Metadata of the chapter that will be visualized online

Chapter Title	A Comprehensive Framework for the Security Risk Management of Cyber-Physical Systems	
Copyright Year	2018	
Copyright Holder	Springer International Publishing AG, part of Springer Nature	
Corresponding Author	Family Name	**Mokalled**
	Particle	
	Given Name	**Hassan**
	Suffix	
	Division	Ansaldo STS
	Organization	Cyber Security Assurance & Control Department
	Address	Genoa, Italy
	Organization	University of Genoa, DITEN
	Address	Genoa, Italy
	Organization	Lebanese University, EDST-MECRL Lab
	Address	Beirut, Lebanon
	Email	hassan.mok7@gmail.com
Author	Family Name	**Pragliola**
	Particle	
	Given Name	**Concetta**
	Suffix	
	Division	Ansaldo STS
	Organization	Cyber Security Assurance & Control Department
	Address	Genoa, Italy
	Email	Concetta.Pragliola@ansaldo-sts.com
Author	Family Name	**Debertol**
	Particle	
	Given Name	**Daniele**
	Suffix	
	Division	Ansaldo STS
	Organization	Cyber Security Assurance & Control Department
	Address	Genoa, Italy
	Email	Daniele.Debertol@ansaldo-sts.com
Author	Family Name	**Meda**

	Particle	
	Given Name	**Ermete**
	Suffix	
	Division	Ansaldo STS
	Organization	Cyber Security Assurance & Control Department
	Address	Genoa, Italy
	Email	Ermete.Meda@ansaldo-sts.com
Author	Family Name	**Zunino**
	Particle	
	Given Name	**Rodolfo**
	Suffix	
	Organization	University of Genoa, DITEN
	Address	Genoa, Italy
	Email	rodolfo.zunino@unige.it

Abstract	Cyber Physical Systems are facing huge and diverse set of security risks, especially cyber-attacks that can cause disruption to physical services or create a national disaster. Information and communication technology (ICT) has made a remarkable impact on the society. A Cyber Physical System (CPS) relies basically on information and communication technology, which puts the system's assets under certain risks especially cyber ones, and hence they must be kept under control by means of security countermeasures that generate confidence in the use of these assets. And so there is a critical need to give a great attention on the cybersecurity of these systems, which consequently leads to the safety of the physical world. This goal is achieved by adopting a solution that applies processes, plans and actions to prevent or reduce the effects of threats. Traditional IT risk assessment methods can do the job, however, and because of the characteristics of a CPS, it is more efficient to adopt a solution that is wider than a method, and addresses the type, functionalities and complexity of a CPS. This chapter proposes a framework that breaks the restriction to a traditional risk assessment method and encompasses wider set of procedures to achieve a high level strategy that could be adopted in the risk management process, in particular the cybersecurity of cyber-physical systems.

Keywords (separated by "-")	Cyber-physical system - Risk management - Cybersecurity - Ansaldo STS

A Comprehensive Framework for the Security Risk Management of Cyber-Physical Systems

Hassan Mokalled, Concetta Pragliola, Daniele Debertol, Ermete Meda, and Rodolfo Zunino

Abstract Cyber Physical Systems are facing huge and diverse set of security risks, especially cyber-attacks that can cause disruption to physical services or create a national disaster. Information and communication technology (ICT) has made a remarkable impact on the society. A Cyber Physical System (CPS) relies basically on information and communication technology, which puts the system's assets under certain risks especially cyber ones, and hence they must be kept under control by means of security countermeasures that generate confidence in the use of these assets. And so there is a critical need to give a great attention on the cybersecurity of these systems, which consequently leads to the safety of the physical world. This goal is achieved by adopting a solution that applies processes, plans and actions to prevent or reduce the effects of threats. Traditional IT risk assessment methods can do the job, however, and because of the characteristics of a CPS, it is more efficient to adopt a solution that is wider than a method, and addresses the type, functionalities and complexity of a CPS. This chapter proposes a framework that breaks the restriction to a traditional risk assessment method and encompasses wider set of procedures to achieve a high level strategy that could be adopted in the risk management process, in particular the cybersecurity of cyber-physical systems.

Keywords Cyber-physical system · Risk management · Cybersecurity · Ansaldo STS

H. Mokalled (✉)
AQ1 Ansaldo STS, Cyber Security Assurance & Control Department, Genoa, Italy

University of Genoa, DITEN, Genoa, Italy

Lebanese University, EDST-MECRL Lab, Beirut, Lebanon

C. Pragliola · D. Debertol · E. Meda
Ansaldo STS, Cyber Security Assurance & Control Department, Genoa, Italy

R. Zunino
University of Genoa, DITEN, Genoa, Italy
e-mail: rodolfo.zunino@unige.it

F. Flammini (ed.), *Resilience of Cyber-Physical Systems*,
Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-319-95597-1_3

