HAL
open science

Segmentation and segregation mechanisms and models to secure the integration of Industrial control Systems (ICS) with corporate system

Khaoula Es-Salhi

To cite this version:

Khaoula Es-Salhi. Segmentation and segregation mechanisms and models to secure the integration of Industrial control Systems (ICS) with corporate system. Systems and Control [cs.SY]. Ecole nationale supérieure Mines-Télécom Atlantique, 2019. English. NNT : 2019IMTA0143 . tel-02298847

HAL Id: tel-02298847

https://theses.hal.science/tel-02298847v1

Submitted on 27 Sep 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THESE DE DOCTORAT DE

L'ÉCOLE NATIONALE SUPERIEURE MINES-TELECOM ATLANTIQUE
BRETAGNE PAYS DE LA LOIRE - IMT ATLANTIQUE
COMUE UNIVERSITE BRETAGNE LOIRE

ECOLE DOCTORALE N° 601
Mathématiques et Sciences et Technologies
de l'Information et de la Communication
Spécialité : *Informatique*

Par
Khaoula ES-SALHI

Segmentation and Segregation mechanisms and models to secure the integration of Industrial Control Systems (ICS) with Corporate system

Thèse présentée et soutenue à IMT Atlantique, le 11 juillet 2019
Unité de recherche : Lab-STICC
Thèse N° : 2019IMTA0143

Rapporteurs avant soutenance :

Ana Cavalli	Professeur, Télécom SudParis
Eric Zamaï	Maître de conférences HDR, Grenoble INP

Composition du Jury :

Examinateurs :	Ana Cavalli	Professeur, Télécom SudParis	(Rapporteur)
	Eric Zamaï	Maître de conférences - HDR, Grenoble INP	(Rapporteur)
	Ahmed Meddahi	Professeur, IMT Lille Douai	**(Président)**
	Laurent Nana	Professeur, Université Bretagne Occidentale	
Directeur de thèse :	Nora Cuppens	Directeur de recherche, IMT-Atlantique	
Co-encadrant :	David Espes	Maître de conférences, Université de Bretagne Occidentale	

Dedicated to
my parents, my husband, my sisters
my brothers, and my son for ***1001*** *reasons.*

Abstract

Industrial business world has a real need to integrate industrial control systems (ICS) with Corporate systems. The integration of these two systems has a lot of advantages such as increased visibility of industrial control system activities, ability to use business analysis to optimize production processes and gaining more responsiveness to the business requirements and decisions to achieve more business competitiveness. For example, ERP and CRM systems can directly interact with industrial processes to adjust production based on actual needs, customer orders, stock and energy or raw material (oil, electricity, steel ...) cost.

However, this integration introduces multiple security problems. Indeed, ICS systems have been designed with no security in mind because they have usually been isolated. This ranges from the use of insecure protocols and technologies to the lack of policies and human resources training on cyber-security practices. Therefore, integration exposes both ICS and Corporate Systems to major security threats. Unfortunately, known IT security practices can not be directly applied to ICS systems because the two types of systems are different by nature and have different requirements in terms of operation and security.

This thesis studies the integration of ICS with Corporate systems from a security standpoint. Our goal is to study integrated ICS systems security vulnerabilities and suggest models and mechanisms to improve their security and protect them against ceyberattacks.

After conducting a study on the vulnerabilities of integrated ICS systems (IICS) and the existing security solutions, we focused on the study of defence in depth technique and its applicability to integrated ICS systems. We defined a new generic segmentation method for IICS, “SONICS”, which simplifies the segmentation of IICS by focusing only on those aspects that are really significant for segmentation.

We next developed an improved version of SONICS, RIICS (Risk based IICS Segmentation), a segmentation method for IICS systems that fills the SONICS gaps by focusing on risk on top of technical and industrial specifications.

To complete the segmentation method, we studied segregation and access control solutions. We studied the use of DTE (Domain and Type Enfoncement) access control for integrated ICS segregation. We extended the initial DTE model and formalized it to define a new flow control model for integrated ICS systems. We provided a generic but extensible access control policy based on the generic functional model provided by the ISA95 standard. This generic policy aims to simplify the deployment of DTE access control and provide a good introduction to DTE concepts.

