CHALMERS
UNIVERSITY OF TECHNOLOGY

Risk Analysis as a Security Metric for Industrial Control Systems

Master's thesis in Computer Systems and Networks

JOSEPH MUKAMA

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2016

Master's thesis 2016:

Risk Analysis as a Security Metric for Industrial Control Systems

JOSEPH MUKAMA

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Computer Science and Engineering
Chalmers University of Technology
Gothenburg, Sweden 2016

Risk Analysis as a Security Metric for Industrial Control Systems

JOSEPH. MUKAMA,

Examiner: TOMAS. OLOVSSON
Supervisor: ERLAND. JONSSON

Chalmers University of Technology
Department of Computer Science and Engineering
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Cover: Visualization of commonly used words from selected key sections of the report. Visualization created by online tool https://wordsift.org/

Printed by Chalmers Library
Gothenburg, Sweden 2016

Abstract

As time and technology advances, the people become more reliant on the services provided by Industrial Control Systems (ICSs). Mainly used in the critical infrastructure industries, the ICSs have realised and enabled a myriad of services essential to individuals, the public and organizations on a daily basis. Developments in networking technologies, open standards and the use of legacy devices in the ICSs have brought about a paradigm shift in the way ICSs interconnect with each other and operate over long geographical distances. The legacy devices come with inherent vulnerabilities which may be costly to patch and/or may not be possible to patch and these in turn are a source of threats to the entire ICS.

In order to mitigate the risks that may arise due to the vulnerabilities introduced into the system, we gained a deeper understanding of the different ICSs and reviewed a number of existing risk analysis approaches and categorized them in terms of their overall goal, whether they are qualitative or quantitative approaches, the stages of risk management addressed, and the scope in terms of issues they addressed. Based on this analysis, we use the NIST and CORAS frameworks as the underlying approaches to develop a Modified Risk Analysis Framework for ICS systems (MRAF-ICS). This framework assigns weights to all the system assets to emphasise the importance/criticality of the asset in the overall system. It uses the a threat modelling approach, FMEA and HAZOP to exhaustively identify the threats, hazards and vulnerabilities in the system.

Keywords: Keywords: Risk management, Risk analysis, security metrics, measurement, Industrial Control Systems.

Acknowledgements

I express my sincere gratitude to my research supervisor, Prof. Erland Jonsson, and examiner, Assoc. Prof. Tomas Olovsson, for the consultative guidance, support and feedback given towards my research.

In the same vein, I thank the Swedish Institute for fully funding my studies at Chalmers University of Technology for the period 2014-2016 and giving me such a great opportunity to study in a dynamic and multi-cultural environment and expanding my network.

Finally, I thank my fiancée, Esther Nampiina, and my family for the continued love, trust and encouragement in all my endeavours.

Joseph Mukama, Gothenburg, October 2016

Contents

List of Figures

List of Tables

List of Acronyms

CI:	Critical Infrastructure
FISMA:	Federal Information Security Management Act
ICS:	Industrial Control System
ICT:	Information and Communication Technology
IEC:	International Electrotechnical Commission
ISO:	International Organization for Standardization
IT:	Information Technology
NIST:	National Institute of Standards and Technology
PCS:	Process Control System
PLC:	Programmable Logic Controller
RA:	Risk analysis
RM:	Risk Management
SCADA:	Supervisory Control And Data Acquisition
SIS:	Safety Instrumented System
SP:	Special Publication
WAN:	Wide Area Network

1
Introduction

In the current information age, it is inevitable for computer systems in any organization to be connected to a network or even the Internet to ensure effective information exchange and collaboration with other partners or shared applications. This chapter gives the overall introduction to the project, the problem statement and justification, the methodology used and an overview of the layout of this report.

1.1 Background

The modern system environment uses various communication technologies and devices to communicate and collaborate with various stakeholders to attain their business goals and the Industrial Control System (ICS) is one such system. For many years, the ICSs have played a major role in the monitoring and control of processes industries such as electric power, nuclear energy, oil and natural gas, automotive and aerospace [2]. In addition, the ICSs form part of the Critical Infrastructure (CI) because they provide services of great importance to the nation such that their failure can lead to adverse effects on security, national economic security, national public health or safety, or any combination of those matters [3]. With the advancement in technology, and as many people increasingly rely on CI to provide essential services on a day-to-day basis, these systems need to be highly secured and protected [4].

Traditionally, the ICSs were greatly isolated from other systems in terms of hardware, communication networks, channels and standards used, and with no connection to the Internet. Today, the growing adoption of cost-effective and emerging technologies such as commercial-off-the-shelf (COTS) devices, smart devices, open wireless sensors, standard operating and even open software, has opened up the system to the Internet exposing it to the world [5, 6]. This variety of technologies and devices comes with a variety of inherent vulnerabilities of which some may be difficult to detect and/or impossible to remove.

Several attacks have been carried out on the ICSs, stuxnet being one of the greatest. Discovered in June 2010, stuxnet, a computer worm, was designed to take control of a certain programmable ICS, manufactured by Siemens AG, causing the sub systems under their control to malfunction silently and yet creating an illu-

sion of normal system operation by false data injection to the system monitors [7]. Furthermore, a study by FireEye Inc, a top cyber security company, revealed that state-sponsored attackers pose the greatest risk to governments and industries of the Nordic countries. For instance, in 2014, a Russia-based Advanced Persistent Threat (APT) group is believed to have systematically carried out the unlawful retrieval of both political and military intelligence from the Nordic countries by phishing emails and spoofed log in pages [8].

The critical nature of the ICSs coupled with the inherent vulnerabilities of the subsystems and components makes the ICSs more susceptible to cyber-attacks, not only from individual attackers but also from well-organised and well-funded groups [5]. Hence, the protection and security of the system resources and information, is of paramount importance to the organizations, and the nation at large. But 'how do we know that the system is secure?', 'how much is enough security?', and 'is there a single system-wide measure of security?' [9, 10, 11]. In a continuous effort to build a body of knowledge, many researchers have attempted to solve these challenges by coming up with a common measure of security, a common metric or framework of metrics.

Many approaches exist to present the security posture of the system but this project concentrated on the use of risk analysis techniques. In addition, risk analysis techniques are widely used, as a measure of security, to mitigate risks in ICSs.

The rest of report is organized as follows; Chapter 2 explores the concept of security metrication to a small extent but enough elaborate the title. Furthermore, it is pertinent to underline the key concepts in Risk analysis, which is a direct subset of Risk Management as presented in Chapter 3. Risk analysis is the main aspect of this project. Risk analysis is wide and it may be carried out differently depending on a specific project, country, or industry. We use ICSs for this, and present an overview, of the systems, how they differ from the usual ICT systems, and the threats and vulnerabilities faced by these systems as presented in the Chapter 4. Chapter 5 looks into the different available risk analysis approaches from various industries, from which we categorise and formulate a suitable framework applicable to the ICSs. Chapter 6 uses the result from Chapter 5 to develop a risk assessment framework for ICS, and we apply and discuss the developed framework in Chapter 7. The report ends in Chapter 8 with concluding remarks from the project.

1.2 Problem Statement

The adoption of emerging technologies (e.g. the Internet, wireless sensors and smart devices), in addition to using legacy devices, introduced a myriad of vulnerabilities in the ICSs making them target systems for both internal and external attacks. Due to the high reliance on technology interconnection and inter-connectivity, ICSs have experienced an increase in potential vulnerabilities and potential risk to the opera-

tions [4, 3]. The situation is further exacerbated by the critical nature of the ICSs, making them attractive to a wider and more sophisticated attack space, ranging from 'script kiddies' experimenting their skills to both passive and active attacks from other nation states, activists and terrorists [4, 5, 8]. Unlike in traditional Information Technology (IT) systems, attacks on ICSs can result in physical damage to the controlled systems and to the people using them [7]. This project focuses on the use of risk analysis techniques as a preventive and security measure to mitigate the effect of such attacks on ICSs.

1.3 Justification

As time and technology advances, many systems, services, people, organizations, and nation are increasingly relying on ICSs. A review by the Department of Homeland Security (United States) reported a continued increase in the frequency and sophistication of cyber-threats against the country's CI with over 145,000 cyber security incidents in the year 2015 [4]. This trend can destabilize national services and cripple the national economy and therefore protecting the ICSs is of utmost importance for both the economy and stability of a nation [12].

According to the National Institute of Standards and Technology (NIST), security metrication facilitates decision making, determining the efficiency and performance as well as the security posture of an organisation [13]. The risk-based approach is an effective approach against cyber-attacks in the ICSs [12]. The NIST Special Publication 800-82r1 further emphasizes the need for assessing and rating risk of possible vulnerabilities [2].

Risk analysis, as an approach for security metrication, guides organisations in their approach to security and helps them manage the security in a systematic, repeatable and formal way. Furthermore, Risk analysis empowers the management with vital information including; justification for cost-effective countermeasures and mitigation approaches, highlighting areas that need to be made more secure and those that can be less secure, and increases security awareness by assessing and reporting the strengths and weaknesses of the security posture an organization.

ICSs have the potential of being much better if the security is enhanced and handled using a more proactive approach. The risk analysis helps in identifying the probable consequences/risks associated with the vulnerabilities and prevent information leakage and security attacks.

1.4 Methodology

The research is vast and wide in terms of both existing approaches of security metrication and application areas. This project focuses on the application of risk analysis methodologies to the Industrial Control Systems and several research papers are reviewed. The papers used for this project are extracted mainly through the *Chalmers' University e-resources library* and the *Google Scholar* website. These are the primary tools for providing access to both the latest and most relevant articles, journals and conference proceedings in the field as reported in the IEEE Xplore and ACM databases. Furthermore, we use the *Web of Science* for purposes of indexing to further qualify our paper selection. These are the recommended and most commonly used search and indexing approaches used in technical research. Furthermore, to a smaller extent, more information is gathered using the general *Google* search engine to supplement the data already gathered. In many cases we use the search terms 'risk analysis' and 'Industrial control systems' as key words but 'risk analysis' and 'risk frameworks' were also used. Figure 1.1 is a representation of the general overview of the systematic research methodology adopted for this project work.

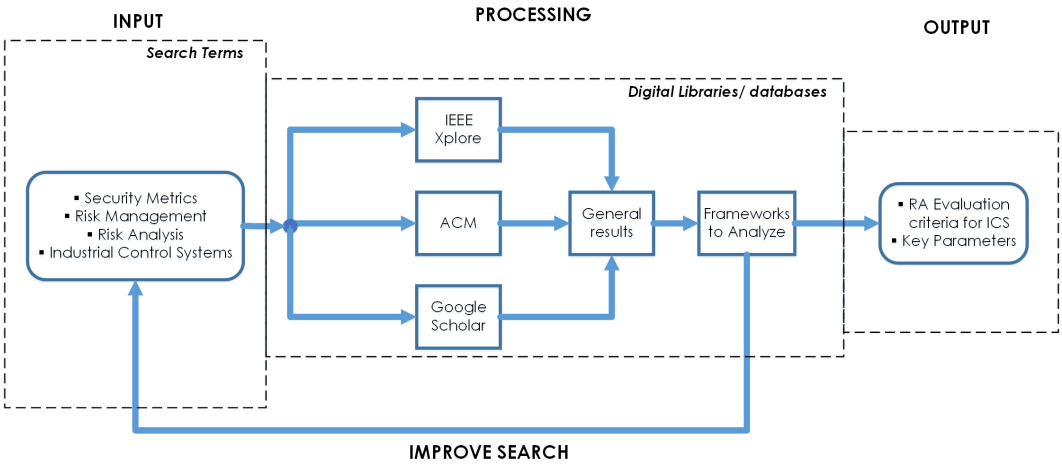

Figure 1.1: Systematic research methodology

During the processing stage, after the using the mentioned search terms, we obtain a general result of the technical papers to review. From the papers, we closely look at the abstract, introduction and methodology/implementation used and the conclusion sections for key information regarding the search terms used. Papers that provide satisfactory information are used for reference and further analysed in this report, whereas the other papers are not considered. This process is carried out iteratively for several papers until we find commonly used risk analysis frameworks to be used as a basis for this review. The candidate frameworks are further scrutinized and evaluated and categorized basing on; their overall goal, whether they are qualitative or quantitative approaches, the stages of risk management addressed, the scope in terms of issues addressed, applicability to different industries and degree of detail given by the approach and the advantages and disadvantages each approach

presents. From this information, we determine a suitable risk model and formulate the Modified Risk Analysis Framework for a general ICS.

