. Evaluate risks and vulnerabilities. The calculated expected values constitute a basis for risk evaluation. Of course, expected values may deviate from real values. So a matrix is formed using components EX and$U$, where U are factors that cause significant deviations of expected values from real outcomes. They include complexity, available information, time horizon, level of risk and uncertainties, manageability/ reduction ability and thoroughness. Each factor is given a score and based on it an index can be established.

h. Propose and takeover countermeasures and then repeat assessment procedure from the third step and beyond taking into consideration implemented countermeasures.

The use of FTA and event trees and other brainstorming techniques to identify consequences scenarios for given initiating threat scenario makes it possible to identify dependencies and interdependencies. FTA is not suitable to identify external system dependencies but rather internal system failures but the combination of event tree may reveal such factors between different systems. Moreover, se of probability distribution and expected values restricts uncertainty as wide probability spectrum is used for calculations. Interrelationship with background knowledge and information using Bayesian patterns enhances probability accuracy. Method considers factors causing significant deviations of expected values from real outcomes. They include complexity, available information, time horizon, level of risk

and uncertainties manageability/ reduction ability and thoroughness. Each factor is given a score and based on it an index can be established. Risk is expressed as the product of unavailability period, for example power outage in the case of power grids, times probability for all events that occur and cause consequences. But, also other observable quantities, like fatalities numbers, can be used for consequences quantification. A set of factors affecting risk referred in paragraphs d, e are taken into consideration during assessment. Significant matters to be examined in this stage are likelihood of event/ attack occurrence in a given time period, condition uncertainties for conditions influencing the occurrence of events and essential factors creating uncertainties. Uncertainties are based on information or study of similar events that had happened in the past. Examination results are probability distributions, known as probability models.

Method is rather vulnerability oriented, examining consequences and risks for systems of particular interest for society, i.e for critical infrastructures taking into consideration threats capabilities and threat scenarios against them. It is a quantitative method using probability distributions and expected values for each distinct value taken from these distributions to provide expected losses. This method is quite simple and applicable considering not just a single probability for each scenario, but rather uses whole probability distribution with all possible outcomes, restricting uncertainties. For high mean deviation multiple values must be included in calculations.

Since consequences are quantified and expressed in financial losses and other observable quantities are useful for operational and strategic layers for direct support to decision making with the right level of abstraction. Identification of potential threat and threat scenarios is based on FTA and events trees and assessing threats that could cause certain consequences exploiting certain vulnerabilities.

To describe vulnerabilities comprehensive taxonomies and checklists are usually used; systemic analysis can be also used including examination of architectural and behavioral design attributes and other general criteria. By systematic review of these attributes vulnerabilities beyond the standard well known cases can be identified. For performance measures observable quantities may be used, but also CIA[4] model for information systems can be used too. Use of FTA further enhances this ability.

Consequences are quantified and expressed as services unavailability periods, for example in case of smart electric power grids it is expressed as duration of outages. They can also be expressed in other observable quantities like financial losses and fatalities. Finally, method objective is to provide a holistic methodology for both risk and vulnerability analysis considering both security and safety for analyzing critical to society assets and functions, i.e. CI.

[4] Confidentiality, Integrity, Availability security principles

3.1.21 Availability based RA for SCADA embedded computer systems

Although in most information and computer systems security focuses on integrity and confidentiality of information, ICS and SCADA systems focus on availability and integrity security principles. In [70] a risk assessment method is described that focuses on SCADA systems where maintaining availability is the primary objective of the system operators.

Prior risk assessment and vulnerability reduction procedure, a team of system experts involved with system operation, design, engineering and management is formed in order to evaluate it. The multi-stepped process of risk assessment and risk reduction, described in the following figure, consists of the steps: architecture identification, identification of possible attacks and their impacts, risk and vulnerabilities assessment, risk level and protective mechanisms identification, protection priorities definition, final protection approach definition, residual vulnerabilities identification and reassessment when it is required.

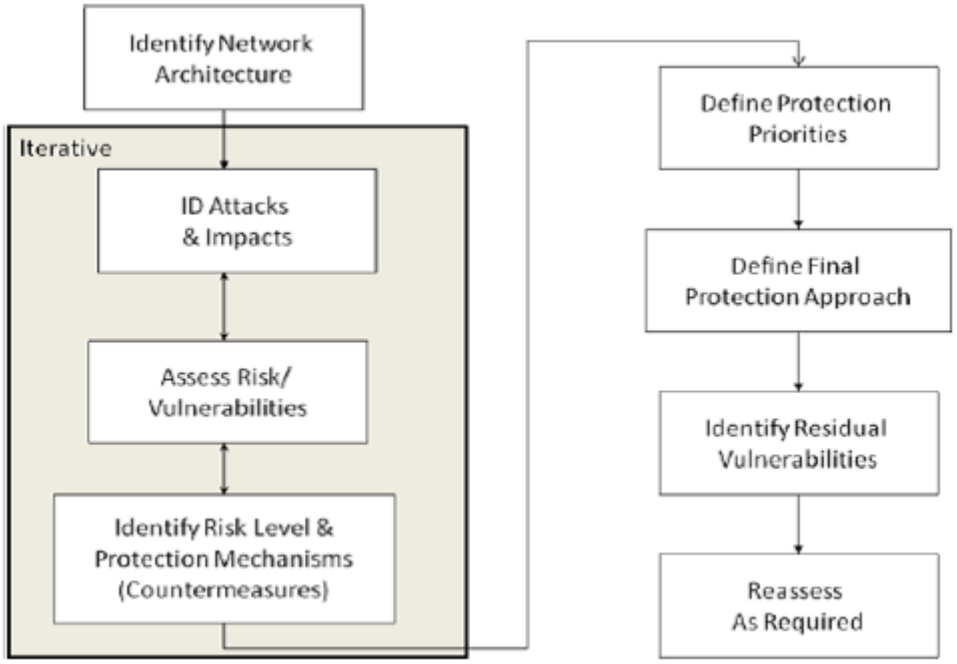


Figure 14: *Risk assessment and vulnerability reduction*

The first step of the process is the identification of all equipment and how it is installed to the network system, hardware, software, internal and external connections, IT protection measures etc. and represented in architectural drawings. Especially for edge devices critical control elements and sub-elements should be identified and described in detail like access points.

Threats against systems are defined as internal (within the organization) and external originating either from unauthorized personnel with network access or

gaining physical access to system resources and compromise them. Paper defines attacks on availability as attacks to prevent system element to perform designed functionality resulting in loss of functionality, loss of services and creation of safety and health hazards. Additionally defines attacks on integrity which aim at modifying software, firmware or data used or generated by system elements and confidentiality attack to obtain information on software, firmware, data or any other information used by the system and not normally be available to attackers. Based on attack types specific attack goals are identified. Root concern on SCADA attacks is loss of availability of functionality and services.

Failure analysis via FTA and event trees is proposed to provide accurate indication of resulting risks associated with availability attacks. Unavailability attack risk is a measurement of the likelihood that an attack could occur with success against a SCADA system and cause loss of availability of one or more redundant or non-redundant system edge devices coupled with the consequences incurred by system loss of availability. Risk assessment aims at threat level identification and appropriate countermeasures implementation in accordance with existing vulnerabilities to protect system against relevant threats, reduce vulnerability level and set prioritization of protective action using risk level criterion. Risk identification process consists of the following steps:

a. System elements, edge devices or interfaces to be evaluated are selected.

b. Effects of failure of these elements are determined.

c. Threats and attack types that could cause element failure are determined.

d. Determination of likelihood of attack occurrence, while being successful and its consequences.

e. Risk scoring of system's elements under evaluation.

f. Protective mechanisms for risk reduction determination.

These steps are repeated for each equipment element. Risk assessment focuses on edge devices controlling system's function, especially critical functions to identify vulnerabilities and relative risk to availability for that system element.

For each attack an initial Consequence of Occurrence C_o and Likelihood of Occurrence L_o are established. Initial assessment is executed with the assumption that no countermeasures are implemented in the SCADA system, so establishing a baseline to compare implementation of countermeasures on each reassessment. L_o is considered inversely proportional to the cost of the attack method. L_o level can be categorized based on possibility of attack using following criteria to define different levels:

a. Low L_o: Very high cost or special knowledge is required to attack. Time to attack is prohibitive. No network or physical access to equipment is available.

b. Minimal L_o: High cost and time required for attack. Technology exists for the attack but is not readily available. Effort is required to access network or equipment. Attack requires special knowledge.

c. Moderate L_o: Moderate cost and time is required for attack. Technology exists and it is available for the attack. Effort is required to access network or equipment.

d. High L_o: A small cost and little time are required for the attack. Technology exists for the attack and it is readily available. Some effort is required to access network or equipment.

e. Very High L_o: Very little cost and time are required for the attack. Technology to attack exists. It is relatively simple and cost effective to attack. Access to network or equipment is readily available.

C_o expresses the loss of availability because of a system impact. Its level can be categorized using the following criteria:

a. Low C_o: No impact to the system, no loss of availability. No effect to market share.

b. Minimal C_o: Negligible to system or functionality, negligible reduction to market share.

c. Moderate C_o: Moderate reduction to system functionality or system operation, reduces market share. Negative impact to organization's public image.

d. High C_o: High loss of equipment or functionality, significant reduction of market share. Significant negative impact to organization's public image.

e. Critical C_o: Total loss of equipment and service, eliminates organization from market place, because of extreme negative impact to organization's public image. Financial responsibility to repair the damage caused by loss of service availability.

L_o and C_o values are independent and each one can vary from low to critical level. Proposed method uses a simple approach to calculate risk with speed and simplicity. Risk is computed by the following sum:

$$\boldsymbol{Risk\ Score = A \times L_o + B \times C_o}$$

Weighting factors A, B selection is based on the system and they sum up to1. In most SCADA systems B is bigger than A, because consequences may be critical or even life threatening, so higher level of protection is needed because consequences can be catastrophic even if probability of attack occurrence is low. Finally for risk calculation a normalized risk matrix is used, where values of L_o and C_o range from 1 to 5 each.

Risk score indicates the level of trust needed and the priority that should be set to the evaluated element in order relevant countermeasures to be implemented and protect its critical functions. Adding countermeasures is possible to reduce L_o level.

C_o is not affected but it can be reduced with system improved security oriented redesign. In turn this may affect initial L_o too.

Risk score represents a Trust Level (TL) which in turn determines a set of protection mechanisms to be used. For each TL set of protective mechanisms provide assurance that system will continue functioning during or after attack. The following TL categorization is used:

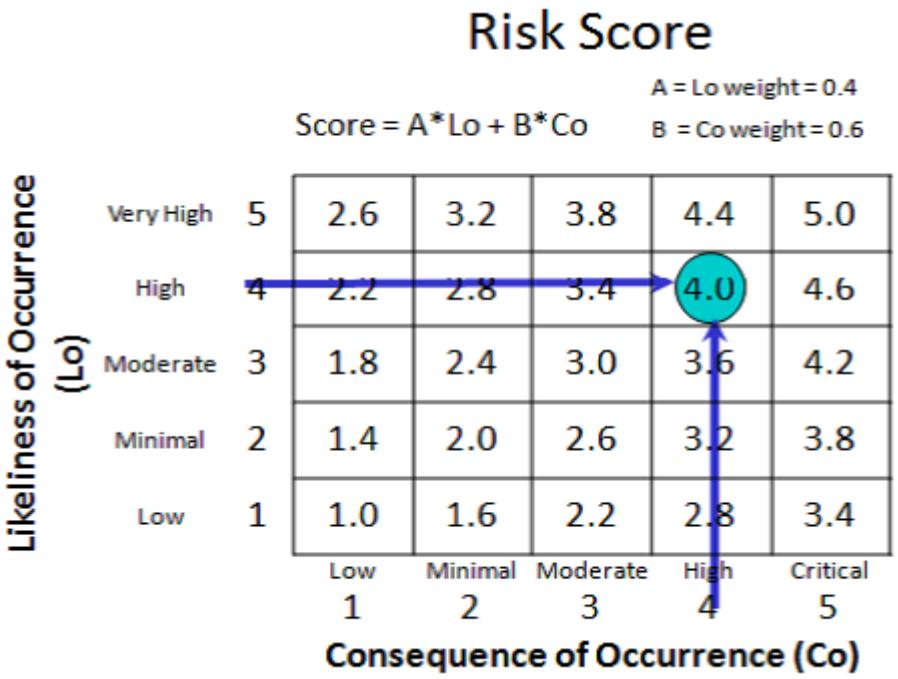


Figure 15: *Risk scoring example table*

a. TL1 representing risk score less than 2 representing a very low risk of loss of availability therefore no specific protection mechanisms are required.

b. TL2 representing risk score less than 3, representing in turn low risk of loss of availability and protection mechanisms should be added at low cost or set in position being ready to be used in demand.

c. TL3 representing risk score than 4. It represents a medium risk of loss of availability and protection mechanisms should be considered for use,

d. TL4 (risk score less than 5) represents a high risk of loss of availability and inclusion of protection mechanisms should be considered while TL5 with risk score equal to 5 represents critical risk of loss of availability. Paper proposes protection mechanisms for each level; each successively higher level includes mechanisms of the lower levels plus extra protection measures.

e. Based on risk scoring, prioritization for element protection is set. High risk systems are protected, but because of financial constraints some systems may stay unprotected. Partial protection may be tested to check security investment

effectiveness. Risk assessment should be iteratively conducted until acceptable risk reduction is met taking into account that unprotected systems result to residual vulnerabilities.

By definition FTA does not examine external attacks but associate internal system's anomalies and undesired states leading to undesirable main states. Additionally to uncertainty which always depends on expert's judgment the additional factors, A and B add more subjectivity to risk assessment. So, this fact may cause greater deviation of probabilities and risk estimation from real cases, as factors A and B are given values based on abstract evaluation and there is no past experience or statistical basis to determine them with high accuracy.

Although system analysis is an iterative and structured procedure, it is executed in an architectural systemic framework not considering system behavior so not examining all possible system dependencies and interdependencies. Though, use of FTA may reveal possible dependencies between system's parts. The probability of this method is assessed in typical qualitative scaling, but its accuracy is enhanced by relating it to adversary knowledge and capabilities factors.

The proposed method is a semi-quantitative approach to risk assessment providing relative risk quantification. Methodology does not take into consideration geographical factor. Assessment is executed for lower layers cyber and physical as well as for higher levels as consequences relate to market impacts, despite the fact that analysis focuses on these lower layers.

Classical definition of risk is not used by the particular methodology. Additional weighting factors affect probability and consequence magnitude weights. So, in SCADA systems where existing threats may cause catastrophic consequences to infrastructures even in low probabilities relevant weighting factor gets higher values than probability corresponding weighting factor. This means that weighting factors vary in accordance with independent risk elements (probability and consequences) significance for each examined case. This approach overcomes low probability ambiguities met when rare events and zero day attacks may occur, being more effective when critical systems are to be attacked and critical consequences take place in parallel. The method drawback is that weighting factors estimation relies in certain degree on operators' subjectivity but their selection may be optimized as he gets more experienced. Risk assessment is performed literately applying various countermeasure strategies until residual risk and residual vulnerability meets acceptable boundaries.

It is extremely time consuming when systems have numerous components and complexity, because process of element analysis and risk scoring is repeated for each one element, sub-element, function and edge device. Moreover, it requires the composition of team analysis consisting of experts on different system aspects. This method is applied on SCADA systems where availability maintenance is main objective; SCADA systems apply in all different energy sectors and in other critical industrial infrastructures.

Though method can be applied to all different infrastructures, SCADA and ICS systems it is oriented for lower layers, cyber and physical analysis, but measured consequences are directly related to operational and strategic layers' interests. Furthermore, threats, identified target system vulnerabilities, that when exploited would cause failure states identified by FTA analysis, causing in turn system FTA top event. Additionally analysts seek information on technology, resources and knowledge availability that would permit potential adversaries to attack effectively the system and then estimate accurate probability of occurrence.

To sum up, this method focuses on SCADA control systems risk assessment, where maintaining availability attribute is the primary objective and on reducing vulnerability level.

3.2 Conclusions

Following the presentation and evaluation of the above RA methods and methodologies the conclusion is that barely some of them fully satisfies the specific demands for a RA methodology that can be applied in CPS.

Most RA methods and methodologies provide only a very generic guideline, dealing with their subjects in a holistic way. Much freedom is left for users who are allowed to act based on their own experience and judgment. Analysis is conducted without any detailed, strict and well-structured guideline framework. Users are forced to use any brainstorming techniques and analyzing tools to support risk analysis process and cover these methodologies' inherent weaknesses, but also there is no limitation in their use. This is particularly viewed in higher level and old fashioned RA methodologies.

In order to identify complex CPS numerous and assets, traditional methods for information systems analysis are not considered efficient for that use. Modern theoretic models applying graph theory, graphical representation capabilities and system modeling are proving to be more efficient for asset and dependencies/ interdependencies identification. In the contrary, older methodologies do not have such possibility. Petri Net is most commonly applied in modern methodologies, while other modeling techniques have been proposed like Viable System Model, CIMS and Operational Architectures Modeling. They represent a structural system view, may simulate relationships and communications between system parts but also between different systems or systems and environment. Petri Net has the ability to simulate different system states and attacks. Graphic representation of systems and their simulation are advantages of these techniques. Drawback of these techniques is that they add more complexity and sometimes difficulty in risk assessment applications. So, it may become obligatory to either use such techniques for examination of simpler systems or use a certain degree of abstraction. Use of computer applications undertaking the simulating weight and automate this procedure providing additionally graphic capabilities neutralize this drawback. This is important because since as level of abstraction in complex nature and structure CPS modeling increases, detail and results credibility is reduced.

Apparently such adopted practices are much more complex and required special knowledge about theoretic subjects like systems theory, graphs theory, mathematical formalizations etc. Moreover, the extremely high complexity of CPS obliges the composition of a large analysis team being consisted of experts of different domains; systems engineers, security engineers, computer scientists, electronic engineers, electrical and mechanical engineers, managers, risk analysts. Each one specialized in his own specialist domain. They are all needed in order to have a complete view or model of the system and examine all different nature subject and parameters. Obviously such procedure would be very time consuming too. Because of the high complexity of such systems these drawbacks seem to be unavoidable.

Interdisciplinary and multidisciplinary approach is needed to deal with such systems. CPSs combine many different technologies: mechanics, electronics, information technologies, etc. And all these different technologies should be combined and intergraded in unique systems, while ways of interrelations should be researched.

Combination of cyber and physical attacks should be taken into account during RA as CPSs consist of two domains/ infrastructures: the physical domain/ infrastructures and the cyber domain/ IT infrastructures and SCADA systems, closely related to each other with the presence of dependencies and interdependencies. Cyber enabled physical attacks or physical enabled cyber-attacks are possible. That means that during RA it is very possible that composite threat scenarios should be examined, estimating or calculating composite probabilities. Accordingly, risks due to both physical and cyber substances and relevant attacks should be considered.

History of cyber-attacks against large scale cyber physical systems has few proven incidents to show. Conditions for such attacks have never been proved to meet during attacks neither have been proved unsuccessful efforts. There has always existed significant difficulty to distinguish accidental failures from cyber-attacks in many occasions. So there is insufficient historical evidence and statistical samples are poor to provide accurate probabilities estimation based on observed attack frequencies. NIST approaches on risk and probability estimation rely on such logic approaches for probability quantification, while ISO 27005:2011 makes a simpler qualitative and rather abstract approach depending more in operator's experience and intuition.

Semi-quantitative and quantitative approaches based on historical data present one more point of inaccuracy: They count attacks during periods of time and use extracted attack frequency for defining qualitatively or quantitatively probabilities of occurrence. But when a zero day attack first happens, a time-period follows where attacks are successful until effective countermeasures are implemented. Any other attacks then become ineffective until a new vulnerability or exploit appears. So, frequency and probability of attack should be measured for time periods from exploit or vulnerability identification to the time that they are effectively protected based on attacks that happen in this particular time period. The longer is this time period or the more of attack happen then the highest are the probability of attack and risk. Successively this means that risk and probability are considered higher in reality.

Analysis based on available data probability of cyber-attacks against ICS and SCADA systems may appear extremely low and perhaps untrusted. Moreover many times cyber-attack strikes may seem impossible to happen. There is an objective difficulty to predict acts like zero days attacks. But even in low or zero probabilities risk remains in very high level because of the great magnitude of the consequences of an impact to a large scale CI. CPS RA methodologies should be able to employ extremely low probabilities and vast magnitude consequences to estimate risk efficiently.

As CPS are usually characterized by dispersion over wide areas, where different conditions are meet in each area and different systems of different value are installed in each one of them, risk varies among all system's geographical areas. So, locational risk should be taken into account.

CPS dispersion, vast size and high complexity, consisting of systems using different technologies would require a multi-level and composite RA procedure performed by numerous RA teams consisting of accordingly specialized personnel. These characteristics make RA procedure complex and time consuming. It would be a good advice to use a holistic shape to deal with all CPS assets, keeping procedure short and simple in other words practical. Extra care and in depth analysis should be taken over for critical assets. But there is some significant danger that when holistic approaches are made, detail and results credibility to be lost. CPSs are characterized by complex structure by nature, so RA procedure complexity and time consumption cannot really be avoided.

Another characteristic common in widespread CPS is the presence of dependencies and interdependencies. Targets presenting these kinds of relationship attributes may appear lucrative to potential adversaries, because with single strikes they may cause high and dispersed damage. So, dependency/ interdependencies attributes should be examined in RA process to determine the most critical assets in addition to vitality and criticality of other assets. Also this means that attacking a critical target/ vulnerability may be executed in more than one way, using multi stepped attacks. When estimating risks, risks resulting from dependent or interdepended assets should be summed up.

As in common Information Systems RA methodologies there is the need of using a reliable scale to measure and prioritize risks. Much difficulty is met when there is the need of comparing and expressing different risks and consequences in order to accomplish prioritization, and this is more obvious in qualitative RA methods. Quantitative RA methods use mostly damage costs expressed in economic form to indicate risk level and set a base for risk management and budget distribution, but still is problematic in dealing with non-economic nature damages or damage that cannot be expressed in numbers such as reputation damage or life losses. In these occasions assurance financial data can be used. Impacts to CPS and CI often are able to cause effects of vast magnitude, chained effects, cascading and escalating consequences to different sectors because of dependencies and interdependencies that apply even in societal and political layers. This range of consequences is not easily measured and hardly partial consequences can be compared.

Most of the RA methodologies do not identify multi-layer dependencies and interdependencies for example between cyber or physical and operational or strategic layers. They just estimate the expected damage for a given probability of an event occurrence and the associated damage caused by a threat's impact on an asset. This damage, usually expressed as financial loss of the strategic stakeholders and they do not identify any other dependency or associate impacts with superior layers; security impacts are assumed to happen at infrastructures cyber and physical layer. For example a DDOS attack against the energy service provider's information systems could harass consumption data gathering from Smart Grid AMI in order to calculate cost and make the billing. This attack is not so important in the cyber and physical layer as it does not affect directly the Smart Grid infrastructures, but attacks directly operational and strategic layers. Attacking corporate computers and stealing confidential data about customers, operators, systems' protocol, industrial planning information (cyber espionage) is another case of attacking higher hierarchy layers.

Most risk analysis methodologies for RA in CI deal with risk and impacts in a rather generic, holistic and sometimes oversimplify way in favor of intuition, applicability, practicality and speed, while they usually examine impacts and consequences from strategic and operational view leaving out of examination most low level technical details. Because of these systems' complexity crucial information, assets, potential threats and vulnerabilities may be omitted.

Modern methodologies approach risk or risk analysis processes goals, risk prioritization, using new alternative techniques, not based on classical risk definition, where risk is expressed as function of event probabilities and relevant consequences. So, weighting factors giving different significance to probability or consequence in accordance with uncertainty level and consequences severeness, risk thresholds for dealing with critical elements, time from detection of event to countermeasure implementation/ time from detection to incident ratios, warning time frames are used to express risks, overcoming difficulties posed by uncertainties and lack of effective metrics in traditional risk assessment. "Time to exploit" systems by potential adversaries used by some methods give a measure of system vulnerability. Sometimes these characteristics may be easily measured, even accompanied with lower uncertainty level, but finally they prove to be less cost effective methodologies at the moment. Harsh attacks may not be so risky, because they may be highly improbable to happen in the near future, while other imminent but weaker attacks may pose more serious threats at the moment. Return of attack investment, in other words cost effectiveness of attacks and threat intelligence may prove to be trustworthy alternatives to risk analysis methods to near future and replace, substitute or just supplement traditional risk analysis methods and methodologies.

Most methods of risk assessment have a holistic character. They are able to deal with different nature of risks, assets and threats. Most of them are oriented to traditional threats in physical layer, like terrorists and physical phenomenon, while impacts are related to physical destruction, stealing, vandalism etc. Cyber-attacks may be considered by these methods, but most usually they are examined from a strategic or operational aspect. Holistic methods have the ability to estimate different risk types in common framework, providing

quick results, but they usually address to management level and often fail in detail and cannot anticipate special cases like cyber-attacks and special effects.

Advanced mathematical models and deterministic methodologies like Monte Carlo Simulation and sensitivity analysis, Contingency Analysis, Project learning analysis, Error and variance analysis are used to provide accurate and consistent probability and risk results, by examining all possible outcomes and variable values. But such practice has the drawback of being time consuming and impractical because vast volume of results is produced, with most of them not being useful and often being unrealistic. So, controlling mechanisms should be applied in order to restrict possible outputs. Such techniques are used in quantitative risk analysis. Semi-quantitative techniques preserve much of needed accuracy, but many times they may add more subjectivity to generated results in accordance with the method of qualitative and initially non measureable estimation quantification.

Many methodologies do not consider residual risk. They are oriented to risk optimization, meaning that risk assessment procedure is iterated until the optimal combination of countermeasures is applied, amplifying systems' defenses, while some methods considers residual risks but residual vulnerability too, remaining after available countermeasure application. When referring to CI accepting residual risk is not a permitted option, since consequences still remain in high level even if probability is low.

Conclusions appearing in comparison table of Appendix A result from current analysis, while criteria efficiency measurement relies on both analysis and evaluation, and abstract estimations based on experience, common sense and intuition. Table A shows a tendency towards asset oriented methods and methodologies. Qualitative approaches seem to be the preference of the majority of analysts. That is because they provide quick results providing guidance for strategies take over, while they do not need as accurate data as quantitative methods do. Next threat oriented methods seem to be preferred, especially by national entities, interrelating criticality with adversaries' capabilities. All examined methods have holistic characteristics. Modern methods acquiring modeling capabilities and mathematical formulation seem to be more analytical. It could be a good idea to combine older but trusted methods with new modeling and simulating tools to enhance their efficiency. In the other hand such modern methods have not been tested enough and they have not proved yet their reliability. They appear to be more efficient to low level cyber and physical analysis, emphasizing to detail in the contrary to traditional methods examining risk from a strategic or operational view. Because of high uncertainties characterizing traditional RA methods, new trends adapting alternative approaches appear, like time to exploit measurements, vulnerability levels and threat analysis.

Summarizing conclusions it seems that there is not any solid methodology oriented to CPS dual essence, dynamic character, size and complexity, used over wide areas connected to CI, able to cover their specific requirements and characteristics. As said these characteristics are magnitude and complexity and possible unpredictable and various states not easily defined and measured, making it difficult to be examined and address this problem in completion, accuracy and with sense of certainty and efficiency.

New era coming is characterized by the intense, multiple cyber threats, while human critical activities and infrastructures, industrial production and energy sector heavily relies on information technology and CPS applications. Information and CPS are extremely high valued targets as if attacked the whole state and population can be severely affected. Although technological means may become available to defend this infrastructures it still remains highly important to have the ability to estimate real threats and apply policies and defenses in the most cost/ effective weight exploiting available limitless valuable resources to achieve the best results.

4 Chapter 4 – Risk Management

Two common terms are *risk management* and *risk assessment*. The notion of trying to determine up front all the various things that 'could' go wrong is definitely a difficult task to undertake.

There are a whole slew of publications available regarding risk management and risk assessment. Degree and certificate programs are also available to those wishing to explore this area further. Truth be told, whole companies and careers are built around the notion of cataloging risks and formulating plans of action should problems appear as well as providing suggestions on how to proceed in order to mitigate potential risks.

With that being said, it is important to take a moment and define some of the key concepts and definitions pertaining to risk managements. What are some of the key takeaways and ideas that a project manager should be mindful of it attempting to perform a risk assessment on their project? What are some of the core principles that they should be aware of in order to best handle their project?

In its purest form, risk management is the identification, classification and priorization of risks. This is generally done in tandem with efforts to monitor, control and mitigate the risks. Risks themselves can be from factors internal to the project, such as the adoption of a new technology, team members that are new to the project manager or resource constrains and internal dependencies. Additionally, risks can also be external, such as the health of the financial markets, competitive pressures, legal liabilities or even accidents. The sheer number and type of risks that may or may not, factor in to a given project gives a good idea of how complex and problematic risk assessment can become.

Figure 16: *Structure of Risk Management*

There are specific core principles in regards to risk management. When looking to perform an actual risk assessment, the following target areas should be part of the overall risk management procedure, as defined by the International Standards Organizations; ISO):

- The process should create value
- It should be an integral part of the organizational process
- It should factor into the overall decision making process
- It must explicitly address uncertainty
- It should be systematic and structured
- It should be based on the best available information
- It should be tailored to the project
- It must take into account human factors
- It should be transparent and all-inclusive
- It should be dynamic and adaptable to change
- It should be continuously monitored and improved upon as the project moves forward

When first addressing a risk management procedure for a project, take note of the aforementioned principles to ensure that your specific assessment is matching up with the core ideas as defined by ISO.
As far as RM process concern, there is a specific procedure that one should follow when it comes to performing a risk assessment. The overall process can be itemized as follows:

1. **Identification:** perform a brainstorming session where all conceivable risks are itemized
2. **Planning:** once defined, plan for contingencies as part of the overall project; implement controls as needed
3. **Derive Safeguards:** place specific 'fallbacks' into the overall project plan as contingencies for risks if they arise
4. **Monitor:** continuously monitor the project to determine if any defined / unexpected risks manifest themselves

Once the risks are identified and the specific risk process has been instantiated, there are actually certain techniques to be aware of pertaining to risk. Being aware of what the risks are will dictate how effective each of the individual risk management options might be.

- **Avoid Risk:** This may seem obvious, but it is an actual technique. There are instances where a perceived risk can be avoided entirely if certain steps are taken. An example of this might be a concern over a vendor supplying a given deliverable at a specific timeframe. It may be decided to perform the actual work for the deliverable in-house thereby eliminating the risk of the external vendor.
- **Reduce Risk:** While some risks cannot be avoided, they can be reduced. This may be accomplished by fine tuning aspects of the overall project plan or making

adjustments to specific areas of scope. Whatever the case, reducing a risk reduces the impact it will have on your project.

- **Share Risk**: If a certain risk cannot be avoided or reduced, steps can be taken to share the risk in some way. Perhaps a joint venture with a third-party will reduce the downside risk for the organization as a whole. This could reduce the sunk cost and potential losses of the project if sharing of risk results in it being spread out over several different individuals or groups.
- **Retain Risk:** This is actually a judgment call. Once all options are exhausted, the team members, sponsor and project manager may just decide to retain the risk and accept the downside potential as is. This decision is usually made by first determining the upside potential of the project. If it is deemed that the project's expected upside far outweighs the sunk cost and downside, than the risk itself may be worth it. Note that in certain cases, insurance can be used to mitigate the downside, although the actual risk retention itself is what is being accepted by the team.