Résumé

Le monde de l'entreprise industrielle a un réel besoin d'intégrer les systèmes de contrôle industriel (ICS) aux systèmes d'entreprise. L'intégration de ces deux systèmes présente de nombreux avantages tels qu'une visibilité améliorée des activités du système de contrôle industriel, une capacité d'utiliser les techniques de Business Intelligence pour optimiser les processus de production et acquérir une plus grande réactivité aux exigences et aux décisions Business pour atteindre une plus grande compétitivité commerciale.

Cependant, cette intégration introduit de multiples problèmes de sécurité. En effet, les systèmes industriels ont été conçus sans aucune sécurité, car ils ont généralement été isolés. Cela inclut l'utilisation de protocoles et de technologies peu sécurisés et l'absence de politiques de sécurité et de formation des ressources humaines sur les bonnes pratiques en cybersécurité. Par conséquent, l'intégration expose à la fois les ICS et les systèmes d'entreprise à des menaces de sécurité majeures. Malheureusement, les pratiques connues en matière de sécurité des IT (Information Technologies) ne peuvent être appliquées directement aux systèmes ICS parce que les deux types de systèmes sont différents par nature et ont des exigences fonctionnelles, opérationnelles et de sécurité différentes.

Cette thèse étudie l'intégration des systèmes ICS avec les systèmes d'entreprise d'un point de vue sécurité. Notre objectif est d'étudier les vulnérabilités de sécurité des systèmes industriels intégrés et de proposer des modèles et des mécanismes pour améliorer leur sécurité et les protéger contre les attaques complexes.

Après avoir réalisé une étude sur les vulnérabilités des systèmes ICS intégrés (IICS) et les solutions de sécurité existantes, nous nous sommes concentrés sur l'étude de la technique de défence en profondeur et son applicabilité aux systèmes ICS intégrés. Nous avons alors défini une nouvelle méthode générique de segmentation pour les IICS, "SONICS", qui permet de simplifier la segmentation des IICS en se concentrant uniquement sur les aspects qui sont réellement significatifs pour la segmentation.

Nous avons ensuite développé une version améliorée de SONICS, RIICS (Risk based IICS Segmentation), une méthode de segmentation pour les systèmes IICS qui comble les lacunes de SONICS en se concentrant sur le risque en plus des spécificités techniques et industrielles.

Pour compléter la méthode de segmentation, nous avons étudié les solutions de ségrégation et de contrôle d'accès. Nous avons étudié l'utilisation du contrôle d'accès DTE (Domain and Type Enfoncement) pour la ségrégation des ICS intégrés. Nous avons étendu le modèle initial de DTE et l'avons formalisé pour définir un nouveau modèle de contrôle des flux pour les systèmes ICS intégrés. Nous avons proposé une politique de contrôle d'accès générique mais extensible basée sur le modèle fonctionnel générique fourni par la norme ISA95. Cette politique générique vise à simplifier le déploiement du contrôle d'accès DTE et à fournir une bonne introduction aux concepts DTE.

Acknowledgement

I would like to express my sincere gratitude to my thesis supervisor **Nora Cuppens** and my co-supervisor **David Espes** for the continuous support of my Ph.D study and related research, and for having invested their full effort in guiding me. Their advice and encouragement has allowed me to progress, improve and surpass myself.

I would also like to thank my thesis supervision committee members: Prof. **Laurent Nana**, and RD engineer. **Cao Thanh Phan**, for their insightful comments, encouragement, and questions.

My sincere thanks also goes to the members of the Jury who honoured me by evaluating and validating my work. A special thanks to Mrs **Ana Cavalli**, and Mr **Eric Zamai** for accepting to be the rapporteurs of this work.

Furthermore, I would like to thank all the members of our team: permanent staff, post-doctoral fellows, doctoral students, interns as well as all the staff at IMT Atlantique for the good working atmosphere.

I would also like to thank my family, for supporting me spiritually throughout this thesis.

Last but not the least, a special gratitude I give to my caring, loving, and supporting husband, Mostafa. Your encouragement and support are much appreciated and duly noted.

Thank you all, this work could not have been completed without your participation.

