Advances in Science, Technology and Engineering Systems Journal
Vol. 2, No. 3, 88-99 (2017)
www.astesj.com

ASTES Journal
ISSN: 2415-6698

Methodology for Management of Information Security in Industrial Control Systems: A Proof of Concept aligned with Enterprise Objectives.

Fabian Bustamante[1], Walter Fuertes[*,1], Paul Diaz[1], Theofilos Toulqueridis[1]

[1]*Universidad de las Fuerzas Armadas ESPE, Department of Computer Sciences, ZIP Code: 17-15-231-B, Sangolqui, Ecuador*

ARTICLEINFO
Article history:
Received: 05 March, 2017
Accepted: 04 April, 2017
Online: 09 April, 2017

Keywords :
Industrial Control Systems,
Information Security,
Automation,
ISMS,
SCADA,
DCS,
PLC,
ISO 27000,
NIST

ABSTRACT

This article is an extended version of the study presented at the IEEE Ecuador Technical Chapters Meeting (ETCM)-2016. At that time, a methodological proposal was designed, implemented, and applied in a group of industrial plants for the management of the information security of the Industrial control systems (ICS). The present study displays an adaptation and improvement of such methodology with the purpose of aligning the proposal for the effective management of information security with the strategic objectives. The development of this study has been divided into three distinctive phases. Firstly, we induced the articulation of PMI-PMBOK v5 and ITIL v3 both for the management of the project and for the verification of risks in the IT services. Second, we applied a set of risk mitigation strategies based on international standards as NIST 800-82 and 800-30. Thirdly, we assembled the two mentioned phases in a Guide for standards-based instructions and security policies, which previously have been encouraged on NIST 800-82, 800-53 and 800-12. Hereby, we observed the reduction of incidents of information security, the correct delimitation of the functions of the direct responsible of the ICS and the improvement of the communication between the operative and technical areas of the involved companies. The results demonstrate the functionality of these improvements, especially in the context of the availability and integrity of information, which generates an added value to the enterprise.

1 Introduction

According to the Guide to Industrial Control Systems (ICS) Security NIST-2nd Revision [1], “threats to control systems may be originated from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders. ICS security objectives typically follow the priority of availability and integrity, followed by confidentiality”.

Facing these issues, the industry has proposed several studies as recommended by [2] where best practices and risk assessment of the ICS have been suggested. In [3] authors documented about Supervisory Control and Data Acquisition (SCADA) system security. In [4] enlightens the myths and facts behind Cyber security in ICS, while in [5] [6] [7] [8] [9], authors present issues, methods and countermeasures to the protection of information, control systems as well as automation. In [10] exposes the research about SCADA security in the light of Cyber-Warfare. In recent studies such as [11] examines the State of the Art in Cyber security risk assessment methods for SCADA systems. In [12] [13] proposes a study on efficiency of an Information Security Management System (ISMS) for ICS with compliance. In [14] presents a formal approach that automates the security analysis of ICS. In [15] explains a process of defense of securing ICS. In [16] presents a theory of security metrics in SCADA

[*] Walter Fuertes, Gral. Ruminahui Ave, Contact No:00593-987392793 & Email: wmfuertes@espe.edu.ec

https://dx.doi.org/10.25046/aj020313

and ICS including resilience. In [17] [18] [19] [20] [21] authors explore the ICS cybersecurity landscape including threats, vulnerabilities, intrusions and cyberattacks. In [22] discusses that the wireless systems in all ICS are subject to cybersecurity vulnerabilities. In [23]gives an analysis of behavior, time, and adaptation in the assessment of ICS Cybersecurity Risk. In all mentioned studies, general recommendation and analysis on the ICS were discussed, but unfortunately they missed to propose a management system of information security. The standards listed in the mentioned studies are predominantly: NIST 800-53, ISA 99, NERC, ISO 27001, ISO 27002 [24], ISO 31010, and ISO 27019.

Despite having controls and procedures in the management of information security of its ICS, the manufacturing companies, fail to reduce and resolve the incidents. In addition, there is little or no evidence of a complete vulnerability, threat and risk analysis of their critical assets and services. This may be attributed to the high level of sophistication of the ICS and the poor knowledge of the present personnel that manages and carries out such tasks [10].

Thus, the main contribution of this research has been to provide a methodology to manage information security in ICS. This has been focused on both, Information Technology (IT) professionals and manufacturing automation professionals. Its stages and methods have been consistently combined with the standards outlined above and are internationally used in traditional IT and ICS. Specifically, these contributions are: (1) Novel guides for the management of the project of implementation of the methodology; (2) Updated methodologies for risk assessment in IT services used in ICS; (3) Methodological procedures to encounter new risk mitigation strategies; and finally, (4) Methodological procedures to develop the manual of security standards and policies for ICS.

Based on the findings and conclusions presented by [24] [26], we agree and confirm that NIST fulfills all criteria needed and has been therefore chosen to be ideally for this study, besides the existence of two further interesting options such as the North American Electrical Reliability Corporation / Critical Infrastructure Protection (NERC / CIP). They represent a set of requirements designed to secure the assets required to operate in North America and the International Automation Society (ISA), being is a series of standards, technical reports and related information that defines procedures for Systems Automation and Control Electronics (IACS). Therefore, we have opted for a reliable standard like NIST stands for, which is not exclusively framed in the organization nor in the technical part only. This allows the possibility to manage in an effective and holistic way different areas that coexist in the SCI being: business, computing, electronics, automation, production processes and people. It is also recognized that NIST is internationally highly disseminated and its best practices exist supplementary information that may be available to the professional stakeholders of this project.

This document is an extended version of a previous conference presentation [27], which has been based specially on NIST. In this present article, areas of knowledge of the PMBOK and ITIL standards have been also included, which served to improve the management of the methodology implementation projects and in the risk analysis of the IT services operating in the ICS. Furthermore, we added detailed evidence and discussions of the results presented in [27].

The remainder of this paper is organized as follows: The conceptual framework that describes the theoretical foundation of this study is described in Section 2. Then, the adaptation and improvement of the methodology proposed is explained in section 3. Results and discusses of findings and their implications are displayed in Section 4. Finally, Section 5 closes with conclusions and some future research lines.

2 Theoretical Framework

This section comprises all the important theory and knowledge about the ICS, tools for IT architecture modeling and expert system validation method that have been used in this study:

2.1 Industrial Control Systems (ICS).

As reported by the Guide to Industrial Control Systems (ICS) Security of the National Institute of Standards and Technology (NIST) [1], the term Industrial Control System includes Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), as well as programmable logic controllers (PLCs). ICS are used in industries such as electricity, water distribution systems, wastewater, petroleum, natural gas, chemical, transportation, pharmaceutical, pulp, paper, food, automotive, aerospace, among many others. On the other side, SCADA systems are also used to control critical infrastructure. As stated by ENISA in [28] critical infrastructure such as electricity generation plants, transportation systems, oil refineries, chemical factories and manufacturing facilities means an asset, system or part thereof located in a country which is essential for the maintenance of vital societal or strategic functions, such as health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact (e.g. disruption to business operations and services but also potential damage and destruction of equipment). As a final point, DCS are used to control production systems within a local area such as a factory using supervisory and regulatory control. PLCs are used for discrete control for specific applications and generally provide regulatory control [1].

2.2 Security incidents in Industrial Control Systems.

The proliferation of connections that use the electromagnetic spectrum, combined with vulnerable source code and errors in configurations of automation systems expose the ICS to potential from cyberspace. Weak IT security policies and weaknesses in the security features of automation systems dramatically increase the risk of a successful cyber-attack [29].