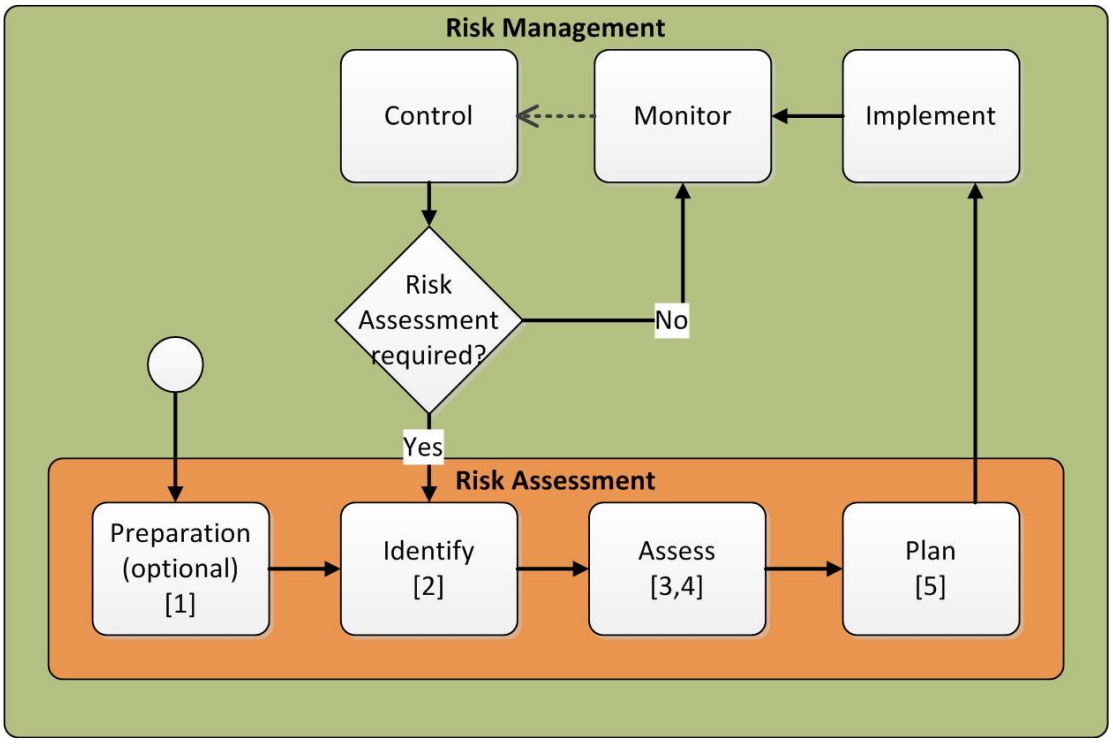


Figure 17: *Overview of a typical Risk Management process*

Finally, we should bear in mind that some methodologies described in above chapter are suitable for both RA and RM and vice versa. More specifically, methodologies such as CRAMM, OCTAVE, CORAS, VSAT and SVA are appropriate for RA and RM. In Appendix there is a summary table describing the methodologies in more details.

4.1 Presentation and Evaluation of Methods and Methodologies

Following there are RM methods and methodologies applied to CPS and CI.

4.1.1 Management Methodology – CRAMM Central Computer and Telecommunication Agency Risk Analysis

CRAMM (Central Computer and Telecommunication Agency Risk Analysis Management Methodology) [23] was originally developed in 1985 due to growing need for security in information systems. Since then it has undergone several major revisions, and now it is the preferred method for use within UK government departments and has been adopted by many commercial organizations and other public administrations throughout the world. It is the most common RM method used in Europe and considered as the most trustworthy one.

CRAMM is applicable to all types of information systems and networks, but also in physical infrastructures and can be applied at all stages in the information system lifecycle, from planning, through development and implementation, to live operation. It is based on standard BS 7799 but also reflects specifications of ISO 27000 standards. It uses a special tool in form of desktop application to go through the entire RA and management processes. It is an asset oriented qualitative RA method.

It is considered as the most complete RM methodology and many other RM methodologies use it as their core component, e.g. CORAS.

CRAMM risk analysis begins by preparing a functional description of the system or project and agreeing with the management the boundary of the review. It identifies the data, software and physical assets within the scope of the review, creating an asset model. It values data assets in terms of business impacts that could result if they had been modified, disclosed, destroyed or set unavailable. It values physical assets in terms of their replacement or reconstruction costs. It also values software assets in terms of their replacement or reconstruction costs or for the impacts of modification, unavailability, destruction and disclosure. In the next phase it investigates threats in relationship to particular assets and assesses their level, i.e. their probability of occurrence. Then it assesses the extent of the vulnerability for each threat (the likelihood of damage or loss combined with the impact that it would cause it). Based on the above results it assesses organization risks caused by system or network threats. During asset identification this method consider the fact that different asset may be located to different places; successively they need different treatment and protection type or level.

Examining CRAMM asset identification process one easily concludes that this method responds to classical ICT systems security needs as its asset database is oriented to common ICT systems rather than CPS. Of course this cannot be

considered as a serious drawback as the CRAMM method had been designed and renewed with direction to specific security requirements. CRAMM links assets taking into consideration possible asset dependencies and this is considered as a point of significance for CPS RA and RM methods. Also, method takes account of the fact that different assets are located in different physical places. In the wide CPS environment characterized by complexity and dispersion across large geographical areas, local risk may appear while risk distribution may depend on time periods and CPS position because certain positions may be more easily targeted or has more critical or symbolic character making them first priority targets.

CPSs are usually dispersed in vast geographical areas. It can be used and provide useful information for all level of users, from technical low level to high level administrative personnel. CRAMM investigates worst case scenarios and consequences due to unavailability of services against various timeframes. Other impacts are described in detailed scales. CRAMM include a “what if” facility, which enables the investigation of the effects of potential changes to the system or network.

In CPSs unavailability usually delivers the most serious impacts to organizational and societal sectors, like in case of attacking electricity smart grids. Size of impacts and consequences of CPS extend far away of CRAMM considerations.

Through threat and vulnerability assessment CRAMM does not investigate threats and vulnerabilities for each single asset but makes the investigation for asset categories in order to save time and computational resources.

Threats and vulnerabilities are related to assets and chosen from certain repositories of CRAMM database. To define threat and vulnerability level typical levels are used: Very high, high, medium, low, very low. It is meant that single threats are examined, but in CPS combination of attack, through cyber and physical domain is possible with different degree of probability each one. Also due to system complexity same effects may be present due to different events or sequences of events. CRAMM does not take into consideration possibility of large scale attacks, neither considers, attacks outside defined company scope like end users data being modified prior their transmission to controlling SCADA in the form smart meters consumption data. It describes the assets dependencies within the systems’ defined scope. A new significant threat appears on smart grids and exposes end user/ energy consumer attacking their privacy by analyzing energy consumption behavior or habits or intercepting relative exchange data. CRAMM is addressed to managerial level RM thus detailed technical system specific vulnerabilities that can be identified by vulnerability analysis or vulnerability detection tools cannot be addressed by the CRAMM tool. Tool’s libraries do not expand to CPS not covering relevant assets.

Consequences, impacts severeness, are evaluated through a series of guidelines involving financial losses, safety, legal and regulatory obligations, personal information, law enforcement, commercial and economic interests, disruption of activities, public order, defense, international relationships, security and intelligence,

public order, policy and operations of public service, loss of goodwill, management of operations of organizations. Method uses appropriate scaling ranging 1 to 10 for each type of impact to measure its severeness. Financial impacts are measured in numerical sizes, financial losses, while other types of impacts, like public order are measured in proper qualitative scaling, corresponding to an appropriate value measured from 1 to 10. Asset values are used to calculate risk using standardized risk tables, constructed based on experience and empirical values as function of values and probability of occurrence, vulnerability and threat level.

As far as assets concerned, are retrieved from tool's database and matched to organization functions identified by operational concept's functional decomposition. CRAMM considers critical processes and assets, processes and assets that direct control or affect human safety, named as safety critical assets. No other special criteria have been defined for criticality characterization. Moreover, threats are associated with specific assets and retrieved from CRAMM repositories. Threat level is defined by using typical scaling: very low, low, moderate, high and very high. CRAMM uses multiple scales for vulnerability and threat levels definition settled on trusted international or national standards while risk is measured in a standardized scale making a semi-quantification approach, while specific scaling has been using empirical data that had been gathered and analyzed.

Furthermore, due to the existence of supporting desktop tool and complete supporting documentation, CRAMM is practical and intuitive in use. Different experts' judgment may be used to identify risks within the organization, but CRAMM provides a practical and intuitive tool to overcome any difficulties. CRAMM tool is used for information system risk as well as different sectors, using a standardized database and risk approach. Additionally, we should not forget that CRAMM uses past experience implemented in statistical scales.

CRAMM is addressed in organizations of all sizes, but its application range it is restricted by its own library contents not describing CPS and since it does not takes into account dependencies it cannot be applied to extremely complex CPS systems' environment. Moreover, CRAMM has been used for many other aspects of risk apart from information systems related risk, such as stationary buildings, health systems, being used widely in public sector. CRAMM has been widely used for risk analysis and risk management purposes. It is based on standard BS 7799 but also reflects specifications of ISO 27000 standards proving to be reliable. It has been supported by a special desktop application tool to automate procedures, being practical and intuitive and provided full method documentation. It has been used as a basic tool for other methodologies too, like CORAS or has influenced the design of other methodologies. It is not anymore supported though and of course it had never been developed keeping CPS cases in developers' minds.

Also, CRAMM considers dependencies between data assets for the identified assets for the defined scope, during asset identification and evaluation phase. Extreme or specialized cases are not included in tool's database, while does not consider multi-layer or infrastructures dependencies and interdependencies. In the degree that

considers these risk elements considers cyber, physical, locational and logical characteristics.

It is known that CRAMM is an asset oriented method, based initially on organization functional decomposition, then matching physical infrastructures to the decomposited functions; physical infrastructures is usually retrieved from method's desktop tool's supporting database.

Although, CRAMM addresses conventional information systems and networks takes into account that these systems may not be located in the same location, but opposite may present a geographical location. It does not examine each asset independently but examines it according to predefined category models. Risk is addressed inside company's boundaries approved by the interested stakeholder. By its nature rather corresponds to cyber, physical layers, communicating risks to the operational layer.

CRAMM functions in qualitative and semi-quantitative mode. What is more is that CRAMM uses empirical and statistical standardized scale to measure risk in a qualitative and semi-quantitative approach. Risk assessment is processed multiple times in order to identify optimal countermeasure implementation for risk level minimizing and residual risk designation, while risk is initially estimated without any countermeasure implementation in order to define a baseline risk level to be used as reference point for later risk level comparison. Consequences (impacts) and their severity are selected from predated lists in CRAMM tool repositories. Consequences define assets' values. They are inserted in empirically constructed risk estimation table along with other criteria of probability, vulnerability and threat to extract risk in qualitative format using typical ranging.

Vulnerabilities are associated with specific assets that have been identified and they are retrieved from CRAMM repositories. Vulnerability level is defined by using a typical scale: very low, low, moderate, high and very high. Finally, CRAMM provides a qualitative risk assessment approach according to interested parts and defined boundaries in order to apply the most effective protective mechanisms to counter risks.

4.1.2 MAGERIT Methodology

Magerit is a methodology created and developed by the Spanish Ministry of Public Administration and which is openly available in Spanish and English. The first version (v.1) of the method published in 1997, while the second embodiment came several years later in 2005.

4.1.2.1 Risk Assessment

a) **Risk Identification**: The process should be divided and includes a preparatory phase (1-2PM), the working group of shareholders (1) and the phase of the composition (0.5 PM).

Performs recognition of assets, relations between them, valuation for the organization, identify threats and risk assessment. The knowledge imported is from the knowledge of the system environment, from reports of similar decisions by statistics where applicable. The availability of data is best illustrated by the representation in quantitative information.

The difficulties in data collection from rare events and the individual systems that have been created and are not taken into account in the basis for decision making.

Data input for the qualitative analysis is to determine the scenarios and for the quantify analysis are the categories of scales and the cost data. It has the ability to convert the quantitative data, to be adopted or to be represented in qualitative data using approximate scales. The data takes into account for the valuation is Confidentiality, Integrity, Availability, Authenticity and imputation responsibility.

b) **Risk Analysis:** Calculates the impact and the risk, possible and remaining values. Quantitative and qualitative, accumulated and deflected. Performs basic risk analysis. The definition of risk based on three parameters where one is the scenario of the threat, the second is the possibility, and third is the consistency (multidimensional, typically measurable using categories scales).
The likelihood is related to a measurement period which is typically the time lasting investments (40 years). The methodology receives qualitative and quantitative data. It provides an Annex including possible types of damage scalable for the user's needs. The probability events included as an element that describes the risks. The dimensions of the effects are often not as a whole.

c) **Risk Assessment:** Prioritize the results and these presented to managers for operational assessment. The basic method of risk analysis supported by creating scenarios (in practice "based on facts") and assessment of consequences and probabilities (frequencies) related to scenarios. The consequences scales are usually graded by categories. The risk measure provides a gradient with a series of alternatives.

d) **Storage Assets and measurement:** Qualitative and quantitative

e) **Business Impact Analysis:** It measures the cost of the Service. It gives data on the development of recovery plans from disasters.

4.1.2.2 Risk Management

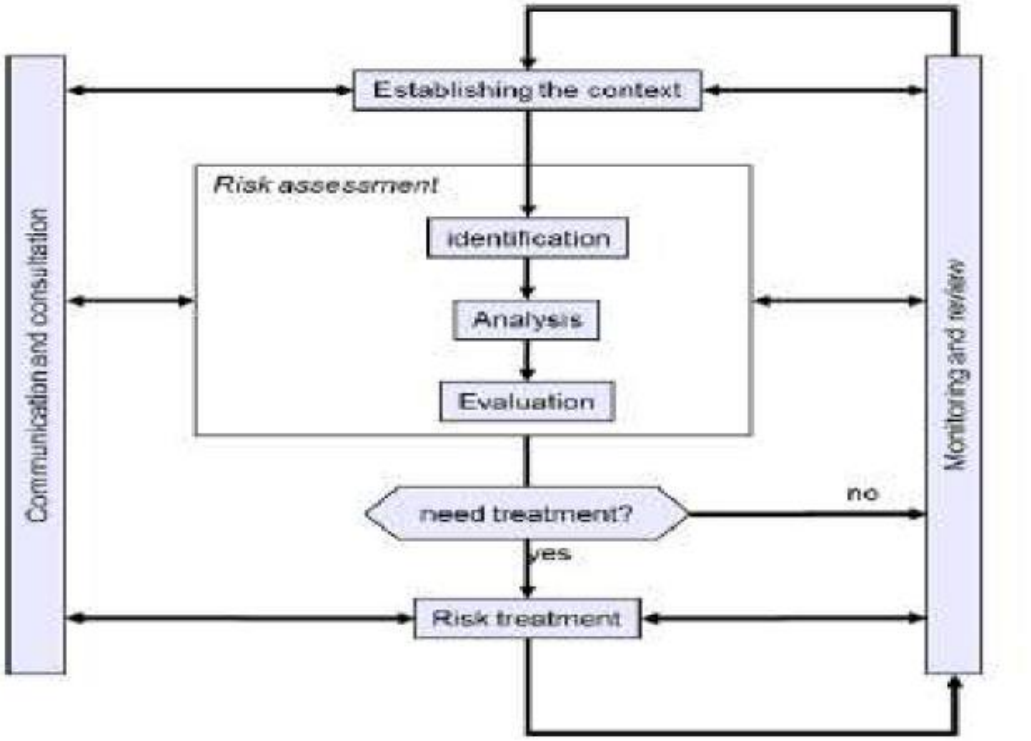


Figure 18: *Risk Analysis Magerit*

Identifies, analyzes and evaluates. Alternatives proposed in accordance with the amount of reduction achieved (or residual risk). The risk is determined as a function of possible loss amounts, and is correlated with possible losses with specific probabilities. The losses are usually measured with different units.

It uses policies to accommodate and other specialized agency agreements. It also has procedures for assessment measures implementing maturity. Furthermore, it reflects the residual impact and risk. Aggregate valuations technical assets and reflected (deflected) value in business processes. Yet also provides many reports. Detailed reports and graphical reports can be exported to other modules. The output of the risk analysis gives values model dependencies between various components and the amount of threats they are exposed to the elements. It also evaluates the effectiveness of existing measures. Finally, it does classification of measures for risk. Security Plan - Total security programs implementing the decisions for risk management.

The Magerit method is a general methodology enables to involve qualitative and quantitative analysis. The impact assessment is based on critical assets, risk assessment takes into account the probability, vulnerability (critical asset) and the impact (threat, asset).

The potential involvement of users in the evaluation process is low. The ability of the method to analyze and combine different overall data appears to be medium. It performs composition scenarios. The process is middle complexity and requires good preparatory work to minimize misinterpretations by the shareholders.

Necessary expertise to carry out the implementation of the tool and methodology is needed.

- The methodology is applied as standard procedure by the academic community, and the application is in complex decision problems where the danger is a sufficient measure to distinguish the performance of alternatives. It can be used on many different occasions and easily implemented with software tools.
- This methodology can be applied to computer systems, telematics media and the general use of electronic posing many risks and should be protected through appropriate countermeasures.
- Through Magerit we can now quantify services and information that may be at risk of setting some values.

Supported by tools such RIGER, Pilar and the whole family EAR tools. It is compatible with the following standards: ISO / IEC 13335: 2004, ISO / IEC 17799: 2005, ISO / IEC 15408: 2005, ISO / IEC 27001: 2005. Also, administrators create their own policies using templates and modifying these policies to meet specific needs. These are connected with the appropriate measures.

4.1.3 Operational Critical Threat Asset Vulnerability Evaluation – OCTAVE

OCTAVE (Operational Critical Threat Asset Vulnerability Evaluation) [24, 25] had been developed by Carnegie Mellon University with large enterprise environments (300 employees and more) in mind and multiple level hierarchies. It presents the advantage of easy implementation from corporate staff that does not need to be fully qualified and have deep knowledge of RA and RM theory and procedures. The application of the method is based on identification of assets, threats, vulnerabilities, risk assessment and provides help in decision making and implementing strategies to handle risks. It sets basis for risk prioritization and definition of degree of residual risk acceptance. The method implementation includes different stages of information collection through all levels of interested company, from management to the technical contacting personnel and uses staff working groups and interviews, so being a time consuming interactive system aiming at asset and countermeasures recognition and description.

The OCTAVE method leads to the prioritization of potential simple threat scenarios based on relative risks estimation. Risk is expressed in relative way and subjective

criteria based on the perception and priorities of the company administration. Based on this prioritization stakeholders will allocate the available budget to reduce the level of risk of assets against identified threat scenarios, accepting a final percentage of residual risk. Method creates, as mentioned, possible threat scenarios, addressing them individually, taking into account the estimated probability of the estimated loss measured on a subjective scale based on configurable options. The risk assessment scale is the prioritization of the company at different types of effects and losses that can accept, e.g. financial losses, reputation damage, personal accidents and material damages, poor productivity, while leaving degrees of freedom for standardization of other subjective criteria / scales for risk measurement. The measurement is based on prescribed sizes. Typically three or four degrees of impact severity are used: low, medium, high. Risk is determined by the most critical systems, whose loss will cause the most severe damage to the company. Operational concept and primary company functions identification, helps in critical assets identifications, by associating assets with these critical functions. The threat scenarios involving damage occurring as disclosure, interruption, destruction, modification and impact of failure of information systems measured as previously mentioned in subjective scale. So in every threat scenario given an overall weighting factor based on the aggregation of all the above factors, which will lead to relative risk against different threat scenarios assessment and prioritization. To identify potential sources of risk / threats standardized chart/ threat trees are used. Probability of threat scenario occurrence is expressed in a scale of low, medium and high probability, giving a rather abstract view of probability estimation without the possibility of examination of composite multiple step scenarios and relative probabilities. By interacting with company personnel in all levels, from top management to low level technicians more information and scenarios may be extracted.

It is understood that the OCTAVE RA and RM method is not configured for use in CPS and CI. Firstly such systems are greatly extended in geographic space and they are very composite and include a lot of critical systems. There are central industrial plants and centralized control units and substations of services production and checkpoints, scattered throughout the territory. Staffed by many employees, at different levels it provides services to hundreds of thousands to millions of people. Multilevel, composite synthesis therefore will cause many difficulties in the implementation process, making it extremely complex and time-consuming, as this method is based in certain degree with interaction with company personnel.

The mentioned systems have a key role in the functioning of the state, economic activity, welfare and health of the population, as indeed are the critical infrastructures of the state. Therefore they pose strategic targets, involving national defense. The overall criticality of the systems and the requirement of continuous operation integrity and availability are not allowing easy prioritization to protect them. Most usually OCTAVE addresses small to medium sized companies and not a vast Smart Grid. The acceptance of residual risk is not desirable and should be

eliminated as far as possible, dictated by the criticality of the systems and of the major impact that can cause the state and societal disruption or interruption of operations.

Given the strategic importance of these systems, geographic dispersion, complexity and diversity, multiple physical access points in its environment or through cyberspace (CAPs), estimated that the threats against them outnumber polytype and threats of a typical information system. So OCTAVE RM is not appropriate in such case. Additionally, there is difficulty in the overall prediction and plotting all threat scenarios. It is also stressed that attacks against such systems may include a combination of actions being identified with varying degrees of success and risk. E.g. A physical penetration and attack in a physical space of CPS can be facilitated after a cyber-attack which aimed to disable security mechanisms controlled by network devices or degrade their function. This type of attack is characterized as cyber-enabled physical attack. Such attacks consisting of successive stages can be distinguished to physical attacks, cyber-attacks, physical enabled cyber-attacks. The latest example happen when an intruder who gained physical access to the computer system attempted cyber-attacks against another linked system, using as attack platform the physically captured system. The OCTAVE analyzes single attack scenarios without multiple stages and composite probabilities corresponding to attack steps. Thus it is inappropriate to apply to CPS or Critical Infrastructures environments. OCTAVE is not effective in dealing with dependencies and interdependencies characteristically for CPS. But, OCTAVE performance can be further enhanced with the use of AT, FTA to include composite threat scenarios and by considering dependency/ interdependency elements.

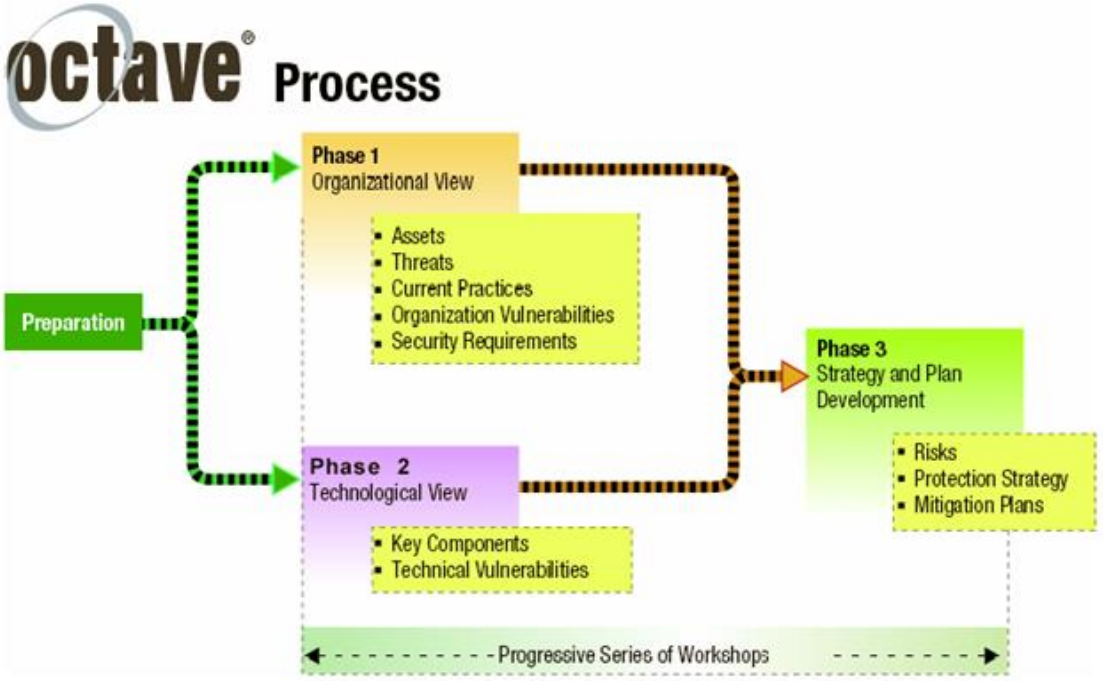


Figure 19: *The three main phases of the main OCTAVE RA method*

Method provides a plan to describe assets in detail and it is based on functional analysis of organization operational concept and operational functions primarily and personnel's' knowledge. It focuses just to the estimated critical assets for the interested organization. Interaction with company personnel is the main way to collect information.

Moreover, company's operational concept and main functions are used to identify critical assets by associating these functions with relevant supporting infrastructures. These functions and assets are considered vital for the company operational continuation. OCTAVE addresses primarily to the Critical Assets of an organization. But the way OCTAVE approaches Critical Assets identification is based on the assumption that specific assets are absolutely necessary to perform the major or critical organization functions. So, it just considers the importance of specific functions according to quantitative criteria corresponding to profit or functional importance in a rather abstract view and not examining other criteria that have been described like the option of back up equipment, alternative functions, the maximum time that specific assets can be unavailable and the restoration time and cost. That means that OCTAVE estimations about critical assets in reality may not be such. Furthermore, no composite threats are examined, but rather simplistic threat scenarios, defined with the help of single threat trees representing all possible threat and hazards sources.

Also, typical qualitative scaling is used based on risk analysts' own judgment, knowledge, intuition and experience expressing company's priorities and impacts on operational function performance measurement associated with different types of effects and losses. This scheme is loose leaving certain degrees of freedom for standardization of other subjective criteria / scales for risk measurement. Measurement is based on prescribed sizes. Typically three or four degrees of impact severity are used: low, medium, high. Standardized numerical values are assigned expressing prioritization and impact severeness.

For a large company OCTAVE requires a whole week to apply all preparation and analysis stages. It is using a composite team consisting of experts' of different domains and address to all involving personnel of the organization. The method itself is intuitive and simple in application providing self-guided method application capability. OCTAVE is a quite practical, easy implemented and intuitive method providing a self-guiding framework for risk assessment. OCTAVE uses brainstorming and interaction within organization parts and members, from top managers to low level technicians in order to identify assets and extract any other valuable information and estimate risks. This method is quite simple and intuitive in application and can be applied in every organization layer. Typical qualitative scales for probability measurement are used; low, medium, high, assigned values of 1, 2, 3.

Generally, OCTAVE method has been developed in Carnegie Mellon University and is consistent with ISO 27005 standard for risk analysis. It is widely used for all

organizations and three version have been designed each one for the needs of a big, medium or small organization. It is well documented and it is subject of systemic examination. Different editions have been developed for different organization sizes. Automated desktop tools can be combined with OCTAVE to provide more precise and quantified results. Furthermore, OCTAVE provides a quite generic risk estimation framework. It is assumed that can be used in different layers and sectors, but it is up to the user to identify and deal with different necessities and particularities.

OCTAVE has been designed with conventional corporate information systems in mind and not cyber physical systems. So it does not address dependencies and interdependencies or composite threat scenarios in risk analysis procedure. Also, OCTAVE is an asset oriented risk analysis method.

Location of asset is included in asset detailed description but it does not affect moreover the risk estimation through a strict and clear guideline, but rather based on analysts' knowledge, experience and intuition. Analysis takes place inside company's boundaries that have been defined by top management considering company's critical assets and functions. Moreover, OCTAVE provides a qualitative approach to risk analysis methods presenting risk levels and residual risk through risk matrixes.

Typical scaling making a qualitative approach, based in certain degree on analysts and other experts' experience, knowledge, intuition. Scaling is user defined while probability estimation scaling is using another three level (low, moderate and high) scaling. Also, brain storming techniques and experts' knowledge about organization assets are helpful for vulnerability identification.

Finally, OCTAVE aims at providing a risk analysis methodology to middle sized organizations, identifying critical assets and functions, threat scenarios and impacts with the help of standardized threat tables, but also based on high interaction with personnel. It determines the risk within company's boundaries and defines residual risk while categorizing risks according to risk level to apply appropriate countermeasure policies.

4.1.4 CORAS

CORAS is summarized in [26, 27, 28, 29, 30, 31, 32, 33, 34]. It is a model based RA and RM methodology. It is a research and development program under European Information Society Technologies Programme. It uses:

a. Hazard and Operability (HAZOP) study.

b. Fault Tree Analysis (FTA)

c. Failure Modes and Effects Analysis (FMEA)/ Failure Modes and Effects and Criticality Analysis (FMECA).

d. Markov analysis.

e. CRAMM as core tool.

f. What – if analysis technique.

This method primarily uses a GUI environment to accurately represent assets, with the help of referred submethods and tools. Interaction with corporate executives wishing risk analysis, at each analysis stage is crucial for successful processes.

The CORAS method has the advantage that it consists of a broad set of proven effectiveness analysis sub-methods and tools and can present effectively and accurately assets, vulnerabilities and threats using a qualitative approach. It seems that it can be expanded to include more trusted tools and analysis methods during the brainstorming procedure, so it appears to be very adaptable to new demands and systems' specifications. The brainstorming technique combined with structured method of analysis offers the capability of detecting and identifying more threats, vulnerabilities and risks effectively and possibly in less time than single individuals would do working separately, while subjects would be examined through many different views combining extensive knowledge backgrounds, expertise and interests. Method uses structured, interactive graphical tools and graphical models in order to effectively involve participants to brainstorming procedures and help ensure an effective communication between the participants and the analysis team. During analysis procedure, participants use notation easy to understand and use. It is considered a very good way to visualize threat scenarios and it is extremely useful for use in presentations. By modeling the RA procedure participants are made more conscious about the target of the analysis and its risks by representing threats and vulnerabilities instead of just making references of them. The language used permits description in more detailed and precise documentation of cause-consequences relationships. But its interactive and complex nature makes it extremely time consuming to implement in large scale CPS. Graphical approach and technical, structured UML language offer the ability to solve the following issues:

a. Facilitate the communication in a group of people with different competences, backgrounds and expertises. It offers a method to cover both high level subjects and technical information without being too complicated to understand.

b. Via graphical representation of risks, complexities are made more manageable. Participants are eased to use their expertises and background knowledge to estimate the probability of occurrence for incidents that have not occurred yet.

c. Document security analysis in a comprehensible manner.

Consequences assessment phase need to be adjusted so that it can cover the extent of consequences of CPS impacts. Also, through threat scenarios analysis, CORAS can describe elements of dependencies and interdependencies; these elements are subjects of examination of submethods and brainstorming techniques. Being an asset oriented RA procedure, CORAS allows detection and identification of all asset and relevant threats not exposing systems to unwanted risks. Risk monitoring technique with use of key indicator ensure that there is sufficient confidence and consistency in assigning correct values to risk and probabilities during their estimation, making risk assessment quite objective and accurate.