Contents

1 Introduction **1**

1.1 Context and Motivations 1

1.2 Contributions 2

1.3 Organization of the dissertation 4

2 IICS Reference Architecture **7**

2.1 Introduction 7

2.2 Existing ICS systems architectures 8

2.2.1 Industrial sectors 8

2.2.2 Geographical distribution 9

2.3 IICS reference architecture 10

2.3.1 Level 4: Enterprise and business system 12

2.3.2 Level 3: Operational Management 12

2.3.3 Level 2 : Supervisory Control 13

2.3.4 Level 1: Local or Basic Control 14

2.3.5 Level 0: Industrial Process 15

2.4 Communication flows 15

2.5 Conclusion 15

3 Problem & State of the Art **19**

3.1 Existing ICS systems security problems 19

3.1.1 Architectural and technological security problems 20
3.1.2 Human and Policy related security problems 21
3.1.3 Impact of ICS security issues 23
3.2 Integration security challenges 25
3.2.1 ICS and Corporate systems have different security expectations 25
3.2.2 Technical security challenges 25
3.2.3 Policy security challenges 26
3.3 Existing solutions 27
3.3.1 Policy measures 27
3.3.2 Technological measures 30
3.4 IICS segmentation 33
3.4.1 Problem statement 33
3.4.2 Existing segmentation methods and models 34
3.4.3 Discussion 38
3.5 IICS segregation 38
3.5.1 Industrial access control solutions 40
3.5.2 New industrial secure protocols 40
3.5.3 Industrial firewalls 41
3.5.4 DTE 43
3.6 Conclusion 43

4 SONICS segmentation method 45

4.1 Introduction 45
4.2 SONICS: the IICS segmentation method 46
4.2.1 The principle 46
4.2.2 The IICS Meta-Model 47
4.2.3 IICS Segmentation Constraints 54
4.2.4 Selecting the potential zones to keep 55

4.2.5 Formalization 57
4.2.6 SONICS Tool 60
4.3 Application and Results 63
4.3.1 Test methodology 63
4.3.2 Test systems 64
4.3.3 Results and Discussion 66
4.4 Conclusion 67

5 RIICS: Risk based IICS segmentation Method 69

5.1 Introduction 69
5.2 Risk Analysis applied to IICS 70
5.2.1 EBIOS Method for IT risk assessment 71
5.2.2 EBIOS Method for IICS risk assessment 73
5.3 Risk based IICS segmentation Method 74
5.3.1 The principle 74
5.3.2 Analysis and modelling 74
5.3.3 Segmentation 79
5.4 Tests and validation 84
5.4.1 Results and Discussion 84
5.5 Conclusion 84

6 DTE Access control model for IICS systems 87

6.1 Introduction 87
6.2 Data Type Enforcement concepts 89
6.2.1 DTE 89
6.2.2 DTE Firewalls 90
6.3 DTE access control Model 90
6.3.1 Security policy definition 91

6.3.2 Domains communication 97
6.4 Access control 100
6.4.1 DTE Hosts 100
6.4.2 Operating procedure 101
6.4.3 DTE Hosts access control 101
6.4.4 Firewall access controls 101
6.4.5 Sharing definitions and rules 102
6.5 Application of DTE access control to IICS 105
6.5.1 Functional Model 105
6.5.2 Generic policy 106
6.6 Discussion 112
6.6.1 Advantages 112
6.6.2 Possible improvements 113
6.7 Conclusion 114

7 Conclusions and Perspectives 117

7.1 Perspectives 119
7.1.1 Segmentation methods validation 119
7.1.2 Implement and test DTE access control 119
7.1.3 Extend our segregation solution with VPN 120
7.1.4 Work on other security techniques 120

A Résumé en français 121

A.1 Introduction 121
A.2 Les Contributions 122
A.3 SONICS: Une nouvelle méthode de segmentation 124
A.3.1 SONICS: Le principe 125
A.3.2 SONICS: Le méta-modèle 125

A.3.3 Outil de segmentation 127
A.3.4 Méthodologie de test 129
A.4 RIICS: Une méthode de segmentation basée sur le risque 130
A.5 Modèle de contrôle d'accès DTE 132
A.5.1 Le modèle DTE 133
A.5.2 Mode opératoire 134
A.6 Application du modèle DTE aux IICS 135
A.7 Conclusion 136

List of Publications **137**

List of Figures **140**

List of Tables **141**

Bibliography **149**

CHAPTER 1 Introduction

This chapter presents the context and the motivations of this thesis, as well as the problem we addressed. We will present the main contributions made during these three years of research work before we detail the structure of this manuscript.