1.5 Limitations

This project is bounded by time, application area and security metrication methodology/approach; *(i)* In the time domain, the thesis is expected to be completed in approximately 20 weeks. *(ii)* The application areas for designing and applying security metrication are enormous but in this project, we confine our research to the ICSs. *(iii)* The research in this project focuses on the risk analysis, as it is one of the many ways used to assess security of at system quantitatively.
We believe this will give a substantial representation of the use of risk analysis for the purpose of security metrication as well as contribute to the existing body of knowledge in the field of risk management in ICSs.

2

Security Metrics and Approaches

METRICS have become an integral part of Information Security but it is often difficult to derive and define a single measure of security that meets the required objectives. This chapter explains the fundamental principles behind security metrics and security methodologies that will facilitate us to understand the context of the research.

2.1 Security Metrics

2.1.1 Concepts and definitions

Computer security: The NIST Computer Security Handbook gives the classic definition of *computer security* as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, confidentiality, and availability of information system resources [14, 15]. Therefore a secure system should protect its information and system resources against; tampering and modification of information, access of the information by unauthorised individuals, and ensure that authorised users get the right information when they need it.

Security metric: Much research has been carried out with the aim of formalising the *security metric* definition and in fact, the Workshop on Information Security System Rating and Ranking (WISSRR) in Williamsburg, Virginia 2001 was a big initiative towards structuring and characterizing the information security measurement problem in order to identify "good practices", and to determine potential research directions [9].

Furthermore, many researchers confirm that 'metrics' are often confused with 'measurements' and therefore argue that a clear distinction between a metric and a measurement is needed to define a metric [16, 17].

Despite the extensive research in this field, the term 'security metric' is still a gray area, receiving several definitions and understands from different researchers. It is still an area of great debate with no single universally agreed definition [18].

In our analysis, we agree that it is not possible to have a general security metric definition for all systems but a specific definition can be addressed within a particular context. Table 2.1 shows a snapshot of the various definitions for IT security metric used in some of the literature reviewed.

Table 2.1: Variability of the 'security metric' definition in literature.

Reference	Definition of IT Security Metric
WISSRR Proceedings (2001) [9]	An Information Security (IS) metric is a value, selected from a partially ordered set by some assessment process, that represents an IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence.
Marianne et al. (2003) [13]	Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
Azuwa et al. (2012) [19]	Information security metric is a measurement standard for information security controls that can be quantified and reviewed to meet the security objectives. It facilitates relevant actions for improvement, provide decision making and guide compliance to security standards.
Chakraborty et al. (2012) [16]	Metrics are a collection of parameters which are used to (i) measure the quality of a system, (ii) make comparison with other systems, and (iii) take decisions and improve performance and accountability through analysis, and reporting of relevant performance of the system
Yasasin & Schryen (2015) [20]	An IT security metric quantifies the security level of an information system and fulfills the following attributes: It is (a) bounded, (b) metrically scaled, (c) reliable, valid and objective, (d) context-specific and (e) computed automatically.

2.1.2 Taxonomy of existing metrics

The need for security metrics has been studied extensively but no single framework has been realised or adopted. The WISSRR workshop proceedings show how challenging it was to develop a formal and universal measure of security and how diverse the metrication domain is. Nevertheless, the workshop resulted in three main non-disjoint categories to the problem i.e. *technical*, *organizational*, and *operational* which are used to describe and compare technical objects, organisation program/processes and operational environments, respectively [9].

McIntyre et al. developed security metric work package for Process Control Systems to address the applicability of security metrics in control and operational environments. similar to WISSRR workshop proceedings, they categorised the metrics development and application into three main categories; organizational, operational and technical metrics [21]. These metric categories interact with each other and some times the boundaries may not be distinctive.

Savola proposed a taxonomy of security metrics which uses metrics from both organizational information security management and product development in the Information and Communication Technology (ICT) industry [22]. It is multi-level hierarchy of metrics emanating from the *business management* metrics as root node (level 0). The security and trust management work emanates from the organisation's business goals and as such, their metrics should be aligned to these business goals. Furthermore, these metrics can have other metrics below them until a more fine-grain metric is obtainable.

More examples on existing metrics can be found in Table 5.5 of Chapter 5.

2.1.3 Benefits and challenges to developing metrics

According to the National Institute of Standards and Technology (NIST), metrics facilitate decision making and improve performance and accountability. They help monitor the status of measured activities and thereby facilitate their improvement applying corrective action based on facts [13].

Organizations are continuously relying on the use of the Internet and as the complexity of the organizations increase, the more security related challenges they face. Based on the security information gathered, security metrics help organizations to;

- Presents organization posture in terms of security.
- Manage risk more effectively.
- Demonstrate compliance to standards and regulations.
- Provide justification for security expenditure.

Security metrics are very important for a security program to give the intended results for good and effective comparison with previous results or with similar systems. However, developing them comes as a very big challenge as briefly described below;

Security metrics are often ill defined [9]. Attempts to define a metric remain vague as discussed in the previous section. This brings about confusion in the development of good metrics. The definition and evaluation of security metrics frequently become distanced from the ultimate use, so that metrics become ends in themselves because the consumer gets lost in the definition of the metric.

Security is wide [10, 22]. During development process, we can not fully define all the potential threats and vulnerabilities from which the metrics can be developed. Therefore, a system can be attacked based on other security loopholes that are not effectively covered by the metrication system developed.

Quantitative vs qualitative nature of security [18, 11]. It is difficult to effectively measure security in an active system. The more result oriented quantitative metrics are not very practical in an actual system which leaves the development of the metrics to a more less effective qualitative approach.

2.2 Security Metrication

2.2.1 Security metrication approaches

Security metrication is the process of formulating metrics to measure security in a given contextual setting. In many cases, metrication is dictated by a previous framework and/or processes whereas in other cases, in the absence of a such a framework, a systematic approach is desired. There exists two main approaches for generating these metrics i.e. using a top-down approach or a bottom-up approach [17];

Top-down approach

The top-down approach uses the overall objectives of the security program as the starting point for metric formulation. In a divergent way, along the lines of the objectives, it identifies metrics that can give an indication that these objectives are met. The approach ends by identifying measurements needed to generate each metric previously obtained. This method generates the most relevant metrics because formulations comes directly from the program objectives.

Bottom-up approach

Unlike the top-bottom approach, the bottom-up approach begins by identifying measurements that are or could be collected for each particular process, product or service and then identifying/generating some useful metrics from the measurements. The approach finally relates the derived metrics to the overall objectives of

the security program. Only metrics that relate positively with the objectives of the program are kept for use whereas the rest are not used for metrication.

Figure 2.1 shows the main steps taken in carrying out the two approaches. In principle, these two approaches 'work in reverse' of each other.

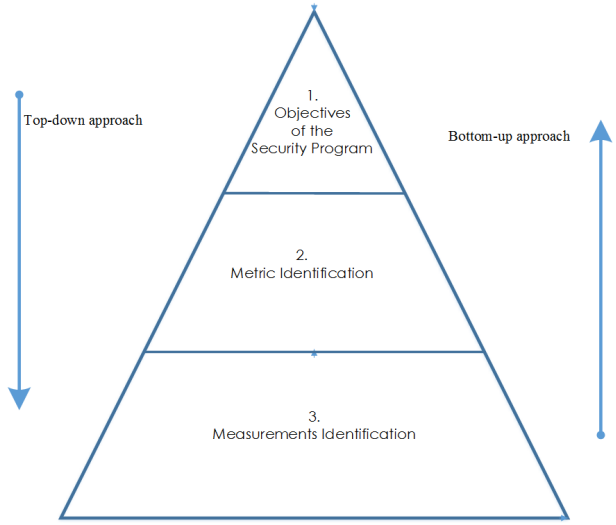

Figure 2.1: Main approaches to security metrication.
Based on approaches by Payne et al. [17].

In both the top-down and bottom-up approaches, the key determinants and major guiding principle to security metrication are the objectives of the security program. All metrics must align to fulfil the overall objectives of the security program.

2.2.2 Developing security metrics

To develop a good security metric, a systematic criteria must be used to meet specific requirements. From literature, IT Security metrics should meet many of the following requirements; they should be bounded, quantifiable, reliable, valid, objective, contextually specific, meaningful and have an obtainable metric input [20, 19, 22, 11].

The SANS Institute, a renowned organisation in the information security training domain, presented a seven-step outline for formulating a security metric program;

Figure 2.2 shows the seven steps involved in developing a metrication program. The figure is drawn based on the 7 steps laid out in the SANS Institute's '*Guide to Security Metrics*' [17]. It is a top-to-down process that starts with a clear definition of the program goals and objectives.

Step 2 involves determination of possible metrics to be generated basing on an existing framework, or using a top-down or bottom-up approach. This is followed by

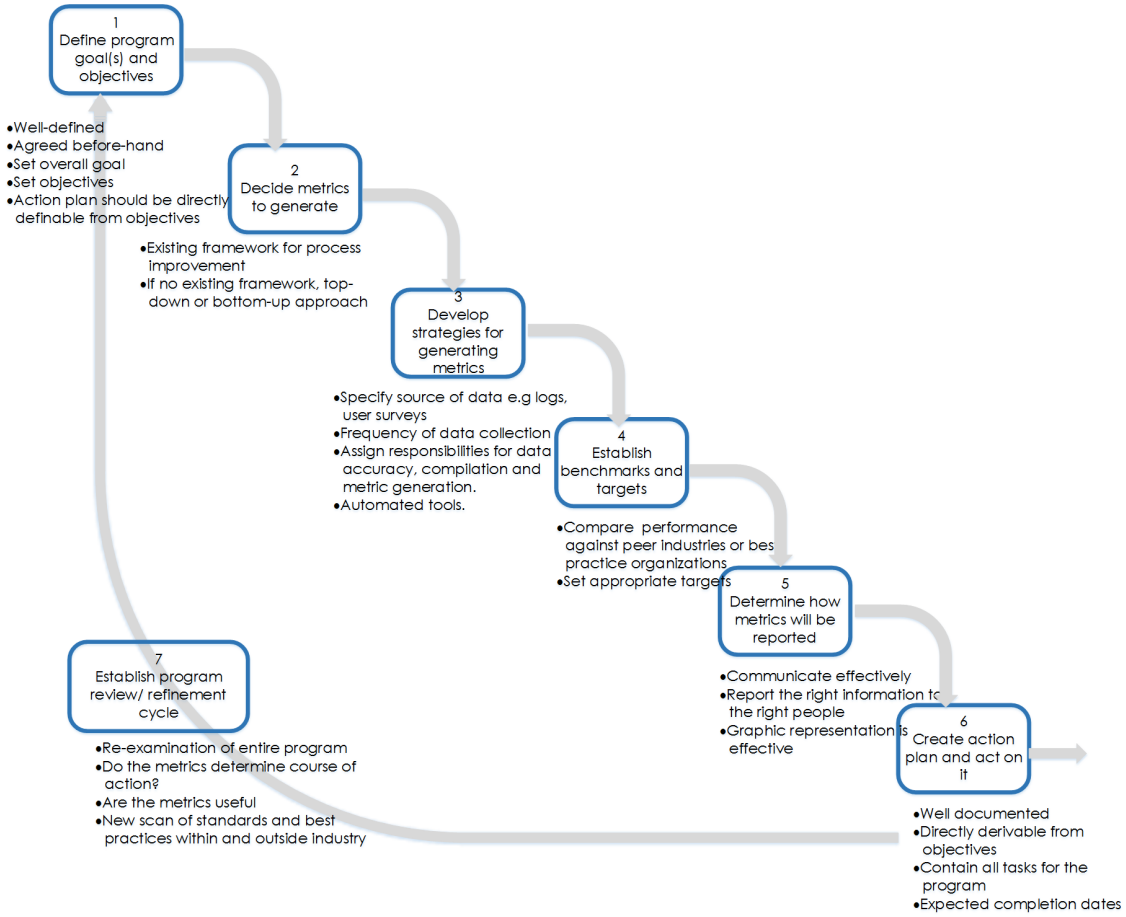

Figure 2.2: Developing a security metric program.
Based on the process developed by Payne et al. [17].

developing strategies for generating the metrics in step 3.