CORAS initially concentrates on understanding of organization major objectives and functions, performing a first risk analysis for major risks and assets, then making a deeper and wider examination. By using graphical tool as a basic process tool, method permits visualizing analyzed system assets, relationships, and processes. This practice permits visualizing and examination of **system behavior.**

As far as criticality concern, CORAS does not include any criticality criteria to identify critical assets and vulnerabilities, apart the use of FMEA and FMECA techniques, although it is highly possible such elements to be identified during the brainstorming procedure and there is no particular treatment method or planning to deal with criticalities. There is no particular method to identify threats. Simple brainstorming and experts' judgment are used.

CORAS may use standardized FMEA, FMECA scaling to set risks priorities, providing a semi-quantitative approach or approach risk estimation through typical qualitative scales and risk matrixes. Using CRAMM as a core element and giving enough flexibility in its application, including many other supportive methodologies and tools offer the capability to use any appropriate scale, for risk measurement, for example could use CRAMM scaling to measure risk, incorporating to analysis techniques all available tools.

CORAS, although, it can be considered quite reliable, is not easily applicable. It requires the forming and cooperation of a group of experts, and there is continuous interaction between groups' members and interested company members. Highly interactive character makes it extremely time-consuming particularly in complex wide area CPS.

CORAS makes a holistic approach for intersectional use since it is not addressed by definition to any particular infrastructures, but rather adopts a generic business model risk analysis process. Brainstorming character makes it really flexible for analyzing any type of systems and infrastructures. To ensure estimated probabilities correctness, CORAS uses key indicators to assure risk level confidence and probability estimation accuracy [33]. Key indicators are quantitative measures that are considered relevant for finding the likelihood of occurrence or the consequence of an unwanted incident. Markov analysis, given the necessary conditions presented in the relevant chapter paragraph may enhance probability accuracy and make

prediction about future states and potential outcomes, allowing more effective treatment.

Being supported by a lot of risk analysis and system analysis methods and tools and also based on judgments of a composite team of experts and its continuous development, CORAS can be adapted and be applicable to any environment and system. As it has already been discussed, CORAS uses interdisciplinary action in its brainstorming and highly interactive procedure where different expertizes' personnel, risk analysts and interested stakeholders and company members from whole organization hierarchy participate. Moreover, CORAS is widely used, offered with desktop graphical tool and it is well documented. It uses trusted supporting submethods to support its operation. Brainstorming, interactive analysis process, where a group of experts is involved, makes assessment process valid. CORAS is a subject of continuous analysis, research and development.

In [32] it is explained how CORAS threat diagrams can capture elements of dependencies and mutual dependencies between system components and expand its use to complex systems or Systems of Systems (SoS) like CPSs are. Introduction of dependent threat diagrams is suggested. Depended threat diagrams are threat diagrams which also express the property of context dependency. In such cases it is desirable that the analysis is decomposed such as the sum of the analyses of its parts contributes to the analysis of the composed system and composing the results of already conducted analysis of its parts into the risk picture for the system as a whole. More over the use of FTA and FMEA/ FMECA may indicate system dependencies between system's parts, although it is not possible to identify dependencies and interdependencies between system or system's elements and other systems and external environment. As a whole, CORAS is an asset oriented methodology.

CORAS can be considered appropriate for use in operational cyber (informational) and physical layers. CORAS submethods FTA, FMEA and HAZOP have a more technical character than operational and strategic making it suitable for low level risk analysis. Of course in terms of abstraction and conceptualization it could be successfully used for higher layers risk analysis according to customers' preferences. Furthermore, Interacting with customers it identifies assets to be protected, defines analysis scope, objectives and analysis focus, having a common understanding of analysis objectives and scope between the participants. Targets and risk are viewed from many different views and competences and visualized using method's graphical tool, for better understanding. We should point that, CORAS is a qualitative risk assessment methodology.

Multiple methods like HAZOP, FTA, FMEA, FMECA, CRAMM and other brainstorming techniques and methods like PHA can be used to support CORAS. So, multiple risk view is achieved with this highly interactive methodology. Graphical representation eases analysis processes visualizing elements and their interaction. Risk indicators assure risk assessments are realistic and constant. Finally, graphical representation

of system assets and the appearing relationships as well as the application of supporting methods like Fault Tree Analysis help the detection and identification of potential vulnerabilities.

4.1.4.1 HAZOP

HAZOP is described in [35, 36]. This method is a brainstorming, structured process of identifying assets, vulnerabilities, threats, causes that create vulnerabilities, especially identify operability problems that may lead to nonconforming products and calculation of risk using qualitative criteria. According to HAZOP the risk is determined by the differential operation of the systems from specific standards which have been prescribed during the design phase.

HAZOP procedure consists of the following steps:

a. Dividing the system into sections
b. Choosing a study node
c. Describe the design intent
d. Select a process parameter
e. Apply a guide word
f. Determine causes
g. Evaluate consequences/ causes
h. Recommend action: What? When? Who?
i. Record information
j. Repeat procedure

HAZOP uses guide words to provide systematic and consistent means of brainstorming potential deviations to operations. The guide words are:

a. No – abnegation of the aim
b. Quantitative increase in a parameter
c. Quantitative decrease in a parameter
d. As well as – an addition activity occurs
e. Part of – qualitative decrease
f. Reverse – contradictory of the intention
g. Other than – absolute substitution

HAZOP is best suited for assessing hazards in facilities, equipment and processes and is capable of assessing systems from multiple perspectives:

a. It assesses system design to meet customers' specifications and safety standards and identifies weaknesses in the systems.
b. It assesses environments to ensure that systems are appropriately situated.

c. It assesses engineering controls, sequences of operations and different operational modes.

HAZOP is helpful when confronting hazards that are difficult to quantify, like hazards rooted in human behavior and performance. It is also helpful when hazards are difficult to be detected, analyzed, isolated, counted etc. It is a systematic and comprehensive methodology and it is simpler and more intuitive than other risk assessment tools. It has the disadvantage that does not assess hazards involving interactions between different parts of systems or processes. It cannot set risk rankings and priorities, but analysts may build in such capability if it is required to.

HAZOP makes a qualitative estimation of risk. Moreover according to the specifications of the method itself is suitable for risk analysis in cases where the effects lie in the area of physical security equipment, personnel and casualties in industrial environment. HAZOP is a time consuming procedure and it is essential to have access to detailed design and operational information. The method provides a thorough analysis, but at the cost of considering many deviations that do not result in adverse consequences of concern.

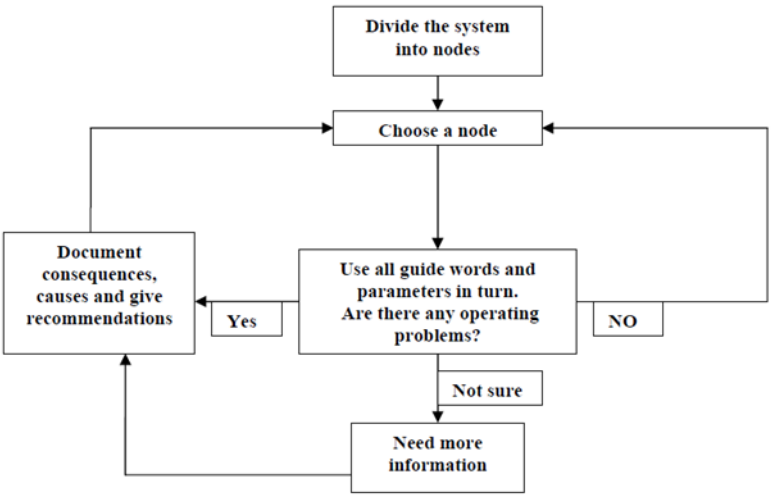


Figure 20: *HAZOP*

4.1.4.2 Fault Tree Analysis – FTA

Fault Tree Analysis (FTA) [37, 38] is a deductive reasoning failure analysis (from system failure to its causes). It describes relationship between hazards and causal factors leading up to hazards. Fault is used to provide understanding of how component failures affect overall system function. Fault trees are useful for understanding any type of random risk, including

incidents caused by natural phenomenons, human error and equipment failure. FTA is a technique that uses a graphical representation of all possible event combinations inside a system. These combinations may cause an undesirable system condition to come up. The most serious from undesirable conditions that can be met is selected as the Top Event. Next a tree diagram is constructed. The tree construction starts with hazards and works backwards to find the hazard causal factors. Tree's branches represent sequences or single events which when coming true may lead system to the most dangerous conditions, the Top Event. Events are combined using the logical operators AND and OR from Boolean algebra. Beginning from the top of the tree (Top Event), possible events which could cause this event are researched. This procedure is repeated, working in the reverse order, from higher levels to root of the tree. Events in lower branches and nodes are researched in order to identify events that sequentially could cause events at higher nodes and branches. So, gradually base conditions that could trigger next level/ branch conditions/ events are discovered, finally leading system to Top Event. In parallel, probability for each condition/ event appearance is estimated, permitting calculation of total probability related to Top Event.

It is apparent that overall risk for selected non-desired state defined as Top Event at the top of the tree diagram can be estimated based on partial risks appearing in tree hierarchical distribution. FTA provides a more in depth understanding of a system as the tree's high level nodes expand deeply.

4.1.4.3 FMEA

FMEA [39, 40, 41, 42] is a detailed failure identification procedure or more correctly identifies deviations from standard functionality or product standards related to predefined standards set during product or system design stage. Failure is *"the non-performance or inability of the system or component to perform its intended function for a specified time under specified environmental conditions"*. It is usually applied after initial stages of design and system manufacturing in order to permit in the future quick, accurate and effective fault detection in operation and production stage. A collection of possible deviations and malfunctions is gathered in order to compose a complete guide. It takes into account not only technical characteristics of systems, subsystems and devices, but examines the interference among them and extends to provided functions and services. It can be applied during whole system lifecycle on purpose to specify the correct functionality according to the predefined standards. Also FMEA detects consequences caused by faults or threats appearance. It is a graphical technique of analyzing any failure of each component and relating the effects from the failures to the system. It investigates possible modes of

failure and from them detects and identifies consequences. So, structural weakness in the design can be identified before implementation.

Procedure concludes to defining Risk Priority Numbers (RPN), in other words sets prioritization to confront dangerous situations using the criterion of assessed risk that characterizes systems, functions and devices. RPN are expressed as function of level of consequences, probability of threat appearance and probability of threat detection. Mathematically expressed as the product of these parameters:

$$\boldsymbol{RPN = Severity \times Occurence \times Detection}$$

RPN is scaled 1 to 1000 using standardized values to estimate product factors.

In case of cyberattacks against CPS, combined or hybrid attacks, given the complexity of CPS system, method appliance is very time-consuming because a number of parameters should be examined in depth requiring a lot of research. FMEA is considered effective for causes and consequences detection in small systems and not wide area dispersed CI CPS. It cannot estimate complex consequences affecting population and State. To adjust method to cover this point it should be applied in successive hierarchical levels to discover hierarchically consequences and interdependencies between successive levels finally applied to CI environment and population.

Because of the technical character of this method it is necessary that it is implemented by specialized personnel knowing in depth its application and systems under analysis. Because of system complexity, analysis should be implemented by accordingly and appropriately specialized team members.

From the outputs of FMEA, FMECA can be continued to consider the importance of the failures to the system. To measure the severity of these failures, FMECA considers the severity of each failure and its related probability of occurrence. So, it is possible to focus on areas where failure occurrence may lead to catastrophic (critical) occurrences.

4.1.5 CYSM

Before start to explain about the CYSM methodology and its previous one, it is better to understand some basic things. First of all, according to the Regulation (EC) No 725/2004 **port facility** is a location where the ship/port interface takes place; this includes areas such as anchorages, awaiting berths and approaches from seaward, as appropriate. Moreover, **port** is a specified area of land and water, with boundaries defined by the Member State, in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport Operations [Directive 2005/65/EC].

The importance of Port Security is very high. More specifically, the port security is of paramount importance for Europe as 3.5 billion tons of freight is loaded and unloaded in EU ports every year and 400 million ferry passengers are transported every year. Furthermore, Greece is a maritime nation since the times of ancient Greece and has ranked 4th globally in 2011. Port Security breaches pose direct threats to life and property and have the potential to cause serious economic damage to operators, and users throughout the supply chain. Therefore, Regulation E.U. 725/2004 and the Port Directive were developed, laying down requirements with regards to Maritime Security.

With the term **Critical Information Infrastructures Protection (CIIP)** we refer that commercial ports are large- scale infrastructures hosting information systems that their degradation/ interruption/impairment has serious consequences on national security, economy, health, safety or welfare of citizens.

Figure 21: *Port Environment*

All Critical Infrastructures (CI) (including transportation ones) are increasingly dependent on the evolving information infrastructures – the public telephone network, the internet, and the terrestrial and satellite wireless networks – for a variety of information management, communications, and control functions. The large-scale infrastructures of commercial ports follow this norm. Thus, the degradation, interruption or impairment of their ICT systems has serious consequences not only on the economy and the general population but on other dependent infrastructures, as well.

The **Port Information and Communication Technology (PICT) system consists** of the following layers:

1. *Physical infrastructures* (e.g. buildings, platforms, gates, marinas, data centers etc.)
2. *ICT infrastructures* (e.g. network, equipment, satellites, servers, relay stations, tributary stations etc.)
3. *Systems and software* (e.g. transmission systems, data identification, maritime navigation, Enterprise Resource Planning, ticketing, Geographic Information Systems, port resilience systems etc.)
4. *Information and electronic data* (e.g. marine and coastal data, trade data etc.)
5. *Services* (e.g. invoicing, navigation, luggage/cargo/vessel management, logistics, e-health etc.)
6. *Users/actors:* (a) internal users (e.g. administrators, personnel), (b) external users (e.g. port authorities, maritime companies, customs, insurance companies, IT and commercial providers etc.)
7. *Other equipment* (e.g. fire alarm systems, CCTV etc.)

A PICT system is secure if all the assets in the above seven layers satisfy all three dimensions of security, i.e. confidentiality, integrity, availability. The existing maritime security standards, methodologies and tools concentrate only on the physical security of the ports (safety), i.e. they manage only the physical risks. Physical security (safety) is considered as a sub-domain of the Information Security knowledge field.

Nevertheless, the port ICT systems face various kinds of physical and cyber threats and vulnerabilities. A holistic risk assessment method for these infrastructures should take into account multiple characteristics and should be combined with physical risk assessment methodologies for ports, as well as with ICT risk assessment methods, or best practices.

The static nature of most risk assessment models (e.g. CRAMM, OCTAVE, ISO27005, NIST-SP800-30 etc.) is an open issue; since existing risk assessment methods depict a snapshot of a transport CI. Transport CI (including port systems) are dynamic systems, a parameter that is reflected on risk as well. Most approaches also fail to connect the risk assessment process to spatial information.

Port infrastructures share a really significant – in number and variable – user-base. In highly critical systems, this factor introduces threats, thus assessing risk on a per-user basis could contribute significantly in mitigating the important insider threat. Such a vast user-base can be also used during the risk assessment process, by using collaborative technologies, in order to ensure more accurate and detailed data collection.

As far as the methodology concern, before CYSM developed there was the S-Port project. More specifically, in order to understand better the S-Port project we should understand the STORM –RM methodology.

In order to meet the PICT system requirements, the risk management methodology STORM –RM modified, in order to be applicable to ports/ICT environments. The creators implemented it as a service in the collaborative port security management

environment S-PORT (a parameterization of the STORM environment).

The STORM-RM methodology is a collaborative and multi-criteria risk management methodology allowing all organization users to participate in the various risk assessment and treatment phases. Precisely, STORM – RM takes into account the requirements of ISO 27001 security standards, and is based on the AS/NZ 4360 and ISO 27005 risk management standards, combining the AHP algorithm in the risk calculation process. STORM –RM treats risk management as a complex multi-criteria and group decision problem enabling different users to provide input for the impact assessment, threat/vulnerability identification and assessment, risk identification and evaluation and the selection of appropriate countermeasures. STORM-RM methodology uses a User Group Model in order to calculate the opinion weights and an Asset Group Model, in order to categorize all the ICT assets of the organization, capture their dependencies, assign to them the specific threats and corresponding vulnerabilities depending to the type of each asset.

The STORM environment utilizes wed 2.0 technologies in order to provide a collaborative security management of PICT system with a series of user friendly services. Remarkable services are (a) the *STORM – RM services* that implement all the phrases of the risk management methodology and offer them as separated services, and (b) the *Security Awareness services*.

In the S-Port project, the SPORM-RM methodology and the STORM environment were extended and customized so as to address the specific security needs of the PICT systems. More specifically, the main parameterizations were the following:

- A new cartography service based on BPMN, was introduced enabling users to design the business processes and identify the related PCIT assets.
- Opinion weights of the risk management methodology were appropriately parameterized in order to adapt to the organizational structure of ports.
- ISPS code specific impacts were embedded into the S-port environment.
- Physical and environmental threats, particular to a port environment, were considered.
- A new taxonomy was introduced, so as to allow the contents of the digital library to take into consideration all the important maritime areas.

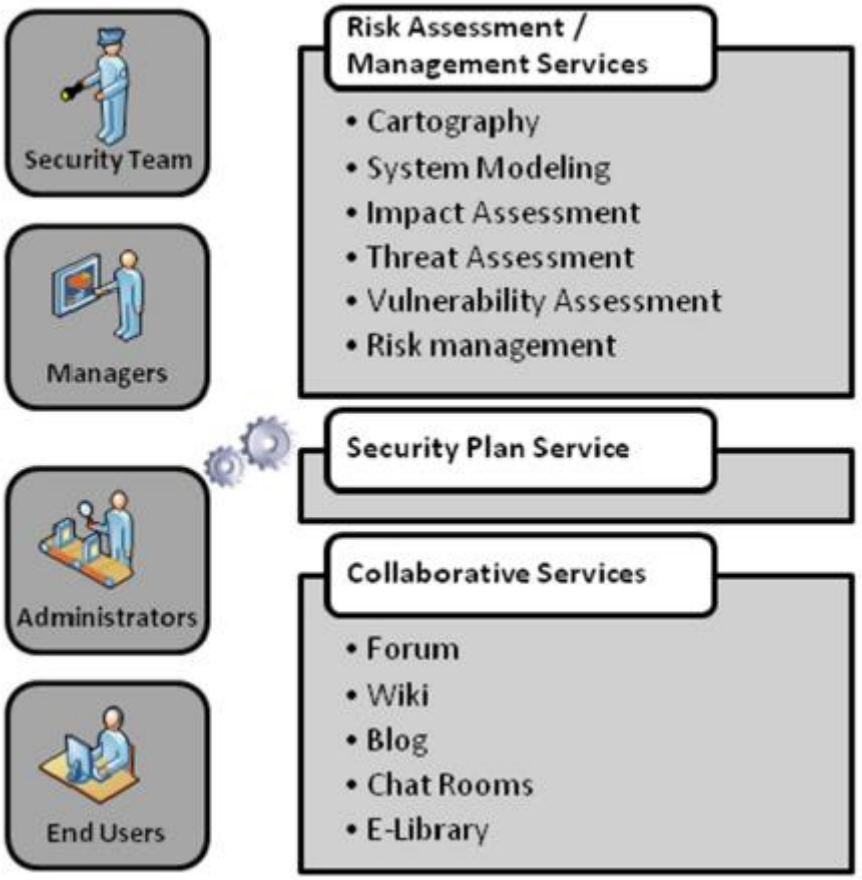


Figure 22: *S- Port Services*

Specifically, through the S- Port services (figure 22) the PICT systems users are able to:

- Identify, design and maintain the business model of PICT systems services through the use of the user-friendly interface of the *System Modeling Service*. Assets are modeled in S-Port on a per e-service basis.
- Identify and assess the impact of security incidents, which is assessed by each user on a five-item scale (1-5). The security officer of PICT is able to view via online forms and charts, print or download the Impact Assessment Results for each port e-service and monitor the personal, group and final results per asset, according to the specific phase of the methodology.
- Identify, evaluate and classify the risks and threats the PICT systems is exposed to, by continuously collecting security knowhow from operational participants of the PICT systems. Threats are assessed on a 1-5 scale, and for each corresponding asset.
- Select reliable and appropriate countermeasures to mitigate the risks the PICT systems are exposed to.
- View the results of risk assessment via charts, or download them in printable repots.
- Develop and maintain the security policy and procedures through the

Security Plan Service.

- Develop a Disaster Recovery Plan including a formal procedure to be followed in case of a disaster.
- Communicate and find daily security problems in the Forum, Blog services.
- Retrieve appropriate security training material in the Wiki service in order to be more confident with the security plans, procedures and their responsibilities.
- Monitor PICT system security requirements, including new laws and regulations, standards and best practices in security and maritime environment with the use of e-library service.

The design of the S –Port system pilot was based on ISO 9646. The tests were performed by the development team in a four-day span, with a total of eight participants. This marked the first successful phase of the pilot for S-Port and it allowed for minor problems to be identified and corrected, in preparation for the pilots of the end users.

The tests were performed by users of the three collaborating ports and they covered all the services of the S-Port systems, namely: System Modeling Service, Impact Assessment Service, Threat Assessment Service, Vulnerability Assessment Service, Risk Assessment Service, Risk Management Service, Security Plan Service, Forum Service, Wiki Service, Blog Service, Chat Room Service, and e-Library Service.

We examine three use cases in order to evaluate the twelve tests above.

Use Case 1: The *Piraeus Port Authority* participated in the pilot, with three users: a) an administrator, b) a security officer and c) an end user. The selected use case was the Car Terminal Service, which is one of the main business processes of this port. It assists the port to serve the demand for transit vehicles in the Eastern Mediterranean, Black Sea, and North Africa. The infrastructures covers two management areas of approximately 190.00 m^2, providing a total capacity of handling 600.000 movements annually, monitored by an integrated management system.

Use Case 2: The *Thessaloniki Port Authority* pilot involved eight users: a) 1 security officer b) 1 manager c) 3 system administrators and d) 3 end-users. During this use case, the users used the S-Port system to model and assess the Container Terminal Service. The 550m long and 340m wide Container Terminal can berth ships with a draught of 12 m. It covers a surface area of 254,000m^2 with an on-site storage capacity of 4,696TEU in ground slots. Activities in the terminal are performed with a Management Information System.

Use Case 3: The *Municipal Port Fund of the Island of Mykonos* participated in the pilot with 3 end-users and 1 security officer, i.e., a total of 4 users. They modeled two services: a) the Cruise Management service, b) the Ferry Management service. Both include the management of ship arrivals, as well as passengers.

The innovations introduced by the S-Port collaborative Information security Management System allow port authorities to provide high levels of confidentiality, integrity, availability, interactivity and interoperability for their critical infrastructures. S-Port services guide PICT systems users to define their impact, identify threats and vulnerabilities and select the appropriate countermeasures, so as to improve the organization's security posture and ultimately maximize port

operations efficiency and productivity. [ ]

The CYSM system aims to aid ports to improve the security and safety posture of their cyber and physical infrastructures. Serving this scope, the system integrates an innovative, open, collaborative, integrated, comprehensive and personalized framework that enables the ports to identify, monitor and treat their cyber and physical risks. The proposed framework incorporates a bouquet of advanced security self-management services (Collaborative Services, Content Management Services and Cyber/ Physical Management Services) that support and facilitate the ports to evaluate their security and safety level. In particular, these services enable the ports to check and control their compliance with requirements and rules imposed by widely used standards, specifications, frameworks and best practices (e.g. ISPS code, and ISO-27001). The collaboration and information sharing within the organizations as well as among the ports are the main principles of the supported self-assessment processes. In order to meet its objectives, the proposed system has been designed and developed upon a set of peak technological and worldwide accepted and mature standards (i.e. SOAP, REST, Web2.0 and AJAX) to build a number of specialized security and safety management processes and tools (such as risk analysis and management mechanisms). The right balance between technical and technological innovation and usability is essential for the development of user-friendly services that help them to solve their particular cyber and physical problems and issues.

The CYSM system aims at acting as the National and European self-management reference point. It intends to provide guides, guidelines and practical advice for all ports as well as for their employees on how to self-assess and self-organize their security issues. In particular, the CYSM system integrates a targeted risk management methodology (CYSMRM) that relies on modeling and group decision making techniques using the collective knowledge of all users, and estimating and rolling up risks (physical and cyber) across diverse target types, attack modes, and geographic levels. CYSM system enables ports' operators to: (i) model physical and cyber assets and interdependencies; (ii) analyze and manage internal/external physical and cyber threats/vulnerabilities; (iii) evaluate/manage physical and cyber risks against the requirements specified in the ISPS Code and in ISO27001.

Figure 23: *CYSM System Architecture*

In order for the CYSM system to meet its objectives, it incorporates a set of advanced security self-management services (Collaborative Services, Content Management Services and):

(i) The Collaboration services foster the communication both between the ports and between the employees and they facilitate the distribution and sharing of the information experience and expertise. They integrate some advanced data collection technologies and tools as well as interactive front-end user interfaces in order to collect "Open Intelligence" and exploit the "wisdom of the crowds" using web 2.0 tools like polls, forums, blogs, etc.

(ii) The Cyber/Physical Management Services provide a straightforward and intuitive approach that can be applied by the ports covering both their security and safety issues and characteristics. These services give the analysis of the cyber and/or physical problems in a unified way. The services examine the overall infrastructures (ICT and/or physical) and enforce common mechanisms, procedures and practices to provide an in-depth and accurate diagnosis of cyber and/or physical risks.

(iii) The Content Management Services provide an intuitive, interactive and graphical way to represent and manage all the security and safety related information and content (e.g. requirements, rules, obligations, recommendations, and advices of the legal, regulatory and standardization framework and regime as well as security and safety content required for automating technical control compliance, vulnerability checking, and security measurement activities).

More specific, one of the strengths of the CYSM web toolkit is that it allows the user to select from an extensive list of preset threats, vulnerabilities and countermeasures or controls to perform a risk assessment on a port facility. Moreover, if necessary, the Port Facility Security Officer, who has administration permissions in the toolkit, has the ability to add new elements that are not included in the preset lists.

Threats and controls are grouped into categories to facilitate their sorting and the subsequent choices to be made by users involved in a risk assessment. More than 90 threats of physical or cyber nature that may happen at a port facility (included in categories such as Physical, Cyber-attacks, Human-caused, Accidental or technical and Other) are identified, which on the one hand have been linked to the categories of assets which can affect (Infrastructures, Physical infrastructures, Hardware, Software and Information), and on the other hand with the facility vulnerabilities that could cause the risk of the threat to become real. Each asset category and each vulnerability is assigned to a set of threats which can affect them. In addition, more than 280 vulnerabilities have also been linked to more than 400 countermeasures to reduce these vulnerabilities and, thus, to reduce the likelihood of a threat occurring or at least to minimize its consequences.

Thus, when performing a risk assessment of a port facility, the CYSM web toolkit selects a series of threats related to the category of assets selected by the users for the facility assessed, and the users assess the frequency with which they think each threat could happen, the impact of failure of each asset and the controls that are currently applied in their facility, so the "brain" of the web toolkit compares these data introduced by the users with the pre-established interrelation to determine the

outcome of the risk assessment, giving as results for each asset the threat level, the vulnerability level and the list of controls that should apply (together with those already applied) to achieve the minimization of the consequences of such threats to the lowest level possible.

4.1.6 Vulnerability Self-Assessment Tool – VSAT

Vulnerability Self-Assessment Tool [45] is an automated method for RA and risk management used in water supply and biological treatment facilities, but can be used to other industrial facilities and companies independently of their size. RA and management procedure are assessed through successive independents stages. It also offers the ability of developing Emergency Response Plan to confront emergency situations taking into account particularities of systems, subsystems and provided services. This method uses a simple automated computer application with comprehensible user interface and offers training aids for quick learning.

At the first stage assets are entered to the application. Assets are distinguished to physical assets (physical plant), personnel, IT, customers and knowledge base (database). Physical assets include the whole infrastructures and IT. Personnel data includes worker data categorized with work location criterion. Generally this method uses this criterion to categorize threats and countermeasures. Knowledge base includes all information related to the whole infrastructures, personnel data, organization certificates, job descriptions, company regulations and functionality restrictions. Knowledge base overlays IT and personnel parts but has different functionality directed to archival support and function. IT includes information processing systems, ICT systems, ICS and SCADA. Customers represent the total units served by the organization, industrial, commercial, residential customers and the State.

Assets can be assessed through menus, submenus and entry fields. Asset description can be entered, modified or assets may be erased. During assets processing each one of them is given a name, description, position (fix), altitude, address, photos and other information.

Countermeasures are distinguished in two categories and menus: Total available and already applied countermeasures. Countermeasures include physical/ technical protective means for example fire-fighting equipment, alarms, barbed wire fences, standard operation procedures (SOP) like cooperation with police, emergency response plans for fire or leaks and IT countermeasures like firewalls.

Countermeasures are also categorized to detection, mitigation and avoidance and business continuation plans. They are further categorized to detection like security cameras, delay like security locks and doors, response like police calling for threats related to human attacks and interference. They are also categorized as preparation, active response and recovery against physical threats. Threat catalogue exists with enrichment capability.

At the RA initial stage all already applied countermeasures should be entered to the

plan. Countermeasure entry, modification and erase are possible. During countermeasures process they are given characterization and description, it is specified whether or not they are already implemented, countermeasure installation and functional costs are given as well as time period that countermeasure is in force. Above mentioned countermeasure categorization is specified and finally assigned countermeasures are interrelated with assets in appropriate matrix.

At the next step threats are distinguished as common or typical and uncommon or not typical while specific threats selection is possible.

Threats are also distinguished as human interference/ action threats like terrorist attacks, asymmetric attacks, and faults appearance during system operation, fires and physical phenomenon like floods. Moreover, threats can be related with specific assets. During threat analysis input threats from current database or new user defined can be selected. In the last case threat characterization and description is given while there is the ability to give more information about adversaries' strength, motivation, etc. Selected threats are assigned to certain assets considered to be their target. All above mentioned refer to human related threats. There is possibility of independent process of physical phenomenon threats using entry data the geographical area of systems. Probability of appearance of such phenomenon is calculated based on available historical data. Threat level, severity and historical damage data are also provided by the application.

Having already gathered threats, assets, environmental data, countermeasures, it is possible for the application to calculate probabilities and risk.

VSAT is a qualitative RA method. It is a multi-dimensional approach, estimating risk, preparing emergency response plans and helping with business continuation plans preparation for recovery, after emergency situations and impacts. Risk R is expressed as function of Consequences C, vulnerabilities V and probability of threat appearance T:

$$\boldsymbol{R = C \times V \times T}$$

Vulnerability is expressed as function of probability of appearance and action of threat and implemented countermeasures. It reflects assets weak points which can be exploited by adversaries. When vulnerabilities are identified they are assessed to determine their vulnerability level or the potential adverse consequences. Four levels are usually sufficient to characterize vulnerability level: low, moderate, high and very high. The exact definition of these levels will be location and condition-specific for each utility and should be defined in that context, although they are somewhat subjective.

Having determined the two fundamentals aspects of risk, probability and consequence, for each of the vulnerabilities a two dimension matrix is built to evaluate risk.

