International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 8, Issue 4, July - August 2019 ISSN 2278-6856

C.Ri.S.P.- Cyber Risk Analysis in Industrial Process System Environment

Antonio Capodieci[1], Vincenzo Capalbo[2,] Giuseppe Filitti[2] and Alessandra Caruso[2]

[1]Università del Salento, Dipartimento di Ingegneria dell'Innovazione,
Via Monteroni sn, 73100 Lecce, Italy

[2]Istituto di Ricerca Ingenia srl
Indirizzo: Via M. Biagi, 6 73100 LecceS.r.l.,

Abstract: ***The increasing adoption, in critical infrastructures and industrial automation, of physical control systems based on interconnected networks has led to a growing and previously unforeseen threat to information security for supervisory control and data acquisition (SCADA) and control systems distributed (DCS). It is essential that engineers and managers understand these problems and know the consequences of remote hacking. In the contest of Industrial Process are very commonly used risk assessment methods such as HHM, IIM, and RFRM that have been successfully applied to SCADA systems with many interdependencies and have highlighted the need for quantifiable metrics and the probability risk analysis (PRA) which includes methods such as FTA, ETA and FEMA and HAZOP. The goal of these methods is, in general, to determine the impact of a problem on the process plant and the risk reduction associated with a particular countermeasure. This document provides a methodology named CRiSP - Cyber Risk Analysis in Industrial Process System Environment. CRiSP tries to define a structured approach needed to analyze the consequence of an undesired remote manipulation. CRiSP allow to analyze the risk related to the manipulation of a single element of the plant and to analyze the consequence restricted to a portion of the plant. CRiSP helps to have a broad overview of cybersecurity and risk and to adopt the necessary countermeasure.***

Keywords: *Cybersecurity, Risk Analysis, Risk management, Industry 4.0.*

1. INTRODUCTION

Adopting the definition of Uk government we can define Critical National Infrastructure (CNI) as "Those infrastructure assets (physical or electronic) that are vital to the continued delivery and integrity of the essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life", and is formed by nine sectors: energy, food, water, transportation, communications, emergency services, health care, financial services and government [1]. A Critical National Infrastructure are, often, an industrial system controlled by an Industrial Control System (ICS). A Supervisory Control and Data Acquisition (SCADA) system is a special type of an ICS.

SCADA systems stand out among other ICSs as systems that monitor and control assets distributed over large geographical areas, and use specific control equipment. Initially, SCADA systems were used in power transmission, gas pipeline and water distribution control systems. Nowadays, SCADA systems are widely used all industry sector, from steelmaking to chemistry and manufacturing facilities[2],[3].

The reliable operation of SCADA systems is fundamental for some sectors of CNI as chemical, water and transportation where both data acquisition and control are critically important. A widespread outage of SCADA and, consequently, CNI may cause serious disturbance to a state and society[4][5]. The consequences of a malfunction of a SCADA system may be detrimental and may range from financial loss due to an equipment and environmental damage to the loss of human life[6].

As author say [6], Cyber security were not the major concerns of early standalone SCADA systems. Security was primarily achieved by controlling physical access to system components which were unique and used proprietary communication protocols. For years, security in SCADA systems was present only as an implication of safety. However, the situation has changed, and a number of standards and directives dealing with the cyber security of SCADA systems have emerged. This aspect is still increasing with the diffusion on Industry 4.0 plant.

In 2004, the National Institute of Standards and Technology (NIST) published the System Protection Profile – Industrial Control Systems which covers the risks and objective of SCADA systems[7]. In 2007, the US President's Critical Infrastructure Protection Board and the Department of Energy outlined the steps an organisation must undertake to improve the security of its SCADA networks in the booklet 21 Steps to Improve Cyber Security of SCADA Networks[8] In 2008, the Centre for Protection of National Infrastructure (CPNI) produced a Good Practice Guide for Process Control and SCADA Security (CPNI). In 2008, NIST released a comprehensive guidance on a wide range of security issues, and technical, operational and management security controls. The guide was updated in 2011 [7], [9] In 2013, the European Union Agency for Network and Information Security (ENISA) released the recommendations for Europe on SCADA patching [10]. Currently, the North American Electric Reliability Corporation (NERC) actively works on the development of a wide range of standards covering many aspects of CNI cyber security [11].

More extensive overviews of SCADA-related security standards and initiatives are provided in[3]Igure et al. (2006) and [12].

Industry 4.0 is a term often used to refer to the developmental process in the management of manufacturing and chain production. The term also refers to the fourth industrial revolution.

The term Industry 4.0 was first publicly introduced in 2011 as “Industrie 4.0” by a group of representatives from different fields (such as business, politics, and academia) under an initiative to enhance the German competitiveness in the manufacturing industry. The German federal government adopted the idea in its High-Tech Strategy for 2020. Subsequently, a Working Group was formed to further advise on the implementation of Industry 4.0.