1 Introduction

A cyber-physical system refers to the system that combines both cyber and physical resources, where there is a strong relation and coordination between these resources. Such systems are controlled or monitored by computer-based algorithms, tightly integrated with the internet and its users. CPS is basically a control system with distributed networked, adapted and predictable, real-time, intelligent characteristics, where human-computer interaction may exist. It is widely used in critical national infrastructure, such as electric power, petroleum and chemical and so on [1]. Moreover, many urban transportation and railway systems around the world have deployed some form of communications-based automatic train control (e.g., [2]). And in those systems, multiple cyber components exist, including wireless communication. The potential implications of this evolution could be multi-faceted and profound, especially when it comes to the issue of security. If such systems were subject to a physical or cyber threat, the consequences will be unimaginable. These systems are susceptible to different types of risks related to information systems vulnerabilities. No one doubts about the hazardous consequences that would occur in case a malicious software succeeds in controlling the system, i.e. any fail in systems controlling drive-less metros will lead to huge loss. Security breaches in the cyber domain, such as falsified information or malicious control logic, can have a complicated impact on the physical domain [3]. "The cyber breach will lead to complicated physical consequences". Cybersecurity breaches can range from no or limited impact to Distributed Denial of Services (DDoS), stealing of data, or even taking over control of systems and harm the physical world [4]. In energy industry, the computer system of Iran Bushehr nuclear power plant was invaded by "Stuxnet" in 2010, leading a serious chaos in the automated operation of the nuclear facilities and a serious setback of Iran's nuclear program. In transport service, in the network for managing and monitoring the operation of the Shinkansen, due to an exception in the management system of control schedule, signaling and line switching point in 2011, Japan's 5 Shinkansen operation management system encountered failure, 15 trains were in outage, 124 trains were delayed and 8.12 million people's travel were affected. In water Industry, in 2011, Illinois water system was hacked and a malfunction occurred in the water pump SCADA, which leading to the pump's damage and scrap. In this way, we can conclude that CPS security is so important that risk incidents in the system may affect national security and stability. Taking all these security incidents seriously, we conclude that any attack in the cyber layer of the cyber physical system could lead to hazardous situations and even to loss in lives [1].

There are several approaches for the problem of risk assessment and treatment: informal handbooks, methodical approaches or supporting tools, where all provide a guide for risk assessment and treatment. However, methods might differ in some steps, or in the way of identifying and valuating the assets or threats. Some are basically used in cyber security of information systems, and others can be used in physical security. Many of the proposed solutions try to measure or estimate the probability and the severity of the risks after identifying the assets and threats using traditional IT risk assessment methods, some of these solutions do not address the characteristics and the complexity of CPS, which needs a broad range of management. The great challenge of these approaches is the complexity of the problem they have to face; in the sense that there are many elements to be considered and, if it is not done rigorously, the conclusions will be unreliable.

Ansaldo STS is a leading Company operating in the sector of high technology for Railway and Urban Transport. The Company has the experience and resources to supply innovative transport and signaling systems for freight yards, regional and freight lines, underground and tramway lines, and standard and High-Speed railway lines. With an international geographical organization, The Company operates worldwide as lead contractor, system integrator and supplier "turnkey" of the most important projects of mass transportation in metro and urban railways. Ansaldo STS has a great experience in the design, implementation and management of systems and services for signaling and supervision of railway and urban traffic [5].

Ansaldo STS believes that there is a critical need to adopt a comprehensive strategy for the problem of applying risk management study to a cyber-physical system. As the complexity of the CPS is greater and such systems need more procedures to be performed, a framework was developed that aims to reach a common high level solution, it is different and broader than a traditional IT risk management methods whose goal is mainly focused on identifying and measuring the severity of the risks and try to reduce it to an acceptable extent. In fact, it encompasses Seven steps and inspired by the PDCA cycle, and centered upon the cyber side and its assets; however, this doesn't mean that the physical assets are out of the frame, as the physical assets of a CPS are mostly controlled by others in the cyber side. This framework is characterized by a set of procedures that starts by modeling the system's assets and functionalities, selection of potential threats to the CPS, conducting risk assessment and treatment through a methodical way, safeguard implementation, vulnerability assessment, ensuring the compliance with global and local applicable laws, and finally applying maintenance and improvement activities. This chapter is divided as follows: Sect. 2 presents a set of aspects that the approach mentions, Sect. 3 describes the proposed framework. Section 4 is the case study that shows how Ansaldo STS Company applies this framework, and finally Sect. 5 concludes the work.

2 Aspects and Requirements

2.1 Cyber Physical System Security

CPS security has some distinct characteristics as it is different from traditional IT system. In traditional IT system the first important aspect of information security is confidentiality. Confidentiality means the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content. However for CPS, the availability comes first, then integrity and confidentiality.

CPS has more attack points and fault points than IT system. Any safeguard measures shall not interrupt the response to the physical system or delay the response. In traditional IT system access control can be deployed without affecting the services of IT system. In CPS all these measures should be discussed and tested to great details. The data flow shall not be hindered or interfered. CPS is a system of systems, the tight coupling between the physical system and cyber system has led to potential cascade effect of the whole system. Malfunction whether in cyber part or in the physical part will spread to other part of system [1].

2.2 Threats and Vulnerabilities

The two main kinds of threats that affect any organization are internal and external threats. Internal threats occur from within the organizations. This is probably one of the most dangerous situations because for instance co-workers may know how to access systems and are aware of how the systems are set up. And external threats are attacks done by externals and hackers [6].

(i) ***Internal Threats***: Statistics [7, 8] show that a large amount of security and privacy breaches are due to insiders. Protection from insider threats is challenging because insiders may have access to many sensitive and high-privileged resources. Similar style of exploitation is reported in [9, 10].
(ii) ***External threats***: External threats are those done by individuals from outside a company or organization, who seeks to break defenses and exploit vulnerabilities. Spying or eavesdropping, DoS, Spoofing, Phishing, viruses, etc. . . . , are all examples of external threats or cyber-attacks.

On the other hand ***vulnerability*** is defined as a weakness in the system assets or safeguards that facilitates the success of a potential threat and could cause damage; they could exist in system, software, network, etc. . . .