Facing such issues, there are some organizations authorized to investigate and combat cybersecurity incidents. For instance, in the United States are the Cybersecurity Emergency Response Team (ICS-CERT) [30] and the Federal Bureau of Investigation (FBI). ICS-CERT in 2015, received and responded to several incidents reported by owners and manufacturers of industrial products in North America. Other reports considered are also those reported by manufacturers and suppliers of equipment, industrial systems, and information security solutions such as: ABB, Allen Bradley, Verizon [31], among others.

In the same context [27] [28] discloses the current maturity level of ICS-SCADA cybersecurity in Europe and identifies good practices handled by European Member States to improve this area. The first and second part of this study introduces the ICS-SCADA cyber security topic, explains the role of ICS-SCADA in critical sectors and summarizes the methodology of this research.

2.3 Guide for Industrial Control System Security NIST 800-82.

The NIST Industrial Control System Safety Guide 800-82 establishes some guidelines for the implementation of safety in ICS. The main reason for using the regulations for an ICS is that these increasingly adopt computer components in their design and operation. While some features are similar between traditional IT systems and ICS, it is fundamental to understand that they are unable to be handled in a similar procedure. ICS and IT include significant risks such as health, protection of human life, environmental damage, financial impact, production losses, etc., [1].

This document is the second revision to NIST SP 800-82 which has been published in March of 2015. Updates in this revision include: ICS threats and vulnerabilities; ICS risk management, recommended practices and architectures; current activities in ICS security; security capabilities and tools for ICS; Additional alignment with other ICS security standards and guidelines; new tailoring guidance for NIST SP 800-53, among others [1].

Risk is present, when the probability exists of an occurrence of a threat or any vulnerability. Threats are able to take advantage of vulnerabilities. In the case of a computer incident, for example, the magnitude of the potential impact results from a successful exploitation of vulnerability [32] and [33] should be determined. Risk assessment, in turn, is the process of identifying the risks of an organization's operations, assets, and individuals by evaluating the likelihood of an identified vulnerability having a potential impact. The risk assessment also has to compare the costs of such safety with those expenses or financial damages associated with a possible incident.

2.4 Guide to the Project Management Body of Knowledge (PMBOK® Guide)–Fifth Edition.

The Guide to the Project Management Body of Knowledge provides guidelines for the direction of individual projects and defines concepts related to project management. It also describes the life cycle of project managements and related processes, as well as the project life cycle. The PMBOK® Guide contains the globally recognized standard and guidance for the project management profession. By standard means a formal document that describes established standards, methods, processes and practices. Similar to other professions, the knowledge contained in this standard evolved from the recognized good practices of the professionals dedicated to the management of projects that have contributed to its development. Acceptance of project management as a profession indicates that the application of knowledge, processes, skills, tools and techniques may have a considerable impact on the success of a project [34].

2.5 IT Infrastructure Library (ITIL)

ITIL is part of a suite of best-practice publications for IT service management (ITSM). ITIL provides guidance to service providers on the provision of quality IT services, and on the processes, functions and other capabilities needed to support them. Organizations are encouraged to adopt ITIL best practices and to adapt them to work in their specific environments in ways that meet their needs. ITIL is not a standard that is mandatory to be followed, it is more likely a guidance that should be read, understood, and used to create value. The ITIL framework is based on the five stages of the service lifecycle, namely Service Strategy, Service Design, Service Transition, Service Operations and Continual service improvement [34] [35] [36].

2.6 Control Objectives for Information and Related Technology (COBIT).

The COBIT provides a comprehensive framework that supports enterprises to achieve their goals and deliver added value through effective governance as well as IT governance of the Organization. In this way, it supports organizations to create optimal value from IT, by maintaining a balance between realizing benefits and optimizing levels of risk and resource utilization. This allows IT and related organizations to be governed and administered in a holistic manner throughout the Organization. This includes the full scope of all functional and business areas of responsibility, taking into account the internal and external interests of IT stakeholders.

3 Methodology Proposal.

3.1 Research Methodology

During this project, we have used the Action research Methodology [37], also known as participatory research which is a testing of theories developed to overcome an immediate on the job-difficulty. In short, action research means learning by doing. In this kind of approach first a solution is devised and evaluated, while depending of the results, a new solution may be constructed in order to try to achieve more sophisticated results. These processes are cyclically repeated until an acceptable performance has been obtained. In one of its formal stages it is established the gathering of pertinent data, material, methods, techniques, and so on for setting into testing periods. All data should be relevant to the problem. Therefore, it has been pertinent for us, to use PMBOK v5 and ITIL PRACTITIONER in their respective areas of knowledge called Communication. As collaborative instruments, workshops were developed with ICS experts as a focus group. The next stage has been to concern the developing plans for implementation of a theory.

The research has been carried out under real conditions of four industrial plants of the principal manufacturing enterprises in their markets. These have approximately 600 employees in the manufacturing area and some 400 more, in the administrative area. The four plants were comprised of two production lines containing four distributed control systems (DCS), 120 Allen Bradley and Siemens PLCs, 40 HMIs Allen Bradley, 48 desktop computers, 15 industrial applications using Rockwell Automation and Wonderware software (including 5 critical mission) and a Local and Wide area networks (LAN/WAN) with Cisco equipment and Checkpoint. Reference standards such as: NIST 800-30, NIST 800-82, NIST 800-53, NIST 800-12, PMBOK v5, ITIL v3, interviews, statistical processes and cost-benefit analysis have been used among the most important ones.

3.2 Modeling of IT frameworks & Methodological proposal.

In order to improve the methodology proposed in our previous study [27], we have considered the adaptation of other standards, referential frameworks, and management systems that are used in Information Technology (IT). With the purpose to understand the context, we have started by modeling the indicated in a hierarchical pyramid that is illustrated in Figure 1. In the base stand the standards used in traditional IT: COBIT, ISO 27000, PMBOK and ITIL. The second level of the pyramid holds NIST, NERC and ISA. At the third level is the proposed methodology. From bottom to top, these standards reveal ICS practitioners "how to do it?", while from top to bottom urges the question of: "what to do?"

Firstly, as part of the COBIT IT governance process, the "BAI01" (Building, Acquiring and Implementing, BAI), called Program and Project Management has been included. There, COBIT indicates "what to do?" According to this process, all the investment portfolio programs and projects are strongly recommended to be managed in a coordinated way and in line with the corporate strategy. In a similar case, chapter 13 of [34] indicates "what to do?" to identify project stakeholders. In the case of this proposed management, the "how to do?" procedure is indicated to discover the stakeholders required at each step of the implementation.