In 2003, they developed and published their first set of recommendations. Their vision entailed that these “Cyber-Physical Systems comprise smart machines, storage systems and production facilities capable of autonomously exchanging information, triggering actions and controlling each other independently. This facilitates fundamental improvements to the industrial processes involved in manufacturing, engineering, material usage and supply chain and life cycle management.”

In this context SCADA systems are highly sophisticated, complex and based on advanced technology systems. SCADA systems are exposed to a wide range of cyber threats also because of the standardization of communication protocols and hardware components, growing interconnectivity and legacy.

In the past we have seen a series of cyber-attacks on CNI and SCADA. The first recorded cyber-attack, 1982, on CNI took place at the Trans-Siberian pipeline and resulted in an explosion visible from space[13].

In the last two decade there was a number of cyber-attacks on SCADA systems and ICS. In 2003, a slammer worm penetrated a network at the Davies-Besse nuclear plant in Ohio[5], [6] and a computer virus named Sobig shut down train signaling systems in Florida[13]. In 2006, a hacker penetrated the operation system of a water treatment facility in Harrisburg, USA[5], [6] and the Browns Ferry nuclear plant in Alabama was manually shut due to the overload of network traffic[12].

In 2007, a dismissed employee installed unauthorized software on the SCADA system of the Tehama Colusa Canal Authority [13]. In 2010, the Stuxnet computer worm struck the Iranian nuclear facility causing the failure of almost one-fifth of all centrifuges [13]. Stuxnet was a game-changer, it attracted the world's attention to cyber threats to CNI by drawing a vivid and horrifying picture of the consequences of a cyber-attack on CNI. In 2011, five global energy and oil firms were targeted by a combination of attacks including social engineering, trojans and Windows-based exploits[13]. In 2012, a malware named Flame was discovered to have been operating in many sites in the Middle East and North Africa for at least two years [13]. A larger number of cyber-attacks on CNI is listed and analyzed in [13] and [12].

The number of SCADA-related incidents also steadily grows. In 2010, the Repository of Industrial Security Incidents (RISI) had 161 incidents listed with about 10 new incidents being added each quarter. In 2013, the RISI database contained already 240 incidents recorded between 2001 and the end of 2012. Additionally, an extensive study,[4], of the current cyber security state of SCADA systems based on a set of interviews with a large number of experts confirmed that cyber threats in SCADA systems are escalating, they are “real and expanding”.

As a consequence of what was said before we can state that risk analysis is fundamental in a modern management of SCADA systems. Risk analysis is an important part of the best practice risk management in ICS and SCADA systems[14], [15]. Risk assessment answers the following three questions [16]:

- What can go wrong?
- What is the likelihood that it would go wrong?
- What are the consequences?

A range of standards and normative documents attending to risk management and risk assessment has been devised over the years for IT systems. ISO 31000:2009 (ISO, 2009) outlines generic, non-industry-specific guidelines on risk management. NIST SP 800-30 contains a guide on risk management for IT systems. NIST 800-37 provides a risk management framework for federal information systems. ISO/IEC 27005:2011[17] is a standard for information security risk management.

A range of general IT risk assessment methodologies is used in industry: Operationally Critical Threat and Vulnerability Evaluation (OCTAVE)[18], Central Computer and Telecommunications Agency Risk Analysis and Management Method (CRAMM) [19], Consultative, Objective and Bi-functional Risk Analysis (COBRA) (RiskWorld) and CORAS [20], a model-based risk assessment methodology for security-critical systems. Also there is a broad range of academic proposals such as for example Information Security Risk Analysis Method (ISRAM) [21]; COst estimation, Benchmarking, and Risk Assessment (COBRA) [22] andBusiness Process: Information Risk Management (BPIRM) methodology [23].

While a large number of IT risk assessment methodologies exists, the specifics of SCADA systems as opposed to IT systems, often prevent the straight forward application of risk assessment methods designed for corporate IT systems to SCADA systems.

An IT risk assessment method must be adjusted to fit the context of SCADA systems.

Risk is[16]:$R = \{\boldsymbol{s_i}, \boldsymbol{p_i}, \boldsymbol{x_i}\}, \boldsymbol{i} = \mathbf{1}, \mathbf{2}, \mathbf{3}, \dots, \boldsymbol{N}$

Where:

- R – risk;
- {} – must be interpreted as a “set of”;
- s – a scenario (undesirable event) description;
- p – the probability of a scenario;

- x – the measure of consequences or damage caused by a scenario; and
- N – the number of possible scenarios that may cause damage to a system.

A system, risk "is a function of the likelihood of a given threat source exploiting a potential vulnerability and the resulting impact of a successful exploitation of the vulnerability"[9].

Risk assessment in SCADA systems shall help to define the priority the components of a system in terms of their importance to the successful operation of the system or in terms of their level of vulnerability to an attack.