VSAT advantages are zero cost, easy implementation without the need of specialization in RA subjects. It is designed for water supply facilities application, but

the application permits the use for different kinds of infrastructures and CI. Risk objectiveness depends on the user judgment and experience. These two parameters are critical factors for the successful implementation of this method. VSAT can calculate risk in two ways of different accuracy: Based on optimal probabilities of threat appearance defined by users and considering probabilities equal to 100%. During risk calculation only one threat-asset combination is taken into account. It is appraised that this method is ineffective against simultaneous or combined threats action, where always procedure should be repeated for each possible combination, but cannot estimate composite probability scenarios. This analysis permits organization executives to allocate budget to protect critical assets from severe impacts. It can help utilities identify potential vulnerabilities and evaluate the potential mitigation of those vulnerabilities, along with documentation of the decision process, rationale employed and relative ranking of risks.

VSAT does not consider dependencies or interdependencies between assets. VSAT uses a typical scaling for probability estimation based on historical data. For critical assets considers probability of occurrence as high as 100%. As a whole, VSAT is a qualitative method. Generally, VSAT takes into account CPS characteristics of wide area coverage and asset dispersion. Moreover, it addresses all possible layers, physical, cyber, operational and strategic. It is possible to address needs and interests of different customers and stakeholders.

Historical and statistical data are used using typical scaling and estimating frequency of events to estimate probability. On absence of such data conditional probabilities are used considering event occurrence certain. When estimating risk, method makes the assumption that risk is estimated independently for different locational and conditional characteristics, enhancing scope of method.

VSAT is an asset oriented method, but method examines asset-threat combinations during risk assessment procedure, repeating procedure for each different combination. Furthermore, VSAT is proposed by American Petroleum Institute and Department of Energy for use. It is provided for free with complete documentation and it is consistent with NIST standards. VSAT is implemented using an easy and practical desktop application. Complete documentation and support is provided in the form of documents or instructional videos. It is very easy and intuitive in implementation. It can be used either from technical personnel, risk analysis experts and top managers due to its simplicity. Also, VSAT tool with proper context customization can be used for other sectors apart from water; chemical industry, natural gas and oil. Tool design permits further customization very efficiently. Moreover it takes into account customers and other stakeholder involvement to estimate risk.

As already stated VSAT makes a holistic approach that permits its use in different application layers and even different energy sectors. Assets are retrieved from VSAT repositories but there is the ability to define new user defined assets. Detailed asset description and geographical fix are included in asset definition. Threats, as assets, are retrieved from VSAT repositories, but there is also the ability to enter user

defined threats. Relevant information about threat motivation and strength are included in threat definition.

Vulnerability identification ability factor has already been discussed. It is a rather subjective assessment describing vulnerability in relevant scaling. This method uses typical qualitative scaling low to high to express vulnerability, probability and risk.

Finally, VSAT considers critical risks by assuming probability of occurrence of threats impacting critical assets as high as 100%, using the resulting values in the prioritization process, apart from considering optimal probability values. Critical asset characterization remains only in analysts' judgment, while method does not distinguish critical and non-critical elements by its own. VSAT is a method for risk analysis for water supply and biochemical facilities helping also in developing of Response Plans.

4.1.7 Security Vulnerability Assessment - SVA

The Security Vulnerability Assessment (SVA) method of the API shown in [46] is used as a structured method for risk analysis in SCADA systems of industries and oil refineries. These plants are characterized by high risk facilities and considered as targets for terrorists and there is a high probability of severe accidents and hazards occurrence.

The SVA makes qualitative approach to RA and it is much based on the analysts' judgment and experience. Method includes procedures for evaluating likelihoods of successful exploitation of system vulnerabilities. Risk is function of likelihood of successful attack against the system and its consequences. Likelihood function is defined as the probability of system being targeted by an attacker, the level of threat posed by the attacker and the level of vulnerability of the system. Availability of information, analysts' knowledge, experience and skills are critical factors for risk assessment success.

Target attractiveness is a risk-affecting factor, defined as a surrogate measure for likelihood of attack; it is a composite estimate of the perceived value of a target to an adversary and his degree of interest in attacking it. Factors affecting target attractiveness are: potential of causing maximum casualties, damage and financial losses to companies, geographic regions, national infrastructures, recognizability of the target, collateral damage, proximity to national assets and landmarks, security measures, asset exposure, symbolic targets and high dangerous materials presence.

Wide range of versatile attack consequences on oil facilities, allow the characterization of criticality. Consequences include:

a. Injury or death.

b. Environmental consequences

c. Direct and indirect damage to the company's network of fuel distribution and supply of petroleum products, partners and the effects on the

national economy and the local market and operation and the operation of powered industrial units.

d. Reputation damage

e. Exposure to press and media

f. Consequences to nearby populations because of environmental damage and danger of hazardous situations after explosions.

Criticality of these facilities makes them high priority target for adversaries. Criticality raises risk characterizing these facilities.

Threat sources are considered terrorist organizations, activist groups, competitors' interests, organized crime and hackers. Infrastructures criticality makes it attractive target for threat originating from other national entities; they are assumed to use asymmetric and unconventional tactics to attack CI. Threats may be categorized as internal and external threats and internal working as colluders with external threats.

Method identifies vulnerabilities which associate assets with specific threats that could affect the business and create threat scenarios. In critical cases services and assets are analyzed, where possible, into components and the component – processes are again analyzed for the resulting subsets of assets.

Risks are examined in two views, generic and specific. The first aims at discussing overall losses, attack consequences and relevant risks for the whole infrastructures and supporting functions. At this point risk assessment focuses in system access mechanisms, measures of physical surveillance and perimeter security relevant to assets characterized by high risk or value.

Second point of analysis applies to assets underpinning the achievement of general security and examines all the relevant points that support the operation and support the assets and services that were analyzed in the first level. Estimation of possible attackers' course of action is made. Risk is higher for assets characterized by high criticality, i.e. potential targets gain higher priority.

SVA consists of the following **five** stages:

a. In first stage assets, particularly critical assets are identified. Critical functions, infrastructures and interdependencies are identified. Existing countermeasures are identified and evaluated. Impacts, hazards and consequences are identified and evaluated. Selection of targets is made for further analysis. Method provides complete instructions for assets identification and information gathering as well as guidance for Critical assets, functions and infrastructures characterization. It addresses all asset including supporting infrastructures, telecommunication, physical and cyber security etc.

b. Second stage is about threat assessment. Adversaries are identified and characterized and targets' attractiveness evaluation takes place. Adversaries are examined in detail; strengths, skills, background, capabilities and motivation are examined. Threat level is evaluated in typical qualitative scale. Operational records

about past events are valuable sources for threat identification.

c. In third assets and threats pairing takes place in order to identify potential vulnerabilities, degree of vulnerabilities. Implemented countermeasures and their level of effectiveness are examined. Finally are formulated threat scenarios taking into account target's attractiveness. Threat/ events scenarios are defined and specific consequences are evaluated. Vulnerabilities are evaluated in typical scales like threats.

d. In next stage risk assessment of successful attacks takes place, where risks are estimated based on probability of events occurrence and their effects and then risks are prioritized.

e. In the last stage countermeasures are analyzed in order to apply the proper mitigation, avoidance, encountering strategies, etc.

In risk hierarchy high-value priority targets and their probability of being targeted are given. Then based on the background information, existence of potential threat is estimated, taking into account vulnerabilities. Assets are characterized in terms of attractiveness for each adversary; threats are identified and characterized for each of the critical assets. Identifying the critical assets their importance is analyzed and dependencies, interdependencies and supporting infrastructures are taken into account too. Potential security vulnerabilities that threaten asset integrity or services are identified. Risk assessment and risk ranking is the next target of RA process. Risk is expressed as the likelihood a specific threat targeting and attacking a specific target or targets' vulnerability to cause a given set of consequences. Criticality is determined by asset's importance and consequences when targeted and attacked and not by just considering important parts for organizations/ companies operation. When assets are both critical and attractive they are considered as potential "targets".

After having performed SVA method a quality review follows in order to ensure that method produced correct results. It is achieved by repeating SVA procedure by experienced and knowledgeable individuals. Criteria of consistency throughout the procedure, explain and identification of assumptions, identification of major a certainties are used for results validation. Once SVA results are validated it is time for operators to prioritize risks. Then higher risks are identified and the reasons for which assets are characterized by high risk are looked up. These researched factors are called risk drivers since they drive risk to higher levels than others do.

SVA is a predictive method meaning that it has an investigative nature, identifying previously unidentified threats and uses past security related events to focus on potential future events.

Standard tabular forms are used for asset, vulnerabilities and attackers identification. Preparation of a comprehensive analysis requires the cooperation of extended panel of staff, including experts in physical security and cybersecurity.

SVA is a structured and detailed vulnerability assessment method. But it is quite

complex too. It suits CPS and CI nature by considering complex systems and examining dependencies and interdependencies for malevolent attacks. It is entirely oriented for CI application, focusing on petroleum and petrochemical industries. It is not a simple and intuitive method, but demands the constitution of a composite team of different expertized individuals. It examines criticality for both company owners and society taking into account multiple aspects of criticality. It is an asset oriented qualitative RA method focusing on critical assets using structured criteria to categorize and scale assets criticality. SVA provides complete guidance formulated in structured, detailed instruction matrices, checklists and questionnaires for asset, threat, vulnerability and dependencies/ interdependencies identification and Criticality classification. It also gives importance to information and intelligence and provides means for information gathering, pointing to appropriate information sources and cooperation with national authorities. Final it aims at adopting the appropriate policy, countermeasures and strategies in accordance with RA results which can be generally categorized as Detect, Delay, Deter and Respond countermeasures.

Method considers dependencies and interdependencies both internal and external, on facilities or other sectors, like energy, water sources, but also supporting ICS and SCADA systems. It provides help in identifying such elements using checklists and reference tables. This practice drawback is that it may be ineffective against non-standard system attacks, rare or unpredictable attack sequences. Also, no particular method is proposed for probability assessment. A qualitative very low to very high scale is used to measure probability of occurrence.

SVA is a qualitative risk assessment method and takes into consideration geographical factor. Moreover, SVA considers assets of higher risk as critical assets, asset attractively to attackers, high level of consequences and high level of vulnerability. Security risk is a function of consequences of a successful attack and the likelihood of that successful attack, where likelihood is a function of target attractiveness, threat level and vulnerability level. Risk operators seek for assets with higher risk to determine mitigation strategies and then look up for the factors that make risks higher for the specific assets. These risk factors are called risk drivers since they drive risks to higher levels for some assets than other.

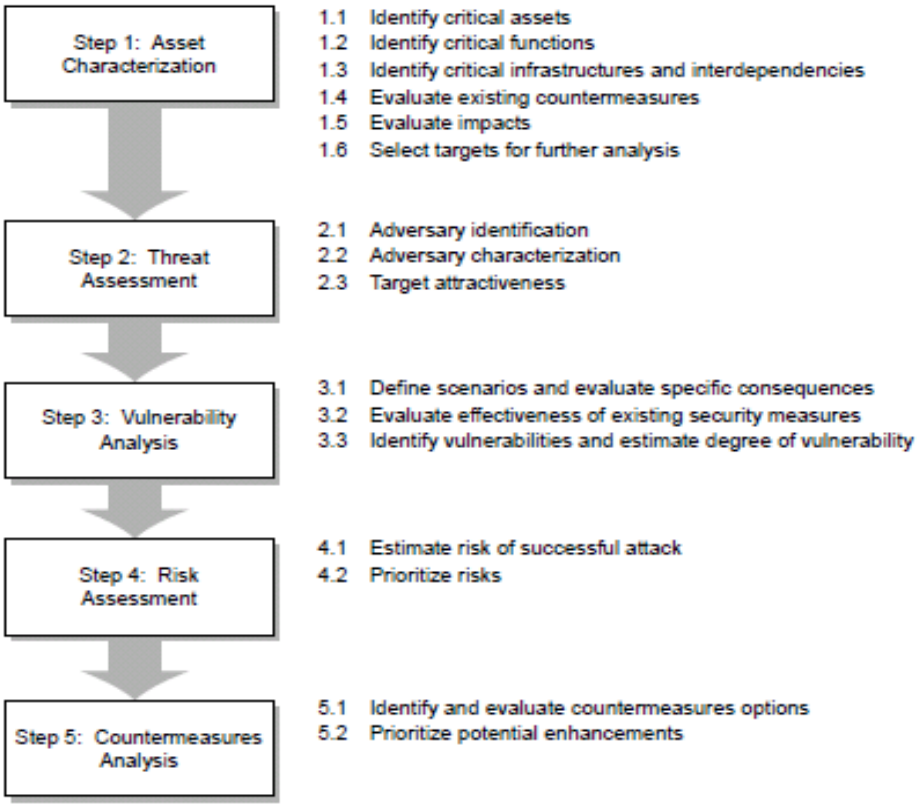


Figure 24: *SVA methodology*

SVA is an asset oriented method and has been developed by the API and DOE. Being developed by top level authorities, automatically adds validity to this method. Complete documentation and support is provided. Moreover it uses trusted national methodologies and standards for method support like Vulnerability Analysis Methodology for Chemical Facilities (VAM-CF) and API RP-70 Security for offshore Oil and natural Gas Operations.

The practicability is accompanied with checklist, reference table and complete documentation. Method has been designed for use in the petroleum and oil refinery industry, but it is possible to be used in other sectors too.

Although method has been developed with petroleum and oil refinery industry in mind, it is assumed than can be used in any other critical fields/ sectors for risk assessment, other than its original orientation. Method uses target attractiveness that is a combination of asset value and attackers' interest in attacking particular assets, using this factor in risk estimation. A complete set of criteria in the form of reference matrix describe asset, define target attractiveness and criticality and some vulnerabilities. Assets are described in technical detail focusing on processes and sub-assets which may contain petroleum or hazardous chemicals and key assets which possibly may cause public impacts.

Method uses target attractiveness. Threats are described in full detail including strength, capabilities, motivation. Method identifies possible attackers from a provided list including insiders, external threats, and colluders with external threats, terrorists, activists, criminals, disgruntled employees and contractors. Analysts should seek information on attackers interested in attacking specific assets. SVA is experience based but also predictive, meaning that is capable of identifying new threats, making use of previous security related events and focusing in future events, including scenarios that have never happened before. It is based on past events, threat assessments, events around the world and intelligence report. If no historical data is available then method considers that potential malevolent events are credible. Security specialists with knowledge of threat assessment, terrorism, weapons, unconvential warfare and cyberwarfare participate in the analysis team. Threat assessment includes three stages:

a. Adversary identification where threat information is evaluated and threat categories and potential adversaries are identified.

b. Adversary characterization, where each potential adversary is evaluated and provided with an overall threat assessment ranking using known or available information. The given ranking varies to very low to very high probability of attacker existence based on available information, historical events, identified capabilities, motivation and intentions in the form of a simple practical assessment table. Target's attractiveness criteria are presented and adversary's interest in attacking specific asset ranking is provided too.

c. Estimation of target attractiveness is based on proximity to symbolic targets like national landmarks, high corporate profile, like defense industries and contractors and impacts to environment, vast magnitude of consequences or targets being exposed make them attractive.

Also, SVA method considers some threats to be continuous while others to be periodic, but also considers that threats are capable of delivering catastrophic impacts. Method provides complete checklist and reference tables for threat identification, adversary characterization and target attractiveness estimation.

Vulnerability is considered a weakness that can be exploited by adversaries, to gain access, damage or steal an asset or disrupt a critical function. It is a variable that indicates the probability of a successful attack given the intent to attack an asset. Vulnerability analysis includes relative pairing of threats and assets to identify potential vulnerabilities related to process security events. This includes identification of existing countermeasures and their effectiveness in reducing vulnerability level. Vulnerability level is evaluated with the formulation of security related scenarios examining possible attacker's action against assets. Vulnerability level is measured from very low to very high in standardized scale using

countermeasure effectiveness criteria. Method provides detailed vulnerability analysis worksheets/ risk ranking and countermeasures forms. Furthermore, SVA uses standardized qualitative scaling varying from very low to very high in order to measure threat level, target attractiveness, probabilities of occurrence vulnerability and risk level.

SVA considers target attractiveness and a set of consequences that affect target attractiveness too, to define critical targets, where magnitude of consequences, critical for national economy, human fatalities and symbolic asset character are included among these consequences. It also considers dependency and interdependency elements as possible critical asset characteristic. Criticality is defined both in terms of potential impacts to workers, environment, community, company and the business importance of assets. Criticality is determined by comprehensive examination of facilities, hazards and impacts, assets and subassets comprising the facility and organization critical functions. So, analysts gain an understanding of assets and functions critical to the organization operations. Criticality refers not only to critical assets but also to critical functions, processes, infrastructures and dependencies/ interdependencies taking into consideration countermeasures and possible impacts and consequences. SVA mostly addresses to critical company functions and assets. So, vulnerability analysis presented in the previous paragraph applies the same for the case of both critical and non-critical assets and functions and this is the only distinction present. If an asset is considered both critical and attractive then it is considered as a potential target.

Finally, the objectives of conducting a SVA is to identify security threats, hazards and vulnerabilities relevant to facility and to evaluate countermeasures to provide protection of public, workers, national interests, environment and company. With this information vulnerabilities can be assessed and strategies can be formed to reduce risks as required. SVA assists management and decision making on the need of countermeasures selection to address threats and vulnerabilities. It characterizes the facilities in order to make it understandable what are the critical assets that need to be secured. It characterizes attackers in terms of their strength and motivation and desirable endstate after their attack. Determine risk by defining probability of attacks and magnitude of consequences, then rank different risks and decide about mitigation and risk reduction strategies taking into account cost/ benefit criterion.

4.2 Conclusions

Following the presentation of the above RM methods and methodologies the conclusion is that barely some of them fully satisfy the specific requirements for a RM methodology applicable to CPS.

Most RM methodologies and methods provide only a very generic guideline, dealing with their subjects in a holistic way. Much freedom is left for users who are allowed to act based

on their own experience and judgment. Analysis is conducted without any detailed, strict and well-structured guideline framework. Users are forced to use any brainstorming techniques and analyzing tools to support risk management process and cover these methodologies inherent weaknesses, but also there is no limitation in their use. This is particularly viewed in higher level and old fashioned RM methodology.

Apparently, such adopted practices showed are much more complex and required special knowledge about theoretical subjects like systems theory, graphs theory, mathematical formalizations etc.. Moreover, the extremely high complexity of CPS obliges the composition of a large analysis team being consisted of experts of different domains; systems engineers, security engineers, computer scientists, electronic engineers, electrical and mechanical engineers, managers, risk analysts. Each one specialized in his own specialty domain. They are all needed in order to have a complete view or model of the system and examine all different nature subject and parameters. Obviously, such procedure would be very time consuming too. Due to the high complexity of such systems these drawbacks seem to be unavoidable.

Interdisciplinary and multidisciplinary approach is needed to deal with such systems. CPSs combine many different technologies: mechanics, electronics, information technologies etc.. And all these different technologies should be combined and intergraded in unique systems, while ways of interrelations should be researched.

History of cyber-attacks against large scale cyber physical systems has few proven incidents to show. Conditions for such attacks have never been proved to meet during attacks neither have been proved unsuccessful efforts. There has always existed significant difficulty to distinguish accidental failures from cyber-attacks in many occasions. So, there is insufficient historical evidence and statistical samples are poor to provide accurate probabilities estimation based on observed attack frequencies. NIST approaches on risk and probability estimation rely on such logic approaches for probability quantification, while ISO 27005:2011 makes a simpler qualitative and rather abstract approach depending more in operator's experience and intuition.

Semi-quantitative and quantitative approaches based on historical data present one more point of inaccuracy: they count attacks during periods of time and use extracted attack frequency for defining qualitatively or quantitatively probabilities of occurrence. But when a zero day attack first happens, a time period follows where attacks are successful multi effective countermeasures are implemented. Any other attacks then become ineffective until a new vulnerability or exploit appears. So, frequently and probability of attack should be measured for time periods from exploit or vulnerability identification to the time that they are effectively protected based on attacks that happen in this particular time period. The longer is this time period or the more of attack happen, then the highest are the probability of attack and risk. Successively, this means that risk and probability are considered higher in reality.

As CPS are usually characterized by dispersion over wide areas, where different conditions are meet in each area and different value are installed in each one of them, risk varies among all system's geographical areas. So, locational risk should be taken into account.

Criticality is another matter of high significance. Many methodologies either do not examine criticality or examine it superficially. Consequences magnitude is used as primary criterion to define an asset or service as primary or critical asset. OCTAVE is applied on organization critical assets. OCTAVE considers critical assets as these which are crucial for organization functioning. THIRA considers thresholds for threatening events. If an event's quantitative or qualitative description suits with the defined threshold then action should be taken to deal with specific event. For example if a cyber-attack causes financial losses greater than $500,000 then it should be considered as a critical event bringing critical consequences. So, as seen time to recover, cost to recover, alternative solutions and backup services are not examined as criteria neither temporal or permanent unavailability consequences. That means that some asset may be treated as critical assets and in turn this is translated to extra protection cost, endangering that real critical assets may remain unprotected. One more significant factor to consider about criticality is that criticality may be considered for the field of organization like OCTAVE or other methods consider criticality of different entities or population like THIRAS does. So, to whom applies criticality is an important question that should be taken into account and answered to define critical assets.

Asset originating point methodologies, in other words asset oriented methodologies may be considered the most suitable for use in the case of wide area CPS and CI. High system complexity and vast number of system components makes a high number of potential targets while systems vulnerabilities are not easy identified and systems protected. Poor historical data about attacks against such systems and infrastructures is not indicative about the potential threats systems may face in the future. Zero day attacks, low probability events and black swans, retaining severe consequences are not easy to be predicted. So new attack types may arise and unknown vulnerabilities may be exploited. These facts make asset oriented analysis most effective as it covers all identified assets risks. Vulnerability analysis based on known data will be ineffective against first seen attacks and vulnerabilities, which though may cause critical consequences. Threat oriented analysis solemnities specific known threats or threats considered of high probability. Additionally threat oriented analysis should be iteratively executed for each known threat, evaluating system and its vulnerabilities each time against specific threat. Procedure is time and effort consuming. Unknown threats will not be examined and not all threats prove to be relevant to systems assets and vulnerabilities. The same disadvantage applies to vulnerability analysis. The conclusion is that in vast and complex systems methodologies other than asset oriented may leave assets unprotected against unpredicted threats and vulnerabilities.

Some methodologies provide standardized guidelines, questionnaires and lists embedded or not to automated tools repositories to detect and identify assets, threats, vulnerabilities, dependencies and interdependencies or other elements relevant to risk analysis. Although this kind of structured methodologies may be really helpful for risk analysts or other specialized or unspecialized operators it may be dangerous if they are not reviewed on

regular basis. It is possible for them not to be able to identify zero day attacks, first time identified vulnerabilities, unconventional or rare threats, making them ineffective against them.

Experts' judgment always has a significant role and weight in assessment process. Many methodologies are not easily manageable, although seem to be well structured like attack trees. Process duration and analysis depth and width may increase; experience and intuition is capable to restrict these actions considering the analysis to realistic, practical and cost effective process results. As seen in comparison table of Appendix A, risk analysis methodologies generally tend to be less structured giving much weight to personal judgment and freedom to capture various, different or unpredictable aspects.

Many methodologies do not consider residual risk. They are oriented to risk optimization, meaning that risk assessment procedure is iterated until the optimal combination of countermeasures is applied, amplifying systems' defenses, while some methods considers residual risks but residual vulnerability too, remaining after available countermeasure application. When referring to CI accepting residual risk is not a permitted option, since consequences still remain in high level even if probability is low.

Attack, event, vulnerability and fault tree seem to be an effective approach being efficient solutions either by themselves or being used as sub methods and tools in other methodologies. These methods vary in characteristics and can be amplified with additional knowledge like partial vulnerability; partial attack stages probabilities, return of investments for partial attacks, return of attacks. Short paths may indicate cost efficient attacks. They can provide guidance for later risk management and countermeasure policy applications. Especially Fault Trees appear as very useful tool in a lot of well-known and trusted methodologies. Methods drawback is that they are not easily managed, but analysts experience and intuition may restrict this kind of analysis to realistic and cost effective paths.

Summarizing conclusions it seems that there is not any solid methodology oriented to CPS dual essence, dynamic character, size and complexity, used over wide areas connected to CI, able to cover their specific requirements and characteristics. As said these characteristics are magnitude and complexity and possible unpredictable and various states not easily defined and measured, making it difficult to be examined and address this problem in completion, accuracy and with sense of certainty and efficiency.

New era coming is characterized by the intense, multiple cyber threats, while human critical activities and infrastructures, industrial production and energy sector heavily relies on information technology and CPS applications. Information and CPS are extremely high valued targets as if attacked the whole state and population can be severely affected. Although technological means may become available to defend this infrastructures it still remains highly important to have the ability to estimate real threats and apply policies and defenses in the most cost/ effective weight exploiting available limitless valuable resources to achieve the best results.

5 Chapter 5 – Standards & Frameworks

Within any Risk Assessment or Risk Management methodology, the concept or Risk occupies a central role. Variations often arise from different interpretations of this concept and what it means to an organization. Differences can also occur in the number, meaning and relationships of the factors driving risk, as well as, how they can be operationalized, measured and computed in order to quantify Risk in a meaningful way.

This chapter attempts to provide an overview of some of the most common conceptualizations of Risk. The list is not exhaustive, as infinitesimal variations can result in an endless array of models, nor is it exclusive, as even the models analyzed below can be adapted, influenced or merged with one another.

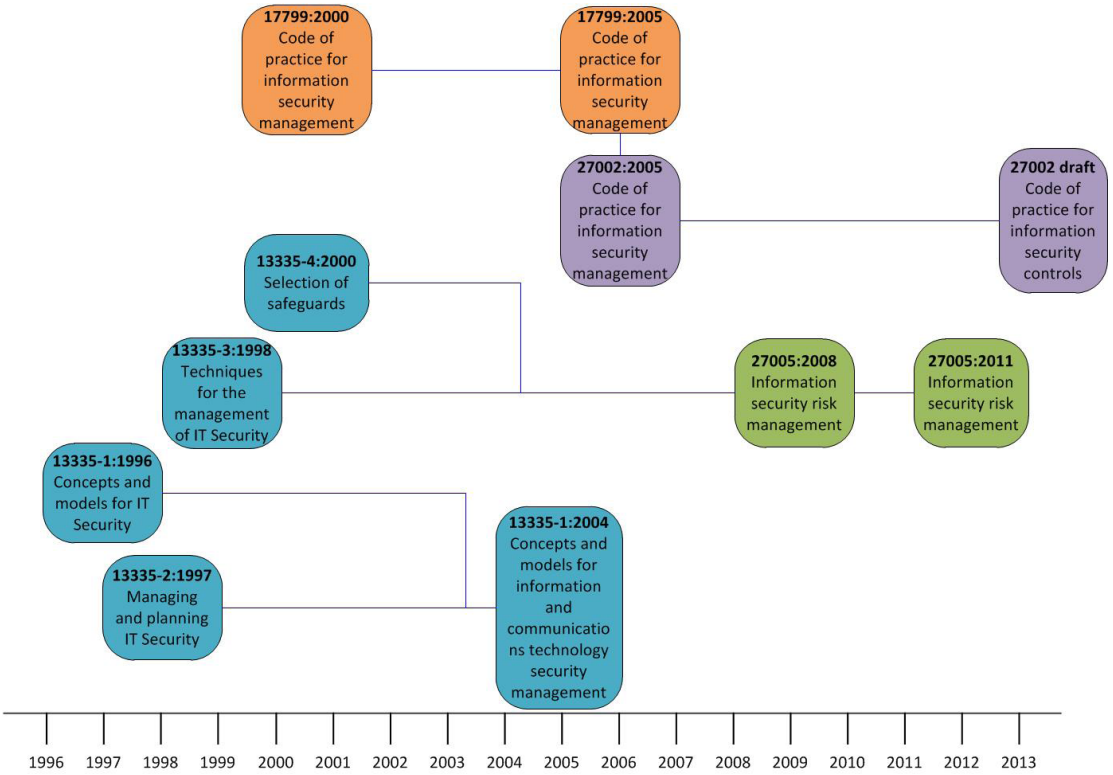


Figure 25: *A time-line of the ISO/IEC standards relevant for Information Security RA/RM*

5.1 Evaluation of Standards and Frameworks

In this section, a number of frameworks will be analyzed in regard to the conceptual model of risk. Only frameworks that explicitly define and decompose Risk, as well as, suggest either a taxonomy of factors or a formula for computing Risk based on these factors are selected. The following list of frameworks was also chosen for their mutual diversity and/or relation to one or more of the methods analyzed in chapter 4.

5.1.1 AS/NZS ISO 31000:2009

The AS/NZS ISO 31000 standard was originally launched as an attempt to promote the old AS/NZS 4360 Risk Management standard to an international standard. AS/NZS ISO 31000 [72] also supersedes the AS/NZS 4360:2004 by redefining risk and introducing some more general guidelines and principles applicable to (theoretically) any RM method. Furthermore, it introduced a new definition of risk, as well as the factors driving it. To this extent, it can be considered a proper Risk Management framework, addressing all areas related to the risk management process.

Concepts:
The new standard defines **Risk** itself as "the effect of uncertainty on objectives", with the following notes [72]:

- An effect is a deviation from the expected — positive and/or negative.
- Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process).
- Risk is often characterized by reference to potential events (2.17) and consequences (2.18), or a combination of these.
- Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (2.19) of occurrence. As such, the standard also conforms to Class 1 approaches to Risk Management.

The AS/NZS ISO 31000:2009 standard is more focused on defining high-level concepts such as the Risk Management and Risk Assessment process, security policies and risk evaluation criteria as well as discussing the different phases involved in implementing these. The concepts are described with a management audience in mind and as such; do not go into much detail when discussing the concept of Risk itself. While it also offers definitions for common terms used in the field or Risk Management (e.g. event, consequence, likelihood or vulnerability), it does not describe causal relationships between these concepts, nor does it suggest a

decomposition or factorization of Risk. Furthermore, the standard is aimed at any Risk Management process, not necessarily one involving Information Security, making it even less relevant to our research questions. This is explainable by the fact that, from available literature, it can be concluded that the concept was designed to be compatible with (most) other Risk models and RM/RA processes. The specific factorization of Risk, as well as the taxonomy of these factors is dependent on the context-specific Conceptual Model and Risk Assessment methodology chosen to augment the AS/NZS 31000's general principles.

Unfortunately, the standard is also not freely available and as such, more information regarding the particular conceptual models it is compatible with was unavailable at the time of writing.

5.1.2 FAIR – ISO 27005

The Open Group describes FAIR as a taxonomy of the factors that contribute to risk and how they affect each other. The FAIR framework is primarily concerned with "establishing accurate probabilities for the frequency and magnitude of loss events" [23].

FAIR main document is "An Introduction to Factor Analysis of Information Risk (FAIR)"[51]. The document starts with a definition of Risk that is consistent with Class 1 RA methods. That is, in order to compute risk, likelihood of the threat, the impact that the threat can have on the asset(s) as well as how vulnerable the asset is to the threat are taken into consideration. Together with a discussion regarding risk analysis at a high-level and the various interpretations of probability, it introduces the main concepts involved in Information Security. Further on, these concepts are decomposed into factors and suggestions as to how these factors can be combines in order to estimate risk is suggested. Thus, risk is iteratively decomposed into fundamental parts. The result is a taxonomy of all possible factors that play a role in driving risk. The document also briefly discusses Controls, by dividing them across three dimensions. Finally, a discussion regarding possible challenges encountered when measuring the described factors is started.