Step 4 involves the establishment of benchmarks and targets in comparison with similar industries or best practices.

Step 5 and 6 are about how the metrics are to be reported to the stakeholders and users of this and from which a suitable action plan is formulated.

The last step of the program is a feedback loop to facilitate continuous improvement through program review and re-examination of the entire program.

3

Risk Management

Risk management (RM) is widely used in operational environments and it is an integral part of the overall management of a company. This Chapter gives some definitions related to RM, the relevant standards and guidelines used for RM, the processes involved in RM and notably risk assessment frameworks and techniques.

3.1 Concepts and Definitions

Risk: Whether we are aware or not aware, risk is present in all activities we perform. At a fundamental level, *risk* is usually associated with the uncertainty that an event occurs and the effect/severity/outcome/consequence in case it actually occurs. The definition is usually context-specific and wide variation arises in how an organization deals with the outcome. For instance, it is common to consider the risk in financial terms which reduces the risk to a single value evaluated by the expression below;

$$Risk = Probability\ that\ a\ threat\ occurs\ X\ Cost\ to\ the\ organization \tag{3.1}$$

Furthermore, Talabis *et al.* breakdown risk into four major components; event, asset, outcome and probability [23]. The event describes an uncertain situation that could occur and the asset refers to the direct or indirect target of an event. The outcome relates to the impact of the event. The probability or likelihood of an event occurring provides the necessary measurement in a risk assessment.

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation resulting from the operation or use of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system; and 4) documenting the overall RM program [24].

Risk Analysis: Examination of information to identify the risk to an information system [24].

Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system [1].

3.2 Regulatory Aspects for Risk Management

The efficient application of the risk management process is many times driven by research from specific organizations which develop standards, guidelines and recommended practices for carrying out the specific tasks. This section gives the notable standards, guidelines and organization necessary for this project.

3.2.1 Benefits of standards

An International Standard is a document that contains practical information and best practices that usually describes an acceptable and agreed way of doing something towards solving a global challenge [25]. Common standards are advantageous to all stakeholders; business, consumers, government, in many ways and these include;

- Compatibility: Through standardization, different organizations can make specific products that work well and fit with each other.
- Cost reduction: In addition to compatibility, organization can focus more on what they produce best in collaboration with other organizations and gaining from improved quality and processes.
- Increased customer satisfaction: Customers and users of the standards have a high degree of satisfaction while using products and services that conform to well-known standards.
- Widens market and customer base because of same standards followed and as a result of compatibility between the different products and services. Products are manufactured in one area and are sold or consumed in the opposite side of the globe.
- Safety purposes: Standardization leads to solutions that address the safety aspects of good and service, compared on an international baseline.
- Good ideas and good solutions: The formulation of standards is slow but nevertheless brings up great ideas from experts in industry that are shared all over the world to every organization, irrespective of competence levels of the employees.

3.2.2 Organizations, standards and guidelines

The **Federal Information Security Management Act (FISMA)** is an information security framework, part of the U.S. e-government act, put in place to secure information systems as well as manage the risk associated with information resources in federal government agencies. It sets requirements for the U.S. federal agencies to

develop, implement and document an information security program to protect the organization assets as well as support the operations and processes.

The **National Institute of Standards and Technology (NIST)** is a U.S. organization that promotes the national economy and public welfare by providing guidance and leadership on the national measurement and standards infrastructure [18, 1, 14]. It provides the 800 series security-specific special publications to assist the governments, industries and academia follow standardised best practices. With the exception of SP 800-53, each 800 series SP gives guidance on a specific subject area. For example, the Special Publication 800-30 gives guides and best practises for conducting risk assessments of federal information systems conforming to the statutory requirements of the FISMA. The publications are updated on a continuous basis with the changing technology advancements.

The **International Organization for Standardization (ISO)** and the **International Electrotechnical Commission (IEC) work in collaboration to** form the specialisation system for world wide standardisation. ISO, in particular, is an independent and non-governmental body that comprises of experts who develop innovative international standards to address the global challenges [25]. With a wide portfolio of standards and regulations in various industries, the following are the most commonly used from the research papers reviewed;

ISO/IEC 17799:2005 (Code of practice for information security management) is the international standard that established the guidelines and general principles used through out the lifetime (initiation, implementation, maintenance, and improvement) of information security management in an organization.

The ISO/IEC 17799 was later revised and replaced by the ISO/IEC 27002:2005 with a change in the reference number but having the same title. ISO/IEC 27002:2005 contains the recommended best practices of control objectives and controls intended to meet the risk assessment requirements during information system management. The current version of the standard is the ISO/IEC 27002:2013 that further enables not only implement commonly accepted information security controls but also develop organization-specific information security management guidelines [25].

The BS7799 was an information security management standard, developed in the United Kingdom to secure the confidentiality, integrity and availability of information assets through security controls used within the organization. It is the foundation of some risk analysis methods such as the CRAMM [26]. BS7799 was used as a basis for certifying organization against its Information Security Management System (ISMS) but later revised and superseded by the ISO/IEC 27001:2005.

The ISO/IEC 27001 (Information security management) family of standards focuses on asset management to help organizations keep their information assets secure [25].

ISO/IEC 27005 (Information security risk management) on the other hand provides guidelines for information security risk management applicable to all organizations and supports the general concepts, models and processes from both the ISO/IEC 27001 and the ISO/IEC 27002 [25].

3.3 Risk Management Process

Risk Management is a complex process that requires input from all stakeholders in an organization from the junior staff operating the systems and supporting the organization's business functions to the top management making strategic plan, goals and objectives, and most importantly, committing to provide the management support throughout the process. The NIST SP 800-30 presents a simplified RM process comprising of four components; (i) framing risk, (ii) assessing risk, (iii) responding to risk, and (iv) monitoring risk [1]. Figure 3.1 shows the effective RM process proposed by NIST and at the very least, each RM system should address all of these four components. As suggested, an effective RM process should facilitate a continuous exchange of information between the individual components.

Figure 3.1: Risk management process by NIST [1].

3.3.1 Framing risk

This is the first step to RM which refers to how organizations define risk and how they establish the risk context. A good framing of risk results in a comprehensive *risk management strategy* for the organization which addresses the risk assessment procedures, how to respond to risk and how to monitor the risk.

3.3.2 Assessing risk

This is a very critical step in the RM process and it specifies how an organization assesses the risk, very importantly, within the context of the organization risk frame stated in the previous step. The NIST SP800-30 emphasizes that risk assessment is used to identify threats and vulnerabilities to organizations in order to determine their impact and likelihood that they will occur i.e. determining risk. This is the main aspect addressed in this project. Risk assessment and analysis relies on the quality of data and expert experience. Relevant data can be be obtained through system inspection, system documentation and interviews by a single analyst, group of analysts or interdisciplinary teams having members of diverse experiences.

3.3.3 Responding to risk

After determining and assessing the risk, the organization acts according to the result obtained. This component ensures a consistent, repeatable, organization-wide response as determined by the organizational risk frame. It helps to develop, evaluate and determine the alternative courses of action for responding to risk consistent with organizational risk tolerance. Furthermore, this component facilitates implementing risk responses based on the selected courses of action.

3.3.4 Monitoring risk

This addresses how the monitoring of the risk over a long period of time in order to; determine the effectiveness of the earlier components, identify changes in the system and the environment that can reduce or aggravate the outcome of the risk, and ensure that the planned risk responses are implemented and in accordance with the federal and industry's regulations, organization business functions, policies, standards and practices.

4

Industrial Control Systems

Industrial Control Systems (ICSs), also known as Industrial Automation and Control Systems (IACSs), constitute part of the critical infrastructure systems whose failure or incapacity can lead to adverse effects on security, national economic security, national public health or safety, or any combination of those matters [3]. This chapter gives an baseline for the ICSs and what makes them different from other non-ICSs.

4.1 Overview of Industrial Control Systems

This section gives an overview of ICSs in terms of system components and some general examples or applications of ICSs. We further look into the network topology of a typical ICS.

4.1.1 What are Industrial Control Systems?

The term ICS, like many other terms used in this report, does not have an exact definition. A good understanding of the ICS is important for this project. Knapp et al. assert that the terminology used has become blurred due to the rapidly evolving socio-political landscape [6]. Terms such as 'critical infrastructure', 'Supervisory Control And Data Acquisition (SCADA)', the 'smart grid' are used freely, sometimes incorrectly and often confused with the ICS. Furthermore, it is important to differentiate ICS systems from Information Technology (IT) systems.

Industrial Control Systems (ICSs) are a broad class of automation systems used to provide both control and monitoring functionality mainly in critical infrastructures and industrial sectors such as electrical, water, oil and natural gas, chemical, pharmaceutical, pulp and paper, food and beverages, and transportation [6, 2]. ICS systems aggregate several systems used for industrial production such as SCADA systems, Distributed Control Systems (DCSs), Process Control Systems (PCSs), and Safety Instrumented Systems (SISs).

4.1.2 System components of an ICS

ICS are installed to support several purposes in different industries. Here, we describe the common components that help in data acquisition, data conversion and monitoring and control of the entire system.

Remote Terminal Units

The Remote Terminal Unit (RTU) collect data from the field devices and uses transducers to change the data into electrical signals and then from analog to digital for relaying to a central processing unit over a communication channel. They are usually placed in remote locations such as a substation or in places that may have limited access to electricity such as along a pipeline [6]. RTUs enable two-way communication by receiving control signals from the command centre to the individual field sensors. These units have limited processing and power.

Intelligent Electronic Devices

An Intelligent Electronic Device (IED) is a microprocessor-based controller used in power system equipment. IEDs provide not only local control and operation of electronic equipment such as circuit breakers, capacitor banks and transformers but also provide remote support using integrated telecommunications approaches [6]. IEDs receive data from sensors, power and electronic equipment and can issue control commands e.g. to trip the the circuit breakers in case of anomalies in key power parameters i.e., voltage, current, frequency.

Programmable Logic Controllers

A Programmable Logic Controller (PLC) is a programmable general-purpose and solid-state digital computer primarily used to automate electromechanical processes in ICS e.g., changing assembly lines in a manufacturing company [2]. A PLC can be used in place or in combination with RTUs [6]. Like SCADA, PLCs are also used extensively in process-based industries. Connected to sensors and actuators, PLCs may contain logic and programming to control some local functions that do not need command from the DCS or the centralized SCADA service.

Human–Machine Interfaces and Supervisory Workstations

Like the name suggests, Human–Machine Interfaces (HMIs) provide a means for operators to interact, visualize and also control other system components. They integrate with the entire ICS architecture and present a user-friendly graphical representation of the entire system that can be manipulate the remote devices by a click on the interface [6]. On the other hand, the supervisory workstations are primarily present for supervisory and monitoring purposes with read-only capability. Supervisory workstations can change some parameters like changing alarm thresholds but they do not control the ICS system components.

Data Historian

Data storage is a crucial and very important component of any system. A data historian is a specialized software system, e.g. a relational database management system that collects and stores data values, alarm events and any useful information from other system components. It presents a centralised platform to store data for presentation, and analysis of historical and current data. Data historians are a critical component of an ICS and should therefore be secured to minimize threats and vulnerabilities that may render them a security risk.