The aim of this paper is to define e methodology of risk assessment shall assist the managers and engineers of SCADA systems with the development of adequate security policies, with the design of secure system and with the rational allocation of often scarce resources.

2. STATE OF ART

Several relevant literature reviews exist. Reviews covering SCADA security and cyber security issues are presented inCheminod[3], [4], [12], [14]et al, 2013, twenty-one risk assessment methodologies for CNI proposed by various commercial and organizations are surveyed in [24], but does not concentrate on SCADA systems. We can found a brief description of several risk assessment methodologies for the oil and gas sector is outlined[25]. An extensive overview of risk assessment methodologies is contained in [26]but only two methods are examined in detail. Authors in [27], provides the most comprehensive and detailed overview of cyber security risk assessment methods applied in the context of SCADA systems.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). [18], is a framework for identifying and managing information security risks developed at Carnegie Mellon University's CERT Coordination Center.

CORAS[20] is a toolsupported by methodology such as fault tree analysis (FTA) and failure mode effect criticality analysis (FMECA).

Several different aspects define the research related to risk assessment. Risk assessment is a multiphase process: it starts with risk identification, proceeds to risk analysis, follows with risk evaluation and ranking, and ends with the management and treatment phases.

Researchers at Georgia Institute of Technology [28] present a qualitative, but very systematic approach to overall risk assessment for information systems.

A number of modeling and simulation approaches under development at Sandia National Laboratories directly address interdependencies and offer insight into the operational and behavioral characteristics of critical infrastructures.[18].

The most comprehensive risk identification methodology to address interdependencies is hierarchical holographic modeling (HHM), [29], [30]. Authors described HHM as a method that "can identify all conceivable sources of risk to SCADA systems and to the utilities and infrastructure that uses them" [67]. This method has been used to identify sources of risk to SCADA systems in the railroad sector[31].

Crowther et al.[32] applied the methods of HHM, to manage risk of terrorism to Virginia's interdependent transportation system; authors developed a tool for assessing the consequences of a failure in the transportation infrastructure.

A generally accepted definition of probabilistic risk assessment (PRA) is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity.

Risk is characterized by the severity of an adverse consequence that can result from an action. In probabilistic risk assessment, consequences are expressed numerically and their occurrence are expressed as probabilities. Determining risk is generally accepted as answering the three questions [16]:

- What can go wrong?
- How likely is it?
- What are the consequences?

In PRA, these are answered by developing a set of scenarios, the evaluating the probability of these scenarios, and then estimating their consequences[33]. PRA quantifies metrics, such as the probability of the top event. Determination of needed basic event probabilities is the most difficult task in applying this technique and can limit the effectiveness of PRA. Many references explain all aspects of PRA[34], [33].

Failure mode effect analysis (FMEA and FMECA) are Inductive approaches, and begin with an initiating event, then induce the end effects [78]. It is important to note that these methods analyze single component faults and their system effects and do not consider combinations of faults. Walker [80], makes a strong case for using FMEA in the early design phase of all engineering projects to determine the project's technical risk.

A deductive failure-based approach is Fault tree analysis (FTA), [24], [35]FTA starts with an undesired event, and then deduces event causes using a systematic backward reasoning process. The qualitative results obtained from FTA are "minimal cut sets", the smallest combination of basic events that result in the top event (fault). Each minimal cut set is a combination of basic events. Quantification of FTA happens when top event probability is determined from basic event information by assigning probabilities to the basic events. Uncertainties in any quantified result can be determined.

The basic difference between deductive methods, as FTA, and inductive methods, as FMEA, is the direction of the analysis. FTA starts with the undesired event and traces backward to causes, whereas inductive methods start with an initiating event and trace forward to consequences. FTA is the appropriate analysis to carry out if a given undesired event is defined and the goal is to determine its cause. FMEA should be used if a given set of causes are identified and the goal is to determine the consequences. A comprehensive PRA might use both inductive and deductive approaches to obtain a complete set of accident sequences, depending on the complexity of the system.

3. MOTIVATION

An industrial plant must satisfy a series of conditions specified in the design phase and of constraints: technical, economic and social. An industrial process must be safe, therefore managed so as not to represent a danger to the population and to the plant itself; this means that the operating variables (temperatures, pressures, concentrations of the fluids involved, etc.) must be kept under control. Must comply with environmental regulations; that is, the emissions must be kept within certain imposed limits, but at the same time must be productive, thus guaranteeing the production specifications, optimizing the capital investment and the use of labor.

During operation, a process plant can be found to work in conditions other than those operating due to disturbances that tend to shift it from stationary conditions. We can therefore have disturbances caused by malfunctions, therefore not desired or derive consequent variations established by the operator of the system.

The control system is the one that takes care of maintaining the process variables on the desired values, ensuring the correct functioning of the equipment.