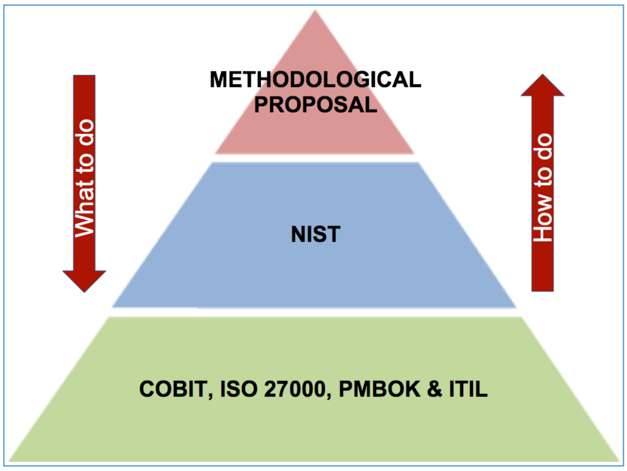


Figure 1: Modeling of IT frameworks & Methodological proposal

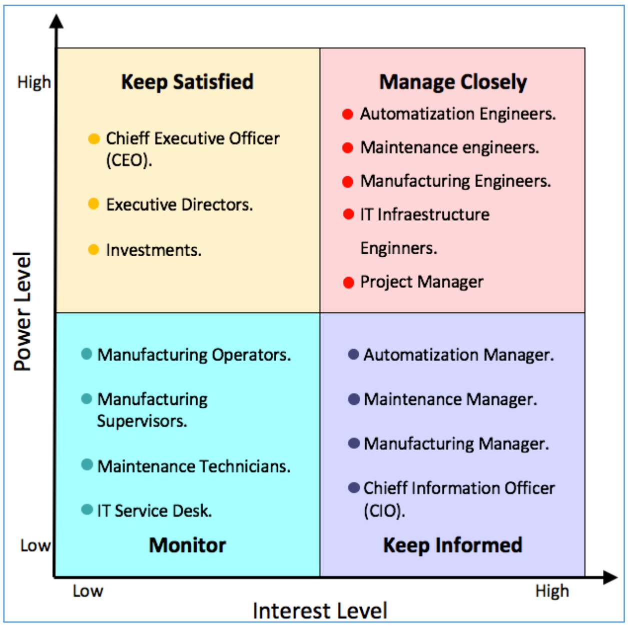
Secondly, [1] indicates "what to do?" to evaluate and mitigate ICS risks. In the case of the management proposal for ICS security, it is indicated "how to do it?"

Although COBIT, ISO27000, PMBOK and ITIL are not fully implemented in the case study, it is necessary to use some of their areas of expertise and refer them to fit the methodological proposal into a form, which is already worldwide established. This avoids the occurrence of inaccuracies of concepts that in the future may not articulate in the management of the information security at managerial, operational, and technical level.

3.3 Project to improve the methodological proposal

For the improvement of this methodology and because its implementation requires to perform a considerable amount of tasks with specific deliverables with a defined time, in which the quality of the information is fundamental, having some stakeholders in account, it has become necessary to include in the methodology standards in the field of project management, which help to keep critical success factors controlled (i.e. cost, quality, scope and time). The main reason for adopting PMBOK [34] has been the better adaptability with NIST, its interdependence and the widespread diffusion that this standard has had in project management.

Prior the implementation of the methodology in an enterprise, several meetings with the responsible of the ICS must be realized. It starts with the collection of information that serves to identify and analyze stakeholders. In line with [34] this point plays a fundamental role in the development and success of a project. Later, a variety of points should be reviewed such as: names and position of who will be the project manager of implementation, identification of the problem to be solved, business need to solve the problem, justifications that lead to implement the methodology in the enterprise, levels of authority of Project Manager, risks that may exist in the implementation, opportunities that the enterprise has with this project, general deliverables, specific deliverables, and pre-allocated resources (i.e., financial, material and human resources). With all this information two documents need to be elaborated to begin the project of implementation of the methodology such as Project Charter and Power-Interest Matrix Stakeholder (see Figure 2). In consonance with [34] the Charter Project must be signed before beginning the implementation of the methodology in order to formalize the support and participation of the entire enterprise. The signers of the charter project are the Project Manager and the Chief Executive Officer (CEO), who is the first and most important stakeholder.



Power Level
High
Low
Keep Satisfied
● Chieff Executive Officer (CEO).
● Executive Directors.
● Investments.
Manage Closely
● Automatization Engineers.
● Maintenance engineers.
● Manufacturing Engineers.
● IT Infraestructure Enginners.
● Project Manager
● Manufacturing Operators.
● Manufacturing Supervisors.
● Maintenance Technicians.
● IT Service Desk.
Monitor
● Automatization Manager.
● Maintenance Manager.
● Manufacturing Manager.
● Chieff Information Officer (CIO).
Keep Informed
Low
High
Interest Level

Figure 2: Power-Interest Matrix Stakeholders of the implementation project.

As stated in [34], the analysis of the power-interest matrix stakeholders illustrated in Figure 2, allows identifying who are the experts of the ICS. Moreover, there it's stated that all the workshops and meetings that are needed to obtain the information, which will be vital for the success of the implementation, must be carried out.

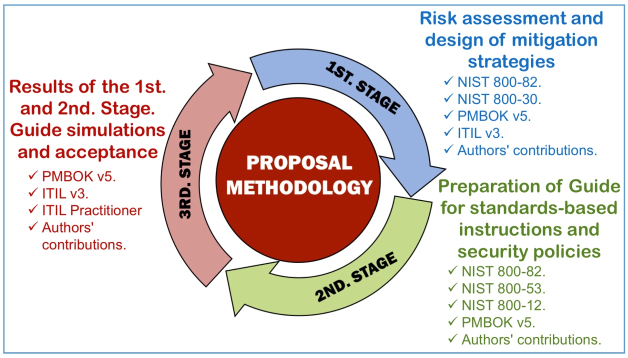
Figure 2 illustrates that these experts are those located in the quadrant entitled ”Manage Closely” (e.g. Engineers of automation, maintenance, manufacturing, and IT Infrastructure Engineering Engineers). Shown in the ”Keep Satisfied” quadrant, investors, executive directors, and the CEO will be placed, because they are only interested in the project for adequate results for the enterprise. Besides, in the ”Keep Informed” quadrant, there are all those who are interested in implementing the methodology, but are not directly involved within. Finally, in the ”Monitor” quadrant, the managers are placed in charge of monitoring what is being implemented and when the methodology is already in place to notify about the incidents and problems that may appear.

Given the experience gained in the implementations acquired by the research team, it is recommended to meet with the project implementation team and the Project Manager to assess progress and review the project's risk status once a week. As inputs, surveys should be carried out by the experts of each workshop and meeting, with whom the methodology is being implemented. In section 4, evaluation of results and discussion implies such behavior. In order to obtain the results of the surveys carried out by the experts, the following formula has been used (see equation 1):

$$P_m = \frac{\sum_{n=1}^{q} (R_m)_n}{q} \; (m{=}1,\, 2,\, 3{,}4) \qquad (1)$$

Where ”P” is the average of the answers of question number ”m”; ”n” is the workshop session number; ”q” is the number of the last workshop; and ”R” is the qualification the expert gave to each question.

Once the adaptation and improvement of the proposed methodology is planned, starts the implementation of the methodology, being divided into three phases represented in Figure 3. A brief schematic description is provided below:



Risk assessment and design of mitigation strategies
✓ NIST 800-82.
✓ NIST 800-30.
✓ PMBOK v5.
✓ ITIL v3.
✓ Authors' contributions.
1ST. STAGE
PROPOSAL METHODOLOGY
Preparation of Guide for standards-based instructions and security policies
✓ NIST 800-82.
✓ NIST 800-53.
✓ NIST 800-12.
✓ PMBOK v5.
✓ Authors' contributions.
2ND. STAGE
3RD. STAGE
Results of the 1st. and 2nd. Stage. Guide simulations and acceptance
✓ PMBOK v5.
✓ ITIL v3.
✓ ITIL Practitioner
✓ Authors' contributions.

Figure 3: Stages of the methodology proposed, as adapted by [27]

Unlike the previous version presented in [27] and as illustrated in Figure 3, in this extended version, areas of knowledge of both PMBOK and ITIL have been added in blue colors in the three stages of the proposed methodology. In stage 1, the PMBOK, NIST and ITIL stakeholder management were used to assess risks in ICS components and services, design of mitigation strategies, including the authors' contribution. In the second phase, only PMBOK stakeholder management are incorporated together with what NIST suggests in the preparation of the guide for standards-based instructions and security policies, as well as the contribution of the authors. Stage 3 includes PMBOK stakeholder management, ITIL service strategy catalogs, ITIL service design and communication management suggested by ITIL practitioner, and the authors' contributions.