1.1 Context and Motivations

Nowadays, one of the major challenges in industrial business world is integrating industrial control systems (ICS) with Corporate systems and keeping the integrated system secured. Industrial business world presently has a real need to integrate industrial control systems with Corporate systems [Keith Stouffer and Hahn 2015, ISA 2013, of France 2013]. The integration of these systems has a lot of advantages such as increased visibility of industrial control system activities and ability to use business analysis to optimize production processes. For example, ERP and CRM systems can communicate with industrial processes to adjust production based on actual needs, customer orders, stock and energy or raw material cost (oil, electricity, steel ...)... ICS and Corporate systems integration ensures more responsiveness to the business requirements and decisions which means more business competitiveness [GSM 2014, Drias et al. 2015].

However, this integration introduces multiple security problems [JUN 2010, GSM 2014, ANSSI 2013]. Unlike Corporate systems that were designed to be protected against malevolence, ICS systems were essentially designed to protect against failure. Cyber-security was definitely not an aspect to take into account in ICS systems because they have mostly been based on private isolated networks [ISA 2013, Keith Stouffer and Hahn 2015]. The only security topics that might have been addressed would be related to physical security and safety. Therefore, existing ICS systems are very predisposed to security problems. This ranges from human and organizational problems such as the lack of staff training and security policy, to infrastructure and architectural problems such as the use of unsecured protocols and the lack of considera-

tion of security in architecture and design [Keith Stouffer and Hahn 2015, CSSP 2009, Kim 2012]. For example, some devices are implemented with no security capabilities (authentication and encryption ...) at all. Some others come with inadequate security properties such as hard coded passwords on their firmware. They therefore cannot be efficiently secured.

Therefore, integrating ICS and Corporate systems exposes both of them to major security threats [GSM 2014, CSSP 2009]. Unfortunately, securing the integration is quite challenging. In fact, most known IT (Information Technologies) security practices can not always be applied to ICS systems because the two types of systems are different by nature and have different requirements in terms of operation and security. On one hand, protecting business data to ensure integrity and confidentiality is the primary need in Corporate systems. On the other hand, availability and responsiveness of real-time critical industrial processes are the main requirements in ICS systems. In addition, ICS and enterprise worlds have always been regarded as totally two separate systems. They have always been using different mechanisms, different technologies, different protocols... and are, more importantly, not designed to integrate with each other from a security point of view. ICS teams have unfortunately no knowledge about cyber-security and IT security specialists have insufficient knowledge about industrial systems. Therefore, securing the integration is really challenging.

In the meantime, securing integrated ICS systems is becoming one of the most urgent concerns that disquiets not only all industrial actors but also governments. Very important number of industrial entities and infrastructures are so critical that any successful cyber attack on these entities can cause huge damage to business, to environment and more severely to national security and people safety [Keith Stouffer and Hahn 2015, Huang et al. 2009].

This thesis studies the ICS systems and Corporate systems integration from a security standpoint. Our goal is to study integrated ICS systems vulnerabilities and suggest new models and mechanisms to improve their security while maintaining the nominal functioning of the systems.

1.2 Contributions

The first part of our work was to elaborate a state of the art study of Integrated ICS (IICS) systems vulnerabilities as well as existing security countermeasures and solutions. We set up a reference architecture of Integrated ICS systems to be the basis of our work and help us to identify more precisely vulnerabilities and solutions

with a special focus on Architecture and Design vulnerabilities, Communication and Network vulnerabilities and Policy and Procedure vulnerabilities. For each identified vulnerability we extracted the solutions proposed by other research works, compared them and evaluate their sufficiency to achieve security objectives, their maturity, and their implementability [Khaoula et al. 2016].