Modern industrial plants are highly automated by this automation, which derives the concept of Industry 4.0, in this regard see next chapter - ie the processes are driven by a calculation unit that provides the commands necessary for the correct operation of the plant and monitors its status. With the obvious consequence of an increase in production speed, the powers available in the process and the quality of the products. The operating units consist of controllers (automatic and / or semi-automatic) interfaced with sensors and actuators of mechanical devices. These can be managed by PLC (Programmable Logic Controller), programmable logic controllers and by DCS (Distributed Control System), distributed control systems.

A distributed control system (DCS, from the Distributed Control System) is an automatic control system consisting of several subsystems, including data acquisition and processing, capable of exchanging information independently with the field (process or system) in distributed architecture, ie non-centralized. In other words, there is not a single controller computer for the entire system, but several controllers located by plant sections and appropriately segregated: the information exchanged by the subsystems is collected by appropriate supervisory centralizers. The loss of a coordinator does not affect the ability to keep the system controlled. Among other benefits, it does not result in accidental shutdown of the system.

As a result, industrial processes, by manipulating potentially dangerous substances, face vulnerability threats similar to those of all computer networks, with risks that often go beyond the loss / disclosure of data, as they can potentially threaten physical safety the plant itself and its surroundings.

The control technologies, while guaranteeing the advantages described above, therefore expose the plants to problems of Security, therefore voluntary attacks coming from outside.

Cyberattacks are actions directed against computer systems aimed at disturbing the operation of the equipment, modifying the processing and software controls or damaging the stored data.

The possible computer terrorist can cause the complete shut-down of the signal or change the setting of the parameters of the production process, modifying the manipulable variables of the system to one's liking.

There are many methods of attack in the cyber war: attack on critical infrastructures, web vandalism, data collection or confidential information but not adequately protected can be intercepted and modified, making espionage possible.

The diffusion also in the industrial contexts of networked equipment has changed both the way the crime is carried out and the author.

The author can be a single individual acting on his own behalf or an associated group, that is real and proper crime companies, organizations that control particular sectors of the economy with a flourishing business.

4. CRISP CYBER RISK ANALYSIS IN INDUSTRIAL PROCESS SYSTEM ENVIRONMENT STRATEGY

A cyberattack is any action, used by individuals or even state organizations, which affects information systems, infrastructures, computer networks and/or personal electronic devices through malevolent acts, generally coming from an anonymous source, aimed at theft, alteration or destruction of specific targets in violation of susceptible systems.[36]

Generally, a cyberattack consists of two phases:

a) System access / hacking.

b) Handling of the system in order to cause damage.

In the first phase the hacker gains access to the system, or rather to a programmable device connected to the system's network, which he can remotely control. In the second phase the hacker manipulates the system, for example modifying the values supplied by sensors or modifying the state of actuators.

The techniques and methods of protection of unwanted access to computer systems are the classic ones of cyber-security and are beyond this work.

As part of this work, attention has been paid to point b), namely that relating to the handling of the systems. In fact, if, as mentioned above, it is difficult to ensure complete impermeability to computer networks, it must, at least try to define a methodology that allows us to reduce the damage caused by a possible intrusion.

Therefore, a systematic tool for the ‘security review’ of the plants will be illustrated below; similar in some ways, as a structure, to the techniques for identifying safety hazards (HazOp, FMEA, etc.).

The proposed methodology is the Cyber Risk Analysis in the Industrial Process System Environment Strategy, also called CRISP, an evolution of the procedure proposed by the authors in [29].

The CRISP methodology is aimed at identifying, in a systematic manner, the consequences of tampering with the plant as a result of a telematic attack.

CRISP allows to analyze both the global consequences of an attack - through the CRISP phase in the Large, and the local consequences of an attack - through the CRISP phase in the Small.

In both phases they are used, as a starting point for risk assessment:

- the P&ID Process and Instrumentation Diagram, or rather the diagrams of the process instrumentation of the plant to be analyzed,

the Assett Management System, or the detailed repertoire of the devices installed in the plant.

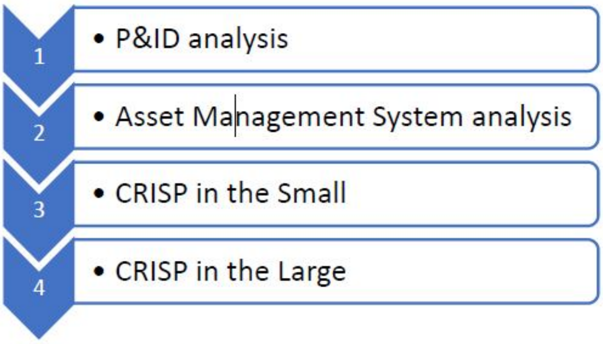


Figure 1CRISP - Cyber Risk Analysis in Industrial Process System Environment Strategy