3.4 Risk assessment and design of mitigation strategies for ICS

The first process in the methodology of risk management is the evaluation of threats and vulnerabilities, according to [1]. To perform such task, the subsequent steps are followed:

Step 1. The characterization of the system. In agreement with [34] it is determined with the whole system of hardware, software, connectivity, data, personnel support and execution processes. They also take into account the revision of existing documentation, the use of exploration tools, questionnaires and stakeholder interviews of the ”Monitor” and ”Manage closely” quadrants of the Power-Interest matrix (Figure 2).

Step 2. Identification of threats. For this step, we have drawn a table with sources based on threats [25], motivations, actions that would yield these threats and a comment of the stakeholders if necessary. Those responsible for conducting workshop sessions from step 2 through step 8 are the stakeholders of the ”Manage closely”.

Step 3. Identifying Vulnerabilities: Interviews were conducted, information related to recent incidents has been gathered and subsequently analyzed. Furthermore, documentation risks of the enterprise, I-CAT NIST database vulnerability, and security requirements were check-listed and later analyzed according to [35]. Although other ways to identify vulnerabilities have been available as proposed by [32], we have used a simplified version of the proposed methodology as suggested by [30].

Step 4. Analysis of Controls: A variety of control methods, control categories, and analysis techniques of control according to [24] were taken into account. The results have been documented due to the realization of workshops.

Step 5. Determination of Probability (P): The motivation of the source of threat (TM), the nature of vulnerability and the effectiveness of controls (EC) according to [24] were considered. In this respect:

1. If TM=High and EC=low, then P=1 (High).
2. If TM=medium and EC=medium, then P=0.5 (Medium).
3. If TM=low and EC=high, then P=0.1 (Low).

Step 6. Determination of Impact: The mission of the ICS has been to review the data criticality and to respect the sensitivity of the data and the information security [38] within the enterprise. In the present case study, the mission, the vision, the strategic plan of the enterprise and the documentation ISO 9001: 2015 held by the enterprise were analyzed.

Step 7. Risk Assessment (R): The risk assessment has been estimated according to the probability of threat sources (P) and the corresponding magnitude of the impact (I). Thus: R = P x I. The risk scale has been used by [24]: being HIGH when 100> value> 50, MEDIUM when 50> value> 10 and LOW when 10> value> 1.

Step 8. Recommended Controls: The recommended controls aim to reduce the vulnerability and risk level of the ICS and its data to an acceptable level for the enterprise, which needs to take into account the lowest possible costs and impacts.

Step 9. Documentation Result: A final report about the achieved results has been developed and afterwards addressed to the stakeholders, being rather systematic and analytical than accusatory in any form. However, finally in the present case study an executive summary has been elaborated and addressed to the CEO. Furthermore, the methodology for risk mitigation has been performed according to [24] (Figure 4).

In order to complement and verify that the ICS risk analysis has been accomplished, it is further recommended to use a risk assessment with respect of computer services in the ICS. Therefore, it is necessary to pick up the ICS services catalog as indicated [35] and [36]. To evaluate the risks in the IT services at ICS, a brainstorming session is held with the experts, without losing sight of the services catalog. In this way it is possible to analyze the probability and the impact in each of them, in the same way that it has been performed with the components of the ICS.

Regarding the data characteristics of the experimentation, we may point out, that for the accomplishment of the present study, confidentiality agreements have been signed with the enterprise of the case study. Consequently, this prevents the disclosure of detailed information on the characteristics of the components of their ICS. However, it should be stressed out, that regardless of the technology used, the proposed methodology would work properly as it has been focused on both management and technical criteria. Even so, the characteristics of the components have been better detailed described in the following points.

3.5 Preparation of the Guide for standards-based instructions and security policies

The security of an ICS according to [1] is based on a combination of effective security policies and a set of security controls configured properly. Such consider-

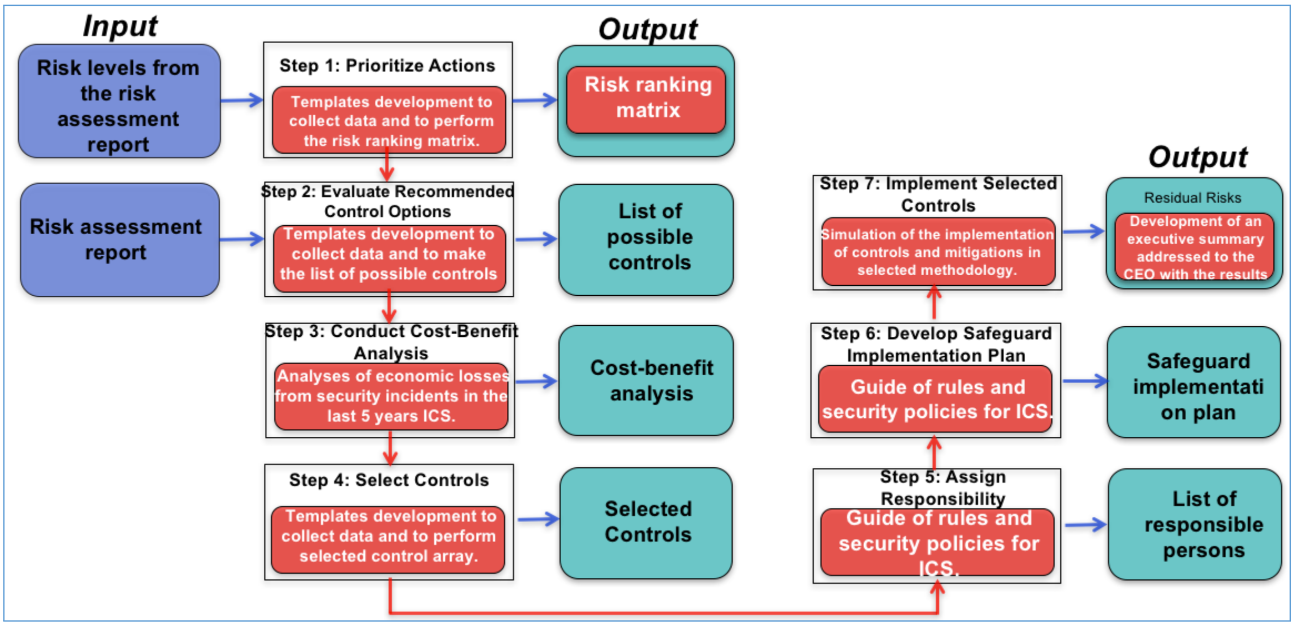

Input
Risk levels from the risk assessment report
Risk assessment report
Step 1: Prioritize Actions
Templates development to collect data and to perform the risk ranking matrix.
Output
Risk ranking matrix
Step 2: Evaluate Recommended Control Options
Templates development to collect data and to make the list of possible controls
List of possible controls
Step 3: Conduct Cost-Benefit Analysis
Analyses of economic losses from security incidents in the last 5 years ICS.
Cost-benefit analysis
Step 4: Select Controls
Templates development to collect data and to perform selected control array.
Selected Controls
Step 7: Implement Selected Controls
Simulation of the implementation of controls and mitigations in selected methodology.
Output
Residual Risks
Development of an executive summary addressed to the CEO with the results
Step 6: Develop Safeguard Implementation Plan
Guide of rules and security policies for ICS.
Safeguard implementati on plan
Step 5: Assign Responsibility
Guide of rules and security policies for ICS.
List of responsible persons

Figure 4: Risk Mitigation methodology conformity with NIST SP 800-30 [24], with Authors' contributions (in red) based on [27]

ations lead to the following five phases:

Phase 1: Meeting with the stakeholders (i.e., the "manage closely", "Keep informed" and "monitor" of the power-interest matrix, Figure 2). The purpose of these meetings is to encounter project requirements, implemented safety controls and other important documentation for the preparation of the manual. For this purpose the basic questions 5W-1H are used.