In general, the ICS components can be placed in four categories as shown in Figure 4.1. Data acquisition is done by devices that obtain analog and discrete data from the environment such as sensors and meters and this data is converted into analog information. The data is transmitted over wired and wireless communication media for presentation and control at the Control Center.

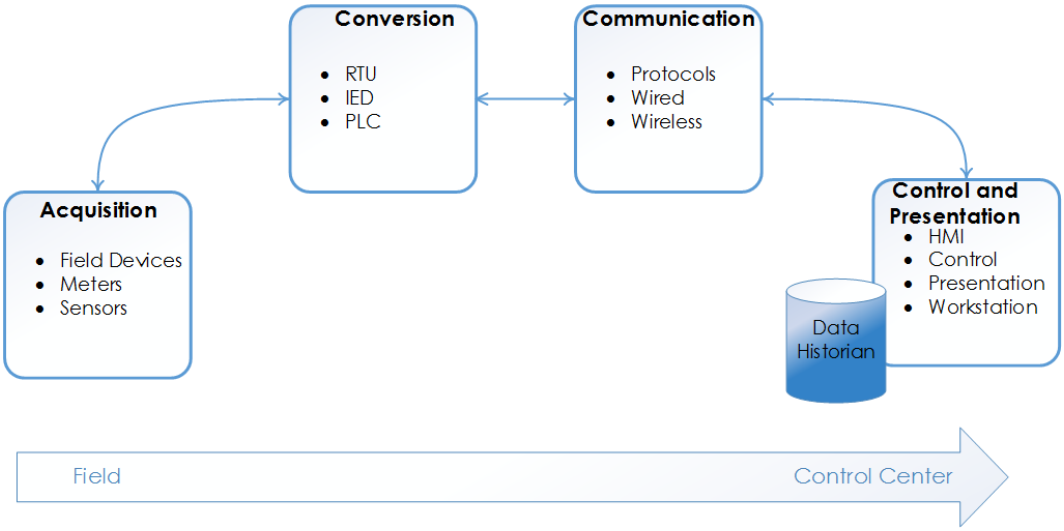

Figure 4.1: Block diagram of an ICS.

4.1.3 Examples of ICSs

The components presented in the previous section are key components of a typical ICS. They are strategically placed in systems to achieve the goals of a particular industry. In this section, we present some of the common examples of the Industrial Control Systems.

Supervisory Control And Data Acquisition

SCADA systems are the most commonly used ICS with numerous applications in electrical power grids, water distribution, oil and gas pipelines, and railway trans-

portation system. A SCADA system enables the remote monitoring and control of the network subsystems and devices and provides for a centralized management of the data acquisition and control processes [6]. Furthermore, the SCADA system is highly distributed and normally spans a very big geographical area. From a control center, over long communication links, the system monitors both the field devices and inter-networking devices and infrastructure, and regularly collects data and responds to to alarms that arise [2]. The data obtained guides the intelligent decision making and initiates automated and/or operator-enabled commands that control the operation of the remote device. Figure 4.2 shows a general layout of a SCADA system according to NIST. A suitable form of Wide Area Network (WAN) is used to connect the remote field sites to the system Control Center.

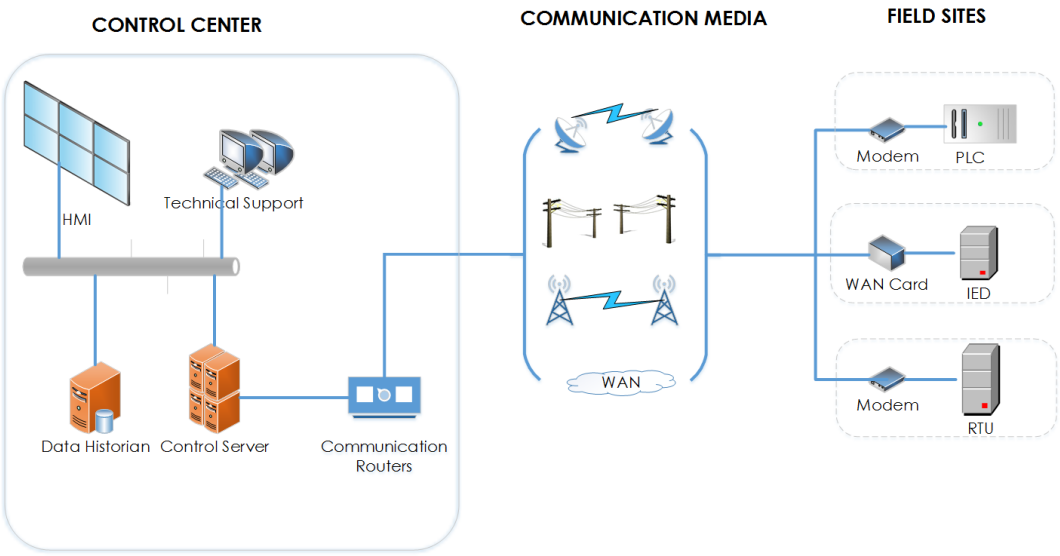

Figure 4.2: General layout of a SCADA system.
Source: Adapted from the NIST SP800-82 [2].

Distributed Control Systems

Unlike SCADA systems, Distributed Control Systems (DCSs) are used for controlling industrial processes at a plant, using custom designed control devices (processors) that are distributed within the system. Each component and each discrete subsystem is controlled by one or two control devices [27]. They are widely used in process-based industries such as nuclear, chemical and electric power generation [2]. The processor uses input modules to receive information from input instruments (usually sensors), processes the information and decides action by the output modules. Process control and monitoring is usually achieved using feedback or feed-forward control loops in a hierarchical network of controllers to maintain process or plant conditions at optimum levels. Figure 4.3 shows the logical hierarchy and functional levels of a typical DCS.

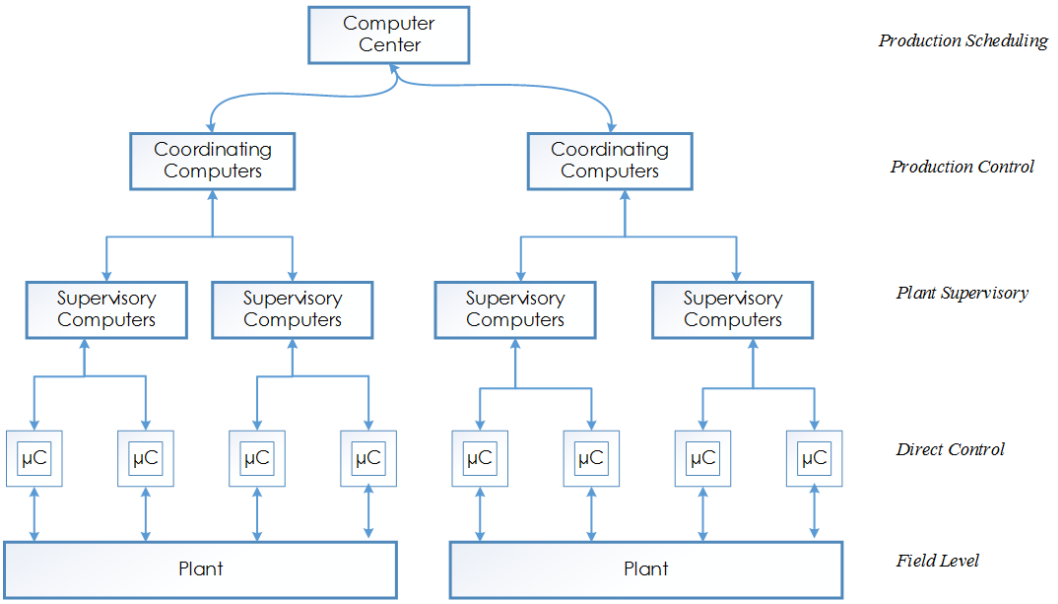

Figure 4.3: Functional levels of a typical DCS.
Source: Adapted from wikipedia.

Process Control Systems

Process Control Systems (PCSs) keep the output of a given process within a specific desired range. The system manipulates a number of process variables e.g., pressure, temperature, viscosity, in order to achieve automatic control. Using PCSs enables mass production with a high degree of quality and consistency within the same product range and through automation, the entire complex process can be controlled from a central room by one operator. The output of the controlled process can be categorized into three forms; discrete output producing distinct items, e.g. in the automotive industry, batch output from mixing known quantities of raw materials under known conditions or continuous output producing values that are not interrupted in time, e.g water temperature.

Safety Instrumented Systems

Safety Instrumented Systems (SISs) are a set of controls (software and hardware) used on safety-critical process systems, i.e. systems which need to be put in a 'safe state' in case operational issues occur while they are running. This is achieved using layers of protection [6]. At the first layer of protection, a SIS uses a basic process control system (BPCS) to operate and maintain a process within a given normal operational range. A SIS can detect and respond to abnormal process events by either maintaining the current operating status or putting the system in a 'fail safe' mode (usually shutting down the equipment) thereby avoiding adverse effects that may damage the personnel or equipment.

4.2 Comparison between ICSs and IT Systems

ICSs may appear relatively simple but can be complex systems. It is their hidden complexity that highly distinguishes them from IT systems. For instance, where a given traditional IT system deals with a limited set of operating systems, communication protocols, and networking capabilities, the ICS can integrate many different devices, from different vendors running applications on several operating systems, communication protocols and connecting with different technologies. Table 4.1 summarises some differences between the IT systems and the ICSs.

Table 4.1: Differences between IT Systems and ICSs.

Reference	IT Systems	ICSs
Risk Management Requirements	High data confidentiality and integrity. Fault tolerance is less important.	Emphasis on personnel safety and then protection of the process. High fault tolerance required. Major risk impact is regulatory noncompliance, loss of life, or equipment.
Technology Support Lifetime	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; same vendor
Security Testing & Audit	Modern methods and processes in place	Testing needs to be tied to system; modern methods inappropriate for ICS
Anti-Virus and Mobile Code	Very common; easily deployed and updated	Can be difficult due to ICS impact; legacy systems cannot be modified
Asset Classification	Common practice and performed annually; results drive security expenditure	Only performed when obligated; critical asset protection associated with budget
Patch Management	Easily defined; enterprise-wide remote and automated	Very long run-up to patch install; device/ component specific; potential for performance impact
Physical and Environmental Security	Poor (office systems) to excellent (critical systems)	Excellent (operations centers, guards, gates, etc.)
Security Compliance	Limited regulatory oversight	Specific regulatory guidance in some sectors

4.2.1 ICS topologies and architecture

The ICS networks are not very different from the traditional IT networks but the ICS networks present additional requirements to ensure the correct functioning and security of the entire system. For instance, the real-time operation and reliability in the control and process areas of the industrial control systems are of critical importance whereas this is not a requirement for the IT systems. The protocols used in ICS networks are of real-time nature and many of them are proprietary compared to their counterparts in the IT systems [6].

Many topologies exist for the IT systems such as star, ring, or bus topologies, to attain specific functions of the system. Star topologies are useful for client-server architectures where several endpoints can use share resources provided by a single server whereas bus topologies are used in shared message transmission domain such as the Ethernet networks. The ring topology easily supports the redundancy requirements needed in ICSs. Therefore, many traditional topologies/architectures can be adopted in the ICSs for the system to provide the correct service in a safe, reliable and secure manner.

4.3 Threats and Vulnerabilities in ICSs

4.3.1 Threats

A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service [24].

Threats are caused by humans or occur naturally but we restrict the discussion to attacks from humans. In this regard, a threat agent/actor is the force that creates a given threat, either actively or passively. The threat landscape for ICSs is wide and the threats may originate from any source motivated by any number of reasons. The threats may originate inside the system by 'insiders' who have the authority and access privileges to use the system or they may originate from external sources. The external actors range from new and random 'script kiddies' to big organised entities and state funded attackers. The threat actors may attack the ICS for financial gains on the stolen data. In other cases, they may want to disrupt and cripple the victims national services. In the Nordic countries, disturbing key findings reveal that state-sponsored threat actors pose the greatest risk, not only to the governments but also to the ICS, in search of state secrets, sensitive personal data, and intellectual property in order to benefit their government's decision makers [8]. Table 4.2 shows the groups of threat agents of ICSs found in the literature studied. It gives some of the reasons why an ICS is of interest to the given threat agents.