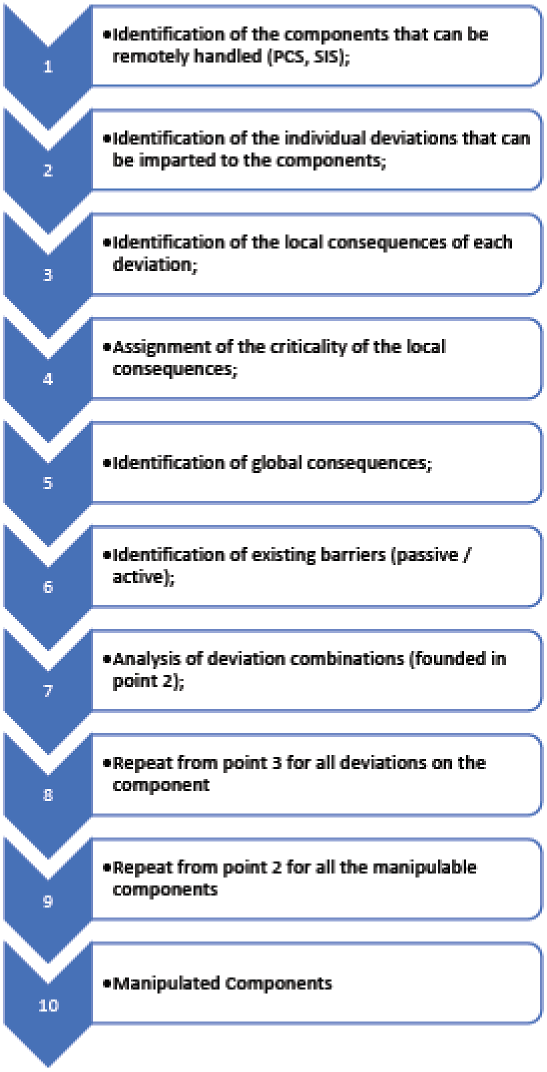
The CRISP in the Small, is used to analyze the consequences of cyber deviations on single machines present in the plant (e.g. valves, pumps) or relatively simple and modular systems (e.g. wind torch systems, compression trains). So it is the analysis that is done as a first step on all the elements 'liable to cyber-attacks' present in the system. Given the standardization and modularity of these components, the CRISP analysis in the Small can be profitably carried out, in addition to the specific components, also for typical assembly of the same. The methodology is based on a structure similar to FMECA (Failure Modes, Effects and Critical Analysis), specially adapted to the analysis of attacks by computer.

The CRISP in the Large is used to analyze the consequences of cyberattacks on the entire system constituted by the process plant. It is therefore able to analyze the repercussions that manipulations on one or more devices may have on the system as a whole. The methodology is based on a structure similar to a 'Reverse HazOp' (Reverse Hazard and Operability analysis): its starting point is the identification of potential release scenarios (Top Event) and systematically traces the entire cause chain effect until identifying the variables that must be manipulated during the attack to make such events happen.

The application of both methods requires as input the typical process documentation required by the corresponding structured methods for identifying hazards (Process Flow Diagram, Piping & Instrumentation Diagram, technical data sheets of manipulable elements) and obviously also the Assett Management System.

4.1 Steps of CRISP in the Small methodology

CRISP in the Small aims to identify and analyze the consequences of cyber attacks on individual machines or relatively simple and modular systems.


1
•Identification of the components that can be remotely handled (PCS, SIS);
2
•Identification of the individual deviations that can be imparted to the components;
3
•Identification of the local consequences of each deviation;
4
•Assignment of the criticality of the local consequences;
5
•Identification of global consequences;
6
•Identification of existing barriers (passive / active);
7
•Analysis of deviation combinations (founded in point 2);
8
•Repeat from point 3 for all deviations on the component
9
•Repeat from point 2 for all the manipulable components
10
•Manipulated Components

1. Identification of the components that can be manipulated remotely (PCS, SIS); In this phase the main components that can be manipulated in a cyber attack are identified. The elements, which may be subject to an external computer attack, on which attention must be focused, are therefore those elements of final control that are managed upstream by a DCS system:

• shut-off and regulation valves (pneumatically and electro-hydraulic operated)

• the operating machines and all those final control elements driven by motors managed remotely by a control system.

In any case, the one on which we must focus the analysis in order to understand what can actually happen at the plant is first of all how the final control element can react to these "disturbances"

2. Identification of deviations: In this phase the parameters that can be manipulated for each component are identified, for example speed of rotation of a motor, and for each parameter the variations that can be imposed during an attack are identified, for example increase in the number of revolutions , or decrease of the same, or interruption of operation.

3. Identification of local consequences: In this phase the local consequences are identified, where local consequences mean those consequences that cause problems at the local level of the component analyzed. For example, for a centrifugal pump motor a local consequence of a variation can be the decrease in the number of revolutions.