Phase 2: *Preparation of the guide*. As a reference has been taken of [1] [39] [40] [41], which serve as guidelines for developing security policies. In order to improve to structure the guide, it has been classified into three types of policies: being management, operational, and technical type, operational and technical. The stakeholders of the "manage closely" quadrant (Figure 2) are in charge of conducting the workshop sessions to elaborate phases 3, 4 and 5.

Phase 3: *Management type*. These are according to [1] security countermeasures to an ICS that focus on risk management and information security management: Evaluation of security and Authorization (CA), Planning (PL), Risk Assessment (RA), System and Services Acquisition (SA), and program Management (PM).

Phase 4: Operating Type. According to [1], these are security countermeasures for an ICS, which are executed and implemented mainly by people (i.e., stakeholders of all quadrants of the power-interest matrix, Figure 2): Personal Security (PS), physical and environmental protection (EP), Contingency Plan (CP), Maintenance (MA) and integrity of the information system (SI), media protection (PM), incident response (IR) and awareness training.

Phase 5: *Technical type*. According to [1], the technical types are security countermeasures to the ICS, which are primarily implemented and executed by the system through mechanisms containing hardware, software or firmware of the system: Identification and authentication (IA), Access Control (AC), Audit and Accountability (AU), System Protection and communications (SC).

4 Evaluation of Results and Discussion.

As indicated in section 3, this study includes the results of evaluations of experts' perceptions regarding the methodology implementation project. These were completed after each workshop session lasting between 60 and 120 minutes. This has been achieved by being informed of how the project is being implemented and better managing the risks related to its factors of success. The questions that were given for these evaluations were the following:

Question 1: Do you think that the time you took to collaborate in this workshop add value to the enterprise? Possible answers: Much (100%), Very (75%), little (50%), Very little (25%) and Nothing (0%).

Question 2: Do you think that the team that worked in this workshop provided all the necessary information? Possible answers: Yes (100%), something (50%) and No (0%).

Question 3: Do you agree that this workshop covered all aspects related to the scope of the project? Possible answers: Yes (100%), something (50%) and No (0%).

Question 4: How would you rate the time that has been used for this workshop? Possible answers: Very productive (100%), productive (75%), Normal (50%), Unproductive (25%) and Nothing Productive (0%).

Figure 5 reveals the averages of the answers to the questions asked in each evaluation according to each of the interested areas indicated in the "Manage Closely" quadrant of the Power-interest matrix indicated in section III: Maintenance, Process, Automation, and IT infrastructure of Figure 2.

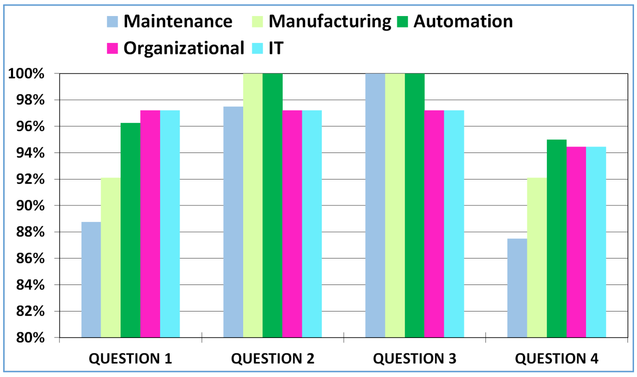


Figure 5: Averages of the scores of the expert's evaluations in the project.

Although the first and the fourth question are similar, it should be noted that the first one assesses whether there is added value to the enterprise or not. In contrast the fourth question assesses the productivity of the expert who has been present. The average answers to question 1 range from 88% to 97%, while the answers to question 4 range from 87% to 95%, respectively. This means that the experts are aware that their time in the implementation of this project gives value to the enterprise. However, it is not very productive or fun for them to spend any given time talking about the subject since their professional profile is more technical than administrative. These results allow important clues about how the project is performing in terms of the cost that the enterprise is investing in implementing such methodology. In addition, it demonstrates if there is any need to motivate the experts with an incentive, which may be analyzed later by the area of human resources and the project manager. In turn, these results indicate that there is a likelihood that the time-cost risks of project experts will be activated, as well as risks due to schedule delays due to fatigue or lack of interest. This information helps the project manager as well as the implementation team of the methodology. In current implementations, the subject of communication with stakeholders has been based on [42] and [34] and is being started in order to mitigate these project risks at the time of its execution.

The averages of the answers in question 2 indicate that the quality of implementation of the methodology is on track, since the corroborating ranks range from 97% to 100%. This question induces to the experts to unholy anything saved for them and to contribute with the vital information required. Also, it indicates to the Project Manager that the risks regarding the quality of the project are unlikely to be activated.

The answers to question 3, range from 97% to 100%, which indicates that the risks in scope are less likely to be activated.

After analyzing the results of risks of the implementation of the methodology, we have proceed to analyze the results of the risk assessment and design of mitigation strategies for ICS. These resulted in five visible threats, 15 vulnerabilities, 17 resulting risk and ten suggested mitigation strategies.

In this study, we assessed the risks from the perspective of ICS components and also of the informatics services. Therefore, the result of lifting the catalog of services according to [35] and [36] of the manufacturing process of the product "P" in the production line "L" is illustrated in Figure 6. There, they found 13 IT Services, 18 Information Systems and 26 informatics components. The risks found in the IT services coincided with items 1,2,6,8 and 9 mentioned in Table 2, and their mitigations would be the same as those analyzed with NIST. For other ICS manufacturing processes the same procedure may be performed.

As for the results obtained in the development of mitigation strategies, as mentioned in section 3, these are directly linked to the cost-benefit analysis presented to the enterprise (case study). Specifically, these indicate a deficiency in the management of the Information Security of this ICS, which forms it adequate to apply the proposed methodology.

Table 1 illustrates the considered variables. These indicate the investment costs of the implementation of the strategies versus the losses if the enterprise avoids the implementation of the methodology. Based on such calculations, the monthly cost of unavailability of the two production lines may reach between $ 109,000.00 in the first production line and $ 226,400.00 in the second production line. These calculations were obtained taking into account an hourly value of $ 5.01, with a total of 160 working hours per month. Total costs of implementation of mitigation strategies have reached up to $ 170,400.00 (i.e. estimated total costs of implementing technology, processes, and personnel requirements for the ten largest mitigations) compared to $ 1,422,760.00, which would be the cost of not implementing them. With these results, we follow that the best decision for the managers of these companies is the application of the proposed mitigation strategies. As mentioned in [38], it is confirmed that availability and integrity are more important than confidentiality in an ICS. Therefore, at this point we may suggest the development of a software application for the management of ICS that is able to evaluate the risks and the cost benefit of information security decisions in a fast and effective way.