2.3 Security Requirements

The cyber security of CPS calls for the use of a wide set of security controls to protect the whole system against compromises of their confidentiality, integrity and availability. The cybersecurity of CPS must address these main security requirements:

(i) ***Integrity***: It means that only the authorized users can change in the assets, it is satisfied if the assets are not changed by an unauthorized party.

(ii) ***Confidentiality***: This means that the assets must not be exposed to unauthorized individuals. And access must be restricted to those authorized. This is satisfied if the assets are not read or accessed by an unauthorized party.
(iii) ***Availability***: This is satisfied if the assets or services are available and without delay.

If the system were exposed to malicious activities, physical components would also be affected and even damaged as a consequence. It can be said that in a CPS, the availability comes first, then the integrity and confidentiality.

2.4 Dependencies and Accumulated Risk

As mentioned above, it is more efficient for a security strategy to start with functional modeling of assets with defining relations and dependencies, as it leads to more precise and coherent study. Dependencies affect all the calculations done to assess the risk. Since assets depend on each other, the occurrence of threats on assets causes a direct harm on them and an indirect harm on others that depend on them.

3 A Comprehensive Framework for the Risk Management–Cybersecurity in CPS

Commonly, when there is a need to assess risks, traditional methods are used to do the job. Traditional risk management methods involve the following step: risk identification, assessment and mitigation plan definition. However, a well-designed risk assessment of CPS will provide an overall view of CPS security status and support efficient allocations of safeguard resources. Though traditional IT system risk assessment is quite mature, a distinct risk assessment method for CPS is needed to cover the growing security issues due to the large differences between IT system and CPS [1]. This framework is inspired by the PDCA (PLAN-DO-CHECK-ACT) cycle. It adds a broader set of procedures for a traditional risk assessment method.

Companies must realize the necessity of managing data protection, they should better treat and manage the security strategy addressing the organizational and the technological aspects of the system [11], and also address the complexity and additional type of assets that a CPS encompass. In order to assure compliance with Security and safety requirements, there is a need to define and adopt a holistic framework for Risk Assessment and Treatment activities of CPSs, and so this section shows the proposed framework. Figure 1 shows how each step of the framework falls inside one of the phases of the PDCA cycle. It is a divided into the following seven steps:

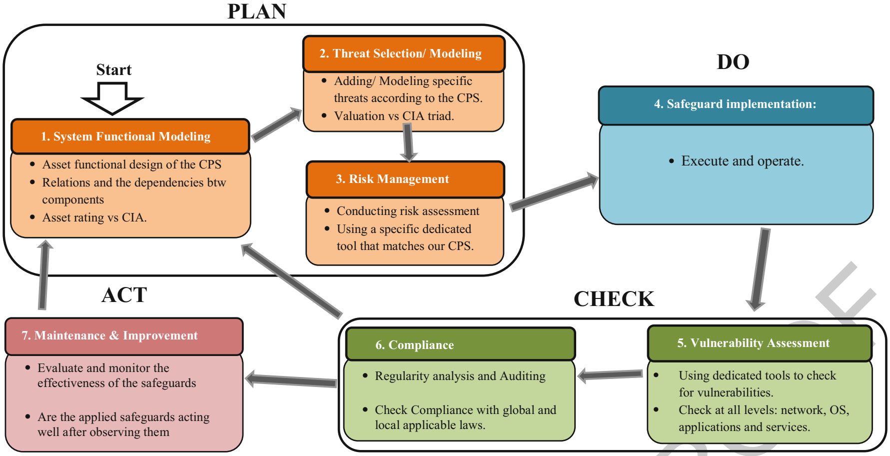


Fig. 1 The proposed framework inspired by the PDCA cycle

1. System Functional Modeling
2. Threat Selection and Modeling
3. Applying a Risk Management method (Assessment and Treatment plan)
4. Safeguard implementation
5. Vulnerability assessment
6. Compliance and Validation
7. Maintenance and Improvement

To ensure the continuous improvement, the framework is based on Deming PDCA Cycle where each phase, because of the complexity of a CPS, can be divided further in a few steps. The steps are applied in order: starting by the "PLAN" phase, first step is the "***System Functional Modeling***" which designs the model for the CPS showing the functionalities, dependencies, relations between the assets and defines also rules and Acceptable Risk Levels. Then the second step, "***Threat Modeling and Selection"*** selects the potential "threats" that match the CPS's assets: this can be done by referring to historical data such as reports, statistics, observations, logs, etc. Finally, always in PLAN phase, the first two steps are the input to the "***Risk Management***" step, where an appropriate method is selected to assess the risk (Risk Assessment) and helps in selecting the appropriate measures for keeping the risks under control (Risk Treatment). After that "S***afeguard Implementation***" takes place, reflecting the "DO" phase of a PDCA, where the chosen decisions in the Plan phase are put into operation. Afterwards there is the CHECK phase, represented by the "V***ulnerability Assessment and Penetration Test"*** process: it plays a key role in revealing the vulnerabilities yet present on the system and not protected by already installed safeguards. Because a CPS contains various set of HW/SW assets such as network appliances, servers, end-points, applications, web services, databases, etc., the Vulnerability Assessment and Penetration Test activity is applied basically on three levels: Application, Network and Operation System Levels. Based on all previous findings and evidences, the CHECK phase is completed by a compliance control to ensure complying of the system to security best practices or international standards, e.g. ISO/IEC 27001/27002. Finally, the Deming Cycle is concluded by the ACT phase which contains ***"Maintenance and Improvement"*** activities to correct and improve the system.