Concepts:

The FAIR framework identifies four primary components of any risk scenario: Threats, Assets, The Organization itself and The External Environment. It goes on to underline the importance of Threats and Assets. The key concepts defined in the framework are [64]:

Threat can be anything capable of acting against an Asset such as to cause harm. Threat Agents are defined as "individuals within a threat population" and can be grouped by Threat Communities (subsets of the overall threat agent population that

share key characteristics). The framework puts heavy emphasis on defining the necessary and sufficient characteristics of such Threat Communities required to get an accurate estimation of the probability, nature, objective and outcome of events.

Asset is any data, device or other component supporting one or more information related-activities (such as access, misuse, disclose, modify or deny-access) such that it can result in Loss.

Loss can be of various forms:

- **Productivity:** – a reduction of the organization to effectively produce goods or services in order to generate value
- **Response:** – the resources spent while acting following an adverse event
- **Replacement:** – the expense to substitute/repair an affected asset
- **Fines and judgments (F/J):** – the cost of the overall legal procedure deriving from the adverse event
- **Competitive advantage (CA):** - missed opportunities due to the security incident
- **Reputation:** – missed opportunities or sales due to the diminishing corporate image following the event

Risk is probable frequency and probable magnitude of future loss, decomposed as follows:

Loss Event Frequency (LEF) is the probable frequency, within a given time-frame that a threat agent will inflict harm upon an asset and can be decomposed into two factors:

Threat Event Frequency (TEF) is the probable frequency, within a given time-frame that a threat agent will act against an asset. This is driven by two factors:

Contact is the probable frequency, within a given time-frame, that a threat agent will come into contact with an asset. Can be random, regular or intentional.

Action is the probability that a threat agent will act against an asset once contact occurs. This is influenced by the threat agent's assessment of: the asset value, the level of effort required to compromise target asset and the probability that he might suffer negative consequences while attempting an attack.

Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent and is driven by:

Control Strength (the strength of a control as compared to a baseline measure of force)

Threat Capability (the probable level of force that a threat agent is capable of applying against an asset)

Probable Loss Magnitude (PLM) is comprised of 4 types of factors:

1. Asset Loss factors:

Value or liability is defined as:

- Criticality = the impact on the organization productivity
- Cost = the cost of replacing a compromised asset
- Sensitivity = the impact of disclosure of confidential information; can be of various types: Embarrassment (exposes the inappropriate behavior company management), Competitive advantage (loss of CA due to exposure), Legal/regulatory (cost of law violations) or General (other losses related to data sensitivity)

Volume or quantity of the asset

2. Threat loss factors:

Competence as the amount of damage threat agent is able to inflict

Action of the Threat Agent on the Asset:

- Access (read the data without proper authorization)
- Misuse (use the asset without authorization and or differently form the intended usage)
- Disclose (the agent let other people to access the data)
- Modify (data or configuration modification)
- Deny access (preventing legitimate intended users from accessing the asset)

Internal vs. External threat agent affiliation

3. Organizational Loss Factors:

Timing of the attack

Due Diligence undertaken by the organization

Response of the organization with regard to:

- Containment (the ability to limit breadth and depth of an event)
- Remediation (the ability to remove threat agent)
- Recovery (the ability to bring things back to normal)

Detection: of the threat in due time

4. External Loss Factors:

Detection of the event by external entities

Legal / Regulatory fines or judgments imposed by regulation, contract law or case law
Competitors taking advantage of the situation
Media reaction
Stakeholders taking their business elsewhere

A complete overview of the decomposition of Risk as proposed by the FAIR taxonomy is visible in Figure 22.
One notable difference between FAIR and most other conceptual models is that FAIR views "Vulnerability" as a probability (that the force applied by the threat exceeds the strength of the available controls" instead of "a weakness that may be exploited". In FAIR, the weakness is defined as a "Potential Vulnerability", with the actual Vulnerability being dependent on the particular Threat and its capabilities.

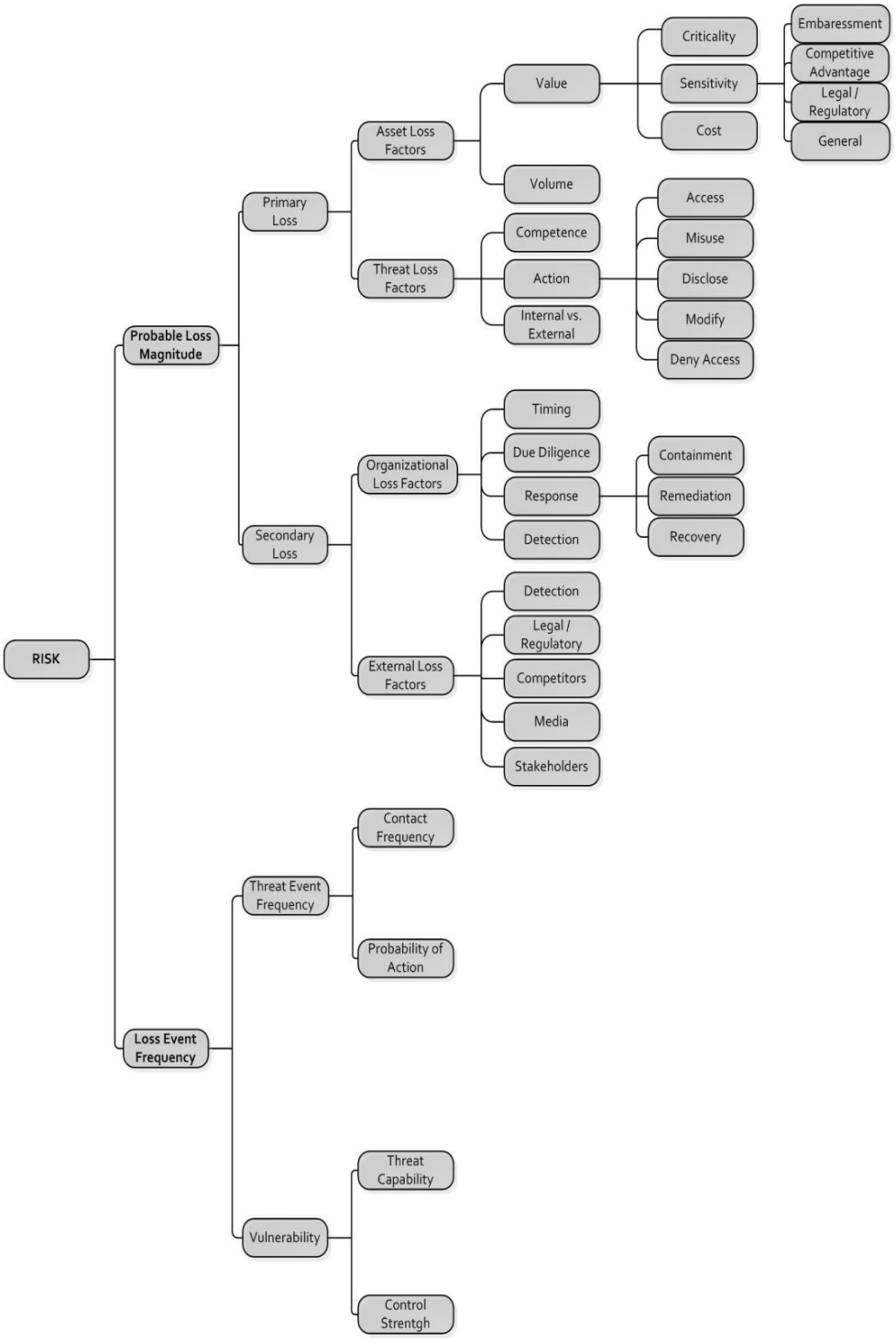


Figure 26: *Decomposition of Risk according to the FAIR framework and The Open Group taxonomy*

5.1.3 ISO /IEC 13335-1: 2004: Concepts and models for information and communications technology security management

The standard's full title is *ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.*
According to its abstract "ISO/IEC 13335-1:2004 presents the concepts and models fundamental to a basic understanding of ICT security, and addresses the general management issues that are essential to the successful planning, implementation and operation of ICT security. Part 2 of ISO/IEC 13335 provides operational guidance on ICT security. Together these parts can be used to help identify and manage all aspects of ICT security." [10] in this section, however, we will focus on Part 1 as it is dedicated to discussing useful concepts and models for managing and planning IT Security. Furthermore, Part 2 as a standalone document has since been made obsolete.

Concepts:

The main concepts required in any discussion about IT Security, are defined by the ISO/IEC 13335-1[10] standard as follows:

> **Assets** are physical assets (e.g. computer hardware, communications facilities, buildings), information/ data (e.g. documents, databases), software, the ability to produce some product or provide a service, people and intangibles (e.g. goodwill, image) that are considered valuable enough to warrant some degree of protection. Assets can have the following attributes: value and/or sensitivity, safeguards.
> **Threats** have the potential to cause an unwanted incident that may results in harm to a system or organization and its assets. The harm can be caused by a direct or indirect attack on the information being handled by an IT system or service. Threats are classified, based on various factors:
>
> - Depending on origin: human or environmental
> - Depending on cause: deliberate or accidental
> - Depending on motivation: financial, competitive advantage, etc.
> - Depending on source: insider or outsider
> - Depending on severity: temporary or permanent
> - Depending on number of targets: one asset or many assets
> - Depending on frequency of occurrence

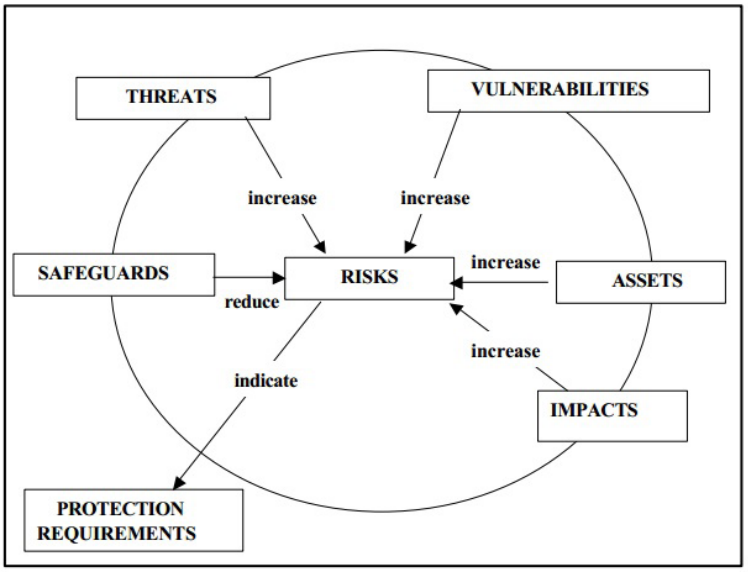


Figure 27: *Relationships between the entities involved in RM/RA according to ISO/IEC 13335-1*

Vulnerabilities include weaknesses in physical layout, organization, procedures, personnel, management, administration, hardware, software or information. They may be exploited by a threat in order to cause harm (either to IT system or business objectives). Not all vulnerabilities are susceptible to all threats (some vulnerabilities are only known to/exploitable by certain threats).

Impact is the consequence of an unwanted incident which affects the assets. Such consequences could be the destruction of certain assets, damage to the IT system, and loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity or reliability. Impact can be measure both quantitatively (e.g. estimating financial costs) or qualitatively (by means of ordinal scales).

Risk is the potential that a given threat will exploit vulnerabilities of an asset and thereby cause loss or damage to an organization. The methodology also describes Risk Scenarios as a description of how a particular threat or group of threats may exploit a particular vulnerability or group of vulnerabilities exposing assets to harm.

Safeguards are practices, procedures or mechanisms that may protect against a threat, reduce vulnerability, limit the impact of an unwanted incident, detect unwanted incidents and facilitate recovery. Safeguards are responsible with performing one or more of the following functions: prevention, deterrence, detection, limitation, correction, recovery, monitoring and awareness.

Constraints set by the organization or dictated by the environment on which the organization operates. Examples: organizational, business, financial, environmental, personnel, time, legal, technical, and cultural/social.

The (causal) relationships between the concepts described above are pictured in Figure 23.

Risk is characterized by a combination of two factors, the probability of the unwanted incident occurring and its impact. However, no formula or indication is given as to how to estimate these values. The notion of **Residual Risk** is also discussed as the level or Risk of which a decision to accept is made. Given this decomposition, the standard also conforms to Class 1 approaches, with Vulnerability being included in the concept of "probability".

It should be noted that these formulas allow the method to be applied both to a quantitative and to a qualitative analysis. The only difference being that in order to compute qualitative values, cross-reference tables should be pre-defined for each of the operations.

5.1.4 Microsoft Threat Model

The Microsoft Threat Modeling [14] process does not qualify as a full-fledged Risk Management or even Risk Assessment framework due to the fact that is does not offer managers output relevant for making decisions regarding the security budget nor does it take into consideration organizational or business factors. The framework does describe a simplified process for "threat modeling" at a technical level, mostly aimed at web developers.

Furthermore, the methodology also describes multiple taxonomies of factors driving Information Security Risk which is in theory applicable to Information Systems as well as distributed software applications. This, together with the definitions of key Information Security concepts, make it interesting with regard to our scope by offering yet another, more technical point of view on how to understand, conceptualize, decompose and compute IT Risk.

Concepts:

Microsoft defines the following key concepts:

Asset A resource of value, such as the data in a database or on the file system. A system resource.
Threat A potential occurrence, malicious or otherwise, that might damage or compromise your assets.

Vulnerability A weakness in some aspect or feature of a system that makes a threat possible. Vulnerabilities might exist at the network, host, or application levels.

Attack/Exploit An action taken by someone or something that harms an asset. This could be someone following through on a threat or exploiting vulnerability.

Countermeasure A safeguard that addresses a threat and mitigates risk.

The process makes use of two methodologies for characterizing and evaluating threats that implicitly introduce a conceptual model that is not only applicable to threats, but can be used when discussing Information Risk in any context [14]:

STRIDE is a classification scheme for identifying and categorizing threats based on the type of attack and the motivation of the attacker:

S poofing identity
T ampering with data
R epudiation is the ability of users to deny specific actions or transactions
I nformation disclosure
D enial of service
E scalation of privileges

DREAD is a classification scheme for computing risk associated with each threat based on the formula

$$\boldsymbol{Risk} = (\boldsymbol{D} + \boldsymbol{R} + \boldsymbol{E} + \boldsymbol{A} + \boldsymbol{D})/\mathbf{5}, \text{ where:}$$

D = Damage Potential or "How great will the damage be in case of a successful attack?
R = Reproducibility or "How easy is it to reproduce the attack?"
E = Exploit-ability or "How easy is it to launch an attack?"
A = Affected users or "How many users are affected?"
D = Discover-ability or "How easy is it to find the vulnerability?"

are evaluated on a ordinal scale (either 1-to-10 or low-medium-high). The calculation can also be extended by including optional factors like Reputation.

The DREAD risk computation methodology is consistent with the traditional (Class 1) approach to Risk evaluation. This is not immediately obvious due to the naming of the factors. However, we could interpret Damage Potential and Affected users as metrics of the Impact. The Discover-ability of the vulnerability and the Reproducibility of attack directly influence the Likelihood of such an attack taking

place. Finally, the Exploitability (i.e. "how easy is it to exploit the vulnerability?") can be translated into the actual Vulnerability level.

5.1.5 OWASP Risk Rating Methodology

OWASP stands for The Open Web Application Security Project, and is a non-profit community comprised of private organizations, educational institutions and private individuals aiming at developing at improving the security of software. Same as the Microsoft Threat Modeling process, the OWASP approach is mostly geared towards software products and less towards Information Systems and enterprise wide security. However, the framework does describe a decomposition of Risk into driving factors as well as describe a method for computing Risk in their OWASP Risk Rating Methodology [11]. The decomposition is, in theory, applicable to an Information System as well as complex software applications.

Concepts:

OWASP defines the following key concepts:

Asset A resource of value, such as the data in a database or on the file system. A system resource.

Threat Agent is used to indicate an individual or group that can manifest a threat. Each threat Agent is defined by its Capabilities, Intentions and Past Activities and can be classified into a group.

Vulnerability is a hole or a weakness, which can be a design flaw or an implementation bug that allows an attacker to cause harm to the stakeholders of an application.

Attack is the techniques that attackers use to exploit the vulnerabilities.

Countermeasure is defensive technologies or modules that are used to detect, deter, or deny attacks.

The OWASP methodology follows a traditional conceptualization of Risk as Likelihood X Impact and suggests the following decomposition of Risk, also described in Figure 24.

Likelihood is determined by:

- Threat Agent Factors

  Skill level of the Threat Agent

  Motive is influenced by the reward the Threat Agent is hoping to receive

Opportunity reflects the amount of resources required for the Threat Agent to succeed in the Attack

Size of the group of Threat Agents seeking similar goals w.r.t the system

- Vulnerability Factors

Ease of discovery or how easy is it to discover certain vulnerability

Ease of exploit or how easy is it to successfully exploit certain vulnerability

Awareness or how well known is a particular vulnerability to this group of threat agents

Intrusion detection or how likely is it to detect attack attempts

Impact is determined by:

- Technical Impact Factors

Loss of confidentiality

Loss of integrity

Loss of availability

Loss of accountability

- Business Impact Factors

Financial damage

Reputation damage

Non-compliance damage

Privacy violation

While the methodology suggests the above factors, it is also very clear on the fact that particular organizations might wish to augment the pre-defined set of factors by adding ones that are important to the organization. Furthermore, weights can be applied to each factor based on the significance it carries for the particular business model.

It is also obvious that this methodology also employs a Likelihood X Impact approach, consistent with Class 1 methods, with Vulnerability again being viewed as a factor of Likelihood.

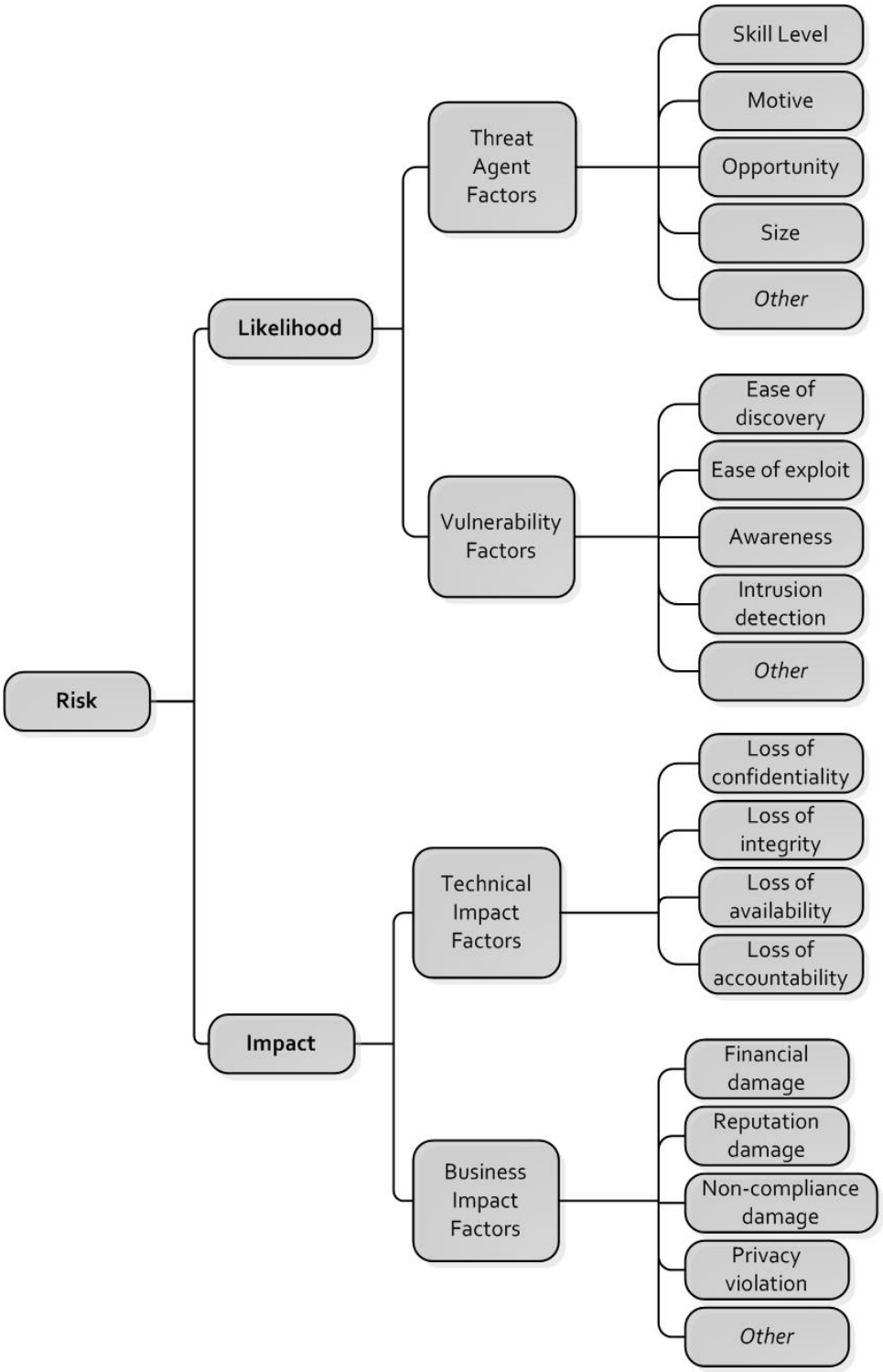


Figure 28: *Decomposition of Risk level (Exposure) according to the OWASP methodology*

5.1.6 The Open Group Risk Taxonomy

The Open Group is a technology-neutral consortium, comprised of hundreds of organizations (both private and governmental) that "enables achievement of business objectives through IT standards" by striving to create what they call Boundary-less Information Flow ™. More specifically, the group works with members from all sectors of IT (customers, suppliers, regulators, standards bodies, vendors, consultants and even academia) in order to facilitate interoperability, promote open source technologies, share best practices and last but not least, promote practical, industry-wide standards and certifications.

In 2009, The Open Group introduced their own definitions and taxonomy for Information Security Risk. These are closely related to the FAIR framework: Risk Management Insight, the developers of FAIR, are members of The Open Group's Security Forum. As such, FAIR was used as the foundation for the development of the new Open Group Standard. Due to this, The Open Group Risk Taxonomy [13] cannot be considered an alternative to the FAIR taxonomy, but simply an extension.

By developing the standard, The Open Group hopes to increase consistency amongst researchers and practitioners regarding the nomenclature involved in Information Systems Risk Management, as well as promote a standardized decomposition of the factors driving risk in such systems and the relationships between them.

Concepts:

The following main concepts are identified in the taxonomy [13]:

Risk The probable frequency and probable magnitude of future loss.

Threat Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.

Vulnerability The probability that threat capability exceeds the ability to resist the threat.

Asset Any data, device, or other component of the environment that supports information-related activities, which can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss.

As it should be obvious from the above definitions, the Open Group taxonomy is fully consistent with the one introduced by FAIR and thus also a Class 1 approach. As for the factorization of Risk, The Open Group also adopts the same one used in FAIR, and decomposed in Figure 23. As a matter of fact, The Open Group Risk Taxonomy[13] is almost word-by-word identical with Risk Management Insight's "An

introduction to Factor Analysis of Information Risk (FAIR)". In conclusions, the Open Group taxonomy and conceptualization of Risk is the same as FAIR's, with the Open Group's document simply aiming at increasing awareness and promoting usage of the FAIR framework.

5.1.7 Structured Risk Analysis

Structured Risk Analysis is mainly a Risk Assessment methodology introduced by Consult Hyperion, a British company. The RA process will be analyzed in the section below. In this section we will look at the way Risk is conceptualized and decomposed, according to the methodology.

Although the Structure Risk Analysis does not constitute a full-fledged Risk Management framework, we are including it here due to the rather unique the concept or Risk is explained, factorized and computed.

In [71], the methodologies main document, several mathematical equations are given that together can be used to estimate risk. For each risk (interpreted as a {physical entity, digital asset} tuple), the Exposure is computed on three dimensions: Confidentiality, Integrity and Availability. Exposure represents the risk level and can be expressed on a ordinal scale or numeral scale. The formula used is:

$$\boldsymbol{E} = \boldsymbol{D} * ((\boldsymbol{G} - \boldsymbol{C}) * (\boldsymbol{1} - \boldsymbol{L}))$$

where L = **Likelihood of capture**, C = **Cost** for attacker , D = **Damage** to organization, G = **Gain** for attacker.

Gain for attacker minus Cost for attacker ($G - C$) is interpreted as **Profit** for attacker (Pr), while the opposite of Likelihood of Capture ($1 - L$) is interpreted as **Probability of Not Getting Caught** (PNC), which gives us the following simplified formula:

$$\boldsymbol{E} = \boldsymbol{D} * \boldsymbol{Pr} * \boldsymbol{PNC}$$

Profit and Probability of Not Getting Caught are further grouped together as **Probability** (P) of attack, which leads to the most simplified version of the formula:

$$\boldsymbol{E} = \boldsymbol{D} * \boldsymbol{P}$$

This final formula closely resembles Class 1 approaches to Risk Management with the estimation of Vulnerability being implicitly assumed to be part of the "Probability" value.

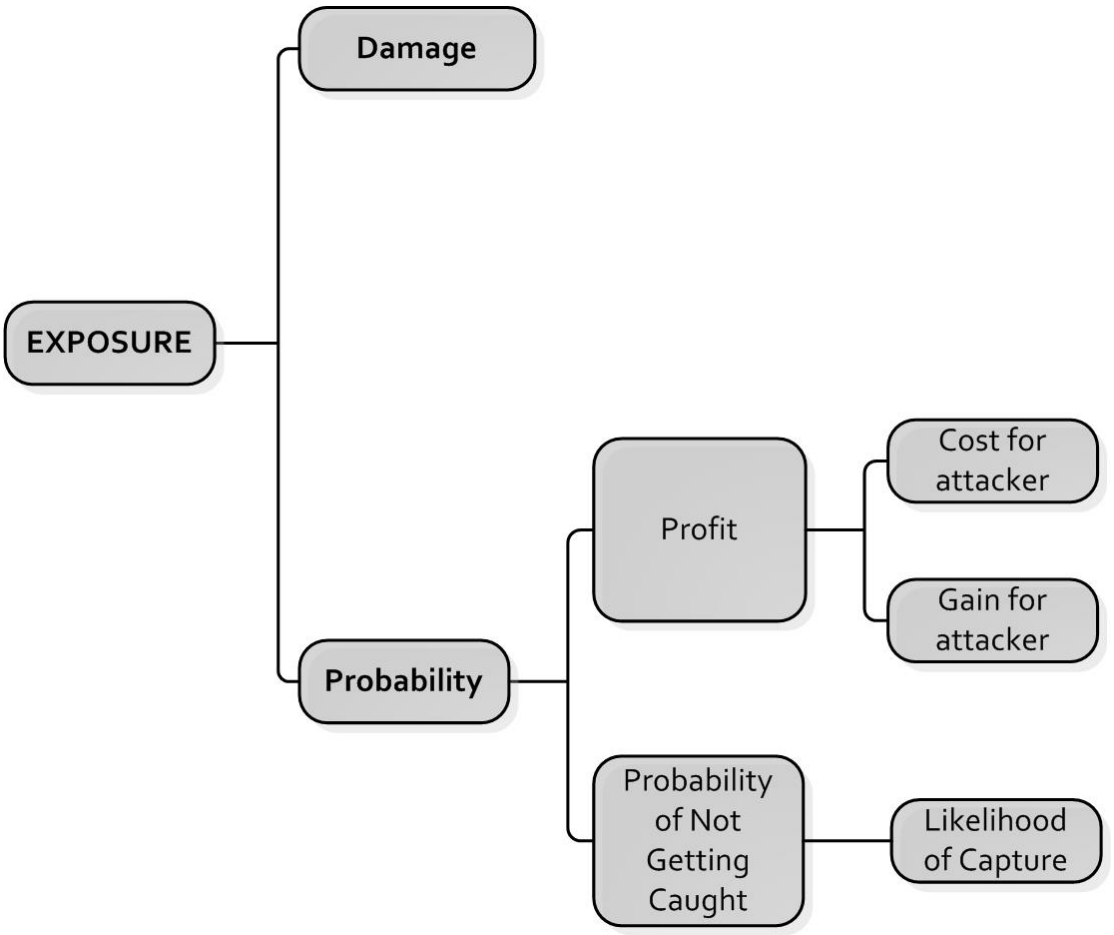


Figure 29: *Decomposition of Risk level (Exposure) according to the SRA methodology*

5.1.7.1 Steps Structured Risk Analysis

The method is made up of a small number of steps. An overview of the process can be found in Figure 26. In the Model Service step, all data entities are identified. Next, in the Assess threats step for each data entity, the Damage for the customer and the Gain for an average attacker that a compromise in Confidentiality, Integrity or Availability might cause is estimated. The Model System step simply decomposes the physical architecture into sub-components and interfaces. The Assess vulnerabilities step estimated the difficulty (average cost and likelihood of capture) of an attack on each component or interface. In the Assess risks step, a cross-reference table is used to describe which data entities are stored, processed, or transmitted by each physical component or interface. Then, using some predefined operators, the overall risk (called Exposure) of each valid component-entity pair is automatically calculated. In the final, Identify countermeasures step, mitigations and treatments are manually identified for the highest risks.

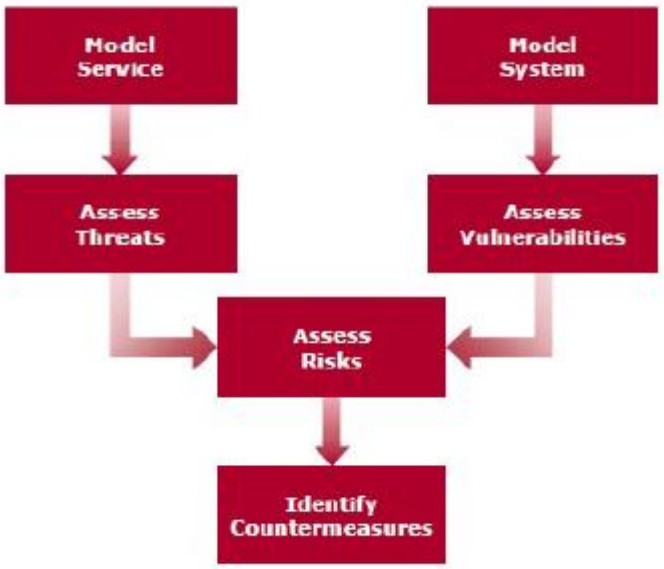


Figure 30: *The basic steps undertaken during a Structured Risk Analysis*

5.1.8 ISO 27001

ISO/IEC 27001 is the international Standard for best-practice information security management systems (ISMSs). It is a rigorous and comprehensive specification for protecting and preserving your information under the principles of confidentiality, integrity and availability. The Standard offers a set of best-practice controls that can be applied to every organization based on the risks you face, and implemented in a structured manner in order to achieve externally assessed and certified compliance.

More specific, ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information security risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts- an important aspect in such a dynamic field, and a key advantage of ISO 27k's flexible risk-driven approach as compared to, say, PCI-DSS.

The standard covers all types of organizations (eg. Commercial enterprises, government agencies, non-profits), all sizes (from micro-businesses to huge multinationals), and all industries or markets (eg. Retail, banking, defense, healthcare, education, government). This is clearly a very wide brief.