Table 4.2: Threat agents of ICSs.

Threat Agent	Description	Motivation for Attacking ICSs
Insiders	-Users from with authorized system access privileges.	-Job dissatisfaction, money gain, revenge [5].
Professional Vendors -Malware and Virus/worm writers	Invest in development malware, virus/worms & management of botnets.	-To gain control of devices and/or system and use them contrary to intended purpose [7, 8]. -To sell/rent out the botnet
Organized Crime -Gangs -Cyber criminals.	Engage in debit and card fraud	-Personal identity theft to gain access to system. -Intent to extort money from system owners [5].
State sponsored -Foreign intelligence	Well-funded and legally protected. -Use any information obtained to their benefit	-Retrieve information regarding national secrets, intellectual property, technologies used and security strategies [8].
Industrial Espionage -Mercenaries	Hired to attack specific corporate assets	Theft of information regarding Intellectual property, production and security strategies [8].
Terrorists or Activists -Motivated groups and individuals	-People joined by common ideologies -Can gather enough resources to cause attacks on systems	-Publicize their cause by sabotaging ICS assets, public sector and government services [5, 8]. -Theft of system plans, layouts and strategies to bring harm to national security.
Competitors	Actors who produce competitive products and services for similar purpose.	-Steal intellectual property for financial gain. -To reduce competition in the marketplace.
Script kiddies	People fairly new to programming and scripting	Experimenting with tools that could affect ICS assets [5].

With the nature of ICSs in providing critical services across the country, many large scale attacks lead to severe implications on the socio-economic development, military security, and political influence of the country [8].

4.3.2 Vulnerabilities

A Vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source [24]. A system is a secure as its weakest link and therefore we need a detailed review of the entire system and applied security procedures to understand the vulnerabilities of the system. From literature and inspired by the NIST SP 800-82r1, the potential ICS vulnerabilities are divided into three main categories; policy and procedure vulnerabilities, platform vulnerabilities and the network vulnerabilities to help in developing optimal mitigation strategies [2].

Policy and procedure vulnerabilities

Policies and procedures guide people in carrying out their duties and activities according to predefined good practices. Vulnerabilities in ICSs result from the lack of security documentation and the use of incomplete or inappropriate security documentation [2].

Initiating a security program requires top management commitment and support to generate the required documentation and training of all users of the system, both operational and non-operational.

The security policies and procedures should be proactive to reduce and prevent potential vulnerabilities. For example having well defined procedures on password use and management for all systems connecting to the ICS.

Platform vulnerabilities

Vulnerabilities can occur due to flaws, misconfiguration and poor maintenance of the platforms used in ICSs i.e. hardware, ICS application software and the operating system used [2].

The NIST SP 800-82r1 elaborates four categories platform vulnerabilities depending on the following platforms; (i) configuration (ii) hardware (iii) software and (iv) malware protection [2].

Network vulnerabilities

Components of an ICS form into a network. With the current trend in adoption of Internet technologies within the ICS, vulnerabilities occur due to flaws, misconfiguration and poor administration of the ICS network and its connection to other networks.

The NIST SP 800-82r1 divides the potential network vulnerabilities into;

- Network configuration vulnerabilities
- Network hardware vulnerabilities

- Network perimeter vulnerabilities
- Network monitoring and logging vulnerabilities
- Communication vulnerabilities
- Wireless connection vulnerabilities

5

Evaluating Risk Analysis Approaches

MANY risk assessment methods and approaches have been carried out both in academia and industry. Some have been driven by the industry, others by need through regulations, and still others depending on the services at hand. In this chapter, we explore some existing risk analysis approaches, we categorize them, and lay a foundation for formulating a suitable framework applicable to the ICS.

5.1 Existing Risk Analysis Approaches

There exists several risk analysis approaches in practice. Many of them are developed and used privately, whereas the ones of importance to this study are those that have been formally published in literature. These methods are mainly developed by the academia, professional and standardization organisations and disseminated through workshops and standards and guidance materials.

CCTA Risk Analysis and Management Method

CCTA Risk Analysis and Management Method (CRAMM) is an automated approach based on the qualitative risk assessment methodology developed in the UK by the Central Computer and Telecommunications Agency (CCTA) to carry out information systems security reviews within the government departments [26]. Currently, CRAMM can be used for all types of organizations to justify security related investments for information systems and networks at a managerial level and also demonstrate compliance with the British standard for information security management (BS7799, later superseded by the ISO/IEC 27001 series) during a certification process. Furthermore, the tool can be used for benchmarking risk and contingency management in organizations. The CRAMM approach review has mainly three stages, namely; (i) identifying and valuing assets, (ii) identifying threats and vulnerabilities, calculating risks, and (iii) identifying and prioritizing countermeasures. The approach uses a risk matrix with predefined values to calculates risks for each identified group of assets against the its level of threats and vulnerabilities.

Hazard and Operability Studies

The Hazard and Operability (HAZOP) method is a highly systematic, formal and structured hazard identification method that helps in identifying possible hazards in a complex system or process, show the current defences and makes appropriate recommendations to avoid accidents [28]. This method was originally developed for the chemical processing plants. It uses a multidisciplinary team of experts, through brainstorming sessions and the use of 'guide words' (e.g. "more," "early," "no"), to identify the hazards and operational problems. For each hazard identified, possible causes and consequences are determined and additional recommendations proposed if needed.

Failure Modes and Effects Analysis & Failure Modes, Effects, and Criticality Analysis

These are a systematic and highly structured approach used to investigate how a system or subsystems can lead to performance problems and even system failure. It helps in identifying potential failure modes of systems processes and products, assess the risk associated with each failure mode, rank the risk and carry out corrective and preventive actions. It evaluates the risk priority numbers (RPNs) which uses three risk factors; occurrence (O), severity (S) and detection (D) [29]. FMEA can be modified to Failure Modes, Effects, and Criticality Analysis (FMECA) to provide more information such as quantitative frequency and/or estimates and rankings of the consequences using a more formal procedure. Both FMEA and FMECA can be used from component level to system-wide level in any well-defined system especially the electrical or mechanical systems.

Risk Assessment for Safety Critical Systems

Risk Assessment for Safety Critical Systems (CORAS) was a research and development project set up to provide method and tools for an efficient, and unambiguous risk assessment for security critical systems [30]. The CORAS approach was modelled using the Reference Model for Open Distributed Processing (RM-ODP) as a reference model and the Unified Modelling Language (UML) to show the interactions and dependencies between the users and the environment. It has four main pillars; (i) a system documentation framework, (ii) a risk management process, (iii) a system development process, and (iv) a platform for tool-integration.

Operationally Critical Threat, Asset and Vulnerability Evaluation

The CERT Coordination Center (CERT/CC) developed the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) approach to manage information security risks by considering both organizational and technological issues [31]. It examines how people use an organizations computing infrastructure on

more regular or daily basis and focuses on mainly two aspects (i) operational risk and (ii) security practices. As a self-directed approach, the people within an organization are responsible to set the organization's security strategy. In addition to the continuous improvements on the approach, the OCTAVE exists in different versions that may be used independently or in combination e.g. OCTAVE method for large organizations and the OCTAVE-S, which is aimed at small organizations. The OCTAVE approach is carried out in three phases that are further broken down into processes. Phase 1 involves building the asset-based threat profile, phase 2 involves identifying the infrastructure vulnerabilities wheres phase 3 deals will developing the security strategy and plans.

Harmonized Risk Analysis Method

The Harmonized Risk Analysis Method (MEHARI) approach created in 1996 by the CLUSIF (Club de la Sécurité de l'Information Français) to enable company executives to manage their information security, IT resources and reduce the security related risks [32]. Furthermore, it helps in the implementation of the ISO/IEC 27005 standard. The approach complies with the ISO 13335 Risk Management standard and is suitable for the ISO 27001 Information Security Management System (ISMS) process. MEHARI framework helps to manage the information security through four phases; (i) analysis and classification of the stakes, (ii) evaluation of security services for vulnerabilities, (iii) risk analysis, and (iv) definition of security plans through monitoring of information.

Common Safety Method for Risk Evaluation and Assessment

Initiated by the European Railway Agency (ERA) and the European Commission to encourage diversity and competitiveness in the railway market without compromising the safety levels, and/or improving them when reasonably practicable [33]. It was put in place to harmonize the risk assessment and evaluation processes and provide documentation during the application of the processes. This approach is used for change management in the railway system when any technical, operational or organisation change is proposed, with emphasis on the impact of the risk management process on the safety of the system. Furthermore, the methodology specifies where on the system this methodology applies and the key personnel to lead and undertake the Common Safety Method for Risk Evaluation and Assessment (CSM RA). Figure 5.1 shows a flowchart of the CSM RA methodology.

Hierarchical, Model-Based Risk Management of Critical Infrastructures (HMRM-CI)

Baiardi et al. developed a quantitative model-based risk management framework that considers a sequence of hierarchical models which describe the dependencies

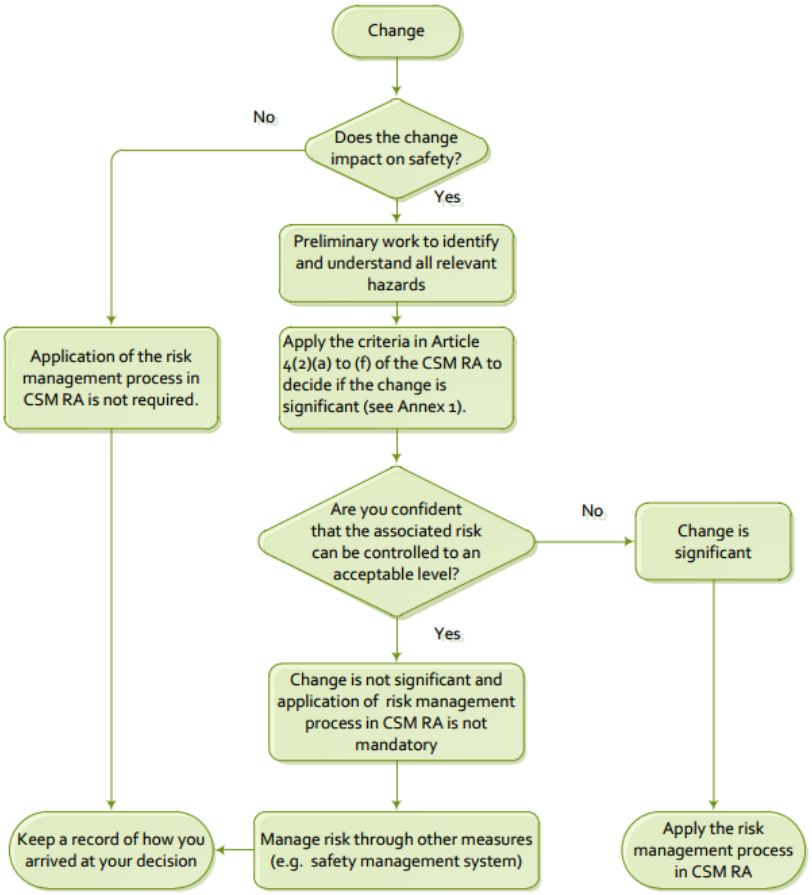

Figure 5.1: CSM RA methodology for technical, operational or organisational change.

Source: Common Safety Method for risk evaluation and assessment [33].

among infrastructure components [34]. Their approach develops two independent graphs; an infrastructure hypergraph which depicts the interdependent system components in terms of their internal states and operations carried out on them [each component has the three CIA security attributes], and an evolution graph which consists of an elementary attack that can be composed into more complex ones. The approach uses mathematical computations and software supporting tools to design the evolution attack graphs for risk analysis and automated mitigation measures.