3.1 System Functional Modeling (Asset Modeling)

Creating a functional model has a great impact in showing the structure and the components of the CPS, and in demonstrating the relations and the dependencies between the different assets, and hence to have a clear and precise simulation for the system in real life. It is the step where the whole framework depends on, in this stage it is meant to model the physical and cyber components and their interactions and operational characteristics. Asset Modeling can be considered as the most important step in this approach, it must be done first with the owners of the system. The scope of this part is to help the system's owners or information sources in creating a system functional model and in the valuation of the system's assets. For this task, two steps are followed:

(i) Creating a functional model for the system which is a structured representation of the system's components (assets) and functions (activities, processes, operations).
(ii) Rating of the assets (based on CIA) using criticality levels and according to the consequences on CIA that would happen case of their protection failure.

The two steps must be done by the owners or under the supervision of them. In this way, a typical representation or a general view for the system is carried out which aids in the risk management study.

3.2 Threat Selection and Modeling

Each CPS differs by the services and functionalities that it offers. Threats vary from one system to another, based on the available assets and their level of valuation. Different CPSs means different assets and though different types of threats. Threats can be grouped and associated to homogenous group of assets called asset classes. Threat selection is about understanding the most suitable threats that are expected to happen and matching them with the different asset classes of the cyber physical system. The appropriate threats-to-assets should be selected in this step to be fed into the "Risk Management study" step, and should be applicable to the assets presented in the previous step. Mainly cyber-security threats are covered; that is, threats applying to information and communication technology assets, but additional non-

Fig. 2 Common threats for the "Threat selection and Modeling" step in CPS

IT threats could also be included in order to cover threats to physical assets that are necessary for the operation of the CPS. This work can be done by referring to historical data, e.g.: reports, statistics, observations, logs, etc.

The ENISA Threat Landscape provides an overview of threats, together with current and emerging trends. It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends. Over 140 recent reports from security industry, networks of excellence, standardization bodies and other independent institutes have been analyzed [12], Fig. 2 shows a sample for some threats that threaten cyber physical systems. However risk analysts are responsible for selecting and valuating the appropriate and expected threats that are likely to occur and match the system's assets. First the general model is obtained by experts, reports, statistics, and then threats that match the context, type of the CPS and the given assets are kept and fed to the next step. Threat Modeling eases the risk analysis study in various ways, mainly it prepares a wealthy and substantial threats-to-assets convenient dataset that fits a case study. There are some dedicated tools that help in threat modeling, and Sect. 4.2 shows one of them which is used by Ansaldo STS Company.

3.3 Risk Management Plan

Risk management is divided into risk analysis and risk treatment, with risk analysis being the systematic process for estimating the risks to which the system's assets are exposed to [13]. Risk management is a part of planning, where treatment decisions are taken. These decisions are demonstrated and established in the implementation step.

1. **Risk analysis:** A risk is an indicator of what could happen to the assets if not properly protected. It is important to know what features are of interest in each asset and to what extent these features are in danger, that is, analyze the system [13]. There are several methods and ways for the problem of analyzing the risks: informal handbooks, methodical approaches or supporting tools, where all provide a guide for risk analysis. However, methods might differ in some steps, or in the way of identifying and valuating the assets or threats. Some are basically used in cyber security of information systems, and others can be used in physical security. Risk analysis study must be applied using an appropriate method and tool for the risk analysis step in the cybersecurity of CPSs. Applying a risk analysis study includes:

   (i) Identifying and classifying assets by types, establishing dependencies between them and evaluating them according to security dimensions.
   (ii) Identifying and valuating threats and their likelihood.
   (iii) Identifying current safeguards and valuating them according to the level of effectiveness.
   (iv) Evaluating the risk on the CPS system where valuations for assets, dependencies, and threats are all involved in the calculation.

2. **Treatment plan:** On the other hand, this sub-step must also carry out the risk treatment activities that should be applied. Risk treatment activities allow a security plan to be prepared which, when implemented and operated, meets the proposed objectives with the level of risk accepted by the Management. In the treatment plan, the right counter measures are selected with types, and then prioritized. Moreover defining their cost/complexity, effectiveness and efficiency metrics must be also addressed. The objective is to deploy the controls selected by type and in a prioritized and effective way. For example, same safeguard can contrast more threats at the same time and overlapping/redundant safeguards should be avoided. However, sometimes, when a series of safeguards are in place and the management process is mature to a certain extent, the system will still be exposed to a risk called "residual".

3.4 *Safeguard Implementation: Operations*

This step deals with the implementation of security plans and decisions taken in the treatment plan, it takes as input the activities defined and puts them into operation. It also deals more with the technical side, and defines the best technological solutions based on the countermeasures to be adopted and the approved budget in accordance with the defined strategy. Implementation of safeguards must ensure the availability and the capability of the organizational staff to manage the tasks scheduled to implement them, as well as other factors, such as the budget of the organization, relations with other bodies, legal, regulatory or contractual changes, etc. So applying security patches and ensuring the secure configuration of all appliances is maintained continuously, also assets are monitored and logs are analyzed to detect any improper actions. Even when the risks have been treated, residual risks will generally remain. Residual risk means that that the current level of risk is accepted and is under a “carefully chosen” threshold, as trying to eliminate it could be extremely expensive.

3.5 *Vulnerability Assessment*

Vulnerability is a weakness in the assets that a malicious attacker could use to cause damage. Increasingly sophisticated tools help to penetrate existing network connections. After implementing the safeguards in the previous step, a vulnerability management process is needed to check if the assets of the cyber physical system are really still exploitable to threats. At the technical level, the focus is on cyber assets, this step is done by vulnerability exposure tools, with simulation of attack paths (similar to MITRE attack matrix). The end result can be patch management or better, in some complex environment, virtual patching (i.e. putting layer of defense that stop the attack before it reaches the endpoint, without the need to change configurations of the endpoint itself). Furthermore, log analysis could be useful in revealing vulnerabilities; but consider that doing manual log analysis requires a significant amount of expertise, knowledge, and is very time consuming. At the end, when detecting issues, it is required to return to the iteration cycles for proposals and solutions.