Moreover, ISO/IEC 27001 does not formally mandate specific information security controls since the controls that are required vary markedly across the wide range of

organizations adopting the standard. The information security controls from ISO/IEC 27002 are noted in Annex A to ISO/IEC 27001, rather like a menu. Organizations adopting ISO/IEC 27001 are free to choose whichever specific information security controls are applicable to their particular information security situations, drawing on those listed in the menu and potentially supplementing them with other a la carte options (sometimes known as extended control sets). As with ISO/IEC 27002, the key to selecting applicable controls is to undertake a comprehensive assessment of the organization's information security risks, which is one vital part of the ISMS.

Furthermore, management may elect to avoid, transferor accept information security risks rather than mitigate them through controls – a risk management decision.

Whereas the standard is intended to drive the implementation of an enterprise-wide ISMS, ensuring that all parts of the organization benefit by addressing their information security risks in an appropriate and systematically-managed manner, organizations can scope their ISMS as broadly or as narrowly as they wish –indeed scoping is a crucial decision for senior management. A documented ISMS scope is one of the mandatory requirements for certification.

5.1.9 ISO 15408

This standard permits comparability between the results of independent security evaluations. More specifically, ISO 15408 provide a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether IT products fulfill their security needs.

ISO/IEC 15408 is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality. Moreover, the standard is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore, users of this International Standard are cautioned to exercise care of this flexibility is not misused. For instance, using ISO 15408 in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, may result in meaningless evaluation results.

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties and methods to determine that an evaluation will provide

meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

Furthermore, ISO/IEC 15408 addresses protection of assets from unauthorized disclosure, modification or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity and availability, respectively. ISO 15408 may also be applicable to aspects of IT security outside of these three. ISO/IEC 15408 is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. Apart from IT security, ISO 15408 may be applied in other areas of IT, but makes no claim of applicability in these areas.

This standard consists of three (3) parts:

a. Introduction and general model
b. Security functional components
c. Security assurance components

The first part of ISO 15408 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the International Standard which in its entirety is meant to be used as the basis for evaluation of the security properties of IT products.
The second part defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet common security functionality requirements of many IT products.
The third part defines the assurance requirements of ISO 15408. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of Protection Profiles (PPs) and Security Targets (STs).

5.1.10 ISO 27002: 2005: Code of practice for Information Security Management

ISO/IEC 27002 was derived from the BS7799 standard, first published in the 90's. It was subsequently integrated into the ISO/IEC 17799 standard and later renamed to its current label. The standard is aimed at 'establishing guidelines and general principles for initiating, implementing, maintaining and improving information security management within an organization'. The standard describes a set of 12 security clauses, each with a number of subcategories for which control objectives are defined and guidelines on how such control can be applied are given. On top of this, the standard gives a few best practice suggestions for conducting a formal Risk Assessment and Treatment.

The standard does not define individual steps that have to be undertaken, but does define a broad outline to which the Risk Assessment process must confirm. The actions that must be part of the Risk Assessment according to ISO/IEC 27002 are:

1. Risk identification, quantification and prioritization based on objectives relevant to the organization
2. Risk analysis: estimating the magnitude of Risks
3. Risk evaluation: determine importance of risks by comparing estimated risk levels against previously defined risk criteria
4. Risk treatment: define risk acceptance criteria and use them to decide if and when treatment is indeed warranted. Then decide which approach to Risk Treatment is suitable to the organization (accept, avoid, transfer or apply controls). A large amount of such controls, grouped on clauses and categories make up the bulk of the ISO/IEC 27002 document.

The ISO/IEC standard, while giving guidelines toward conducting Risk Assessments, does not offer sufficient practical tips towards completing such a task. Instead, its focus is on suggesting controls for various known vulnerabilities. As such, its focus is on Risk treatment, and it should be augmented by using a third-party Risk Assessment method before-hand, in order to get a better idea of which controls are relevant and required for an organization. Once a Risk Assessment consistent with the suggested guidelines is implemented, ISO 27002 can be used for selection and implementation of controls.
However, in practice, ISO/IEC 27002 alone can be used as a basis for Risk Assessment. This is known as ISO 27002 Gap Assessment/Analysis and the main idea is that the existing controls are compared to the ones described in the standard. Any deviation, or gap, is noted and evaluated. As a result, Risk can be estimated based on these identified gaps, and mitigation strategies can also be derived. In some sense, the standard is used as a benchmark for assessing the effectiveness of existing controls and identifying possible weak spots.

Evaluation:

PROs:

- Supported by extensive taxonomy, conceptual model and Risk Management Framework (ISO 13335)

CONs:

- Only describes the Risk Assessment process at a very high level
- Needs to be in conjunction with a lower-level Risk Assessment methodology in order to be relevant to management users
- Focuses mostly on Controls and Risk Treatment instead of Risk Identification and Analysis

6 Chapter 6 – Case Study: General Hospital

6.1 Scope of the analysis

This security study considers the Information Systems and documents of a General Hospital. A characteristic of the specific hospital is that most software applications utilized, have been developed by the same organization, and consist the Information System (IS) of the General Hospital.

6.2 Range of the analysis

Software applications utilized, have been developed by the same organization, and consist the Information System (IS) of the General Hospital.

6.3 Methodologies and tools

The methodologies used for the analysis are Magerit (through the Pilar software tool) and CRAMM. The decision for using these methodologies was based on the aforementioned analysis. These two methodologies cover most of the criteria and are best suited for the information system that will be studied.

6.4 Summary of the MAGERIT methodology

In the terminology of the ISO31000, MAGERIT implements the Analysis and Risk Management process as shown below:

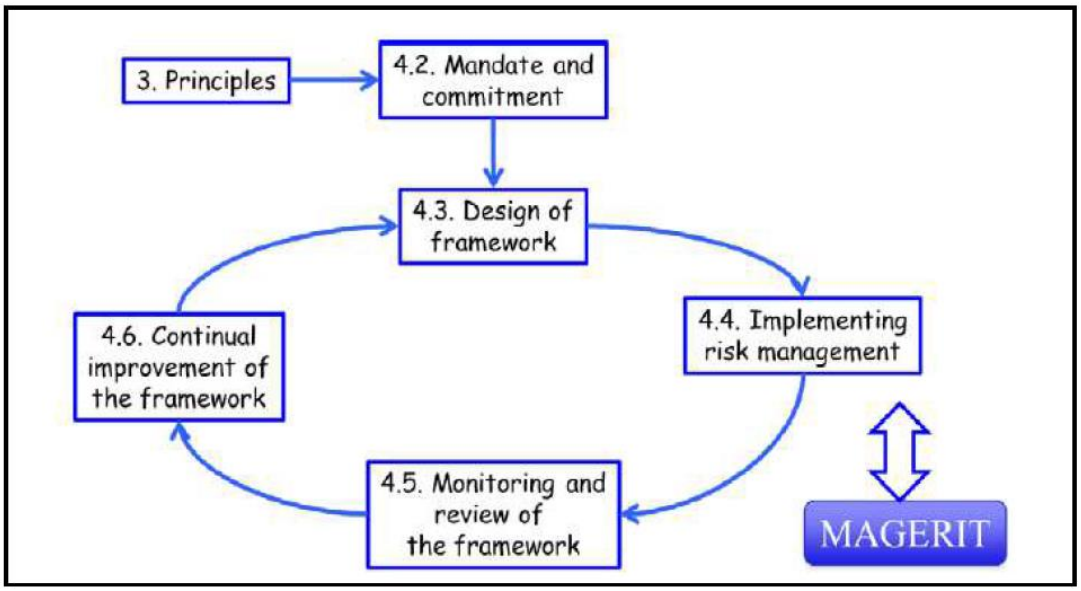


Figure 31: *Magerit process*

The MAGERIT methodology performs the following objectives:

1. Inform responsible for information systems risk being and the need to address. It provides a systematic method for risk analysis.
2. Plans for the Hospital of the evaluation, control, and certification.

The MAGERIT methodology follows the steps below:

1. Characterization of assets which includes:
    a. Recognition of assets
    b. Relationships between them
    c. Evaluation of assets
2. Characterization of threats:
    a. Definition of threats
    b. Assessment of threats
3. Identification of security countermeasures:
    a. Definition of the relevant security countermeasures
    b. Evaluation of the security countermeasures
4. Calculation of risk situation:
    a. Calculation of the effect
    b. Risk calculation

The RM methodology MAGERIT follows the following steps:

1. Assessment – interpretation of the residual impact and the risk values.
2. Risk acceptance
3. Risk treatment

6.5 Summary of CRAMM methodology

The CRAMM process comprises three main stages, as shown below:

- Identification and valuation assets
- Risk analysis
- Risk management

Stages	*Step stages*
1. Identification and Valuation assets	*Step 1.1*: Description of IT systems and facilities *Step 1.2*: Valuation of the assets of the Information System *Step 1.3*: Confirmation and Validation of valuation
2. Risk Analysis	*Step 2.1*: Identifying threats on each asset *Step 2.2*: Assessment of threats and vulnerabilities *Step 2.3*: Calculation of risk combination of asset – threat – weakness *Step 2.4*: Risk Valuation
3. Risk Management	*Step 3.1*: Identifying proposed countermeasures *Step 3.2:* Information Security Systems Plan

Table 5: *CRAMM stages*

Step 1: Identification and assessment of assets

The first stage relates to the identification and evaluation of IS data requiring protection. It consists of the following steps:

- Stage 1.1: Description of IT systems and facilities
- Stage 1.2: Valuation of the assets of the information systems
- Stage 1.3: Confirmation and validation of valuation

Specifically, each individual step includes:

Stage 1.1: Description of IT systems and facilities

It relates to the identification data of the Information System which require protection. These elements are mainly the data handled by the Information System, as well as the software and hardware of the Information System. These elements are in interaction. For example, the data processed by the software, which is supported by hardware components, such as computers, network equipment and peripherals.

Data protection requires the protection of software and hardware that stores and processes the data. Moreover, necessary is the protection of communications media used for data transfer. For this reason, as part of the methodology created a model of the system, showing the correlations between the elements of an Information System.

Stage 1.2: Valuation of the assets of the information systems

When valuing the IS elements emphasis is placed on evaluation of data managed by the IS. The goal is to determine the importance of the data for the organization. Thus, we can identify those categories of data which require special protection and in particular the type of protection required.

The value of each class / category of data valued by the Impact which would have been the loss of data. Specifically examined the magnitude of the effect in the case of destruction, unauthorized modification, disclosure and unavailability. In particular, the following cases shall be considered:

- *Non-availability* [Less than 15 minutes, 1 hour, 3 hours, 12 hours, 1 day, 2 days, 1 week, 2 weeks, 1 month, 2 months and more].
- *Destruction* [loss of data since the last backup. Loss of all data with the copy kept].
- *Disclosure* [Disclosure of data on individuals within the organization. Disclosure of data to people outside the organization. Disclosure of data to service providers].
- *Non-authorized changes* [Small-scale errors. Major mistakes].
- *Deliberate alteration of data.*
- *Errors in data transmission*.

For each case estimated the worst case scenario and calculated the effects of its realization. The magnitude of the effect quantitatively estimated based on the scale of 1-10. The methodology provides specific guidelines for assessing the impact. Also valued software and hardware of the IS. Their valuation is based on the replacement cost. Subsequently, the software CRAMM calculates, based on the IS model, the implied value of the IS data. For example, the loss of a computer (eg. Theft) entails loss, albeit temporary, of data processed and the value of the latter should be added to the PC value.

Stage 1.3: Confirmation and validation of valuation

Valuing the IS elements critical to the conduct of Risk Analysis. For this reason, at this point should the valuation be confirmed by the organization. The working group presents the report form the results of the first stage in competent personnel carrier. The results are considered together and validated.

Step 2: Risk Analysis

The steps following the second stage are:

- Stage 2.1: Identifying threats on each asset
- Stage 2.2: Assessment of threats and vulnerabilities
- Stage 2.3: Calculation of risk combination of asset – threat – weakness

- Stage 2.4: Risk Valuation

Details of each individual step includes:

Stage 2.1: Identifying threats on each asset

The method is not limited to the identification of potential threats facing one IS in general but focuses on identifying specific threats for each Good of IS. The CRAMM provides an indicative list of Threat and recommendations on which categories Goods IS usually a risk of this threat. The software, with a complete model of the IS, has the ability to take into account that when one of the goods of the IS faced with a threat, then the data and services that it supports face the same threat. For example, when a computer is facing the threat of theft, then the data has been stored will steal him. So the analyst does not have to count myself all the correlations and interactions.

The CRAMM software asks from the analysts to relate the asset categories to threat from above. The software is driven to conclusions based on the system model. So, whether a threat (eg. Fire) associated by the analyzer to a location (eg. Computing center), then the software concludes that the threat that concerns all material that is in a specific location (eg. Computing devices, peripherals, network equipment).

Stage 2.2: Assessment of threats and vulnerabilities

For each combination Threat – asset, estimating the size of the Threat and Vulnerability severity of which can lead to realization. This assessment is structured questionnaires. Assessing the Threat is in the range 1-5 (very low, low, medium, high, and very high) automatically by the instrument, based on the replies to the questionnaires. Respectively for completed questionnaires Weaknesses, weaknesses and severity of Deficit is calculated on the scale 1-3 (low, medium, high). The answers given to the questionnaires are derived from data collected by analysts from users of the system. The tool provides a questionnaire for each combination Threat Good. The answers of the questionnaires entered into the tool that calculates the level of threats and weaknesses. It also enables analysts to change prices automatically calculated.

Stage 2.3: Calculation of risk combination of asset – threat – weakness

The CRAMM calculates the level of risk for each combination of the Asset-Threat-Vulnerability. We have not, just a degree of risk for the IS in its entirety, but we have a specific assessment of risk for each individual combination Asset-Threat-Vulnerability. For this purpose, using both the results of the assessment of threats and weaknesses, and the system model is created from the first stage. Thus, the Risk Score takes into account the correlation between the IS Goods. Essentially the Risk Rating reflects the security requirements for each Good of IS, as greater risk implies higher demand for security. The calculation of the degree of risk follows the scale 1-7. The Risk Rating for each combination of the Asset-Threat calculated by the instrument. The analyzer is able to intervene and change some values, if it deems appropriate. The

number of Asset-Threat of combinations and mainly the complexity of the interrelationship of Goods under an IS, make practically impossible the empirical and manuscripts calculating risk.

Stage 2.4: Risk Valuation

The Risk Score will be used in the next step of selecting Countermeasures. Therefore, the accuracy of the estimates made during the second stage should be checked before the next stage of the methodology.

Step 3: Risk Management

Based on the results of the Risk Analysis (Step 2), the CRAMM produces a proposed Security Plan. This consists of a series Countermeasures - Security Measures, which are considered necessary for the Risk Management, which will be implemented in IS.

The stages of the third stage include:

- Stage 3.1: Identifying proposed Countermeasures.
- Step 3.2: Information Security Systems Plan.

Details of each individual step includes:

Stage 3.1: Identifying proposed Countermeasures

The CRAMM software has a Countermeasure base. The Countermeasures are technical, administrative and organizational. The software automatically selects a list of proposed countermeasures based on the results of the Risk Assessment. The Countermeasures are divided into groups according to the type of threats that are facing and the type of goods that are meant to protect. From the proposed list should be made certain choices. The Countermeasures library includes about 2,500 countermeasures, divided into groups and prioritized according to the level of security they offer. The software automatically selects the Countermeasures Stakeholders accordance with the results of the Risk Assessment.

Step 3.2: Information Security Systems Plan

During this step a security plan is written which includes:

- Security policy design
- Security measures
- Strategy for the implementation of Security Plan

Note that the security policy is characterized as "plan", since its adoption requires any final processing and approval of the relevant services and possibly the organization's management.

6.6 Assets

Carry identification of the assets of the Information System of the hospital in the following categories:

- **Data Assets:** It all those data in categories personal data, sensitive personal and sensitive data belonging to employee data categories, patient data and payroll data.
- **End User Services:** It's all those end-user services. They provide services to the user.
- **Materials Details:** It's all those material elements which process the data for which is performed the risk analysis.
- **Locations:** All premises in which it is installed hardware for the Information System of the Hospital.
- **Software:** Includes all software (operating software, application software, software support.

Due to the fact that the assets associated with each other, that means that the data services and equipment which processes them, the methodology offers the creation correlation model of the above, to calculate the values in the evaluation.

6.6.1 Recognition of items in the Information System

The main components of the system hardware, software, data, procedures and personnel were studied by studying a specific hospital and were as follows:

Data

The categorization of IS data can be done, according to their legal status, in three categories. The non-personal data, the personal data and sensitive personal data. Sensitive personal data are a subset of personal data. Specifically, the main data groups tested are:

- ***Patient data:*** Relating to patient care and are sensitive data. They include data on patient visits to outpatient, data drug delivery, medical data and laboratory test data and the donations. At the same time, respected and economic data needed to recover the medical expenses of patients by insurance providers.
- ***Employee data:*** This data includes personal and economic data concerning the employees in the hospital and are mainly related to the payment of their salaries and the payment of payroll contributions.
- ***Financial and accounting data:*** These include personal and financial details of the transactions with the hospital, such as the hospital's suppliers, the data on financial transactions, the details of the protocol, as well as balance sheets and accounts information.

Hardware

- One (1) server with operating system Windows 2000 Server, which operates the Electronic Protocol application of the company. The server is located on the premises of the Secretariat and the Protocol.
- One (1) server with Solaris 7.0 operating system, which is housed in the Department of Information and Organization of Hospital. There operate the hospital's applications which used by the Department of Import Patient, Pharmacy, the Material Office, the Treasury, the Department of Nutrition, and the Surgeries Foreign Secretariat Offices medical expenses, clothing and medical supplies.
- One (1) server with Windows operating system, with the Blood Donation Department applications and is established in this Section.
- Personal Computers with Windows operating system with the implementation of Payroll and located in this section.
- One (1) Line Printer for the central server is established in the Department of Computer Science and Management.
- Network equipment of central systems.

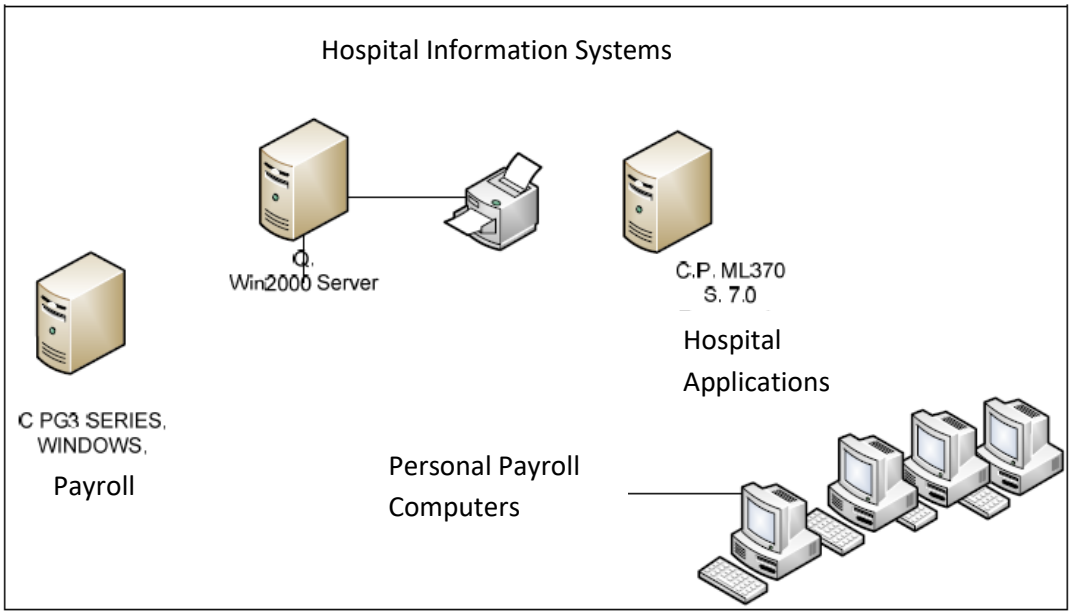


Figure 32: *Hospital Information Systems Topology*

Workstations

Workstations that act as terminals of the central System of Hospital applications, serving applications users Pharmacy, Office Material, the Cash Office (Accounting), the Office of hospital fees, the Import Patient Department, the Department of Nutrition, the Surgeries Foreign Secretariat, the Office of Sanitary and clothing department.

- They are also **workstations** for use in local applications in Blood Donation Station, the Secretariat - Protocol to the Payroll Office, the Personnel Office and Office Supplies.
- There are **personal computers** of the hospital for professional and scientific use in all hospital department.
- They are also two (2) **personal computers** in the IT and Organization Department for Internet access (Internet Room) from the hospital staff.
- There are also **personal computers** in health centers.
- Overall the number of PCs used at the hospital are about one hundred and twenty (120). Overall, for the internal network of the hospital operating at around two hundred and fifty (250) jobs for users of Information Systems.
- Network equipment: It includes the network devices such as routers, terminals etc., used for the operation of Information Systems Hospital. The network and telecommunications services provided by third parties (eg. OTE) and the corresponding equipment, are not included. Taken, however, considered in this study security as possible sources of threats and risks.

Relevant systems

The IS of the hospital are not directly interconnected with other organizations or service systems. Access to these systems have (via modem) companies that have developed and are charged with the maintenance and technical support companies, was, however, into account the ability of users to access some Internet applications via modems.

Services

The IS Hospital support the basic management functions of the hospital. Specifically, the CP they support the following functions:

- Financial Management
- Accounting Management
- Collection and disposal pharmaceutical and medical supplies
- Manage personal and financial data of employees
- Services to inpatients and outpatients of hospitalization of patients
- Provision of pharmaceutical care
- Provision of laboratory test results

6.7 Software and applications

This security study has included the following software:

- Software systems and application development: They consist of operating systems for servers and workstations (Windows, Solaris). Also include utility software (eg. MS Office), database software (Oracle), e-mail management

software (e-mail) and software for the security of Information Systems (McAfee Antivirus, Karspersky)

- Applications Hospital Management Information System (ISH): Include all of the Department of Patient Admission applications, and other hospital applications.
- Local applications: Includes all Blood applications, Payroll applications and Electronic Company Protocol applications.
- Special applications: Special software used for specific purposes, such as firewall.

6.8 MAGERIT Methodology

Because the managed information and services depend on assets such as equipment, communications, meaning the degree of which depends from a security incident a higher level asset from a low is important.
Although it is necessary that the Hospital be analyzed as a separate case in accordance with the methodology, the assets can be presented structured in levels where the upper levels depend on lower levels. The correlation model gives values for the measurement data.

6.9 Valuation of assets of ISH

This chapter describes the results of the evaluation of the data managed by the IS. The methodology followed attaches *great importance to data* and *less on hardware and software.* It uses multiple features for the evaluation of data or depending on the scenario. In our case an analysis for the evaluation of data in accordance with the impact of loss of availability, integrity, confidentiality.

6.9.1 Data determination

The Magerit methodology has two basic types of IS data. Information managed and the services it provides. The data were analyzed by the Magerit methodology are presented below:

Software	Data
Payroll Management System	Payroll
Patient – Customer System	Financial
Personnel Management System	Financial

It should be noted that all data managed by the Information Systems are separated and studied in representative groups, depending on the characteristics and security needs they have. Specifically, evaluated the effects on the following data sets Workshops Data, Personnel Data, Payroll Data.

6.9.2 Valuation of assets

The valuation of the assets of the IS was the risk analysis team information in collaboration with Hospital IT director, which examined the impact on the operation of IS for cases of unavailability, non-integrity, non-confidentiality considering the most pessimistic scenario.

For the valuation of the residual risk we took into account existing security measures of IS and the impact of the company in the event of threats. The categorization of the most critical services was based on the opinions of the company's executives.

The value determined for the critical assets (information and services) and recorded in the security domain. Their assessment is based on the information of end users pay for the Hospital Information System of the scale is the Pilar.

Since we introduced the assets in Pilar software and their interdependencies, we created a report with the evaluation of the assets. For the implementation we interviews by managers, by the responsible people for the assets, the services, and for each asset set a description of characteristics:

- Code
- Name, description
- Type which characterize the asset
- Responsible staff
- Technical or geographical location
- Amount, where appropriate, for instance 300 office PCs
- Limits within which an asset is relevant
- Calculate the assessment
- Explanation of the evaluation
- Interviews

The results of the assessment depends on the completeness of the estimates-replies to analysts. For the valuation taken into consideration, the accumulated value of goods.

The evaluation was guided by the need to protect assets elements. The more valuable that is, the higher was the level of protection an asset, the greater is the need of protection. Therefore, the more is the countermeasures required to meet the security requirements of confidentiality, integrity, and availability.

The valuation takes account of the replacement costs, labor costs, loss of income, loss of function, penalties not legal compliance, the damage to other property or people and to environmental damage. The conclusions resulting reduced the total of each group of data.

The hardware and software was valued based on the cost of replacement.

The valuation scale is as follow:

Value		Criteria
10	Very high	Very great harm to the organization
7-9	High	Serious damage to the organization
4-6	Medium	Significant damage to the organization
1-3	Low	Little damage to the organization
0	Minimum	Irrelevant for practical reasons

The following sections describe in detail the impact assessment of the n Breach of security of the three data sets were evaluated in the study. All items are rated as very high should protect them immediately.

6.9.3 Patient data (customer)

Content: Patient Data consist of personal information hospitalized, or not, patients have been examined by the laboratory and sensitive medical data (eg disease diagnosis, examination results). These data do not include data relating to infectious diseases.

Related System: Patient data is stored in the system each respective facilities Laboratory.

At the same time, there manuscript Patient file that kept referrals from clinical and laboratory analyzes. A proportion of these elements then destroyed by their use, while the books are stored in Archive.

Availability loss of patient data

Impact: The unavailability of Patient data will not bring about significant impact on the smooth functioning of hospitals kept manuscripts. In addition, test results are returned to the clinic that requested and then part of the data is destroyed.

Valuation: therefore, the consequence of loss of availability for up to a day measured with a grade **three (3)**, in the range 0-10.

Data integrity Loss Patients - Deliberate Distortion Data workshops

Impact: The deliberate alteration of the results of examinations of laboratory can endanger the life and security of peer-reviewed, and patients' data define the actions for the medical monitoring of patients. In conclusion, a successful deliberate alteration of such data might harm the security of the hospital patients.

Valuation: In accordance with the above scenario, the consequence of deliberate tampering valued grade **five (5)**, on a scale of 0-10.

Loss of confidentiality

Impact: The Patient Data are sensitive personal data. According to Law. 2472/97 eventual disclosure may result in criminal penalties and direct impact on the public image and credibility.

Law 2472/97 provides for significant fines and prison sentences for the data controller does not comply, which reach up to ten (10) years in exceptional cases.

Valuation: The impact of the disclosure to third parties of patient health data measured by grade **six (6)** in the range 0-10.

Impact Category	Effects on hospital	Rate valuation
Availability loss of data	1 day	Economic loss	3
Integrity loss of data	Data corruption	Criminal sanctions – Destruction reputation	5
Confidentiality loss	Disclosure of data to 3rd parties	Criminal sanctions	6

6.9.2.1 Personnel data

Content: The Personnel Data include personal data of employees of the hospital and their professional position and their sick leave figures. In addition, these data include sensitive personal data relating to criminal records of each employee.

Related System: The Personal Data kept in the Personnel application housed in the Computer Room, in the hospital basement. In addition, all relevant information (eg. personal details and criminal record) is stored in handwritten form in physical file housed in the Personnel Department on the ground floor the main building of the hospital.

Availability loss of personnel data

Impact: The unavailability of such data does not interrupt the proper functioning of the Personnel Division. The impact of the loss of availability of personnel data is not important, as is the use of manual records.

Valuation: The impact of the unavailability of such data is evaluated with a grade **three (3)** for up to one day, on a scale of 0-10.

Data integrity Loss Patients - Deliberate Distortion Data workshops

Impact: The incorrect import data are then entered by taking the last backup, or loss of data, it has the effect of reintroducing there. Another implication in this case involves the costs incurred by the respective man-hours required for the reintroduction of the data. Greater impact resulting the erroneous insertion of criminal record data, which can adversely fix professional development of employees.

Valuation: The consequence of loss of data integrity in accordance with the above measured with grade **three (3)**.

Confidentiality loss (revelation) of personnel data

Impact: The disclosure of other employees personal data of employees or third parties, would impact any personal, financial and other benefits for them. In this case the Hospital subject to the provisions of the law set by law for the loss of confidentiality of personal data, including both financial consequences and criminal consequences for it. In addition, the hospital includes the sensitive personal data of criminal records of each employee, any disclosure is a serious violation of Law. 2472/97 with the corresponding penalties.

Valuation: The impact of the disclosure of Personal Data to third parties is valued with grade **six (6)**.

Impact Category	Effects on hospital	Rate valuation
Availability loss of data	1 day	Economic loss	3
Integrity loss of data	Data corruption	Criminal sanctions – Destruction reputation	5
Confidentiality loss	Disclosure of data to 3rd parties	Criminal sanctions	6

6.9.2.2 Payroll data

Content: The data include personal (such as licenses, but mainly financial information regarding employees at the Hospital and loan data received by employees of the hospital.

Related System: The Payroll Data kept in the Payroll application housed in the Payroll Department facilities on the ground floor of the hospital.

Availability loss of payroll data

Impact: The loss of availability of payroll data lead to default which could lead to lawsuits against the company and resignation. The personal effects arising mainly the difficulty issuing payroll statements and additional man-hours required. The unavailability of these data not will impede the smooth operation of the Payroll Department.

Valuation: Due to the fact that wage statements can be supplemented using handwritten data, the operation of the section can be carried out smoothly if the application is not available for several days. The impact of the unavailability of such data is evaluated with a grade **three (3)** for one week or more, on a scale of **0-10**.

Integrity loss or Partial Data Destruction of Payroll data

Impact: The alteration of Payroll Data, including the spare copies, requires re-entering the data in the application, based on the original data kept in natural Payroll file. Significant effects can import errors in financial losses for the hospital. Additional problems arise

regarding the employee loan details (dues, fees etc.) that causes additional cost Recovery of these assets by the respective creditor.

Valuation: Consequently, it is estimated that there will be a financial burden on the man-hours necessary for the introduction of data. The effect of the partial destruction of the data likelihood valued degree **three (3)**, in the range **0-10**.

Confidentiality loss

Impact: The payroll data is generally confidential. Unauthorized disclosure them to other employees or third parties, would result in any personal, financial and other benefits for them. Therefore it has the effect of violating the law due to the fact that the data is sensitive.

In this case the hospital will suffer the consequences that the law states for the loss of confidentiality of personal data, which include both fines and penal consequences.

Valuation: Based on the above, the result of the disclosure of such data is measured with a grade **three (3)**, on a scale of **0-10**.

Impact Category		Effects on hospital	Rate valuation
Availability loss of data	1 day	Economic loss	3
Integrity loss of data	Data corruption	Criminal sanctions – Destruction reputation	5
Confidentiality loss	Disclosure of data to 3rd parties	Criminal sanctions	3

Overall assessment of these cases is:

	Availability loss	Integrity loss	Disclosure to 3rd parties
	1 day	Total destruction	Disclosure of data to 3rd parties
Patient data	3	**5**	**6**
Payroll data	1	3	3
Accounting data	**5**	**6**	1

6.9.4 Material valuation

Following we evaluate the material according to their monetary value in case of replacement.