NIST Special Publication 800-30

The NIST SP 800-30 proposes a guide for conducting risk assessments for federal IT systems and organizations with processes similar to those given by the ISO/IEC [1]. It provides best practices of carrying out a risk assessment following nine (9) steps. The approach given is a general guideline for information systems and can always be applied and modified to specific needs in a given industry.

Automated Risk Management System

Henderson et al. proposed ARMS, an automated risk modelling framework to address the deficiencies left by the traditional risk modelling frameworks such as CRAMM and OCTAVE. The framework identifies and addresses four main aspects of timeliness, granularity, accuracy and comprehension that are not efficiently addressed by the traditional threat and risk assessment methods [35]. The framework is particularly good in large environments because it uses automated dependency modelling to monitor the system linkages and graphs the risk posture using a series of metrics on a continuous basis. It can discover the cascading failures that may be caused by a given fault.

Table 5.1 shows a brief summary of the methods that have been discussed in this section with information about existing versions, nature of risk analysis approach, the year of formulating the approach, place it was developed and the applicable standards/frameworks followed in developing the approach.

Table 5.1: Snapshot of the discussed existing risk analysis approaches.

Approach	Versions	Type	Year	Country	Standards
CRAMM	V5.0	Qualitative	2002	UK	ISO/IEC 27001
CORAS	V1.4	Qualitative	2002	European	Australian/New Zealand standard AS/NZS
OCTAVE	OCTAVE Method V2.0, OCTAVE-S V1	Qualitative	2003	USA	Depends on domain e.g HIPAA or ISO/IEC 27002
MEHARI		Qualitative	2010	France	ISO 13335, ISO 27001
CSM RA		Qualitative	2013	UK	Regulation (EC) 352/2009
FMEA & FMECA	Updated	Semi-Quantitative		USA	IEC60812, BS5760-5:1991
HAZOP	Updated	Qualitative	2003	UK	IEC 61882
HMRM-CI	One version	Quantitative	2015	Italy	IEC 1025 1999
NIST SP800-30	Revision 1	Qualitative	2012	USA	FISMA
ARMS	One version	Quantitative	2012	Canada	ISO27005:2011, NIST SP800-30

5.2 Evaluation of Risk Analysis Approaches

To gain a better understanding of the risk analysis approaches above, we give a clear definition and goal of each analysis and then categorize them in a more comparative way including; goals of the approach, qualitative or quantitative nature, scope and stages involved in the risk management process.

5.2.1 Definition and goal of the approaches

First, the approaches are distinguished by their intended purpose. Table 5.2 shows the brief objective of the RA approaches. In general, the main goal of all the approaches can be reduced to risk identification, risk analysis and risk mitigation. By definition, the approaches range from comprehensive risk analysis approaches, frameworks, guidelines, risk assessment platforms and model-based frameworks. This provides a wide range of approaches from which we can obtain a suitable framework for ICS.

Table 5.2: Definition and goals of the each RA approach

Approach	Definition and Goal
CRAMM	Comprehensive tool for identifying security and contingency requirements, and justifying expenditure on necessary countermeasures especially of an IT operation [26]
OCTAVE	To identify, prioritize and manage information security risks [31]
MEHARI	Intended for organizations to identify risks, quantify level of risk, reduce inadmissible risks to acceptable level, ensure risk tracking [32]
CSM RA	The CSM RA applies when any technical, operational or organisational change is being proposed to the railway system [33].
FMEA	Framework for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service.
HAZOP	To identifying potential hazards in the system and identifying potential operability problems with the system and in particular identifying causes of operational disturbances [28]
NIST SP 800-30	Guidelines to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in SP 800-39 [1]
CORAS	A platform for precise, unambiguous, and efficient risk assessment of security critical systems [30]
HMRM-CI	Model-based approach to provide a formal definition of risk mitigation plan and the evaluation of the infrastructure robustness [34]
ARMS	Model-based approach to counter the known limitations in organizations' ability to identify and respond to systemic vulnerabilities and their cascading impacts [35].

5.2.2 Qualitative or quantitative approach

It is clear that there are two main risk analysis approaches: quantitative or qualitative.

Qualitative approaches are the most common type of risk analysis methods and extensively used and employed in many industries. They follow a given procedure, a variation of Threat and Risk Assessment procedure which address the steps recommended by NIST; Determining assets of value; Identifying threats associated with the assets; Evaluating existing controls; Determining the risks to assets; Making recommendations to deal with the risk in a given priority order using the severity, likelihood and consequence as key parameters. Qualitative methods classify risks in terms of non-numeric levels such as low-medium-high for a simple evaluation.

Generally, quantitative approaches use two metrics for the risk model; probability of an event occurring and the loss that may be incurred. These two metrics are quantified and multiplied to produce a single risk figure which is the *expected loss* for the given period of time. Risk is calculated for several events and then ranked for the purpose of making decisions and mitigating the risk. The challenge with this type of analysis also lies in how accurately and reliably one can measure probability and estimate the potential loss caused. In this category, we review the three quantitative approaches from Table 5.1: FMECA, HMRM-CI and ARMS.

5.2.3 Scope of the approach

The approaches were also grouped in scope, as shown in Table 5.3, by the degree of detail they provide, key issues addressed (organizational, technological or Operational) and its flexibility in terms of ability of applying the approach to a different area or field as-is. The three main issues addressed by the methods can be reduced to organizational, i.e. relating to the organization e.g. management decisions, technical, i.e. relating to the actual systems and operational, i.e. relating to processes. The level of detail refers to how much detail the approach provides regarding the related RA activities.
CORAS, HMRM-CI and ARMS are more focused on the technical aspect of risk analysis than on the organizational or operational nature. In addition, these approaches are not very flexible because of the way the way they are designed. HMRM-CI and ARMS take on a more mathematical approach and applicable to a very narrow scope of systems which lowers their applicability in this project. CSM RA addresses all the three aspects; organizational, technical, and operational but not flexible and mainly applicable when there is a significant change in the system that affects the safety of people and the system components. MEHARI, HAZOP and NIST SP800-30 address both the operational and organizational aspects of the system and they are flexible, easy to apply and customize from one system to another. The NIST SP800-30 is preferred for its level of detail, supported by other special publications in relation to the risk analysis. On the other hand, a combination

Table 5.3: Scope of the Risk analysis approaches

Approach	Issues Addressed	Flexibility	Detail
CRAMM	Organizational, Technical	Flexible	Low
CORAS	Technical	Not Flexible	Low
OCTAVE	Operational, Technical	Flexible	Low
MEHARI	Operational, Organizational	Flexible	Low
CSM RA	Organizational, Technical, Operational	Not Flexible	Low
FMEA	Organizational, Technical	Flexible	Low
HAZOP	Operational, Organizational	Flexible	Low
HMRM-CI	Technical	Not Flexible	Medium
NIST SP800-30	Operational, Organizational	Flexible	Medium
ARMS	Technical	Not Flexible	High

of HAZOP and FMEA provide a good match for organizational, operational and technical approach in the hazard and risk identification process of risk management.

5.2.4 Stages of risk management addressed

The approaches were examined against the risk management (RM) how they fulfil the fundamental aspects of risk RM. Table 5.5 is a summary of the results obtained. The table includes the number of RM steps in a given approach whether the approach establishes a context and the metrics used. From the table, the symbol "√" implies that the step is addressed to a good detail. The symbol "/" means that it is difficult to trace or insufficiently described and the blanks indicate no specif mention of the parameter. As expected, the approaches address the risk analysis component of RM. A few traditional approaches have between 3 and 5 steps whereas those with more than 5 steps tend to expand and be more clear on the procedure. The ARMS approach has good documentation but lacks clearly pointing out the number of steps and a mention of the context.

HMRM-C as well as CORAS and FMEA uses a 5 step RM approach but it does not state or elaborate the risk evaluation used. Furthermore, due to its quantitative nature, it uses different sets of metrics to measure the security of the system.

CORAS, FMEA and NIST SP800-30 sufficiently address all the most important steps in the RM process. CORAS, based on the Australian/NewZealand standard and the NIST SP800-30 have well built and overlapping RM steps. We find that FMEA has strengths during the risk identification process in order to determine the different failure modes of the system components and this greatly helps in the establishment of attack vectors. FMEA a unique set of risk factors for defining the

risk model i.e. severity (S), frequency of occurrence (O) and detectability (D) as opposed to the traditional factors used by CORAS and the NIST SP800-30.

5.2.5 Pros and cons of the risk analysis approaches

All the RA methods have their strengths and weaknesses. Table 5.4 shows the relative advantages and disadvantages of the RA approaches.

Table 5.4: Advantages and disadvantages of the RA approaches

Approach	Advantages	Disadvantages
CRAMM	-Can be fast to conduct security reviews. -Consistent results for similar risk profiles.	-Need for qualified and experienced users -Full reviews may consume time -Does not provide a single entire system measurement of risk
CORAS	-Facilitates communication between the actors involved during risk analysis. -Improves accuracy	Shows no relation between risks.
OCTAVE	Encourages organizations to self-assess their own practices. Low cost	-Addresses strategic, rather than tactical security issues. -Shows no relation between risks.
MEHARI	-Free and open-source	-For High-level strategic use -Does not address technical risks well.
FMEA & FMECA	-Flexible -Good for safety and reliability newline -Knowledge base of failure mode and corrective actions. -Use of simple tools to record results	Not accurate; the three risk factors are mostly difficult to estimate. -No relationship among failure modes -Inefficient for big systems with many components.
HAZOP	-Systematic, disciplined and documented approach. -Covers safety of equipment and humans	considers system parts individually, depends greatly on the ability and experience of the team members.
HMRM-CI	-Automated approach. -Produces optimal risk mitigation plan	-Need for qualified and experienced users -Highly formal approach and difficult to implement in actual environment
NIST SP 800-30	Applicable to all industries	More vulnerability-centric with little insight into CIA
ARMS	-Automated approach -Good for large environments Addresses timeliness, granularity considered more accurate	-Need for qualified and experienced users

Table 5.5: Stages of RM addressed by the RA approaches

Approach	RM steps(#)	Context	Risk Identification	Risk Analysis	Risk Evaluation	Risk Treatment	Risk model/Metrics
CRAMM	3		√	√	√		Assets, threat level, vulnerability level, risk matrix
CORAS	5	√	√	√	√	√	Likelihood, consequences, threats
OCTAVE	8 (in 3 phases)		√	√	√	√	Assets, threats, vulnerabilities, security requirements
MEHARI	4		√	√	√	√	CIA, exposure, Impact
CSM RA	9	√	√	√	√	/	change, hazards, impact on safety
FMEA	5	√	√	√	√	√	severity, frequency of occurrence , detectability
HAZOP	8	√	√	√	√		hazards,guide words
HMRM-CI	5	√	√	√		√	Security dependency among the system components, attack strategies, the optimal set of countermeasures
NIST SP 800-30	9	√	√	√	√	√	threats, vulnerabilities, likelihood, impact
ARMS		/	√	√	√	√	CIA, inter and intra dependencies in levels, cascading impact of events, granularity, accuracy

KEY: '√' implies the step is addressed in detail '/' step is insufficiently described.

6

Modified Risk Analysis Framework for ICS

The ICS systems are increasingly being exposed to both internal and external pressure due to the high reliance on technology interconnection and interconnectivity hence an increase in potential vulnerabilities and potential risk to the operations [3]. In this chapter we suggest a new framework, the Modified Risk Analysis Framework for Industrial Control Systems (MRAF-ICS) and gives a discussion of of the framework.

6.1 A Modified Framework for Industrial Control Systems

Based on the risk analysis methods that we studied, we propose a new method the Modified Risk Analysis Framework for ICS systems (MRAF-ICS). It uses NIST SP800-30 and CORAS approaches as an overall guideline. FMEA and HAZOP procedures are used in the threat identification stages. MRAF-ICS puts emphasis on the technical aspects rather than the organisational and operational ones.