The results of the simulations of the application of the above mentioned mitigations are listed in Table 2. The residual risk has been reduced in most cases from 100% to 10%, as well as the probability of execution of the threats. However, the impact remained almost unchanged. Simulations include only risks that would potentially have a high impact on SCI. The other minor risks should not be ruled out, but were carried out in a similar analysis, which produces a complete risk management in the ICS. Analyzing the whole context, we are able to appreciate that the continuous changes in the processes, the behavior of the people and the technology documented in this study, besides the in-

Table 1: Cost–Benefit Analisis

Number	Strategy/Control	Impact of implementation	Aditional costs/ investment	Impact of omited implementation	Aditional costs/ investment
1	Implentation of antivirus and firewall in the network ICS	MEDIUM	$24.000	HIGH	$81.750
2	Implementingan application, whic changes control and manages backups	MEDIUM	$20.000	MEDIUM	$226.400
3	Introduction of a security cameras system in control rooms	LOW	$24.000	HIGH	$60.000
4	Implementation of an application for asset management and inventory	LOW	$15.000	HIGH	$60.000
5	Acquisition of an additional PLC to quality control and later integration into the network	MEDIUM	$16.000	HIGH	$283.000
6	Introduction of an authentication a system (where possible) and daily backups	MEDIUM	$14.000	MEDIUM	$251.550
7	Physical access controls in control rooms	MEDIUM	$15.000	HIGH	$134.160
8	Introduction of a coordination procedure between Automation and IT	LOW	$2.400	HIGH	$45.000
9	Review of software licensing and other major equipment programs for the maintenance of ICS	MEDIUM	$24.000	HIGH	$226.400
10	Documenting algorithms and programs for changes of PLC	LOW	$16.000	MEDIUM	$54.500
			$170.400		**$1.422.760**

dications of [43], demonstrate that it is essential to mitigate and reduce the risks in an ICS. This leads to a risk assessment and mitigation strategy to be performed at least once a year.

For the Guide for standards-based instructions and security policies, the different formats and templates used by the enterprise for this type of documentation have been used. In order to carry out the evaluation of the Guide, a ten-person committee composed of management, technical and operational personnel (stakeholders of the quadrants: ”manage closely” and ”keep informed”) was elected. This group had the task of reviewing, commenting, and proposing changes to improve the content of the policy manual. The collected responses were subsequently evaluated using statistical formulas and graphs (frequency, means, fashion, median, standard deviation and central tendency) as an evaluating tool to visualize the results (Figure 7). From a total of eleven data, the acceptance percentage has a median of 75%, an average of 79.09% and an acceptance for most questions of about 90% (fashion). In general, the Guide lists 18 clear and precise guidelines, which contain the point of view of management and the enterprise, thus considering all aspects of the management of the ICS safety guide. Therefore, it complies with what it stands for [12], where a policy also helps to reduce investment costs in technology control, induced by appropriate management processes and assigned functions.

Due to the Guide evaluation, the low values of about 55.24% may reflect poor judgment or knowledge of the contestants, in which an additional survey may be able to analyze its potential causes. Nonetheless, evidently users accept the Guide, allowing having high expectations that its application will significantly improve management and reduce potential future incidents.

In the Guide-induced simulations, ten stakeholders were consulted (i.e. from the ”manage closely”, ”keep informed” and ”monitor” quadrants, Figure 2). Figure 8 illustrates that out of a total of 100 data (ten questions asked to these 10 ICS stakeholders), the percentages of perception of policy compliance vary from

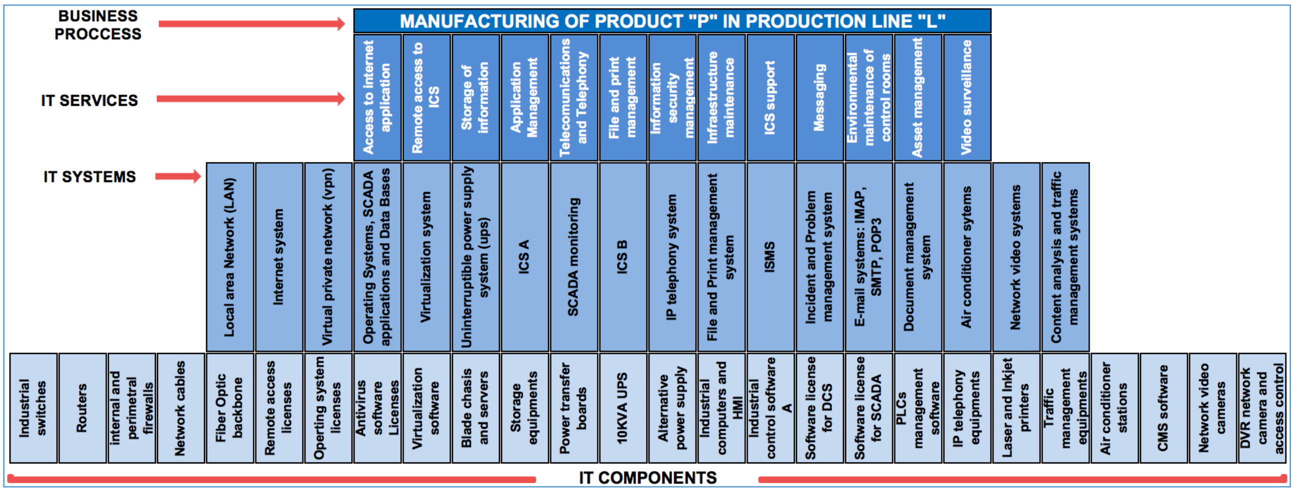

BUSINESS PROCCESS
IT SERVICES
IT SYSTEMS
MANUFACTURING OF PRODUCT "P" IN PRODUCTION LINE "L"
Access to internet application
Remote access to ICS
Storage of information
Application Management
Telecomunications and Telephony
File and print management
Information security management
Infraestructure maintenance
ICS support
Messaging
Environmental maintenance of control rooms
Asset management
Video surveillance
Local area Network (LAN)
Internet system
Virtual private network (vpn)
Operating Systems, SCADA applications and Data Bases
Virtualization system
Uninterruptible power supply system (ups)
ICS A
SCADA monitoring
ICS B
IP telephony system
File and Print management system
ISMS
Incident and Problem management system
E-mail systems: IMAP, SMTP, POP3
Document management system
Air conditioner sytems
Network video systems
Content analysis and traffic management systems
Industrial switches
Routers
internal and perimetral firewalls
Network cables
Fiber Optic backbone
Remote access licenses
Operting system licenses
Antivirus software Licenses
Virtualization software
Blade chasis and servers
Storage equipments
Power transfer boards
10KVA UPS
Alternative power supply
Industrial computers and HMI
Industrial control software A
Software license for DCS
Software license for SCADA
PLCs management software
IP telephony equipments
Laser and Inkjet printers
Traffic management equipments
Air conditioner stations
CMS software
Network video cameras
DVR network camera and access control
IT COMPONENTS

Figure 6: Services catalog of Industrial Control System.

Table 2: Results of The Simulation of Applications of Mitigation Strategies on ICS(The Top 10)

Item	Risk description	Probability	Impact	Risk	Strategy mitigation	Probability	Impact	Residual risk
1	Virus infection and malware network of ICS	1	100	100	Implementation of antivirus and firewall	0,1	100	10
2	Information loss and configuration errors in the ICS	1	100	10	Implementing an application for managing change controls and backups	0,1	100	10
3	Robbery of computers and devices of the ICS backup	1	100	100	Introduction of a camera security system in control rooms and workshops	0,1	100	10
4	Critical infrastructure lacking insurance policy	1	100	100	Implementation of an application for asset management and inventory	0,1	100	10
5	Damage of PLC of Quality Control in the 2nd production line (Outdated equipment)	1	100	100	Acquisition of an additional PLC for quality control, program support, and integration into the control network	0,1	50	5
6	Intentional alteration of information of the ICS	0,5	100	50	Introduction of an authentication system where possible and daily backups	0,1	100	10
7	Failures in ICS caused by unauthorized persons	0,5	100	50	Implementation of physical access controls	0,1	100	10
8	Improper acquisitions by outdated information security technology	5	50	50	Introduction of adequate and contemporary coordination procedure between Automation and IT	0,1	50	5
9	Inadequate sizing of technology resources in ICS maintenance	0,5	100	50	Regular software licensing review and other major equipment programs for the maintenance of ICS	0,1	50	5
10	Allen Bradley PLC Failure (control room 3)	1	50	50	Documenting Algorithms and programs for changes in the PLC	0,1	50	5

15% to 80%, while the average perception of compliance yielded an average of 41.05% and a median of 45%. Despite the negative trend shown in this figure, the slope (about 45 degrees) indicates a reliable distribution of the data collected for this analysis. On the other hand, as illustrated in Figure 8, 60 of the 100 questions answered are between the average (41.05%) and 80% of the fulfillment of perception. This may be considered as satisfactory values of the simulation. It is therefore thought that in the future stakeholders will support the improvement of the proposed methodology for the security of management information in ICS once they become familiar with such a procedure.