Asset	Quantity	Valuation grade	Replacement cost
Work station	250	4	1000
Router/ switch	6	4	5800
Printer	5	2	1500
Server payroll application	4	2	4500
Client server application	1	3	2200
Server DB	2	3	2200

6.9.5 Software valuation

For the evaluation of the software evaluation method followed by their replacement cost shown as follows:

Software destruction	Consequently for the hospital	Rate Valuation
Software system of patients	Financial loss	8
Software payroll system	Financial loss	9
Software personnel management system	Financial loss	4

6.10 Impact Assessment

6.10.1 Identification of threats to IS

Below shows the assets:

Threat	Requirements related to security
Criminal impersonation	Authentication
Unauthorized use of application	Authorization check
Introduction of virus – like software	Introducing prevention mechanisms virus-like software
Filtration – interference communication	Confidentiality - Integrity - Availability
Server failure	Technical assistance
Network fault management server or appliance or gateway	Technical assistance
Error handling or user	Staff training
Stopping power	Uninterrupted power supplies
Conditioning failure	Technical assistance
System software failure and network software	Quality software
Application software failure	Testing and quality applications
Hardware maintenance error	Technical assistance
Software maintenance error	Technical assistance
Fire	Fire prevention mechanisms
Flood	Flood prevention mechanisms
Natural disaster	Functions continuation plan
Lack of staff	Functions continuation plan
Theft	Protection against theft
Intentional damage – vandalism	Personal control

To implement the Magerit methodology created many scenarios that take into account the threats on all assets of the Information System. In most of these threat scenarios may appear more than once and in different degrees.

6.10.2 Assessing threats to IS

6.10.2.1 Methodology

When an asset is vulnerable does not mean that all the security dimensions equally affected. So we need to determine that the threat can harm an asset to the report of the element in this has two parameters:

- Degradation: The amount of damage done to the value of the asset.
- Likelihood: How often the threat occurs.

When threats are not deliberate enough to know the part of the natural loss of the asset to measure the loss of value. In case of deliberate intent, the attacker can cause more damage indirectly.

The likelihood is more complex. Sometime modeled quantitatively using the following scale. The following table shows the degradation values.

VH	Very High	Almost certain	Easy
H	High	Very high	Medium
M	Medium	Potential	Hard
L	Low	No possible	Very hard
VL	Very Low	Very rarely	Extremely hard

When an asset is suffering a threat, loses part of its value. The shortfall may be between 0% and 100% and takes values from 0.0 to 1.0. Rarely, the probability is numerically modeled as a percentage events. It is customary to use the one year as the reference, so that the display be made as annual amount as a measure of the probability that this happens.

Typical values (likelihood) are:

100	Very often	Every day
10	Often	Monthly
1	Regular	Annually
1/10	No often	Every few years

The following scale is a tool to rate the assets, the size of the impact:

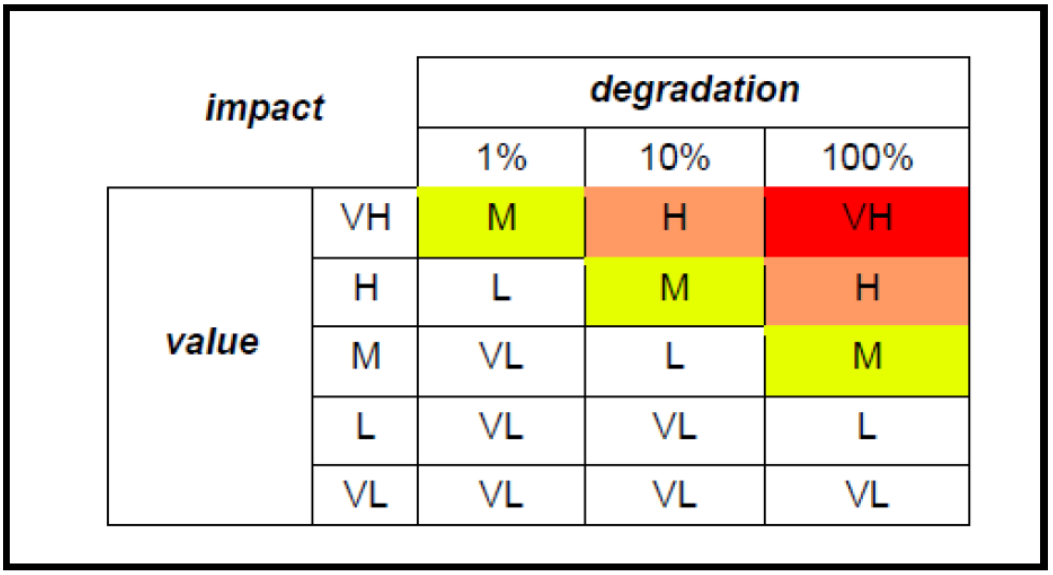


Figure 33: *Size of impact*

6.10.2.2 Determination of the potential impact

The effect is to measure the loss per asset arising from the emergence of the threat. Knowing the value of the assets (for various security requirements) and the loss caused by the threats, their impact on the system that can be readily deduced.

Initially, the potential (potential) impact is calculated per asset which does not take into account existing security measures which we have defined and evaluated in the previous step.

6.10.2.3 Accumulated impact

The accumulated impact is measured for each asset for each threat and each evaluation dimension.

As for an asset measure the accumulated impact (its own in addition to the total value of the assets that depend on it). The accumulated impact is calculated as the higher value of the values included between the assets and all those who depend on the number and total threats they are subject.

The overall impact of the threat to an asset is to measure the total loss of value. If an asset has a total value of vx and the reduction value is d then the value of the overall impact of the threat is:

$$\boldsymbol{Impact = Vround(Xx\ d)}$$

The greater the total valuation of the asset and the degradation of the aggressor asset, the greater the impact. Must take into account the dependencies between assets. Often the value of information system is to provide services and data handling while threats usually appear on interdependent assets.

6.10.2.4 Deflected impact

The deflected impact is calculated for each asset for each threat and each security requirement as a function having the actual value and the degradation caused.

If an asset A depends on an asset B, threats of B will affect the element A. If B is subject to a "d" decrease, this will happen in the "A" and the impact on A would be the loss of basic value. If the value of A is «V» then the value of the effect is:

$$\boldsymbol{Impact = V\ x\ d\ x\ degree(AB)}$$

The deflected impact is estimated for each asset.

6.10.2.5 Residual impact

Calculate the residual impact of asset taking into account existing security measures of the system. The calculation is based on the Magerit methodology.

6.10.2.6 Valuation Results threats

For assessing threats were answered scenarios on interviews. The procedure was carried out took several meetings with IT managers.

We chose from the suggested threats the most appropriate for the case of the Hospital, then from the options menu options chose to manually import the threats valuation prices and not automatically as shown by the following image parameters. According to the default values of parameters for threats.tsv file that has information about the assessment of threats, the frequency for each security requirement for each asset. That is, for example the threat E2 frequency of 1.0, the security requirement for D is applied to a loss of 20%, as they correspond to the security domain: base is selected as follows:

threats.tsv	meaning
<?xml version="1.0" encoding="UTF-8" ?> <threat-standard-values> <family F="HW"> <threat Z="E.2" f="1.0" s="6h"> <set D="D" deg="0.2"/> <set D="I" deg="0.2"/> <set D="C" deg="0.2"/> </threat> <threat Z="E.23" f="1.0" s="1d"> <set D="D" deg="0.1"/> </threat> <threat Z="E.24" f="10.0" s="30m"> <set D="D" deg="0.5"/> </threat> <threat Z="E.25" f="1.0" s="2d"> <set D="D" deg="1.0"/> <set D="C" deg="0.5"/> </threat> <threat Z="A.6" f="1.0"> <set D="I" deg="0.1"/> <set D="C" deg="0.5"/> </threat>	format: XML for every asset of class HW … apply threat E.2 with frequency 1.0 apply to dimension D, degradation 20% … and so on … please, notice that security dimensions are in Spanish D for availability I for integrity C for confidentiality A for authenticity T for accountability

More specifically showing the match in the following Table:

applicable	family	threat	likelihood	step	D=D	D=I	D=C	D=A	D=T	D=V
	arch.ip	E.15	1			10%				
	arch.ip	E.18	1	1d	10%					
	arch.ip	E.19	1				10%			
	arch.ip	A.5	1			50%	50%	50%		
	arch.ip	A.11	1			50%	50%			
	arch.ip	A.15	1			50%				
	arch.ip	A.18	1	5d	50%					
	arch.ip	A.19	1				50%			
	D	E.1	10	2h	10%	10%	10%			
	D	E.2	1	6h	20%	20%	20%			
	D	E.15	1			1%				
	D	E.18	1	1d	1%					
	D	E.19	1				10%			
	D	A.5	10			10%	50%	100%		
	D	A.6	10	1d	1%	10%	50%			
	D	A.11	100			10%	50%			
	D	A.15	10			100%				
	D	A.18	10	2d	50%					
	D	A.19	10				100%			
	D.conf	E.4	1			1%				

Also downloaded from the website of the NIST https://nvd.nist.gov files CVE-2015-5434, CVE-2015-6860 to the vulnerabilities. We introduced these files with the values of the valuation of vulnerabilities in the menu technical vulnerabilities (cve) for computer hardware (server, compaqproliantml370, personal computer) of the system under analysis. Vulnerability degree is how easily the worst can happen to an asset.

The summary results of the process of threat assessment are shown below:

Threat	Asset	Likelihood
Impersonation by internal users	Software of patient system Software of payroll system Software of personnel management system	VH VH M
Impersonation by service providers	Software of patient system Software of payroll system Software of personnel management system	VL VL VL
Impersonation by external users	Software of patient system Software of payroll system (Host DB) Software of personnel management system	H H H
Stopping power	Material system of patients Material payroll system Material payroll system	VH VH VH
Conditioning failure	Material system of patients Material payroll system Material payroll system	M H H
Application software failure	Server payroll application Staff applications Patient applications	VH VH VH
Hardware maintenance error	Material system of patients Material payroll system Material payroll system	VH L L
Software maintenance error	Material system of patients Material payroll system Material payroll system	L L L
Wrong user	Software of patient system Software of payroll system (Host DB) Software of personnel management system	M M M
Fire	Central building Building 2 Building 3	VL VL VL
Flood	Central building Building 2 Building 3	VL VL VL
Theft by internal users	Work station Switches Printers	L L VL

6.10.2.7 Discussion of the results

From the above table it appears that some threats are more important in criticality level from other.

Threats by rating High, Very High and above should be taken seriously and addressed appropriately as the most critical. Since the threats with the lowest score may cause the vulnerability of the entire IS should be considered a priority.

Points deemed critical workstations for a day are as follows:

- Virus – like software
- Impersonation of Internal Users
- Impersonation by External Users
- System Software Failure and Network Software (the implementation payroll)
- Failure Application Software
- Wrong User
- Electricity blackouts
- Theft of documents or other IS goods (from people outside the Hospital)

These threats were rated with high scores so should be given great attention and priority to the implementation of the measures to address the fact that they have a big impact in IS. But this should not mean that they will not take into account other threats. Although all threats must be treated with the seriousness that they deserve, it is known that a strong system security is as much and security of the weak point.

6.11 Calculation of the IS risk

6.11.1 Methodology

The methodology Magerit calculates the risk as follow:

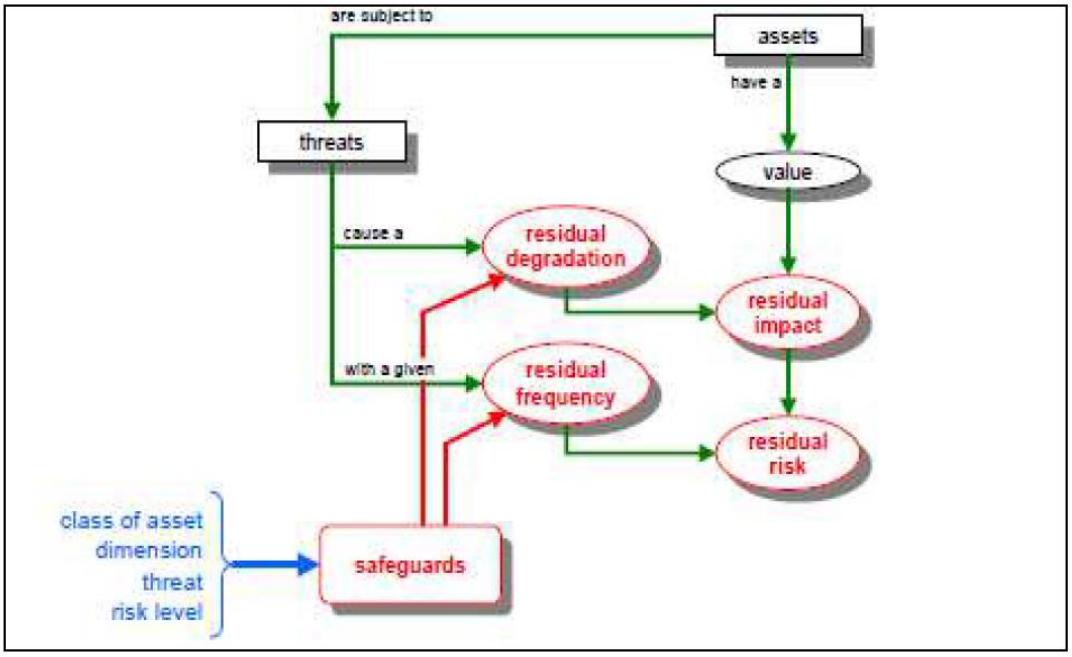


Figure 34: *MAGERIT calculation of risks*

The risk is calculated as a function of the effect and frequency:

$$\boldsymbol{Risk} = (\boldsymbol{effect}, \boldsymbol{frequency})$$

Risk is a real value greater than zero. Prices are in Euro and frequency counts annual events. If 0.1 means once every 10 years for an asset that has value 900,000 then the estimated risk is 900.000ch 0.1 = 90000.

The frequency of threats

The frequency of threats described by a series of symbolic values.

A threat has j frequency points to the overall incidence rate fj.I be modeled by a simple scale.

- VF: very frequent (daily)
- F: frequent (monthly)
- NF: normal frequency (yearly)
- I: infrequent (every few years)

risk		*frequency*			
		PF	FN	F	MF
impact	VH	H	VH	VH	VH
	H	M	H	VH	VH
	M	B	M	H	VH
	L	VL	L	M	H
	VL	VL	VL	L	M

The calculated impact is the cost arising from the threat and the target (Target) is calculated as the risk to annual losses.

6.11.2 Determination of theoretical risk

The risk is to measure the possible damage to the system. Knowing the impact of threats to assets, the risk can be calculated directly taking into account the probability of their occurrence. High impact and very high probability produce high risk. The potential risk to which the system is subject, taking into account the value of assets and assessing threats but not the countermeasures used.

6.11.3 Determination of residual risk

Carry out a selection of existing security measures with the **Statement of Applicability** and then their valuation. Subsequently, performed an assessment of the appropriateness of Safeguards, the quality of their implementation, user training in their use.

Then, the remaining risk takes into account the residual impact and effectiveness of the measures implemented. It is estimated that the risk of the remaining frequency and remaining impact.

$$\boldsymbol{Residual\ Risk} = (\boldsymbol{Residual\ Impact}, \boldsymbol{Residual\ Frequency})$$

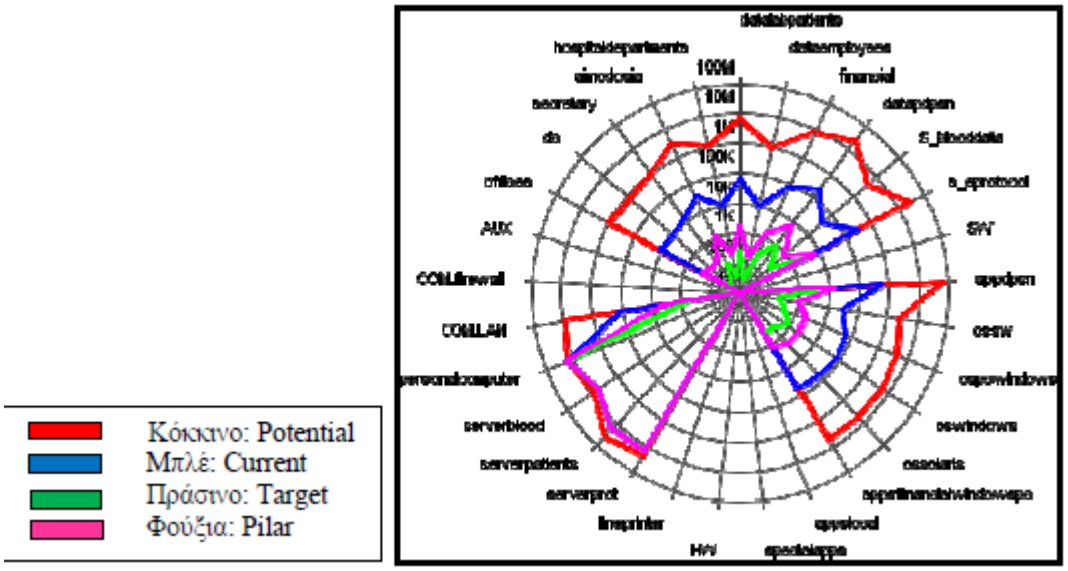
Because the reflected impact is estimated to have assets assess their own value, allows determining the consequences in technical events. The results of this evaluation therefore best help the administration to obtain critical decisions on information risk analysis: to make acceptable a certain level risk.

6.11.4 Results of risk assessment

The table and figure below show the assessment of risks to the critical assets of IS elements. When interpreting the results process became a priority in the assets subject to the greatest impact and the greatest risk. Pilar software automatically calculates the degree of risk since the previous completed stages of asset evaluation, threat. The Pilar automatically calculates the risk as the amount which must be taken into account for annual losses. The following table shows the measurement of the deflected risk in connection with the threats that are likely likelihood 10% and the impact in the hospital is 50%.

Father	Child	Threat	Risk	Current	Target	PILAR
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	2,00E+13	1,68E+11	7,43E+08	4,65E+09
[financial] finlogisticssubcontractor	[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	2,00E+13	2,12E+11	2,55E+09	4,38E+09
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[A.11] Unauthorised access	1,04E+13	1,32E+11	7,13E+08	2,17E+09
[dataemployees] dataemployees	[datapdpsn] datadpsn	[E.2] System / Security administrator errors	1,00E+13	7,87E+10	3,70E+08	2,78E+09
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	4,30E+12	4,41E+10	4,68E+08	9,35E+08
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	4,30E+12	4,05E+10	2,69E+08	8,70E+08
[financial] finlogisticssubcontractor	[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	4,30E+12	3,61E+10	1,59E+08	1,02E+09
[financial] finlogisticssubcontractor	[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	4,30E+12	4,05E+10	2,69E+08	8,76E+08
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[A.24] Denial of service	2,43E+12	3,00E+10	1,02E+08	1,08E+09
[dataemployees] dataemployees	[datapdpsn] datadpsn	[E.2] System / Security administrator errors	2,15E+12	1,52E+10	7,67E+07	4,74E+08
[dataemployees] dataemployees	[datapdpsn] datadpsn	[E.2] System / Security administrator errors	2,15E+12	1,52E+10	7,67E+07	4,74E+08
[dataemployees] dataemployees	[datapdpsn] datadpsn	[E.2] System / Security administrator errors	2,15E+12	1,52E+10	7,67E+07	4,75E+08
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[E.2] System / Security administrator errors	2,15E+12	1,66E+10	7,72E+07	3,94E+08
[dataemployees] dataemployees	[appdpsn] appdpsnsolarisml370	[A.11] Unauthorised access	2,09E+12	2,48E+10	8,46E+07	4,34E+08
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[A.22] Software manipulation	1,22E+12	1,61E+10	7,70E+07	4,80E+08
[financial] finlogisticssubcontractor	[oswindows] oswindows200serve	[A.22] Software manipulation	1,22E+12	1,52E+10	7,70E+07	6,31E+08
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[I.6] Power interruption	1,05E+12	1,37E+10	4,67E+07	3,65E+08
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[A.27] Enemy over-run	1,00E+12	1,30E+10	4,44E+07	5,63E+08
[dataemployees] dataemployees	[ossolaris] solaris	[A.8] Malware diffusion	9,70E+11	1,05E+10	3,58E+07	1,33E+08
[dataemployees] dataemployees	[appsfinancialwindowspc] logisticsexternalpatients	[A.8] Malware diffusion	9,70E+11	1,05E+10	3,58E+07	1,33E+08
[financial] finlogisticssubcontractor	[serverprot] questwinerserver	[A.8] Malware diffusion	9,70E+11	1,05E+10	3,57E+07	1,48E+08
[financial] finlogisticssubcontractor	[oswindows] oswindows200server	[A.8] Malware diffusion	9,70E+11	1,05E+10	3,58E+07	1,33E+08
[dataemployees] dataemployees	[serverpatients] compaqproliantml370	[E.25] Equipment loss	1,15E+11	1,48E+09	5,96E+06	4,47E+07
[dataemployees] dataemployees	[dc]	[A.27] Enemy over-	1,00E+11	1,30E+09	4,44E+06	5,63E+07
	datacenterpliroforikhsorganwsis	run				
[dataemployees] dataemployees	[offices] workingroomisthodosias	[A.27] Enemy over-run	1,00E+11	1,30E+09	4,44E+06	5,63E+07
[financial] finlogisticssubcontractor	[s_eprotocol] s_eprotocol	[E.2] System / Security administrator errors	1,00E+11	7,70E+08	3,57E+06	1,95E+07
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[A.27] Enemy over-run	1,00E+10	1,30E+08	0,00E+00	5,65E+06
[dataemployees] dataemployees	[hospitaldepartments] hospitaldepartments	[N.1] Fire	1,00E+10	1,31E+08	0,00E+00	5,06E+06
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[N.2] Water	1,00E+10	1,77E+08	0,00E+00	5,50E+06
[dataemployees] dataemployees	[aimodosia] workingroomaimodosia	[N.1] Fire	1,00E+10	1,31E+08	0,00E+00	5,06E+06

Specifically, the total valuation of the deflected impact for risk likelihood 10% and 10% impact.



1. The total risk calculated under certain conditions.
2. In accordance with the methodology Magerit the residual risk calculated in efferent assets.
3. Calculated the total risk assets have interdependence and nothing in common with the higher hierarchy of dependencies assets.
4. Calculated risk delivered from different threats on the same property element as well as the risk of a threat with different security requirements.
5. There was summed the total risk of dependent assets.

6.12 CRAMM Methodology

In the previous section we presented the reasons why applying the principle of proportionality is a precondition for the development of a security plan that will be rewarding, in cost-benefit terms, ie there will be no waste of resources for implementing countermeasures protection faced insignificant threats, while effectively address the threats are significant. The methodology ensures the application of the proportionality principle is the Risk Analysis.

The Risk Analysis based on the analysis of threats, vulnerabilities and impacts. It is obvious that the number, variety and complexity of threats facing a IS not allow simplistic-empirical treatment of the subject. Although the experience and skills of a security analyzer are positive elements in order to perform the entire process, the risk of default or devaluation of a threat cannot be ignored. The same is true for system weaknesses. Moreover, the threats and weaknesses combinations will have to be considered, it is so that it is impossible to analyze without using an automated tool. Also, the correct choice of countermeasures is

greatly facilitated by using an automated tool, which can directly connect the proposed countermeasures on the size and nature of Risk.

The risk analysis methodology applied to this project has the following characteristics:

- It is proven in similar magnitude and significance IS.
- The members of the project team have sufficient experience of its application to respective environments.
- It covers all stages of the Risk Assessment.
- Covers all aspects of security.
- Accompanied by an automated tool.

6.13 Data valuation

The data are evaluated on the basis of the views of end-users of information provided by the information systems of the hospital. As part of the methodology followed, the valuation does not take into account the likelihood of a threat, but only the effect of possible successful completion of this threat. The accuracy of measurement depends on the accuracy and completeness of data and relevant estimates communicated to scholars.

The evaluation is carried out numerically on a scale of 0-10 and the values attributed arising from the Valuation Tables accompanying the method and CRAMM software tool.

In this context he asked the executives of the Hospital to describe the most pessimistic, in their view, scenario for the impact that would have each of the following scenarios, ignoring the existing security measures:

- loss of data availability
- loss of data integrity
- disclosure of data

In some cases, where further analysis, considered separately and the sub total destruction of data and deliberate alteration of data.

Note that all data managed by IS separated and studied in representative groups, depending on the characteristics and security needs they have. Specifically, evaluated the effects of the following sets of data: *Personnel Data, Payroll Data and Patient Movement Data.* Consequently, the conclusions drawn relate to the whole of group data.

A future revision of the Security Plan, possible options should be considered again by the number of major changes that may have taken place in the hospital information systems and services they offer.

6.14 Valuation of the results

The following sections describe in detail the assessment of the effects of the breach of security of the data sets were evaluated in the study.

6.14.1 Personnel data

Content: The Personal Data include personal data relating to workers in the hospital and their professional status, and evidence of long term sick leave for workers, without mentioning the condition. Furthermore, the data from this group include sensitive personal data relating to criminal records of each employee.

Related System: The Personal Data kept in application Pre-personnel housed in the Department of Computer Science facilities (Computer Room), in the hospital basement. In addition, all relevant information (eg personal details and criminal records) are kept in print in physical file located in the Personnel Department on the ground floor of the central building facilities of the Hospital.

Loss of Personnel Data Availability

Impact: The unavailability of these data will be very difficult to work of the Personnel Division and smooth operation. The unavailability of the Personal Data no significant effects will result in the smooth operation of the department, as is the use of manual records.

Valuation: The impact of the loss of availability of the data measured in degree **three (3)** for up to a day and with a **five (5)** for one week or more, in the range 0-10.

Destruction of Personnel Data

Impact: The total destruction of Personal Data, including backup, implies the reintroduction of the data in the application, on the basis of primary documents kept in natural Personnel file. Thus it is estimated that there will be economic costs on the man-hours necessary for the introduction of data.

Valuation: The impact of total destruction of the data potential is measured with a grade **five (5)**, on a scale of 0-10.

Loss of Partial Integrity Personal Data

Impact: The loss of data is then entered by taking the last backup, or introducing errors in the data, involves the re-introduction. Significant impact resulting from the incorrect insertion of criminal record data, which can influence the professional development of employees. Another implication in this case involves the costs incurred by the required time of reimportation and the corresponding man.

Valuation: The consequence of loss of data integrity in accordance with the above measured with grade **three (3)** to the case for introducing errors on a small scale and with a **five (5)** cases of partial loss and introduction of extensive errors in scale 0- 10.

Deliberate Distortion Personnel Data

Impact: The deliberate alteration of Hospital Personnel data would result in the same economic or other benefit for the person who made the alteration. Benefit from the deliberate alteration of the Personal Data could have person has no criminal record.

Valuation: In accordance with the above scenario the consequence of deliberate alteration of the Personal data measured by the extent of **five (5)** in the range 0-10.

Disclosure of Personnel Data

Impact: The disclosure of other employees' personnel data of employees or third parties, would result in personal, financial and other benefits for them. In this case the hospital will suffer significant consequences provided by law for the loss of confidentiality of personal data, including both financial penalties and criminal consequences for the controller. But as the data are integrated and sensitive personal data of criminal records of each employee, any disclosure is a serious violation of Law. 2472/97 and will bring about penalties.

Valuation: The impact of the disclosure of Personal Data to third parties is valued with grade **six (6)**.

6.14.2 Payroll data

Content: These data include personal, but mainly financial information regarding employees at the Hospital. Also, include information relating to authorizations, sick and others received by workers and loan data they receive workers through the hospital.

Related System: The Payroll Data kept in the Payroll application housed in the Payroll Department facilities on the ground floor of the hospital.

Loss Data Availability Payroll

Impact: The unavailability of these elements will not impede the smooth operation of the Payroll Department. The operation of the section can be carried out smoothly if the application is not available for days, as wage statements can be supplemented using handwritten data. The effects arising mainly the difficulty issuing payroll and extra man-hours required.

Valuation: The impact of the loss of availability of the data measured by the extent of **one (1)** for up to a day and with a **three (3)** for one week or more, in the range 0-10.

Destruction of Data Payroll

Impact: The total destruction of Payroll Data, including backup, implies the reintroduction of the data in the application, on the basis of primary documents kept in natural Payroll file. In case of loss and natural Payroll file, the data can be drawn from the Personnel Department. Thus it is estimated that there will be economic costs on the man-hours necessary for the introduction of data. Problems arise with respect to employee loans data (debts installments etc.). Consequently there will be an extra cost of repairing these elements through the respective creditor.

Valuation: The impact of total destruction of the data potential is measured with a grade **three (3)**, on a scale of 0-10.

Partial Damage or Loss of Integrity Data Payroll

Impact: The loss of data entered after taking the last backup involves re-introduction. The main impact of the expenditure resulting from the required time of reimportation and the corresponding man. More serious effects of the introduction of errors in the data, as it can lead to financial losses for the hospital.

Valuation: The impact of data integrity loss is measured by the extent of **one (1)** for the partial loss of data and the limited existence of errors, and with a **three (3)** in the case of extensive errors in the range 0-10.

Deliberate Distortion Data Payroll

Impact: The deliberate alteration of Payroll Data would result in a financial or other benefit for the person who made the alteration and consequently financial losses for the hospital. Under this scenario, it should be noted that the possibility of a possible lesion appears limited, as the repeated checks and cross-checks carried out will reveal inaccuracies.

Valuation: In accordance with the above scenario the consequence of deliberate alteration of Payroll data measured with degree **three (3)**, on a scale of 0-10.

Revelation Payroll Data

Impact: The payroll data is generally confidential. Possible non-authorized disclosure to other employees or third parties, would result in personal, financial and other benefits for them. In this case the hospital will bear the consequences which the law provides for the loss of confidentiality of personal data, including both financial penalties and criminal consequences for the controller

Valuation: Based on the above, the result of the disclosure of such data is measured with a grade **three (3)**, on a scale of 0-10.

6.14.3 Customer traffic data

Content: The Patient Data Movement involving personal and sensitive personal patient data, the system introduced, other than personal patient data and medical information, including diagnosis input and output.

Related System: The Patient Data Movement met by the central management system housed at the Department of Informatics and Organization installations in the hospital basement and used by the Traffic desk. At the same time, they kept handwritten envelopes Patients of physicians who include sensitive medical data and stored in the respective offices of each physician.

Loss Patient Movement Availability Data

Impact: The unavailability of Patient Data Movement creates problems particularly in relation to the communication office with patients. Even short periods of unavailability can cause intense resentment to the public and harm the image of the hospital. At the same time, non-availability of Movement Patient data will prevent the issue of certificates Nursing and recovery of medical expenses from the pension funds, which creates problems in the smooth functioning of the financial transactions of the hospital. Larger delays cause problems to the overall function of the hospital, as it is possible to monitor imports of patients or issuing discharges.

Valuation: Based on the above, the consequence of the loss of availability for one-hour period is measured by the extent of **one (1)** for twelve hours by grade **three (3)** for a period of one day or more in grade **five (5)** to 0-10 scale.

Destruction Patient Movement Data

Impact: In the case of total destruction of Patient Data Movement hospital will incur significant costs for the reintroduction of the data from the large-volume manuscript file, provided that the latter is kept in top condition. Furthermore, the Patient Movement Office will not allow smooth operation, which is critical of the hospital point of contact with the hospitalized and significantly affect the operation and the remaining parts of the hospital, such as clinics. Furthermore, economic impacts arise hospital on the recovery of medical expenses from the insurance fund.