6.2 The Risk Model

Assets, threats, vulnerabilities and consequences are the main risk factors in most of the approaches. Given the nature of ICSs as part of the Critical Infrastructure systems, we introduce an asset '*criticality weight*' factor to depict the degree of criticality and relative importance of a particular threat or vulnerability of an asset. For simplicity, we restrict the criticality values to a range between 1 and 1.5, varying in steps of 0.1 giving 5 levels of system asset criticality. The value 1 refers to normal criticality level, whereas 1.5 is highly critical such that attacking it may lead to damage to equipment and loss of life. Therefore, risk is modelled as;

$$Risk = Criticality * Likelihood * Impact \tag{6.1}$$

6.3 The MRAF-ICS

Risk management is adopted in many organizations world-wide because it is systematic, standardized and guides the decision making process. The MRAF-ICS is a 9-stage risk analysis framework and this section elaborates the stages carried out for the successful implementation of the analysis.

1. System definition

The approach begins with a clear establishment of context for the assessment. This takes into consideration of the scope, functions, parameters and interfaces of the system. It is important to clearly identify all the interconnection points between the ICS network with any other non-ICS networks such as the organization's IT-backbone. The overall definition must be presented in great detail and provide an outline for the remaining steps. The technical scope should be in-line with the organization's technical goals.

2. Identify assets and asset criticality weight

Identify the assets of the system by consulting with the person in charge of the system and a team of competent technical personnel. Keep a record of the all the asset, type of each asset and where they are located in the network both logically and physically.

3. Identify risks

Identifying risks is one of the most important stages of the approach because only those risks that are identified can be used in the following stages. It is practically impossible to identify all the potential risk sources but a consultative process can help identify the most relevant and possibly most frequent risks. In this approach, like in the NIST recommendation, we identify risks through threat modeling and determining the potential vulnerabilities to the system.

Threat modelling: It is necessary to make a logical diagram and identify the components that may be access points to the system. This helps to determine potential attacking points and also draw boundaries and identify the control points.

The system is further broken down into subsystems and components with specific information on technologies used such as devices, interfaces, protocols and intended functions. Here, possible attack paths/vectors can be explored, based on the current security posture and trends.

Further, determine the possible threat actors that could or would want to attack the ICS network and the potential reasons for the attack. The threat

actors may be categorized according to intent of attack, resources and skills level of the attacker. It is important to document the ways in which these actors could attack the system.

System Vulnerabilities: The approach borrows from the NIST RM framework to categorize the System vulnerabilities in terms of *platform vulnerabilities* as a result of flaws, misconfiguration and poor use of software/hardware and *network vulnerabilities* due to any communication the system may have within its subsystems or external connections.

Figure 6.1 shows the interactions between the different steps of risk identification. The assets are decomposed into constituent components. The threat actors use known vulnerabilities to attack the components but in some cases, they may attack the asset. Therefore, control mechanisms are applied to the components to mitigate the vulnerabilities.

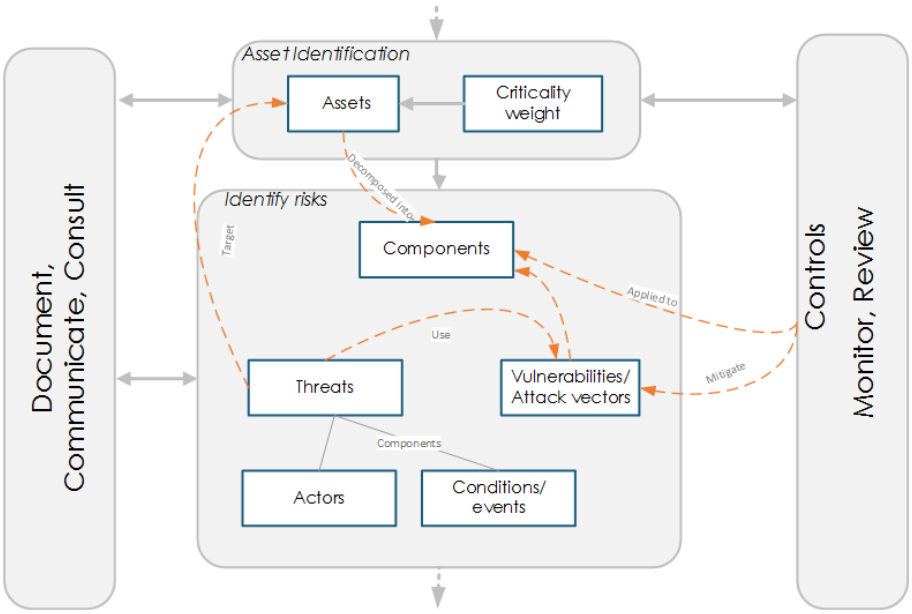

Figure 6.1: Relationships in threat modelling.

4. Analyse risks

Risk analysis is a tool for decision making and a direct input to the risk evaluation step. It involves a careful estimation of the positive and negative impact and the probability of likelihood of occurrence.

In this approach, we identify the likelihood that the identified threat actors will exploit the vulnerabilities and also be successful with the attack. Next, the adverse impacts of a successful attack on the components, equipment, and people is

estimated for each threat. In this approach we use a criticality weight factor to emphasize the relative importance of the critical system components. It is a weighted component attached every asset and also considered in evaluating the risk.

Finally, we determine the risk loss as a combination of the three parameters; asset criticality weight, likelihood and impact as shown in Equation 6.1.

5. Evaluate risk

Risk evaluation is very important because it facilitates the decision making process. The outcome determines the priority ordering for risk treatment and their treatment strategies.

This step uses the result from risk analysis to compare the all the risks identified. From this comparison, the risk treatment strategies and the priority of application can be identified.

6. Risk treatment strategies

Risk treatment provides strategies and remedies for dealing with the evaluated risk. It results in one or more choices for modifying the risks in such a way that the overall treatment is cost-effective and does not adversely affect the organization's objectives.

If the calculated risk is within the acceptable region and the organization does not need to spend extra resources on it, the process may proceed to the next step.

If the risk can not be tolerated, the proper risk treatment options should be employed. From Figure 6.2, we further examine, iteratively, if the risk can be reduced. If the risk can be reduced, then we use the available monitoring controls to modify the evaluated risk parameters i.e. the likelihood and/ or impact. This is done until the risk level is 'as low as reasonably possible'.

If the risk can not be reduced, other risk treatment methods should be considered including;

- Avoiding the risk by cancelling the activity or removing the risk source.
- Accepting the risk based on informed decision.
- Sharing the risk with a third party such as insurance companies, or other specialized entity, through contractual obligations.

7. Monitor and review process

Risk management is a continuous process. In order to make it more effective and to improve the overall performance of the system, we need to monitor all the steps on a regular basis and review each process so that they are still appropriate and relevant.

Furthermore, we must ensure that the approach is in support of the organization's security goals and objectives and risk management plan.

Its output is a comprehensive report including decisions of how this approach can be improved to facilitate the continuous improvement of the framework.

8. Maintain documentation

Documentation is an integral part of the approach and the right documentation tools should be used and kept at every stage. All documentation should be kept for future reference for a period long enough to serve their importance. For instance, the quick notes kept during the approach can be kept until the next evaluation period whereas the guiding documents need to be kept for a much longer period.

9. Consult, communicate and share information

The RM process affects the entire organization. We saw that threats can come from anywhere and it is possible that losses can occur unintentionally. Therefore, we encourage a stakeholder involvement at every stage of the process.

Consultation with all stakeholders, both internal and external, and potential direct users of the system should take place all throughout the entire process. The stakeholders need to be part of the process in order to own it and therefore use it effectively. This helps in establishing the context more effectively, identifying all the assets and estimating the relative criticality weighting of the respective assets and ensures proper risk identification and evaluation.

The results should be effectively communicated to the various stakeholders to the most appropriate detail needed by the group.

Figure 6.2 shows a flow chart of the MRAF-ICS approach highlighting the key steps discussed above.

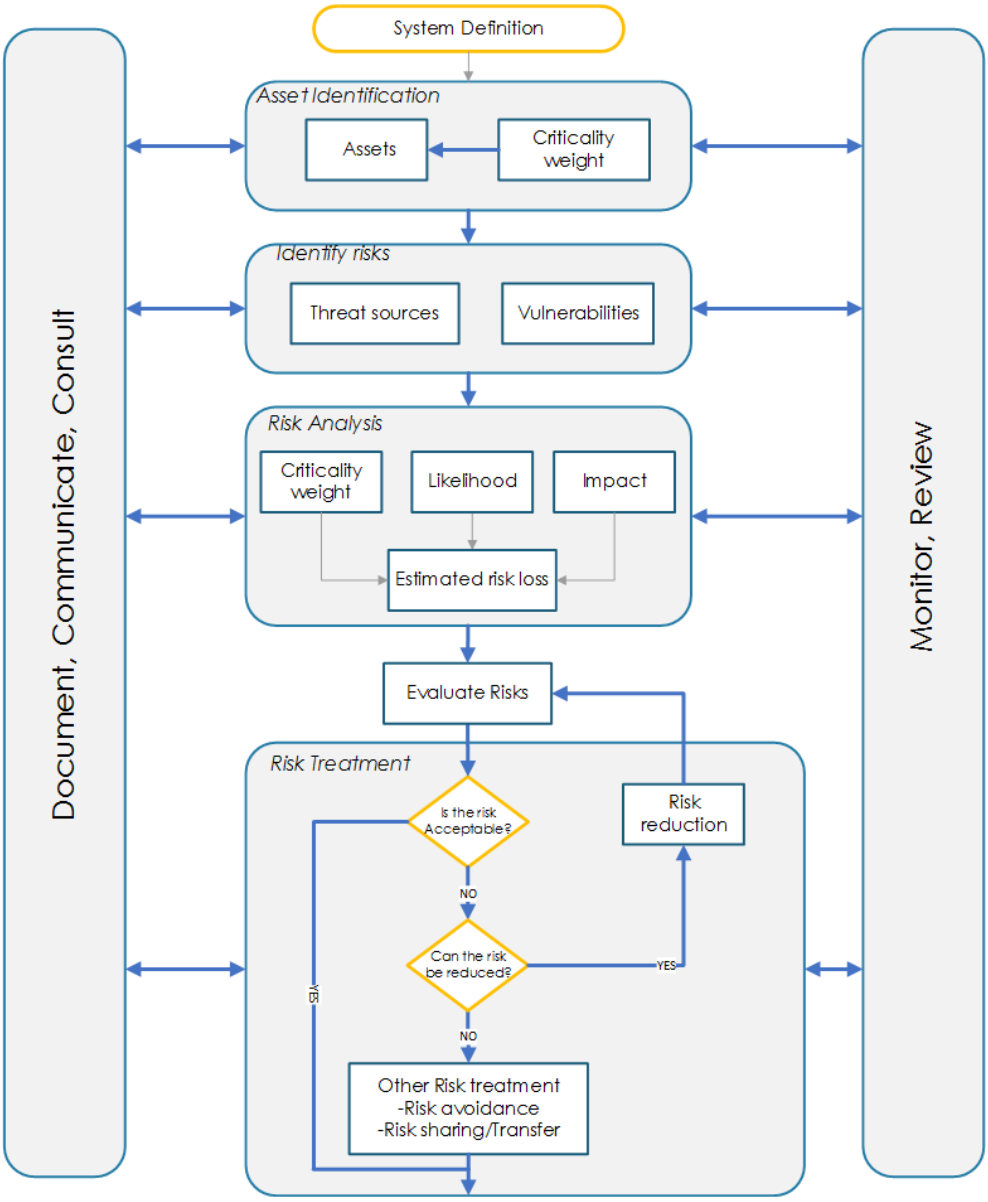

Figure 6.2: Flow chart of the MRAF-ICS approach.

7
Discussion

This Chapter gives a discussion of the framework we developed, the MRAF-ICS. In the first part, we discuss the developed framework. Secondly, we compare this framework to the base frameworks and finally identify the potential challenges faced by the framework.