4. Identification of the global consequences: In this phase the global consequences are identified, where by Global consequences we mean instead those events / consequences that occur downstream of the process plant being analyzed, such as the undesired increase of the flow rate of the plant.

5. Assignment of Criticality: In this phase the criticalities of a local consequence are detected, or a parameter is defined that quantifies the level of severity and / or damage to the component that can be caused by the cyberattack. In CRISP in the Small this analysis is limited only to the local consequence.

In fact, to consider the criticality of the global consequence is not very reliable in this phase, since it depends on what is in the system to which the considered element is connected.

Criticality indices are defined as follows:

• Criticality I (critical): these are the events that cause irreversible damage to the component analyzed, or an important local consequence. • Criticality II (not very critical): events with a reversible local damage or easily solved can be considered as such.

• Criticality III (not problematic): these are the events that lead to a local consequence that is not relevant.

6. Identification of Barriers: In this phase the barriers that can prevent the manipulation of a given element results in a local or global consequence are identified. Barriers are classified as:

• Active/Procedural: means all those active safety elements - for example controller devices, interlocks, emergency shutdown systems - aimed at detecting potentially damaging process changes and taking appropriate corrective actions to defuse the danger. Active / procedural barriers, however, could be, at least in principle, victims themselves of cyberattack;

• Passive: those hardware systems appropriately inserted in the system that reduce or eliminate the dangers through design features, without requiring the active operation of any device. Ex. PSV (safety valve). The functioning of these barriers cannot be altered by the cyberattack. CRISP in the Small

7. Analysis of the combinations of deviations: In this phase the consequences of multiple variations on the same element are analyzed. In fact, in a given component the terrorist can decide to attack only one element or more than one, or to make more than one variation at the same time. The analysis of multiple variations proceeds in the same way as single ones.

A multiple variation is traced back to the individual variations, which compose it, in the event that it does not present different and / or worse consequences of the consequences found in the aforementioned individual variations.

4.2 Steps of the "CRISP in the Large" methodology

The purpose of the CRISP in the Large methodology is to identify which variations and / or deviations on the system components, carried out by a cyberattack, can actually cause a critical event, serious events, in a complex system consisting of multiple components.

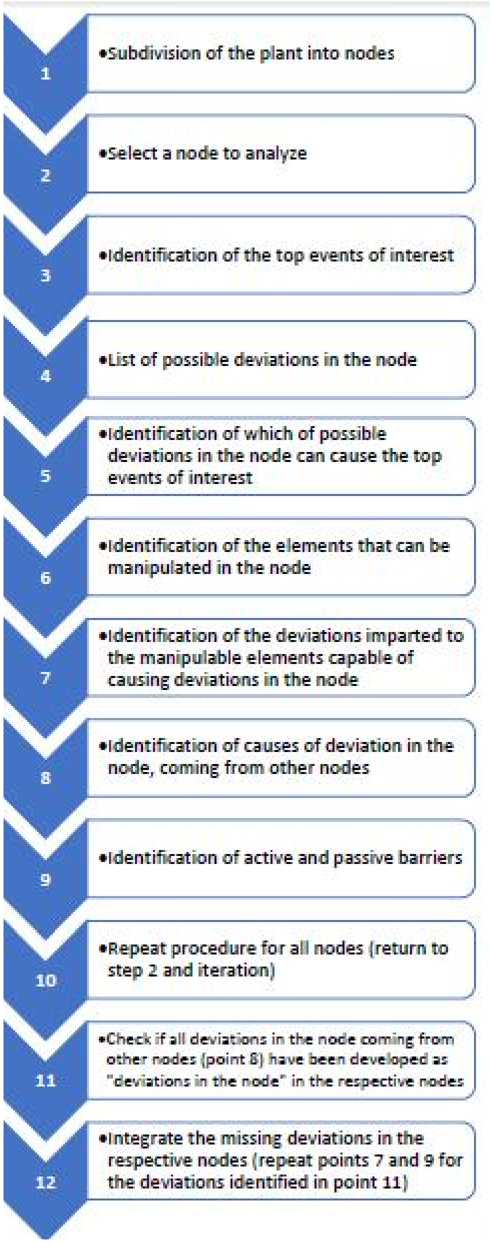
In summary, the CRISP in the Large structure differs from the CRISP in the Smal structure in that it aims to offer a global view, with respect to the plant being analyzed, of the consequences of a cyberattack.

The procedure can be assimilated to a modified Reverse Hazop in which, taken a node, only the deviations that can actually produce a top event are identified.

The methodology was developed as a complement to the CRISP in the Small procedure. Although in theory the CRISP in the Small procedure is able, by itself, to produce a complete evaluation of all the possible consequences in a plant of manipulations resulting from a cyberattack, its application to very complex systems can be severely limited in practice from the resources and time required.