3.6 *Compliance*

Assessing the adherence of security configurations to the policies, requirements and regulations are set out in this stage. Compliance activities also involve regulatory analysis in order to ensure the compliance with global and local applicable laws based on the requirements, or even with respect to verification schemes to be achieved or maintained. And in case of non-compliance, it is required to return to the iteration cycles for proposals and solutions.

3.7 *Maintenance and Improvements*

Finally, the evaluation of the effectiveness and efficiency of the applied safeguards is measured to achieve the needed improvement and maintenance. It is recommended to deploy some elements that allow controlling the measures implemented in order to assess their effectiveness and to have an insight about them to figure out if there are new problems or there is a need to update their level.

4 Case Study: Adopting the Framework by Ansaldo STS Company

This section shows how the proposed framework is applied at Ansaldo STS Company. Each subsection describes the procedure followed in the goal of adopting it. The seven steps are demonstrated below, showing how they were applied to achieve this overall high level framework of Risk analysis and treatment for CPS.

4.1 *System Functional Model*

The first step is to design a functional model for the system, i.e. it is fundamental to define the scope of the system, the basic components forming the CPS and their composing assets (physical and cyber), and also establishing the relations and dependencies between them. This step is done based on information coming from the owners, since they are familiar and have the knowledge about their system. The functional model will be used to rate the assets against the basic security dimensions Confidentiality, Integrity and Availability (CIA triad), as shown in the Fig. 3:

Then provide a high level asset rating for each with the assistance of the system's owners and based on the tables defined below. Figure 4 gives an example of the asset's security dimensions rating, where each asset has a triad rating that represents respectively the confidentiality, integrity and availability rate.

The assets' rating is carried out on each security dimension. Rating represent a pre-valuation step for the assets, where criticality levels will be used with a scale from 1 to 4, where "1" describes the lowest critical level and "4" is the highest. And so, each security dimension gets one of the four levels representing the rate value. For each level, a description is given that helps in choosing the suitable asset's level. The three tables below explain the levels of rating according to each security dimension (Fig. 5 and Tables 1, 2 and 3).

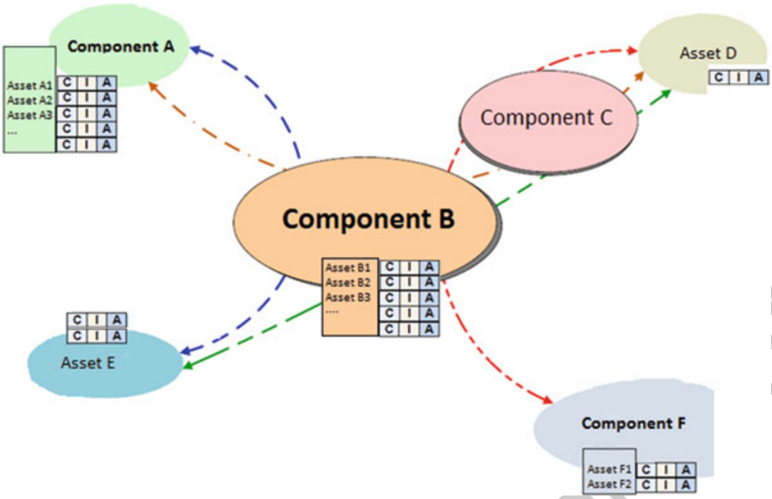
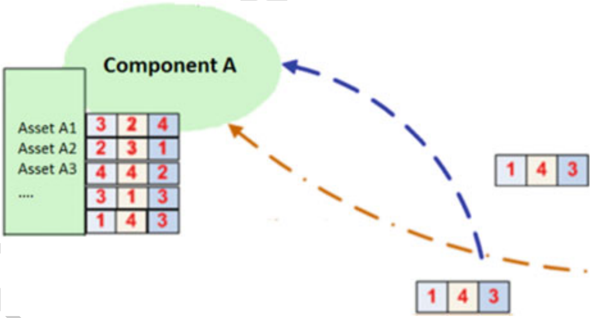


Fig. 3 A functional model example for the CPS

Fig. 4 Rating each security dimension for each asset



4.2 *Threat Modeling and Selection: Using RMAT Software*

Threat modeling and selection step is about preparing a set of appropriate threats and associate them to asset classes and organizing them also into classes. In particular to execute these actions a dedicated commercial tool, called RMAT, has been identified and adopted. Modeling is meant to prepare the threats selected; RMAT software can be used in the modeling. RMAT is used to create TSV files using a GUI, a TSV file is a representation for threats. Identifying threats for the TSV file is made by associating threats to asset families. The left panel of Fig. 6 shows the asset families and the threats associated to each one, while the right panel shows the single threats and the asset families associated to each one.