Defense-in-depth is one of the measures we studied. It is one of the most important security techniques that are strongly recommended for Integrated ICS systems. Unfortunately, we could not find detailed and precise information about how to implement it. Defense-in-depth is mainly based on segmentation and segregation. Segmentation is the operation of segmenting a system into multiple security zones that can be separately controlled, monitored and protected. Segregation is controlling communication through the security zones boundaries based on a set of predefined rules. The segmentation of an IICS (Integrated ICS) may be based on various types of characteristics such as functional characteristics, business impact, risk levels, or other requirements defined by the organization. Although many research works have proposed some segmentation solutions, these solutions are unfortunately not generic enough and do not sufficiently take into account all of the IICS specificity such as their heterogeneous technical and functional nature as well as real industrial constraints and conditions. Besides, the aspects that should be considered for segmentation are not obvious.

Therefore, We defined a new generic IICS Segmentation method “SONICS” that aims to simplify IICS segmentation. This new method is based on a simple meta-model of IICS systems that allows to describe systems’ elements by focusing only on aspects that are really meaningful for segmentation. Some of the meta-model aspects require performing a risk analysis to describe more precisely the system. The method itself consists of multiple cycles where new potential security zones are progressively identified based on one aspect of the meta-model at a time. The new identified zones are kept or not depending on a constraints analysis performed on IICS elements that are involved in the new potential zones. The constraints analysis allows to check that the creation of a new identified zone does not lead to a violation of the system's functional requirements nor to a technical cost overrun [Khaoula et al. 2017, Khaoula et al. 2018b].

The next step was to extend the method to cover more security aspects. We believe that the concept of risk is one of the best ways to characterize a system’s components from a security standpoint. We therefore created RIICS (Risk based IICS Segmentation), a new segmentation method for IICS systems that fills the gaps of SONICS and tries to simplify security zones identification by focusing on systems technical industrial specificities and risk. The risk associated with data, components or processes is assessed using a slightly adapted version of the EBIOS risk assessment method for

which the risk is based on the probability and gravity of the possible threat scenarios [Khaoula et al. 2018a].

Furthermore, defense-in-depth can not only be achieved with segmentation. Identifying security zones is necessary but not enough. Communication flows through the zones boundaries have to be filtered. We are therefore convinced that our segmentation method should be completed by a segregation solution.

The issue with ICS integration represents a new use case in terms of flow filtering mechanisms. When integrating the two systems, it is necessary to:

- Apply strict controls on all flows, especially on communication with other networks
- Respect the timing requirements of industrial systems
- Allow to customize packet inspection to extend supported protocols
- Simplify the definition of control rules to make it easier for administrators, especially industrial system administrators because they are less familiar with security concepts.

We therefore setup about studying possible segregation solutions to improve flows controls of integrated ICS systems. We decided to use and enhance the Domain and Type Enforcement (DTE) access control for Integrated ICS segregation. DTE is an access control mechanism that holds promise to provide needed flexibility to respond to the requirements listed above. We have extended the original DTE model, and formalized it to define a new model of flow controls for integrated systems. We also proposed a generic but extensible access control policy based on the generic functional model provided by ISA95. This generic policy is intended to simplify the deployment of DTE access control and provide a good introduction to the concepts of domains and types of packets for administrators.

1.3 Organization of the dissertation

Chapter 2 – IICS Reference Architecture – ICS systems configurations are numerous and cannot be covered by a single study. We therefore had to limit the scope of the study by defining a reference architecture to be the basis of our research. It will be presented in Chapter 2.

Chapter 3 – Problem & State of the Art – This chapter provides a state of the art study of the existing ICS systems vulnerabilities and security countermeasures.

We carried out an in-depth review of vulnerabilities and solutions. We classified them and identify issues that are not yet fully covered.

Chapter 4 – SONICS segmentation method – This chapter focuses on our Segmentation Method **SONICS**. It formalizes and explains the main concepts of the method, and presents the test tools and results.

Chapter 5 – RIICS: Risk based IICS segmentation Method – This chapter presents RIICS an improved version of the SONICS method, that takes into account more aspects for segmentation.

Chapter 6 – DTE Access control model for IICS systems – This chapter presents our study of using DTE for controlling ICS and Corporate systems flows. We present our new DTE model and a generic ruleset based on the generic model provided by ISA95 [ISA 2004].

Chapter 7 – Conclusions and Perspectives – This chapter concludes the dissertation by summarizing the contributions and presenting the different perspectives for possible further work.