However, the main interest of a procedure for the analysis of potential cyberattacks can be effectively restricted to the identification of the only combinations able to give serious events, and in particular losses of containment of dangerous materials. Starting from this consideration, the CRISP in the Large procedure was then developed.

CRISP in the Large part, not from the analysis of the single components and the possible consequences caused by their possible manipulation, but, adopting a Top-Down approach, from the possible top events of interest, and leads them to the manipulations of the elements during the cyber -attack, already analyzed in the local detail by the CRISP in the Small procedure.



1 •Subdivision of the plant into nodes

2 •Select a node to analyze

3 •Identification of the top events of interest

4 •List of possible deviations in the node

5 •Identification of which of possible deviations in the node can cause the top events of interest

6 •Identification of the elements that can be manipulated in the node

7 •Identification of the deviations imparted to the manipulable elements capable of causing deviations in the node

8 •Identification of causes of deviation in the node, coming from other nodes

9 •Identification of active and passive barriers

10 •Repeat procedure for all nodes (return to step 2 and iteration)

11 •Check if all deviations in the node coming from other nodes (point 8) have been developed as "deviations in the node" in the respective nodes

12 •Integrate the missing deviations in the respective nodes (repeat points 7 and 9 for the deviations identified in point 11)

5. CONCLUSION

The CRISP methodology includes two CRISP in the Small and CRISP in the Large structures, these intersect and complement each other. In fact, through the CRISP in the Small procedure we are able to detect harmful events, and their causes and consequences on each individual component, while through the CRISP in the Large procedure we can identify the critical events for each node; then using the results of the CRISP in the Small we can go back to the single components that are, and / or can be, the object of a terrorist attack to which particular deviations can be given, capable of generating the critical events defined above.

Finally, among the strengths offered by the adoption of the CRISP we can observe:

• Ability to analyze analytically, punctually through the CRISP in the Small phase, overall through the CRISP in the Large phase, an entire plant both in terms of installed components and in terms of possible consequences of undesired deviations.

• Glossary and approach similar to other "Reverse HazOp" (Reverse Hazard and Operability analysis) methodologies very common in the industrial field While the weaknesses are certainly:

• The cost and complexity of application of the method to large-scale plants.

• The excessive cost of updating and aligning the analysis with the evolution of the plants However, these aspects can be a stimulus to improve the management of the plants also in relation to the maintenance aspects.

In conclusion, we need to reiterate that the security of a complex system cannot be tackled with a "technological oriented" approach, there is no turnkey technology that can secure an industrial plant. Safety is a process - set of activities, roles and responsibilities, approaches and methodologies, and technologies - which continuously evolves together with the organization and industrial plants and which must be oriented to the continuous and rational monitoring of business processes in order to implement and constantly improve the appropriate protection strategy and quickly highlight the symptoms of a possible attack; to do this it is necessary to start from a risk analysis supported by a methodology such as the one presented in this document.

References

[1] Cabinet Office, Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards, 2010.

[2] A. Daneels and W. Salter, “What is SCADA?,” International Conference on Accelerator and Large Experimental Physics Control Systems, pp. 339–343, 1999.

[3] V. M. Igure, S. A. Laughter, and R. D. Williams, “Security issues in SCADA networks,” Computers and Security, vol. 25, no. 7, pp. 498–506, 2006.

[4] M. Henrie, “Cyber security risk management in the SCADA critical infrastructure environment,” Engineering Management Journal, vol. 25, no. 2, pp. 38–45, 2013.

[5] J. Guan, J. H. Graham, and J. L. Hieb, “A digraph model for risk identification and mangement in SCADA systems,” presented at the Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, ISI 2011, 2011, pp. 150–155.

[6] S. Patel, R. Tantalean, P. Ralston, and J. Graham, “Supervisory control and data acquisition remote terminal unit testbed,” Intelligent Systems Research Laboratory Technical Report TR-ISRL-05-01, 2005.

[7] NIST, “System Protection Profile-Industrial Control Systems v1.0,” System protection profile – industrial control systems, 2004.

[8] U. D. of Energy, “21 Steps to Improve Cyber Security of SCADA Networks,” White Paper, 2005.

[9] NIST, Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security, 2011.

[10] ENISA, Window of exposure a real problem for SCADA systems? Recommendations for Europe on SCADA patching, 2013.

[11] NERG, Project 2014-02 critical infrastructure protection standards version 5 revisions, 2014.

[12] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare,"Computers and Security, vol. 31, no. 4, pp. 418–436, 2012.

[13] B. Miller and D. C. Rowe, "A survey of SCADA and critical infrastructure incidents," presented at the RIIT'12 - Proceedings of the ACM Research in Information Technology, 2012, pp. 51–56.

[14] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," IEEE Transactions on Industrial Informatics, vol. 9, no. 1, pp. 277–293, 2013.