The structure of .TSV files that is used to create threat families is:

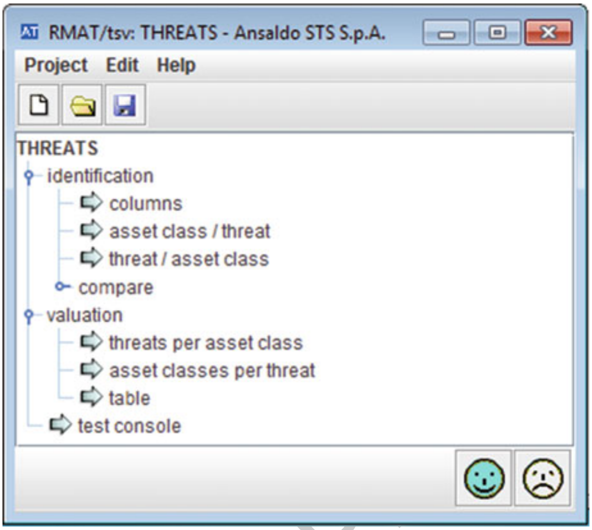


Fig. 5 Creating TSV file using RMAT

Table 1 Asset's rating levels for Confidentiality

CONFIDENTIALITY			
Level	**Title**	**Description**	**Consequence in case of loss of confidentiality**
4	**Confidential Asset**	Asset with a special sensitivity which must be accessed by special authorized staff or services.	***Serious impact***: Damage could affect directly the system, Customer or organizations.
3	**Restricted Asset**	Assets which must be accessed only by authorized staff members or services.	***Significant impact:*** the reputation of the system can be harmed.
2	**Internal Asset**	Assets for internal usage in the system which must be accessed only by internal staff.	***Negligible Impact:*** If the confidentiality is breached, small or inconsiderable consequences will happen for the system.
1	**Public Assets**	Assets of the system which can be accessed by anyone or any service.	***Insignificant impact***. No damages for the System, Customer or Organizations.

Table 2 Asset's rating levels for Integrity

Integrity			
Level	**Title**	**Description**	**Consequence if there would be an Integrity failure**
4	**High**	The assets must not be compromised by anyone.	**Serious impact**: The consequences could be catastrophic for the system.
3	**Medium**	The assets can be compromised by only service personnel with privileged or extended user rights.	**Significant impact**. The consequences are major and widespread. System errors and services breach persist for a substantial amount of time.
2	**Low**	The assets can be compromised by internal users even if not having any privileged and extended user right.	**Minor Impact**. The consequences are noticeable but workaround can be implemented within the system.
1	**Negligible**	The assets can be compromised by anyone even external users.	**Negligible impact**. Small or inconsiderable consequences which will not have noticeable influence on the system's operation.

Table 3 Assets' rating levels for Availability

AVAILABILITY			
Level	**Title**	**Description**	**Consequence of Availability deficiency**
4	**Significant**	Unavailability is unacceptable. The asset fails immediately and cannot be re-established by a workaround.	**High impact** on system's operation, which may lead to a complete stop or a main impact on the system. Impacts on the public image of the system and/or of the customer.
3	**Major**	A very short period of unavailability can be accepted during which assets will be unable to provide the intended work.	**Medium impact** affects the system partially and may lead to a delay in the operation of the system.
2	**Minor**	A short period of unavailability can be accepted,assets can be re-established by the implementation of alternative procedures.	**Small impact** on the operation. Small delay with low impact on the operation.
1	**Insignificant**	Unavailability is acceptable. Asset's continuity is not affected.	**Very-small impact** on the operation. No direct delay on the system.

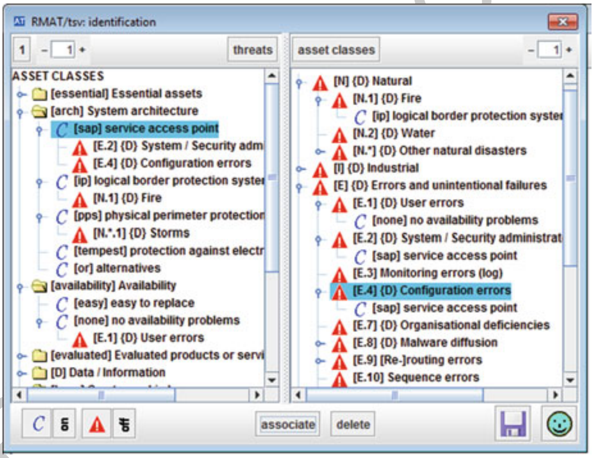


Fig. 6 Associating threats to asset classes using RMAT


```
file ::=
        <threat-standard-values>
                { family }0+
        </threat-standard-values>
family ::=
        <family F >
                { threat }0+
        </family>
threat ::=
        <threat Z f [ s ] >
                { set }0+
        </threat>
set ::=
<set D deg />
```

After creating the appropriate set of threat families, next is to use it as input to the risk analysis study.

4.3 *Conducting Risk Management Study Using MAGERIT Method*

For performing this job, Ansaldo STS has identified and adopted a commercial tool, named PILAR, that implements a method called MAGERIT which is suggested by the European Union Agency for Network and Information Security (ENISA). Following a methodical way in a risk management study is significant in order to obtain an efficient study. The objective of MAGERIT method is to cover both risk analysis and treatment for a thorough risk management. MAGERIT is an open methodology for Risk Analysis and Management, developed by the Spanish Ministry of Public Administrations. The purpose of this method is directly related to the generalized use of IT systems, communications, and electronic media. This method follows the international concepts as in ISO 31000 and ISO/IEC 27005 [13]. MAGERIT offers a systematic method for analyzing risks, and helps in describing and planning the appropriate measures for keeping the risks under control. And finally, prepares the organization for the processes of evaluating, auditing, certifying or accrediting, as relevant in each case. On the other hand, PILAR software implements MAGERIT method and is used to perform its steps. Its GUI (graphical user interface) enables the user to execute the MAGERIT method in an understandable and easy way, also making it reproducible. The tool provides fast calculations and generates a quantity of textual and graphical reports. PILAR software has been funded by the Spanish National Security Agency. It is designed to support the risk management process along long periods, providing incremental analysis as the safeguards improve [14]. PILAR enables the user to create a project, identify the assets for the system under study, and generate threats and safeguards and other functionalities (Fig. 7).