Valuation: In accordance with the above scenario, the consequence of the total destruction is measured by the extent of **five (5)**, on a scale of 0-10.

Partial destruction or loss of integrity Patient Movement Data

Impact: In case of partial loss or destruction import errors Data hospitalized, consistency is limited to the cost for the reintroduction of the data from the manuscript file, provided that

the latter is kept in top condition. Meanwhile, during data re hampered the smooth functioning of Patient Movement Office, as the work will have to be handled manually.

Valuation: The consequence of the limited existence of errors measured by the extent of **one (1)** and the loss of integrity, and the widespread availability of errors in grade **three (3),** on a scale of 0-10.

Deliberate Distortion Patient Movement Data

Impact: The impact of the deliberate alteration of the hospital's Patient Data Movement could provide personnel, financial or other benefit to the person who would carry out the lesion and hampers the smooth operation of the Traffic Office.

Valuation: In accordance with the above consistency deliberate tampering of these assets is measured by the extent to **three (3)**, on a scale of 0-10.

Disclosure of Patient Movement Data

Impact: The Patient Data Movement constitute sensitive personal data. Possible disclosure is the violation of Law. 2472/97 and brings criminal penalties. Law 2472/97 provides for significant fines and prison sentences for the data controller does not comply, which reach up to ten years in exceptional cases. In addition, the hospital would gather significant negative publicity, with direct impact on the public image and credibility.

Valuation: Consequently the valuation of revealing impact of these data to third parties is **six (6).**

6.14.4 Total data value measurement

The table below summarizes the impact assessment by making the threats, as described in the preceding paragraphs. Note that the threats whose consequences were evaluated with several degrees, depending on the threat scenario implementation (e.g. cases of partial loss) Table only the highest degree shown.

	Loss of Availability					Loss of Integrity			Disclosure to 3rd parties
	1 hour	12 hours	1 day	2 days	1 week	Total destruction	Partial destruction	Intentional corruption	
Personnel data		3	3		**5**	**5**	**5**	**5**	**6**
Payroll data	1		1		3	3	3	3	3
Traffic data patients	1	3	**5**			**5**	3	3	**6**

6.15 Risk Assessment

The valuation of property is one of the two factors that make the risk of IS, the effect. The second factor, the probability (likelihood), composed of the threat and vulnerability, as follows:

$$\boldsymbol{Threat\ x\ Vulnerability = Likelihood}$$

$$\boldsymbol{Likelihood\ x\ Effect = Hazard}$$

For example, if a threat is important and the IS is vulnerable to it, then the probability of realization is great and although the impact is significant, the risk becomes high.

In this chapter and the threats faced by IS hospital valued, grouped into the following categories:

- Access by unauthorized persons in the system
- Failure of hardware and software
- Unintentional injury, human errors
- Physical threats and disasters

Threats and specialized scripts - any threats are created, the likelihood of which is evaluated on a scale 1-5 (very low, low, moderate, high, very high). For each combination of threat - property of IS calculated a level of vulnerability in a 1-3 scale (low, moderate, high).

The degree of risk level is calculated on a scale 1-7. The calculation of the IS risk occurs automatically, as a combination of the following factors:

- Effect of loss of availability, integrity or confidentiality of the system of goods
- Level of threats faced by the system property
- Level vulnerabilities - weaknesses in the system.

6.15.1 Threats

The table in section 6.10.1 presents the main threats faced by IS and the main Building of the hospital facilities along with the corresponding requirements of security measures.

Within the scope of CRAMM methodology created many scenarios covering the possible threats for all elements of the system based on the above categories. Under these scenarios, any threat can be for more than one system components and even in different degrees.

For the hospital, the most important of these threats (likelihood Very High or High range Very High, High, Medium, Low, Very Low) listed below:

- Impersonation of Internal Users
- Impersonation by External Users
- System Software Failure and Network Software (the Payroll application)
- Failure Application Software
- Wrong User
- Electricity blackouts
- Theft of documents or other goods CP (from people outside the hospital)

6.15.2 Weaknesses and security problems

The weaknesses and vulnerabilities related points of the IS of the hospital which may allow or facilitate a threat to cause damage to it. Beyond the use of scenarios to assess the vulnerability of the IS, which has been under the methodology, the one IS weaknesses identified by site inspection, observation and interviews with relevant officers. Based on interviews with the hospital staff and the experience of the study, the project team identified the following points of the major weaknesses and the security problems regarding the IS of the hospital:

Basic weaknesses and security problems of IS
1. The hospital IS managing sensitive personal data, which are critical for the health of hospitalized patients.
2. A limited degree of awareness and training of a significant proportion of users in security.
3. Lack of organizational-administrative of IS security management scheme.
4. Piecemeal application of specific measures to protect personal and - especially - sensitive personal data.
5. Use systems / applications which are not managed by the IT department.
6. Problems of the premises housing the IS, related to the physical security of CP (e.g. inadequate maintenance of installations, pipelines being in places that host servers or other material value).
7. Staff workload, coupled with inadequate training in the use of applications, a large proportion of staff

The following are the results of the assessment of the main threats (likelihood Very High or High range Very High, High, Medium, Low, Very Low) and their respective vulnerability to the IS and the hospital facilities.

Impersonation by internal users

Asset	Event(s) (in case of threat realization)	Threat probability	Weakness level
Blood data, Laboratory data, Personnel data	Availability loss (up to 2 days), Partial destruction of data, data Disclosure within the Hospital	High	Medium
	Deliberate data modification	High	High
Communication data	Availability loss (up to 2 days), partial data corruption, data disclosure within the hospital, deliberate data modification	Very High	High
Pharmacy data	Availability loss (up to 2 days), Partial destruction of data, data Disclosure within the Hospital	Very High	Medium
	Deliberate data modification	Very High	High
Patient traffic data, Outpatient data	Availability loss (up to 2 days), Partial destruction of data, data Disclosure within the Hospital	High	Low
	Deliberate data modification	High	Medium
Accounting data	Availability loss (up to 2 days), Partial destruction of data, data Disclosure within the Hospital	High	Low
	Deliberate data modification	Very High	Medium
Payroll data	Deliberate data modification	High	High
Hospitalization data	Availability loss (up to 2 days), Partial destruction of data, data Disclosure within the Hospital	Very High	Low
	Deliberate data modification	Very High	Medium
Suppliers and contract data	Deliberate data modification	High	Medium

Impersonation by external users

Asset	Event(s) (in case of threat realization)	Threat probability	Weakness level
Blood data	Availability loss (up to 2 days), Partial destruction of data, deliberate data modification	High	Low
	Data disclosure in the Hospital	Very High	Low
Communication data, Laboratory data, Accounting data, Payroll data, Personnel data	Availability loss (up to 2 days), partial data corruption, data disclosure outside the hospital, deliberate data modification	High	Low
Pharmacy data	Availability loss (up to 2 days), Partial destruction of data	High	Low
	data Disclosure outside the hospital, deliberate data modification	Very High	Low
Patient traffic data, Outpatient data	Availability loss (up to 2 days), Partial destruction of data, deliberate data modification	High	Low
	Data disclosure in the Hospital	Very High	Low
Hospitalization data, Suppliers and contract data	Availability loss (up to 2 days), Partial destruction of data, data Disclosure outside the Hospital	High	Low
	Deliberate data modification	Very High	Low

Failure of System Software and Network Software (Payroll application)

Asset	Event(s) (in case of threat realization)	Threat probability	Weakness level
Payroll application server	Availability loss up to 15 minutes	Very High	High
	Availability Loss 1 hour up to 12 hours	High	Low

Failure of Software Application

Asset	Event(s) (in case of threat realization)	Threat probability	Weakness level
IS Management Application, *Office Application,* *Blood Application,* *Payroll Application,* *Firewall,* *Oracle DB*	Availability loss up to 15 minutes	Very High	High

User Error

Asset	Event(s) (in case of threat realization)	Threat probability	Weakness level
Blood data, *Accounting data,* *Payroll data*	Unauthorized change data (Small Scale)	High	Medium
Outpatient data, *Pharmacy data,* *Patient traffic data,* *Hospitalization data,* *Suppliers and contract data,* *Personnel data*	Unauthorized change data (Small Scale)	High	High

Power Cut

Asset	Event(s) (in case of threat realization)	Threat probability	Weakness level
Buildings hospital Facilities *Blood Station* *Payroll department* *IT and Management department* *Personnel department*	Availability loss up to 15 minutes	High	Low

Theft of documentations or other assets of IS (from people outside the hospital)

Asset	Event(s) (in case of threat realization)	Threat probability	Weakness level
Buildings hospital Facilities	Data disclosure in the Hospital	High	Medium

6.15.3 IS Risk Assessment

The risk level is calculated for each combination of threat, weakness and property valued at a scale 1-7. The calculation does not take into account the already established countermeasures. The price level of risk is used to select specific protection measures within the Security Plan.

The following tables present the assets combinations (data) of the IS of the hospital and threats, for which the highest risk scores were calculated (5-6).

Threat: Impersonation by internal users

Asset	Effect	Risk
Pharmacy data	Deliberate data modification	6
	Availability Loss 1 up to 2 days	5
Blood data, *Accounting data,* *Personnel data*	Deliberate data modification	5

Threat: Impersonation by external users

Asset	Effect	Risk
Blood data, *Pharmacy data,* *Patient traffic data*	Data disclosure in the Hospital	5
Pharmacy data	Deliberate data modification	5

Threat: Introduction virus-like software

Asset	Effect	Risk
Work Station	Total data corruption, unauthorized alteration data (Major), deliberate data modification	5

6.15.4 Risk Assessment Facilities

As for the data of the IS, for the premises, the risk level is calculated for each combination of threat, weakness and asset (facility) and evaluated on a scale 1-7. The calculation does not take into account the already established countermeasures. The price level of risk is used to select specific protection measures within the Security Plan.

The following table present the plant combinations hospital and threats, for which the highest risk scores were calculated (5-6).

Threat: Theft of documentations or other assets of IS (from people outside the hospital)

Asset	Effect	Risk
Buildings hospital Facilities	Data disclosure in the Hospital	5

6.16 Conclusions

After the evaluation done above seems that Magerit methodology is more suitable for Critical Infrastructures. More specifically, this methodology is more friendly to the user than it is the CRAMM and easier to find it. Moreover, it is very convenient the fact that there is a 30 days trial so as to try if it suitable for each organization and the price to buy it is reasonable. Furthermore, this methodology accompanied by an automated software tool

that supports all stages of the application and selecting countermeasures and covers all aspects of security, including the technical factor, processes and personnel issues, physical security, network security, etc. Finally, PILAR software supports all the complex calculations required to determine the risk, and integrates the basis of countermeasures and selection mechanisms appropriate countermeasures.

In contrast, someone require to have expert knowledge in order to use the CRAMM methodology. Another drawback in CRAMM methodology is the fact that full assessments can be lengthy or overly-complex and it can only be used in conjunction with dedicated tool. Finally, the price to buy the software is very high and the annual license is costly, as well.

7 Chapter 7 – Conclusions and Future Work

With the rise of the need to properly secure information systems has come a rise in the number and diversity of methodologies and tools to help achieve this. From national's regulations to international standards and from third party tools to RM frameworks, this multitude of resources can be confusing for a company seeking to improve their information security. However, the applicability and benefits offered by each can be traced back to their original context and purpose.

In this document, a total of methodologies, tools and conceptual models have been analyzed, described and reviewed in order to provide at least basic information regarding each of the vast amount of instruments available for conducting and support Risk Assessment. Furthermore, comparisons and cross – comparisons have been conducted and guidelines have been designed in order to facilitate the selection process an organization might have to go through when it decides that a Risk Assessment is required or might bring added value and security to their business. Finally, a series of conclusions can be drawn based on this work.

Some methodologies are designed for security – critical systems, while others are created with certification in mind. Some tools are expensive and can only be used by experts while others are free and easy to use. Some frameworks are overly complex and only suitable for large project and organizations while others can be implemented by a few skilled employees. Such criteria can be used to not only classify and understand the scope, applicability and benefits offered by each methodology, framework and tools, but also as indicators for any business environment and protection requirements.

While a large number of methodologies that can be used to perform IS Risk Assessment, the number of tools that can be used in conjunction with these methodologies is even larger. With tools falling into three (3) categories depending on their relation to a particular methodology (independent, generic, specialized), it is hard to identify what exactly are the differences between two (2) tools falling in the same category.

One particular framework sets out from the rest. This is the ISO/IEC set of Information Security standards. The current documents with relevancy to this topic are: ISO/IEC 13335-1. ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005. ISO/IEC 13335-1 described Risk at a conceptual level, 27001 is solely used for certification, and ISO/IEC 27002 and 27005 go into more details regarding implementing and maintaining an Information Security Risk Management, including how to perform Risk Assessments. All these documents form a central core to which most other tools and methodologies refer or comply to. This is possible also due to the high level of abstraction the documents tend to maintain to order to allow a broader spectrum of applicability. As such, while these standards can be used to show official compliance, they are less relevant when the goal of the Security or Risk Assessment is different from this. In such situations, lower granularity is required in the descriptions of the analysis steps. This is offered by other third-party tools and methods. Of course, a hybrid solution is achieved in practice, where the high-level standards are used in conjunction with

compatible implementation-level tools or more technical methodologies. In this way, desired output can be extracted from the Risk Assessment, while possibilities for certification, for showing compliance to certain rules/regulations or for performing standardized audits still remain, while also enjoying the benefits of the up-to-date, internationally sanctioned catalogs and good practices contained within the standards.

Underlying most methodologies is either a generic or custom conceptual model of Risk. Differences can be seen in the way Risk and related concepts are defined and related to each other, as well as in the way Risk it-self is decomposed. The number, naming and importance of factors driving Risk, as well as the way these factors are computed in order to evaluate Risk Levels differ from one framework to the other. While some might use different names for the same concept or factor, a set of fundamental entities seem to be present in all of them: Threat, Asset, Vulnerability and of course, Attack. Each framework, and even individual methodologies disagree with regard to the attributes that are relevant for each entity, as well as how these factors can be operationalized and measured. One other notable conclusion is that most Information Security Risk Assessment methods employ a Likelihood x Impact fundamental decomposition of Risk. Variations arise in the further decomposition of these two factors and the metrics used to estimate them. While models seem to be very closely related to the Likelihood (Threat, Asset) $\otimes$ Impact (Threat, Asset) interpretation of Risk, the concept of Vulnerability is always being taken into consideration, usually as one of the factors driving Likelihood. This approach stems from the traditional interpretation of Risk, outside of the IT field. However, even in general Risk Management, this approach is mostly recommended when several risks need to be evaluated in order to compare and prioritize them and does not give a good indication of absolute Risk. This is due to the fact when estimating Likelihood as probability or frequency, a certain time-frame is implied. For example: "probability of event taking place (within a year)" or "number of occurrences of event (per year)". The issue here stems from the fact that this time-frame is not always constant and sometimes not even made explicit thus creating a threat to the reproducibility of the results. Even when this is made explicit, catastrophic events make the issue of choosing the right time period in the interpretation of Likelihood as probability even more difficult: the probability of a fire destroying the archive servers within a year is very low, but within the lifetime of the infrastructures it is significant. The ISO/IEC conceptual model of Risk mostly described in ISO/IEC 13335-1:2004, that supports all other ISO Information Security standards in the 2700x series is the most widely accepted model, and most tools and methodologies are compatible to it and at least one 2700x RA/RM standard. It is also the most abstract one, described at a high-level with lack of technical details

Moreover, in the case study of the hospital a comparison between two methodologies was done in order to choose which one is the best option for Critical Infrastructures. Through the comparison we conclude that MAGERIT methodology via PILAR tool is better as is more user friendly and simpler.

As far as my proposal for future work concern, I would say that a new methodology must be made. More specifically, this new methodology will have elements of both MAGERIT and CRAMM methodologies for a comprehensive result. Furthermore, this methodology must be

accompanied with a software which will be easy to use and open-source in order to be accessible from the general public.

8 Chapter 8 – References

[1] R. J. Turk, “Cyber Incidents involving Control Systems”, INL, Idano Falls, Idaho, INL/EXT-05-00671 Oct. 2005

[2] S. Baker, G. Ivanov, S. Waterman, “In the Crossfire: Critical Infrastructure in the Age of the Cyber War, a global report on the threats facing key industries”, McAfee Inc, Santa Clara, CA, 7795rpt_cip_0110, 2010

[3] N. Falliere, L. O. Murchu, E. Chien, “W32 stuxnet dossier”, Symantec Corp, Cupertino, CA, Symantec security response version 1.4, February 2011

[4] M. Abrams, J. Weiss, “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services”, MITRE Corp & Applied Control Solutions, Australia, July 2008.

[5] J. Carr, S. Goel, “Project Grey Goose Report on Critical Infrastructure: Attacks, Actors and emerging Threats”, Grey Logic, January 2010

[6] R. M. Lee, M. J. Assante, T. Conway, “ICS CP/PE (Cyber to Physical or Process Effects) case study paper, German Steel Mill Cyber Attack”, SANS ICS, ICS Defense Use Case, 30 December 2014

[7] C. W. Axelroad, “Managing the Risks of Cyber Physical Systems”, Decilog Inc, Melville, NY

[8] System Engineering Handbook, 3.2.2 version, INCOSE

[9] National Science Foundation (NSF), Cyber-Physical System (CPS), Program Solicitation NSF 10-515, 2010, nsf.gov, [Online], Available: http://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm

[10] Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management, 2001

[11] The OWASP Foundation. The owasp risk rating methodology. htpps:// www.owasp.org/index.php/OWASP_Risk_Rating_Methodology , accessed on 03.03.2016

[12] W. Wang, Z. Lu, Cyber Security in the Smart Grid: Survey and Challenges, Survey Paper, Department of Electrical and Computing Engineering, North Carolina State University, Raleigh, NC 27606, USA , Computer Networks,

[13] The Open Group. Technical Standard to Risk Taxonomy. Number C081. January 2009

[14] Michael Dunner, Srinath Vasireddy, Ray Escamilla, J.D. Meier, Alex Mackman and Anandha Murukan. Improving web application security: Threats and countermeasures. http://msdn.microsoft.com/en-us/library/ff649874.aspx , 2010

[15] The Smart Grid Interoperability Panel – Cyber Security Working Group, Guidelines for smart grid cyber security, NISTIR 7628 (2010) 1–597.

[16] USA, NIST, Special Publication 800-82,Guide to Industrial Control Systems (ICS) Security, U.S Department of Commerce

[17] US Department of Energy, "Risk Management Guide", Washington: Department of Energy, [Online], Available: https://www.directives.doe.gov, [Accessed: Dec. 14, 2014]

[18] EURACOM, Deliverable D2.1, Common Areas of Risk Assessment Methodologies

[19] US Department of Energy, "NIST Special Publication 800-30, Revision 1, Guide for conducting Risk Assessments", Washington DC, Department of Energy, [Online], Available: http://www.nist.gov

[20] G. Giannopoulos, R. Filippini, M. Schimmer, Risk Assessment Methodologies for Critical Infrastructure protection. Part I: A state of the Art, JRC technical notes

[21] D. D. Dudenhoeffer, M. Manic, CIMS: a framework for infrastructure interdependency modeling and analysis, University of Idaho, Idaho national laboratory

[22] https://inlportal.inl.gov/portal/server.pt?open=512&objID=255&mode=2

[23] CCTA, CRAMM userguide

[24] OCTAVE, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, USA

[25] P. Marek, J. Paulina, The OCTAVE methodology as a risk analysis tool for business resources, Academy of business in Dabrowa, Gornicza, Poland

[26] T. Dimitrakos, B. Ritchie, Model based Security RA for web Applications: The CORAS approach

[27] F. Braber, G. Braendeland, H. Dahl, I. Engan, I. Hogganvik, M. Lund, B. Solhaug, K. Stolen, F. Vraalsen, The CORAS Model Based Method for Security RA, SINTEF Oslo, September 2006

[28] CORAS tool, Norsk Regnesentral, Oslo, Norway

[29] I. Hogganvik, K. Stølen, A graphical approach to risk identification, motivated by empirical investigations, SINTEF ICT and Department of Informatics, University of Oslo

[30] I. Hogganvik, K. Stølen, Structured semantics for the CORAS security risk modeling language, SINTEF ICT, Cooperative and trusted systems, September 2007

[31] I. Hogganvik, A graphical approach to security Risk Analysis

[32] G. Braendeland, I. Engan, I. Dahl, K. Stølen, Using dependent CORAS diagrams to analyze mutual dependency, SINTEF ICT, Department of Informatics, University of Oslo, Norway

[33] A. Refsdal, K. Stølen, Employing key indicators to provide a dynamic risk picture with a notion of confidence.

[34] J. Aagedal, F. Braber, T. Dimitrakos, B. Gran, D. Raptis, K. Stølen, Model based Risk Assessment to Improve Enterprize Security

[35] Risk Management Training Guides, Hazard & Operability Analysis (HAZOP), Manufacturing Technology Committee, Risk Management Working Group

[36] Risk Management Training Guides, Manufacturing technology committee – Risk management working group

[37] Vesely W, Stamatelalos M, Dugan J, Fragola J, Minarick J. Fault tree handbook with aerospace applications. Report by NASA Office of Safety and Mission Assurance, [Online], Available: http://www.hq.nasa.gov/office/codeq/doctree/fthb.pdf; 2002 [accessed 2006].

[38] Vesely W. Fault Tree Analysis (FTA): Concepts and Applications, [Online], Available:

http:// www.hq.nasa.gov/office/codeq/risk/ftacourse.pdf; 1998 [accessed 2006].

[39] Walker RW. Assessment of technical risks. In: Proceedings of the 2000 IEEE international conference on management of innovation and technology. 2000.

[40] Quantified Risk Assessment Techniques-Part 1, Failure Modes and Effects Analysis, FMEA, Health&Safety Briefing No 26a, The institute of Information and Technology, August 2012

[41] Quantified Risk Assessment Techniques-Part 3, Fault Tree Analysis, FMEA, Health&Safety Briefing No 26c, The institute of Information and Technology, August 2012

[42] A. Nannikar, D. Raut, R.M. Chanmanwar, S.B. Kamble, FMEA for manufacturing and assembly process, VJTI, Mumbai

[43] P. Grossi, H. Kunreuther, Catastrophe modeling: a new approach to managing risk

[44] J. Depoy, J. Phelan, P. Sholander, B. smith, G.B. Varnado, G. Wyss, Risk Assessment for physical and cyber attacks on Critical Infrastructures

[45] VSAT, US Department of Energy, Pensylvania, USA

[46] Security Vulnerability Assessment for the Petroleum and Petrochemical industries, American Petroleum Institute, May 2003

[47] EURACOM, Deliverable D2.3 Integrated report on the link between Risk Assessment and Contingency Planning Methodologies

[48] EURACOM, Deliverable D1.1, Generic System Architecture with relevant functionalities for hazard identification

[49] Baseline Protection Concept for Critical Infrastructure, Recommendations for the Companies, Federal Ministry of the Interior

[50] IT baseline manual, Federal Agency for Security in Information Technology, October 2000

[51] Jack A. Jones. An introduction to Factor Analysis of Information Risk (FAIR). http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf , accessed 06.03.2016 ,2005

[52] I. B. Utne, P. Hokstad, G. Kjølle, J. Vatn, A. Tøndel, D. Bertelsen, H. Freidheim, Risk and Vulnerability Analysis of the Critical Infrastructures – The DECRIS approach, J. Røstum, SINTEF technology and society, safety and reliability

[53] US Department of Energy, "Security guidelines for the electricity sector: Vulnerability and Risk assessment", Washington DC: US department of Energy, [Online], Available: https://www.esisac.com

[54] RVA, Danish EmergencyManagement Agency, Denmark, [Online], Available: http://www.brs.dk

[55] C. W. Ten, C. C. Liu, M. Govindarasu, Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees, IEEE

[56] R. Schneier, "Attack Trees", Schneier.com, [Online], Available: https://www.schneier.com/paper-attacktrees-ddj-ft.html#rf2

[57] S. Vidalis, A. Jones, Using vulnerability trees for decision making in threat assessment, University of Glamorgan, Pontiprydd, Wales, UK

[58] P. A. S. Ralston, J. H. Graham, J. L. Hieb, Cyber security risk assessement for SCADA and DCS networks, University of Louisville, [Online], Available: http://www.sciencedirect.com

[59] S. Vidalis, Assessing cyber threats in the information environment, Newport Business School, Department of Computing

[60] Threat and Hazard Identification and Risk Assessment Guide, Comprehensice Preparedness Guide (CPG) 201, first edition, 2011, Homeland Security

[61] http://www.dhs.gov

[62] M. H. Henry, R. M. Layer, K. Z. Snow, D. R. Zaret, Evaluating the Risk of Cyber Attacks on SCADA Systems via Petri Net Analysis with Application to Hazardous Liquid Loading Operation, The Johns Hopkins University Applied Physics Laboratory (JHU/ APL), 11100 Johns Hopkins Road, Laurel, MD 20723-6099

[63] PHAworks, Primatech, Ohio, USA, [Online], Available: http://www.primatech.com/software/phaworks

[64] Risk Management Insight LLC. FAIR (FACTOR ANALYSIS OF INFORMATION RISK) Basic Risk Assessment Guide. Risk Management Insight LLC, 2006

[65] T. Spyridopoulos, I. A. Topa, T. Tryfonas, M. Karyda, A holistic approach for cyber assurance of critical infrastructure through Viable System Modelling, University of the Aegean

[66] M. A. McQueen, W. F. Boyer, M. A. Flynn, G. A. Beitel, Quantitative Cyber Risk Reduction Estimation Methodology for a Small SCADA Control System, Idaho National laboratory, USA

[67] S. Patel, J. Zaveri, A Risk-Assessment Model for Cyber Attacks on Information Systems, Department of Information Science and Systems, Morgan State University, Baltimore, MD 21251

[68] A. C. Vieira, S. H. Houmb, D. R. Insua, A graphical adversarial risk analysis model for oil and gas drilling cybersecurity, Royal Academy of Sciences, Madrid, Spain – Secure NOK AS, Stavanger, Norway

[69] T. Aven, A united framework for risk and vulnerability analysis covering both safety and security, University of Stavanger, Norway

[70] S. M. Papa, W. D. Casper, S. Nair, Availability based risk assessment for SCADA embedded computer systems, HACNET labs, Computer Science and engineering department, Bobby B. Lyle School of engineering, Southern Methodist University, Dallas, TX 75275, USA

[71] Neil A. McEvoy and Andrew Whitcombe. Structured risk analysis. In Proceedings of the International Conference on Infrastructure Security, InfraSec '02, pages 88-103, London, UK, UK, 2002. Springer- Verlag

[72] Standards New Zealand. Risk Management – Principles and guidelines. Australian / New Zealand Standards. Standards Australia International and Standards New Zealand, as/ nzs 31000: 2009 edition, 2009

[73] S – Port: Collaborative Security Management of Port Information Systems, Despoina Polemi, Theodoros Ntouskas, Emmanouil Georgakakis, Christos Douligeris, Marianthi Theoharidou, Dimitris Gritzalis, 2013

9 Appendix: Summary – Comparison of CPS RA & RM Methodologies

				Comparison and evaluation criteria																	
		Methodology				Originating point					Identification										
Orientation	Method	RA	RM	Criticality	Dependencies	Asset	Threat	Impact	Vulnerability	Holistic	Threats	Assets	Vulnerabilities	Applicability	Layer	Practical/ intuitive	Reliability	System behavior	Adaptability	Resilience	Robustness
Qualitative	CORAS	✔	✔		✔	✔				✔	Graph/ interaction	Graph/ interaction	Graph/ interaction	High	All	Medium	High	✔	✔	✔	
	VSAT	✔	✔			✔				✔	Database	Database	Database	High	All	High	High				
	RVA	✔				✔				✔	Expert knowledge	Expert knowledge	Expert knowledge	High	strategic		High				
	CRAMM	✔	✔	✔	✔	✔				✔	Database	Database/ functional analysis	Database	High	Operational, Cyber, physical	High	Low				
	MAGERIT	✔	✔	✔	✔	✔				✔	Database	Database/ functional analysis	Database	High	Operational, Cyber, Physical	High	Low				
	OCTAVE	✔	✔	✔		✔				✔	Threat table	Interaction/ functional analysis	Interaction	Medium	Operational, cyber, physical	Medium	Medium				
	BPC	✔		✔	✔		✔			✔	Standard checklists and questionnaires/ expert knowledge	Standard checklists and questionnaires/ expert knowledge	Standard checklists and questionnaires/ expert knowledge	High	Operational, strategic	High	High				
	EURAM	✔		✔	✔	✔				✔	Intelligence	Functional analysis	Expert knowledge	Medium	Operational, strategic		High	✔	✔	✔	
	SVA	✔	✔	✔	✔	✔				✔	Intelligence	Standard tables	Expert knowledge	High	All	Medium	High		✔		✔
	PHA	✔			✔			✔		✔	Expert knowledge	Expert knowledge	Expert knowledge	High	Operational, physical	Medium	High				
	Hybrid	✔			✔		✔			✔	Expert knowledge	Expert knowledge	Expert knowledge	High	Operational, cyber, physical	High	High	✔	✔		✔

	Petri Nets	✔			✔		✔			✔	Expert knowledge/ graphs (PN)	Expert knowledge/ graphs (PN)	Expert knowledge/ graphs Graph (PN)	Low	Cyber, physical	Low	High	✔	✔	✔	✔
	DECRIS	✔		✔				✔		✔	Expert knowledge	Expert knowledge	Expert knowledge	Low	Operational	Low	Low				
	THIRA	✔		✔			✔			✔	Expert knowledge	Expert knowledge	Expert knowledge	High	Strategic	High	High				
	TAME	✔				✔				✔	Expert knowledge	Expert knowledge	Expert knowledge	Low	Operational	Low	Low				
	ES-ISAC	✔			✔	✔				✔	Expert knowledge	Expert knowledge	Expert knowledge	Medium	Strategic, operational	Medium	High				
	RMG-DOE	✔			✔	✔					Expert knowledge	Expert knowledge	Expert knowledge	Medium	Strategic, operational	Medium	High				
Quantitative	MAGERIT	✔	✔	✔	✔	✔				✔	Database	Database/ functional analysis	Database	High	Operational, Cyber, Physical	High	Low				
	Catastrophe modeling	✔				✔				✔				Low	Strategic, operational	Low	Low		✔		
	Vulnerability Trees	✔							✔	✔	Experts knowledge	Experts knowledge	Experts knowledge/ vulnerability analysis	Medium	Cyber and physical	Medium	Low		✔		
Semi-quantitative	CORAS - FMEA	✔	✔	✔	✔	✔				✔	Graph/ interaction	Graph/ interaction	Graphs/ interaction	High	All	Medium	High	✔	✔	✔	
	Attack Tree Vulnerability Assessment	✔			✔				✔	✔	Expert knowledge	Expert knowledge	Expert knowledge	✔	Cyber and physical	Medium	Low		✔		
Other	CIMS	✔		✔	✔	✔				✔	Simulation	Simulation	Simulation	Medium	Operational, cyber, physical	High	Medium	✔	✔	✔	✔
	CYSM		✔	✔		✔				✔				High	Cyber, Physical	High	High				