7.1 The MRAF-ICS

The MRAF-ICS approach is a 9-stage and self-developed risk assessment framework built to benefit from the advantages of both NIST SP800-30 and CORAS frameworks. The main goal of the MRAF-ICS is to identify, manage and prioritize the security risks in ICSs with additional emphasis on the relative importance/criticality of the assets used in ICSs. It is designed to be used specifically in ICSs with a multitude of critical components.

From the RA approaches discussed in Chapter 5, the MRAF-ICS uses NIST SP800-30 and CORAS frameworks as the base frameworks for the overall risk management cycle. NIST SP800-30 addresses both operational and organizational aspects of risk management through guidelines for conducting risk assessments whereas CORAS is a risk assessment platform for security critical systems that addresses the technical aspects as shown in Chapter 5. NIST SP800-30 had the biggest number of steps (9) for the RM process. The two approaches, NIST and CORAS effectively addressed the key stages of RM that we were interested in, i.e. establishing the context of the analysis, identifying the risk, risk analysis, risk evaluation and risk treatment.

In the second stage (asset identification) of the framework flow, we identify the assets of the system under review and then additionally assign a criticality weight that varies from asset to asset. It is possible for two assets to have the same criticality weight.

In this approach, we consider the identification of risks to be a very important stage in the entire process and therefore use a threat modelling approach and additionally benefit from the widely-used and highly systematic approaches from HAZOP and FMEA. Threat modelling identifies the possible threats and vulnerabilities in the system and helps to map the threat actors with the possible vulnerabilities they

can exploit through some attack vectors. Both FMEA and HAZOP identify more hazards that affect the safety of the system that may be missed using the threat modelling approach providing a wider coverage for identifying potential risks.

During the risk treatment, we first evaluate if the evaluated risk is acceptable and can be managed by the organization. If the risk is not acceptable, the approach encourages the application of existing security controls to ensure that the risk is reduced to the lowest possible level before other treatment mechanisms can be used. This helps to keep the cost of risk treatment low through the use of already existing controls.

7.2 The MRAF-ICS and the Base Frameworks

From the RA approaches discussed in in Chapter 5, only 3 of them are quantitative. This is so because during the research, we found out that most risk analyses in live environments are qualitative in nature. Quantitative risk analysis requires the use of specialised tools that are usually closed applications and not easy to modify for organization use. IT further requires additional training of staff with a certain minimum technical skill-set leading to overall high cost of carrying out the analysis and finding the necessary resources. Therefore the MRAF-ICS adopted a qualitative approach because of ease of applicability in a live ICS environment.

Table 7.1 shows the differences in the scope between the three approaches. The MRAF-ICS mainly focuses on the technical parameters and not on organizational and operational parameters. Despite the role and contribution made by an organizational aspect, we believe this can be handled by many available documentations such as the NIST SP800-30. Furthermore, we note that the approach is designed for ICSs which limits its potential when applied to other systems. For this reason, the approach is not flexible. The approach is relatively more detailed than the CORAS approach because of the elaborate steps used in the RA process.

Table 7.1: Scope of the MRAF-ICS, CORAS and NIST SP800-30

Approach	Main issues addressed	Flexibility	Detail
MRAF-ICS	Technical	Not Flexible	Medium
CORAS	Technical	Not Flexible	Low
NIST SP800-30	Operational, Organizational	Flexible	Medium

In terms of stages used in the RM process, the MRAF-ICS and NIST SP800-30 are more detailed and benefit from 9 steps as opposed to the 5 step presented by the CORAS approach. In all the 3 approaches, the context is establish as a first step in carrying out the approach.

All the three approaches are Threat and Risk Assessment approaches that use threats, vulnerabilities, likelihood and impact as the risk factors. The CORAS and NIST SP800-30 do not deal with the critical elements of an ICS system. Therefore, whereas they are effective in information systems, they are not as effective in ICSs which has several assets that vary in criticality. Unique to the MRAF-ICS is the 'asset criticality weight' a 5-level figure between 1 and 1.5 that attaches a criticality measure on the asset under consideration. Thus, the calculated risk is evaluated based on three parameters; asset criticality, likelihood of a threat occurring and the potential impact as a result of the threat occurrence. We believe this is a very important addition to the the risk assessment approach.

The MRAF-ICS uses a threat modelling approach to identify the threats and vulnerabilities in the ICS under review. The assets are further reduced to components from which security holes can be found at the lowest level. The process involves formulation of possible attack vectors to enable identifying all possible threats, threat actors and activities/events that can lead to the exploitation of the vulnerabilities. Furthermore, the approach uses additional procedures for risk identification similar to those of FMEA and HAZOP approaches. This ensures that most of the potential risk possibilities are exhaustively considered. This exhaustive risk identification approach is not used by other methods. The MRAF-ICS puts a lot of emphasis on documentation at every stage of the process, similar to the CORAS approach.

7.3 Challenges of the MRAF-ICS

The MRAF-ICS is a qualitative approach. Therefore it inherently suffers from the subjective definition of the process, a challenge that is not present in the quantitative approaches. Therefore two different analyses by two different groups on the same system definition may result in different analyses.

The approach was designed for ICSs which vary in functionality, size, composition, application and so on. In order to encompass all the different types of ICSs, the framework was modelled to be more general.

Furthermore, the framework employs a criticality weight for each asset in the system. One challenge with this is that the assets in the system under review should have different degrees of criticality. This implies that the framework is not effective for analysis on a one-asset system definition or on a number of assets having the same criticality weight.

8

Conclusion

Security measurement is very important for determining the security posture of an organization. It is of critical importance in ICSs because of the services such systems offer to the nation in important areas, e.g production and manufacturing, transportation, energy and others. We used risk analysis as a measure of security in ICSs, explored and analysed several existing risk analysis approaches. Based on this we formulated a Modified Risk Analysis Framework suited for ICSs. The framework, built on the NIST Risk analysis guidelines and the CORAS approach, introduces the asset criticality weight in the risk evaluation. We believe that, in addition to the traditional risk factors used in traditional IT systems, a special parameter, asset criticality weight, will produce a more precise measure of risk, depending on the ICS asset that may be attacked.

The modified framework defined in this report was more focused on the technical aspect of the system but the organizational and operational views are equally important. Risk analysis is a continuous process and there must be top management support for the analysis to be effective. Finally, there exists no single risk analysis framework for ICSs and therefore the MRAF-ICSs is a general framework that adds to the existing RA frameworks.

Bibliography

[1] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments ," *NIST Special Publication 800-30 Revision 1*, 2012.

[2] K. A. Stouffer, J. A. Falco, and K. A. Scarfone, "SP 800-82. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), Revision 1," tech. rep., Gaithersburg, MD, United States, 2013.

[3] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cyber-security," February 2014.

[4] National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team, "NCCIC/ICS-CERT Year in Review," *FY 2015*, 2015.

[5] H. Christiansson and E. Luiijf, "Creating a European SCADA security testbed," vol. 253, pp. 237–247, 2008.

[6] E. D. Knapp, J. T. Langill, R. Samani, and M. I. Cruz, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and other Industrial Control Systems*. Waltham, Massachusetts: Syngress, 2nd ed., 2015.

[7] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[8] FireEye Threat Intelligence, "Report: Cyber Threats to the Nordic Region," *May 2015*, 2015.

[9] Applied Computer Security Associates, "Workshop on Information Security System Rating and Ranking (WISSRR): Information System Security Attribute Quantification or Ordering," May 2001.

[10] K. J. S. Hoo, "How Much Is Enough? A Risk-Management Approach to Computer Security," June 2000. Accessed: 2016-03-26, `http://iis-db.stanford.edu/pubs/11900/soohoo.pdf`.

[11] W. K. Brotby, G. Hinson, and M. E. Kabay, *Pragmatic Security Metrics: Ap-*

plying Metametrics to Information Security. Boca Raton, Fla: CRC Press, 1 ed., 2013.

[12] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, and S. Huang, "Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–16, 2015.

[13] S. Marianne, B. Nadya, S. John, H. Joan, and G. Laurie, "SP 800-55. Security Metrics Guide for Information Technology Systems ," tech. rep., Gaithersburg, MD, United States, July 2003.

[14] G. Barbara and A. R. Edward, "SP 800-12. An Introduction to Computer Security: The NIST Handbook ," tech. rep., Gaithersburg, MD, United States, October 1995.

[15] C. Vasilescu, "Trends and Advances in the Information Assurance Analysis Using Synthetic Evaluation Metrics," (Brasov), Romanian National Defense University, Regional Department of Defense Resources Management Studies, 2008.

[16] A. Chakraborty, A. Sengupta, and C. Mazumdar, "A Formal Approach to Information Security Metrics," in *2012 Third International Conference on Emerging Applications of Information Technology*, pp. 439–442, IEEE, 2012.

[17] S. C. Payne, "A Guide to Security Metrics," *SANS Institute Information Security Reading Room*, 2006.

[18] W. Jansen, "NISTIR 7564: Directions in security metrics research," tech. rep., 2010.

[19] M. Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, "Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard," *International Journal of Cyber-Security and Digital Forensics*, vol. 1, no. 4, pp. 280–288, 2015.

[20] E. Yasasin and G. Schryen, "Derivation of Requirements for IT Security Metrics-An Argumentation Theory Based Approach," *ECIS 2015 Completed Research Paper*, 2015.

[21] A. McIntyre, B. Becker, and R. Halbgewachs, "Security metrics for process control systems," *Sandia National Laboratories, Sandia Report SAND2007-2070P*, 2007.

[22] R. Savola, "Towards a Taxonomy for Information Security Metrics," pp. 28–30, ACM, 2007.

[23] M. Talabis, J. Martin, and E. Wheeler, *Information Security Risk Assessment Toolkit: Practical assessments through data collection and data analysis.* Amsterdam: Elsevier, 2013.

[24] Committee on National Security Systems, "National Information Assurance (IA) Glossary ," *CNSS Instruction No. 4009*, 2010.

[25] ISO, "ISO/IEC JTC 1/SC 27 - IT Security techniques."

[26] Z. Yazar, "A qualitative risk analysis and management tool-CRAMM," *SANS InfoSec Reading Room White Paper*, 2002.

[27] J. F. Broder and E. Tucker, *Risk analysis and the security survey*. Amsterdam;Waltham, MA;: Butterworth-Heinemann, 4th ed., 2012.

[28] British Standard and IEC, "Hazard and operability studies (hazop studies)—application guide," 2003.

[29] F. Filip, "Theoretical Research on the Failure Mode and Effects Analysis (FMEA) Method and Structure," in *4th International Conference on Manufacturing Engineering, Quality and Production Systems*, pp. 176–181, 2011.

[30] J. O. Aagedal, F. Den Braber, T. Dimitrakos, B. A. Gran, D. Raptis, and K. Stolen, "Model-based Risk Assessment to Improve Enterprise Security," pp. 51–62, IEEE, 2002.

[31] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," *Pittsburgh, PA, Carnegie Mellon University*, 2003.

[32] Club de la Sécurité de l'Information Français (CLUSIF), "MEHARI 2010: Fundamental Concepts and Functional Specifications," August 2010. Accessed: 2016-06-10, `https://www.clusif.asso.fr/en/clusif/present/`.

[33] Office of Rail Regulation, "Common Safety Method for risk evaluation and assessment," March 2015. Accessed: 2016-07-12, `http://orr.gov.uk/__data/assets/pdf_file/0006/3867/common_safety_method_guidance.pdf`.

[34] F. Baiardi, C. Telmon, and D. Sgandurra, "Hierarchical, model-based risk management of critical infrastructures," *Reliability Engineering & System Safety*, vol. 94, no. 9, pp. 1403–1415, 2009.

[35] G. Henderson, R. Sawilla, S. Matwin, E. Bacic, L. Tremblay, J. Sayyad-Shirabad, and E. N. de Souza, "Automated risk management system," 2012.