Furthermore, PILAR can be customized to use TSV files created by RMAT as input for the risk management study, so in this case the threats will be selected based on the model created before in" Threat Modeling" step.

4.4 *Safeguard Implementation*

The safeguard implementation step reflects the "DO" phase of the PDCA, which is putting the chosen decisions in the previous treatment plan into operation. At Ansaldo STS, the Defense in Depth (DiD) approach is adopted while implementing safeguards, an approach that is based on layering and that helps in faster detection and slowing down of attacks. In IT environments, DiD is intended to increase the costs of an attack against the organization, by detecting attacks, allowing time to respond to such attacks, and providing layers of defense so that even successful attacks will not fully compromise an organization. A DiD strategy is necessary because of the new security threats and the importance of IT security monitoring of assets (Fig. 8).

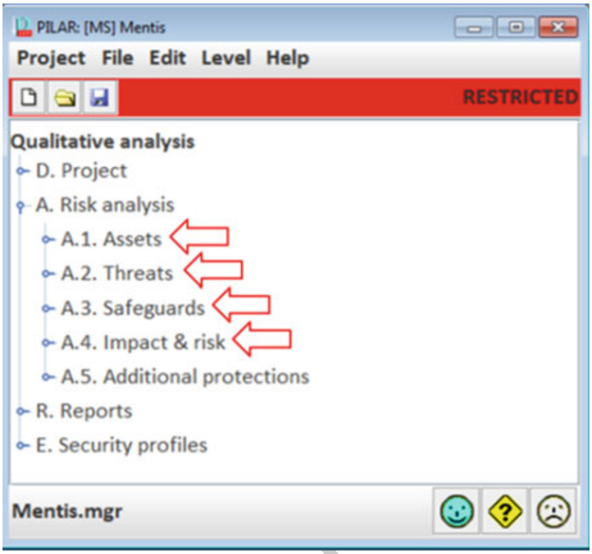


Fig. 7 PILAR software: homepage

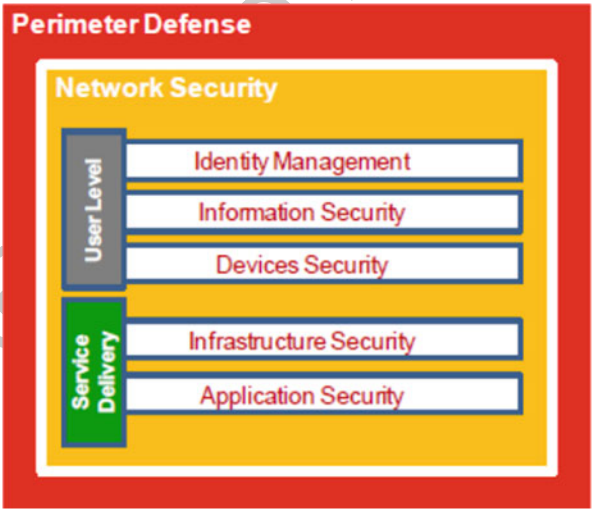


Fig. 8 Layering: defense in depth

4.5 Vulnerability Assessment for Cyber Assets

The cyber side of a CPS contains various set of assets such as network appliances, servers, software, web applications, databases, etc. At Ansaldo STS, vulnerability assessment is applied basically on 3 levels: operating system, netowrk and application levels.

- ***OS Vulnerability Assessment:*** On the level of operating system, what is meant is to apply host vulnerability assessment through scanning specific hosts. This allows the administrators to go beyond testing for known network vulnerabilities, but also examining more vulnerabilities such as patch levels, check OS configuration, and installed software on computers running operating system.

- ***Network Vulnerability Assessment:*** Network scanners are useful to analyze the network, and hosts on the network to detect vulnerabilities. Nmap (Network Mapper) is a security scanner used on this level to discover hosts and services on a computer network, thus building a "map" of the network. Nmap features include host discovery, port scanning, OS detection, which all help in finding and exploiting vulnerabilities in the network.
- ***Web Application Vulnerability Assessment:*** This can be done using automated web application and web services vulnerability scanning solutions that apply attack algorithms and determine the existence and relative severity of vulnerabilities. Some dedicated tools employ an extensive arsenal of attack agents designed to detect security flaws in web-based applications. Such tools probe the system with thousands of HTTP requests and evaluates each individual response. This assessment detects vulnerabilities, pinpoint their location in the application, and recommend corrective actions.

4.6 Compliance

Compliance can be oriented to internal policies and rules or to external laws and regulations, but in any case it represents a fundamental step in order to maintain the organization control inside its specific regulatory environment. PILAR software can be also used to conduct this step by using a security profile (EVL file) that is a description for a list of policies that a system would comply to. It is a view over a collection of safeguards that aim to protect a system. Security profiles may focus on some specific aspects, or may be general. The use of a security profile in a project is basically to check and ensure compliance. It is also possible to create custom security profiles, while some widely known are already available e.g.: ISO/IEC 27002. PILAR maps security profiles to its safeguards in such a way to estimate to which extent the system is compliant (Fig. 9).

After loading a security profile into the project, the set of controls for that particular profile are given a score based on the evaluation of safeguards that are relevant to those controls only, thus giving a measure to check the compliance of the system to the selected security profile.