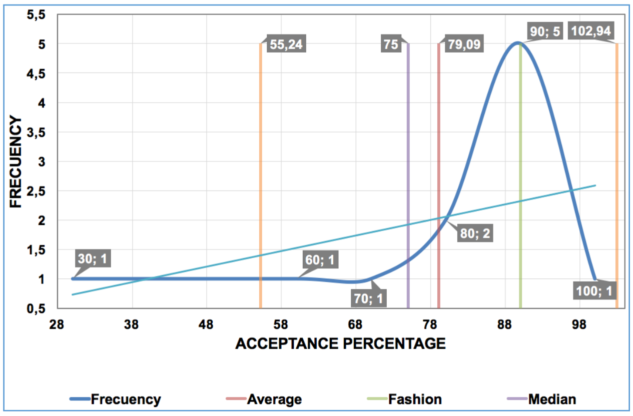


Figure 7: The statistical process, which results by the evaluation of the acceptance of the Guide for standards-based instructions.

In Figure 9 the perception of compliance with the application of the manual that are outside the range between 20.61% and 61.49% may result from the lack of judgment or even ignorance of the respondents regarding the Security of the ICS, since it is a contemporary and new topic for many professionals in the industrial field.

According to enterprise executives in this case study, the percentage of compliance with other policies and standards manuals of the organization vary in the range of 40% to 50%. This suggests that 40% is not a coincidence but the result of the organizational culture of such an enterprise. According to these results a proposal of a follow-up may rise, where the target may be of how an organizational culture has a potential impact or relation with the compliance of the rules and policies of an enterprise. Simultaneously, it should also be considered to propose the development of a software application that simulates the performance of the manual, in order to be able to determine the degree of information security management of an ICS that is a useful tool for the managers and stakeholders of the quadrant ”Manage closely”.

Finally, the proposed approach and the set of industry standards analyzed in this study have been complemented with each other. Therefore, the substantial difference is situated in the amalgamation and articulation of proven techniques, methods, and the adaptation of other standards, referential frameworks, and management systems that have been used in IT for both project management and industrial security in the same place where the facts are occurring. This allowed significant improvements to effectively and holistically manage the different and complex areas, which coexist in the ICS: business, computing, electronics, automation, production processes and people.

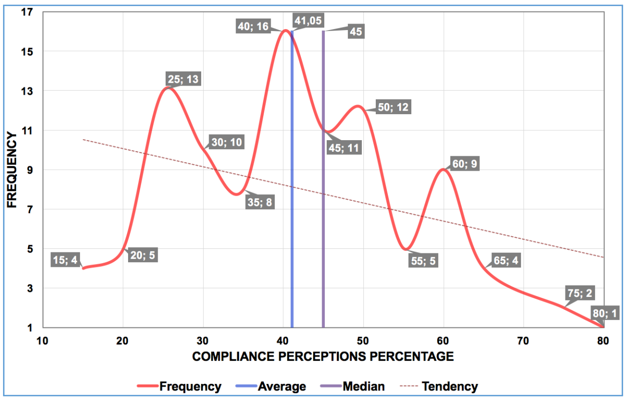


Figure 8: The statistical process, which resulted by the perception of the compliance of the Guide for standards-based instructions.

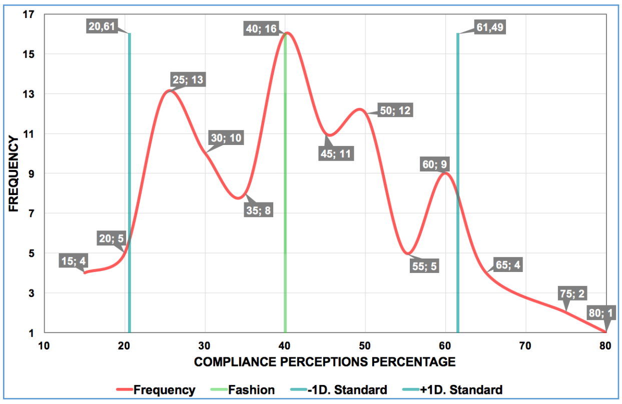


Figure 9: The statistical process, which results by the simulation of the application of the Guide for standards-based instructions.

5 Conclusions and Future Work.

Based on the results obtained, it is concluded that the set of mitigation strategies and the Guide for standards-based instructions and security policies for a manufacturing enterprise may achieve a reduction of 40% of security incidents in its ICS in the contexts of availability, integrity and confidentiality of information. At the same time, it is observed how the project of implementation of the methodology has been favorably accepted by the stakeholders creating motivation, collaboration and synergy in the areas that use, operate and manage the ICS. As for NIST 800, PMBOK, COBIT and ITIL, it has been perceived that they are highly strategic international standards, robust and in line with the management proposal presented for the ICS. That means that in turn, that the management proposal is perfectly articulated with the managerial, operational, technical areas of such enterprise. The proposed methodological process may be compared with ISO 27000 ISMS, being recommended to be used in manufacturing companies to manage information security in industrial control systems.

As future lines of studies, it is planned to combine the proposed methodology with DSS02, DSS03 and DSS04 of COBIT 5, the ITIL service operation stage, and a general guide of information security policies as well as norms throughout the enterprise according to ISO 27000, and NIST 800-82, in order to maintain proper management of traditional IT and ICS. In addition, the design and implementation of an information security incident response team (CSIRT) for ICS, based on NIST 800-61 as a framework and ITIL V3, has also been considered in order to analyze the involved computer services.

Conflict of Interest. The authors declare not to have any conflicts of interest.

Acknowledgment. We would like to thank Comercializadora San Remigio and in particular Engineer Rafael Simon (CEO) for allowing to apply the concept of this study and also the analysis of the required information for this research. This work has been partially funded by the Universidad de las Fuerzas Armadas ESPE within the research project entitled “Training Computational Platforms, Experimentation, Management, and Mitigation of Cyber security Attacks”, Code: ESPE-2015-PIC-019.

References.

[1] Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., Hahn, A., ”Guide to Industrial Control Systems (ICS) Security”, NIST SP 800-82, Rev. 2, pp. 1-249, May 2015. Last update: March 1st, 2017.

[2] Francia III, G. A., Thornton, D., & Dawson, J., “Security best practices and risk assessment of SCADA and industrial control systems”. In Proceedings of the International Conference on Security and Management (SAM) (p. 1), Alabama, January, 2012.

[3] Ning, C., Jidong, W., &Xinghuo Y., ”SCADA system security: Complexity, history and new developments,” Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on, Daejeon, 2008, pp. 569-574.

[4] Byres, E., & Lowe, J. “The myths and facts behind cyber security risks for industrial control systems”. In Proceedings of the VDE Congress (Vol. 116, pp. 213-218), October, 2004.

[5] Tieghi, E. M. “Introduzione alla protezione di reti e sistemi di controllo e automazione (DCS, SCADA, PLC, etc.)”. Quaderni CLUSIT-Associazione Italiana per la SicurezzaInformatica. Italia, 2007.