CHAPTER 2 IICS Reference Architecture

2.1 Introduction

"*Industrial Control System*" (ICS) is a general term that encompasses several types of control systems used in industrial production, including *Supervisory Control And Data Acquisition* (SCADA) *systems* [Cai et al. 2008, Boyer 2009], *Distributed Control Systems* (DCS), and other control system configurations often found in industrial sectors and critical infrastructures [Keith Stouffer and Hahn 2015].

Integrating an ICS system with a Corporate system consists of interconnecting components from the ICS system to components from the Corporate system for some functional or technical purpose ensuring their communication, their interoperability, their security as well as the whole system security [Cai et al. 2008, Huang et al. 2009, Ten et al. 2010]. Unfortunately,Integrated ICS systems are very different from one organization to another. The components to interconnect from both sides depend on the organizations functional and technical needs. For example, business specialists may need more visibility on industrial activity to be able to make more appropriate decisions. Business analysts may want to interconnect their business intelligence tools to the industrial system to make use of these tools capabilities. There are also several other technical interconnections that may be needed for urbanization or cost optimization such as printing streams, DNS, emailing flows [GSM 2014]... Not only the integration requirements differ from one organization to another, but existing ICS and Corporate systems architectures are also so various that studying all the possible configurations is unthinkable.

Therefore, to study Integrated ICS security topics, we set up a reference architecture that was used as the basis of our studies. It is, moreover, itself a useful asset for researchers, engineers and architects who are interested in ICS and Corporate systems integration.

For the rest of this document, we will use the term "IICS" to refer to "integrated ICS". An IICS is an ICS that is integrated with its organization's Corporate system.

2.2 Existing ICS systems architectures

ICS systems have various architectures and infrastructure configurations depending on different aspects such as the industrial sector, the production activities or the size of the organization.

2.2.1 Industrial sectors

Industrial sector affects industrial system properties and needs and has a direct impact on the infrastructure configuration and architecture of an ICS. There are two main industry sectors as illustrated in Figure 2.1 [Force and Initiative 2013]:

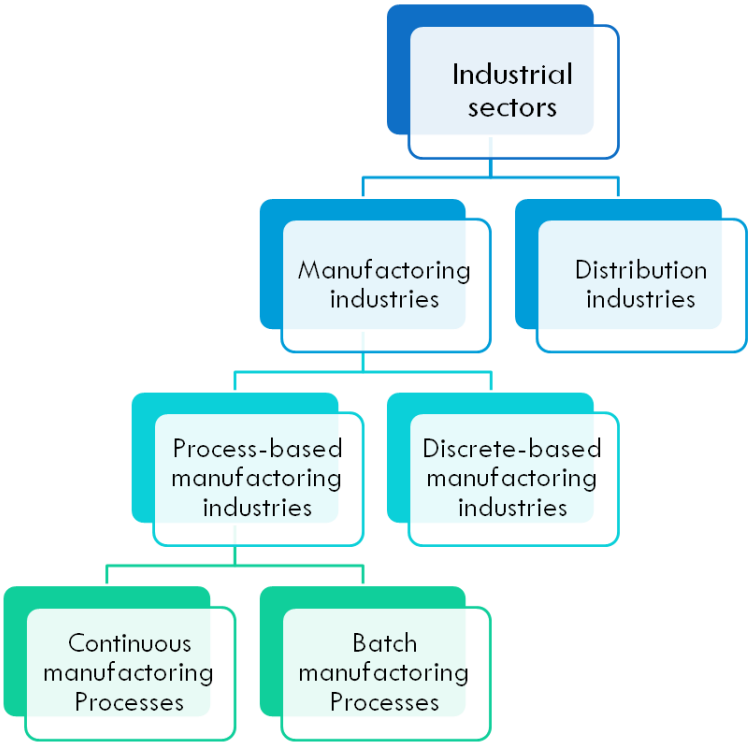

Figure 2.1 – The main industrial Sectors.

- **Manufacturing industries**

  In this type of industry, the main activity of a plant is the manufacturing of some type of goods. There are two types of manufacturing industries:

  - **Process-based manufacturing industries**

    They include *Continuous manufacturing processes* such as fuel and steam flow in a power plant, and *Batch manufacturing processes* such as Food manufacturing.

  - **Discrete-based manufacturing industries**

    They conduct a series of steps on a single device to create the end product as in electronic and mechanical parts assembly.