4.7 Maintenance and Improvement

At the end, after executing all the steps of the framework, it is critical to monitor and observe if the decisions taken were effective, and if there is a need for maintenance or improvement or even adding a missing measure. On the other hand, in some

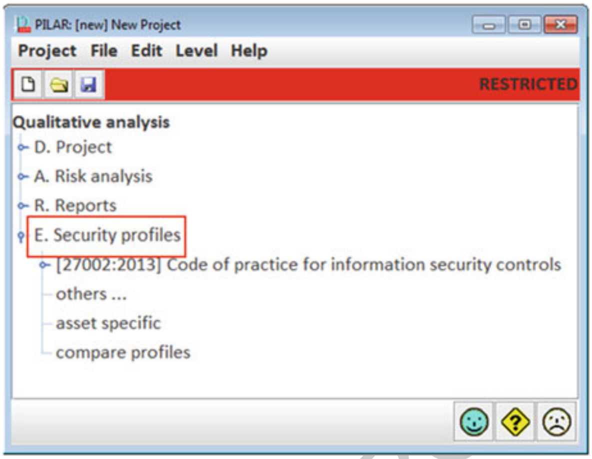


Fig. 9 Applying the security profiles in the compliance step

Fig. 10 Safeguards values in PLAN phase

current	target
L1	L1-L3
L2	L3
L1	L1
L1	L1-L3
L1	L1-L3
L2	L2
L3	L4

situations it could be necessary to reduce the cost of a certain countermeasure. Using PILAR in the PLAN phase, the "current" stage represents the current state of the system, and "target" stage represents the goal to reach (Fig. 10). However, now in the "ACT" phase, a new target (Fig. 11) will represent the new goal to achieve based on the new observations and analysis done, and putting all (new) safeguards into operation. The system is monitored and a set of investigations and observations based e.g. on some key performance indicators is done to apply the refinement in case it is required.

5 Conclusion

In recent years, a growth has been seen in the development of various types of Cyber-Physical Systems (CPS). They have brought impacts to almost all aspects of our daily life. Many of such systems are deployed in critical infrastructures, and so,

Fig. 11 New Safeguards values in ACT phase

target	new target
L1-L3	L2-L5
L3	L2-L4
L1	L2-L3
L1-L3	L2-L4
L1-L3	L2-L4
L2	L2-L4
L4	L2-L5

they are exposed to different types of attacks. A Cyber Physical System (CPS) relies basically on information and communication technology, which puts the system's assets under certain risks especially cyber ones. On the other hand, because of the characteristics of a CPS, it is more efficient to adopt a solution that is wider than a method, and addresses the type, functionalities and complexity of a CPS. Moreover, following a comprehensive framework ensures a lot of key points such as organizing the steps of a management study, preserving the order of the tasks without missing one, and basically doing the work once in a formalized structure, which is the key spirit of what is called "Comprehensive", and this should lead automatically to the customer satisfaction and ensuring that the risk management study is complied with laws and regulations. In this chapter, a holistic framework is proposed that breaks the restriction to a traditional risk assessment method, and encompasses wider set of procedures which can be followed in the risk management study for the CPSs, giving more attention to the cyber side that usually controls the physical side of CPSs. Finally, this framework is also ready to accommodate another two security dimensions which are the "authenticity" and "traceability", that are relevant and should be addressed as security requirements for the risk management of CPSs.

References

1. Peng Y, Lu T, Liu J, Gao Y, Guo X, Xie F (2013) Cyber-physical system risk assessment. Paper presented at ninth International conference on intelligent information hiding and multimedia signal processing
2. Ansaldo STS CBTC communication based train control. http://www.ansaldo-sts.com/sites/ansaldosts.message-asp.com/files/imce/cbtc.pdf. Accessed 4 May 2018
3. Chen B et al (2015) Security analysis of urban railway systems: the need for a cyber-physical perspective
4. Andrew F, Emmanouil P, Pasquale M, Chris H, Fabrizio S (2016) Decision support approaches for cyber security investment
5. Ansaldo Signalling and Transportation Systems (Ansaldo STS). http://www.ansaldo-sts.com/en/about-us/. Accessed 4 May 2018

6. Balvir S, Amarjeet S (2015) A roadmap to data security of automated university examination system
7. Annual Emerging Cyber Threats Report. Georgia Tech Information Security Center. http://www.gtisc.gatech.edu/. Accessed 4 May 2018
8. Internet Security Threats Report. Symantec. http://www.symantec.com/threatreport/. Accessed 4 May 2018
9. The CERT guide to insider threats: how to prevent, detect, and respond to theft of critical information, sabotage, and fraud. www.cert.org/archive/pdf/insidercross051105.pdf. Accessed 4 May 2018
10. Hunker J, Probst CW (2011) Insiders and insider threats—an overview of definitions and mitigation techniques. J Wirel Mob Netw Ubiquitous Comput Depend Appl 2(1):4–27
11. Mokalled H et al (2017) The importance to manage data protection in the right way: problems and solutions. In: Optimization and decision science: methodologies and applications: ODS. Sorrento, Italy, September 4–7, pp 69–82
12. ENISA Threat Landscape Report 2017. 15 top cyber-threats and trends. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017. Accessed 4 May 2018
13. MAGERIT – version 3.0. Methodology for information systems risk analysis and management. Book I – The Method, Madrid, July 2014
14. PILAR. Risk analysis and management- help files, version 6.2, August 17, 2016

AUTHOR QUERIES

AQ1. Please confirm the corresponding author.
AQ2. Please confirm the inserted call-out for Figs. 3.3, 3.5, 3.7, 3.8, 3.9 and 3.1.-3.3.
AQ3. Please note that the shades are retained and captured as media object in the Tables 3.1, 3.2 and 3.3.