[6] Green, B., Prince, D., Roedig, U., Busby, J., & Hutchison, D., “Socio-technical security analysis of industrial control systems (ICS)”. In Proceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research 2014 (pp. 10-14). BCS. Sept., 2014.

[7] Yang, W., & Zhao, Q., “Cyber security issues of critical components for industrial control system”. In Guidance, Navigation and Control Conference (CGNCC), 2014 IEEE Chinese (pp. 2698-2703), Aug. 2014.

[8] Hadziosmanovic, D., Bolzoni, D., Etalle, S., & Hartel, P., “Challenges and opportunities in securing industrial control systems”. In Complexity in Engineering (COMPENG), 2012 (pp. 1-6). IEEE, Jun., 2012.

[9] Krotofil, M., & Gollmann, D., “Industrial control systems security: What is happening?” In Industrial Informatics (INDIN), 2013 11th IEEE International Conference on (pp. 670-675). IEEE, Jul. 2013.

[10] Nicholson, A., Webber, S., Dyer, S., Patel, T., and Janicke, H., “SCADA security in the light of Cyber-Warfare”, Computer & Security, Volume 31, Issue 4, June 2012, Pages 418-436.

[11] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., &Stoddart, K. "A review of cyber security risk assessment methods for SCADA systems". Computers & security, 56, 1-27. 2016.

[12] Seo, J., Song, M., and Lee, K., "A Study on Efficiency of ISMS for ICS with Compliance", International Journal of Multimedia and Ubiquitous Engineering", Vol.9 No. 5, pp 301-306, 2014.

[13] Drias, Z., Serhrouchni, A., & Vogel, O. "Analysis of cyber security for industrial control systems". In Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on (pp. 1-8). IEEE, 2015, Aug.

[14] Lemaire, L., Vossaert, J., Jansen, J., & Naessens, V., "A Logic-Based Framework for the Security Analysis of Industrial Control Systems". Automatic Control and Computer Sciences. 2017

[15] Mansfield-Devine, S., "A process of defense–securing industrial control systems". Network Security, 2017(2), 14-19. 2017.

[16] Collier, Z. A., Panwar, M., Ganin, A. A., Kott, A., & Linkov, I., "Security Metrics in Industrial Control Systems". In Cybersecurity of SCADA and Other Industrial Control Systems (pp. 167-185). Springer International Publishing. 2016.

[17] McLaughlin, S., Konstantinou, C., Wang, X., Davi, L., Sadeghi, A. R., Maniatakos, M., & Karri, R., "The cybersecurity landscape in industrial control systems". Proceedings of the IEEE, 104(5), 1039-1057. 2016.

[18] Keliris, A., Konstantinou, C., Tsoutsos, N. G., Baiad, R., & Maniatakos, M., "Enabling multi-layer cyber-security assessment of Industrial Control Systems through Hardware-In-The-Loop testbeds". In Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific (pp. 511-518). IEEE. 2016, Jan.

[19] Graham, J., Hieb, J., & Naber, J., "Improving cybersecurity for Industrial Control Systems". In Industrial Electronics (ISIE), 2016 IEEE 25th International Symposium on (pp. 618-623). IEEE, 2016, Jun.

[20] Abe, S., Fujimoto, M., Horata, S., Uchida, Y., & Mitsunaga, T., "Security threats of Internet-reachable ICS". In Society of Instrument and Control Engineers of Japan (SICE), 2016 55th Annual Conference of the (pp. 750-755). IEEE, 2016, Sept.

[21] Ponomarev, S., & Atkison, T., "Industrial control system network intrusion detection by telemetry analysis". IEEE Transactions on Dependable and Secure Computing, 13(2), 252-260. 2016.

[22] Martellini, M., Abaimov, S., Gaycken, S., & Wilson, C., "Vulnerabilities and Security Issues". In Information Security of Highly Critical Wireless Networks (pp. 11-15). Springer International Publishing. 2017.

[23] Busby, J. S., Green, B., & Hutchison, D. (2017). Analysis of Affordance, Time, and Adaptation in the Assessment of Industrial Control System Cybersecurity Risk. Risk Analysis.

[24] ISO 27000, "Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary," International Organization for Standardization ISO, Geneve, 2013.

[25] Stoneburner, G., Goguen, A., and Feringa, A., "Risk Management Guide for Information Technology Systems", NIST SP 800-30, pp. 1-56, 2002, July.

[26] Konstantinos K. Automated cyber security compliance assessment. 2017. TRITA-EE, 2016:202. Master Thesis.

[27] Bustamante, F., Fuertes, W., Díaz, P., & Toulkeridis, T., "A methodological proposal concerning to the management of information security in Industrial Control Systems". In Ecuador Technical Chapters Meeting (ETCM), IEEE (Vol. 1, pp. 1-6). IEEE, 2016, Oct.

[28] ENISA, "Analysis of ICS-SCADA Cyber-security Maturity Levels in Critical Sectors". ENISA, 11 Dec 2015. Accessed on February 28th, 2017. URL: https://www.enisa.europa.eu/publications/maturity-levels/at_download/fullReport.

[29] Järekallio, T., "Methods for Identification and Classification of Industrial Control Systems in IP Networks", Master's Thesis, School of Electrical Engineering, Aalto University, 2016, Aug.

[30] ICS-CERT, "Industrial Control Systems Cyber Emergency Response Team", U.S Department of Homeland Security, pp. 1-24, 2015.

[31] Vertical Insight, "Data Breach Investigations Report Manufacturing", Verizon, MC1591204/14, pp. 1-60, 2014.

[32] Blank R. M. and Gallagher, P. D., "Guide for Conducting Risk Assessments/Information security ", NIST Special Publication 800-30 Revision 1, pp. 1-95, 2012, Sept.

[33] Locke, G., and Gallagher, P., "Managing Information Security Risk", NIST SP 800-39, pp. 1-88, 2011, March.

[34] Rose, K. H., "A Guide to the Project Management Body of Knowledge (PMBOK® Guide)—Fifth Edition". Project Management Journal, 44: e1. doi:10.1002/pmj.21345. 2013.

[35] Cannon, D., Cannon, D., Wheeldon, D., Lacy, S., & Hanna, A. "ITIL service strategy". TSO. 2011.

[36] Hunnebeck, L., Rudd, C., Lacy, S., & Hanna, A. "ITIL service design". TSO. 2011.

[37] Coughlan, P., & Coghlan, D. (2002). "Action research for operations management". International journal of operations & production management, 22(2), 220-240.

[38] Cheminod, M., Durante, L., &Valenzano, A., "Review of security issues in industrial networks". Industrial Informatics, IEEE Transactions on, 9(1), 277-293. 2013.

[39] Blank, R., and Gallagher, P., "Security and Privacy Controls for Federal Information Systems and Organizations", NIST SP 800-53, Rev. 4, pp. 1-460, April, 2013 updates as of 01-22-2015

[40] Gallagher, P., "Recommended Security Controls for Federal Information Systems and Organizations", NIST SP 800-53, Rev. 3, pp. 1-11, 2009, August.

[41] Guttmann, B., and Roback, E., "An Introduction to Computer Security: The NIST Handbook", NIST SP 800-12, pp. 1-296, October, 1995.

[42] Karu, K., Ferris, K., Hunebeck, L., Rae, B., & Rance, S. (2016). ITIL Practitioner. The Stationery Office.

[43] Talib, M., Barchi, M., Khelifi, A., and Ormandjieva, O., "Guide to ISO 27001: UAE Case Study", Issues in informing Science and Information Technology, 7(2012), pp. 331-349, 2012.