[15] H. M. Leith and J. W. Piper, "Identification and application of security measures for petrochemical industrial control systems," Journal of Loss Prevention in the Process Industries, vol. 26, no. 6, pp. 982–993, 2013.

[16] S. Kaplan and B. J. Garrick, "On The Quantitative Definition of Risk," Risk Analysis, vol. 1, no. 1, pp. 11–27, 1981.

[17] ISO, ISO/IEC 27001:2005, Information Technology - Security Techniques - Information Security Management Systems - Requirements, 2015.

[18] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," Introduction to the OCTAVE Approach, 2003.

[19] Z. Yazar, "A qualitative risk analysis and management tool–CRAMM," SANS InfoSec Reading Room White Paper, vol. 11, pp. 12–32, 2002.

[20] J. Ø. Aagedal, F. Den Braber, T. Dimitrakos, B. A. Gran, D. Raptis, and K. Stolen, "Model-based risk assessment to improve enterprise security," presented at the Proceedings - 6th International Enterprise Distributed Object Computing Conference, 2002, vol. 2002-January, pp. 51–62.

[21] B. Karabacak and I. Sogukpinar, "ISRAM: Information security risk analysis method," Computers and Security, vol. 24, no. 2, pp. 147–159, 2005.

[22] L. C. Briand, K. El Emam, and F. Bomarius, "COBRA: A hybrid method for software cost estimation, benchmarking, and risk assessment," presented at the Proceedings - International Conference on Software Engineering, 1998, pp. 390–399.

[23] R. S. Coles and R. Moulton, "Operationalizing IT risk management," Computers and Security, vol. 22, no. 6, pp. 487–493, 2003.

[24] G. Giannopoulos, R. Filippini, and M. Schimmer, "Risk assessment methodologies for critical infrastructure protection. Part I: a state of the art," Technical Notes. European Commission Joint Research Centre Institute for the Protection and Security of the Citizen Luxembourg EUR 25286 EN-2012, 2012.

[25] P. Kertzner, D. Bodeau, R. Nitschke, J. Watters, M. Young, and M. Stoddard, Process Control System Security Technical Risk Assessment Analysis of Problem Domain, 2005.

[26] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," ISA Transactions, vol. 46, no. 4, pp. 583–594, 2007.

[27] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for SCADA systems," Computers & Security, vol. 56, pp. 1–27, Feb. 2016.

[28] F. Farahmand, S. B. Navathe, G. P. Sharp, and P. H. Enslow, "Managing Vulnerabilities of Information Systems to Security Incidents," presented at the Proceedings of the ACM Conference on Electronic Commerce, 2003, vol. 5, pp. 348–354.

[29] Y. Y. Haimes, "Hierarchical Holographic Modeling," IEEE Transactions on Systems, Man and Cybernetics, vol. 11, no. 9, pp. 606–617, 1981.

[30] Y. Y. Haimes, Risk Modeling, Assessment, and Management, 1998.

[31] C. G. Chittester and Y. Y. Haimes, "Risks of terrorism to information technology and to critical interdependent infrastructures," Journal of Homeland Security and Emergency Management, vol. 1, no. 4, pp. 25–46, 2004.

[32] K. G. Crowther and Y. Y. Haimes, "Application of the inoperability input-output model (IIM) for systemic risk assessment and management of interdependent infrastructures," Systems Engineering, vol. 8, no. 4, pp. 323–341, 2005.

[33] M. Stamatelatos, W. Vesely, J. Dugan, J. Fragola, J. Minarick, and J. Railsback, "Fault tree handbook with aerospace applications," 2002.

[34] H. Kumamoto and E. J. Henley, Probabilistic Risk Assessment and Management for Engineers and Scientists, 1996.

[35] B. Vesely, "Fault tree analysis (FTA): Concepts and applications," NASA HQ, 2002.

[36] L. Scott, "Baldrige Cybersecurity Initiative," 2016.

AUTHORS

Antonio Capodieci, PhD in Information Engineering, adjunct professor of Computer Science at Polytechnic of Bari and at University of Bari, former member of the Board of Directors of the University of Salento. Graduated in Engineering at the Polytechnic of Turin, he had Master in Public management and Egovernment. He has had important international training and professional experiences at UTS, University of Technology in Sydney, at the University College of London, and at the Universitè Catholique de Lille in France. Author of numerous international scientific publications and member of the organizing committees of various international scientific conferences, he has participated in numerous projects in scientific research.

Vincenzo Capalbo Management Engineer, Certified Project Manager is a Process Analyst, Expert of organizational systems and business management models. He has gained significant experience in research and development at the helm of important private research centers and scientific foundations. His research activities are concentrated in the field of business management and organizational systems.

Giuseppe Filitti Economist and Auditor, he specializes in finance and administrative accounting. Expert in the design and management of corporate governance models. His research activities are concentrated in the field of business management and organizational systems.