- **Distribution industries**

  Include all distribution based industries such as water distribution and wastewater collection systems.

The two industry families have different characteristics and needs. For example, in terms of localization, manufacturing industries are usually located within a confined factory or plant-centric area, whereas distribution industries are geographically dispersed. Besides, communication in manufacturing industry are usually performed using LAN while distribution industry systems usually communicate through WAN [Keith Stouffer and Hahn 2015, ISA 2013].

2.2.2 Geographical distribution

Geographical distribution is a key aspect that directly impacts an ICS architectural configuration. There are three types of ICS systems [ANSSI 2013, ISA 2012] with regard to this aspect as illustrated in Figure 2.2:

Figure 2.2 – The types of ICS systems according to geographical distribution.

- **Distributed control systems**

  Distributed control industrial systems control multiple industrial equipments and

subsystems that are scattered over a large geographical extent (such as a region or a country territory). To communicate with each other, the subsystems are mainly interconnected using wired or wireless WAN infrastructures (Satellite, GSM, Internet...). This type of control systems are usually found in transport, railways, electricity and water distribution industries.

- **Local industrial control systems**
  This control systems of this type have a limited geographical extent (usually within one building). They very often contain a local area network (LAN) usually based on Ethernet/TCP/IP. The LAN provides a unified communication link between all the components of the network. This type of systems is used in process-based manufacturing industries such as food manufacturing.

- **Isolated manufacturing machinery**
  Some manufacturing systems do not need to be connected with a network as they already integrate all the needed components (sensors, actuators, programmable automate...) and thus are completely autonomous. Only direct point to point communication by means of serial cable or USB is possible when it is needed to program the system or update its firmware.

2.3 IICS reference architecture

To state the problem clearly, we chose to focus our research works on "Local Manufacturing industrial control" systems. Therefore we set up a reference architecture of a quite representative system to be the basis of our studies.

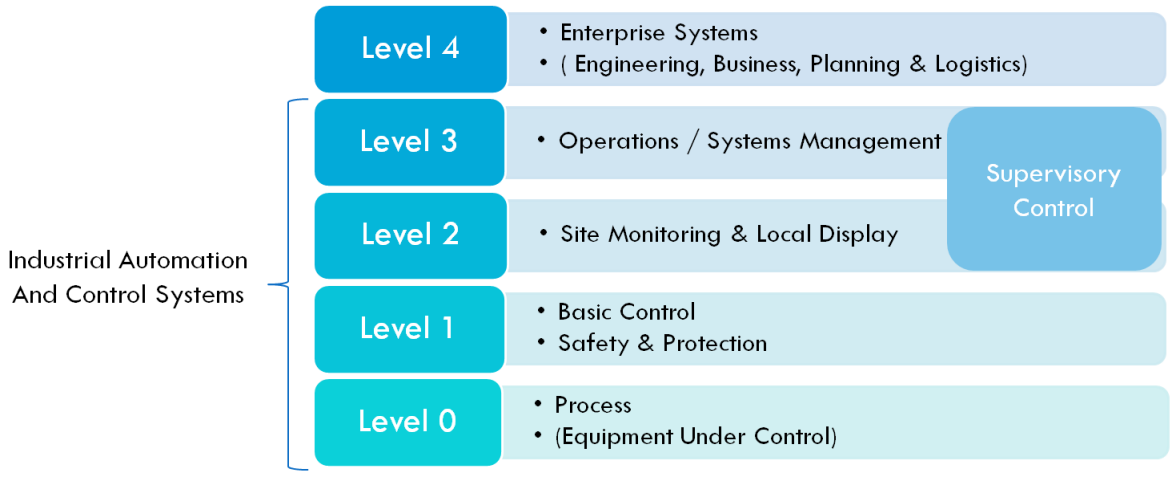

Figure 2.3 – Functional Hierarchical model [ISA95] [ISA 2004].

Our reference architecture is based on the standardized hierarchical functional model provided by ISA-95 [ISA 1999]. This model (Figure 2.3) depicts the different functional levels of Integrated ICS systems and highlights the relationship between Business and Industrial activities. In other words, it provides a high level picture of the functional architecture of an IICS with a special focus on the ICS and Corporate system functional integration at the interface between Level 4 and Level 3 where industrial and business functions are integrated.

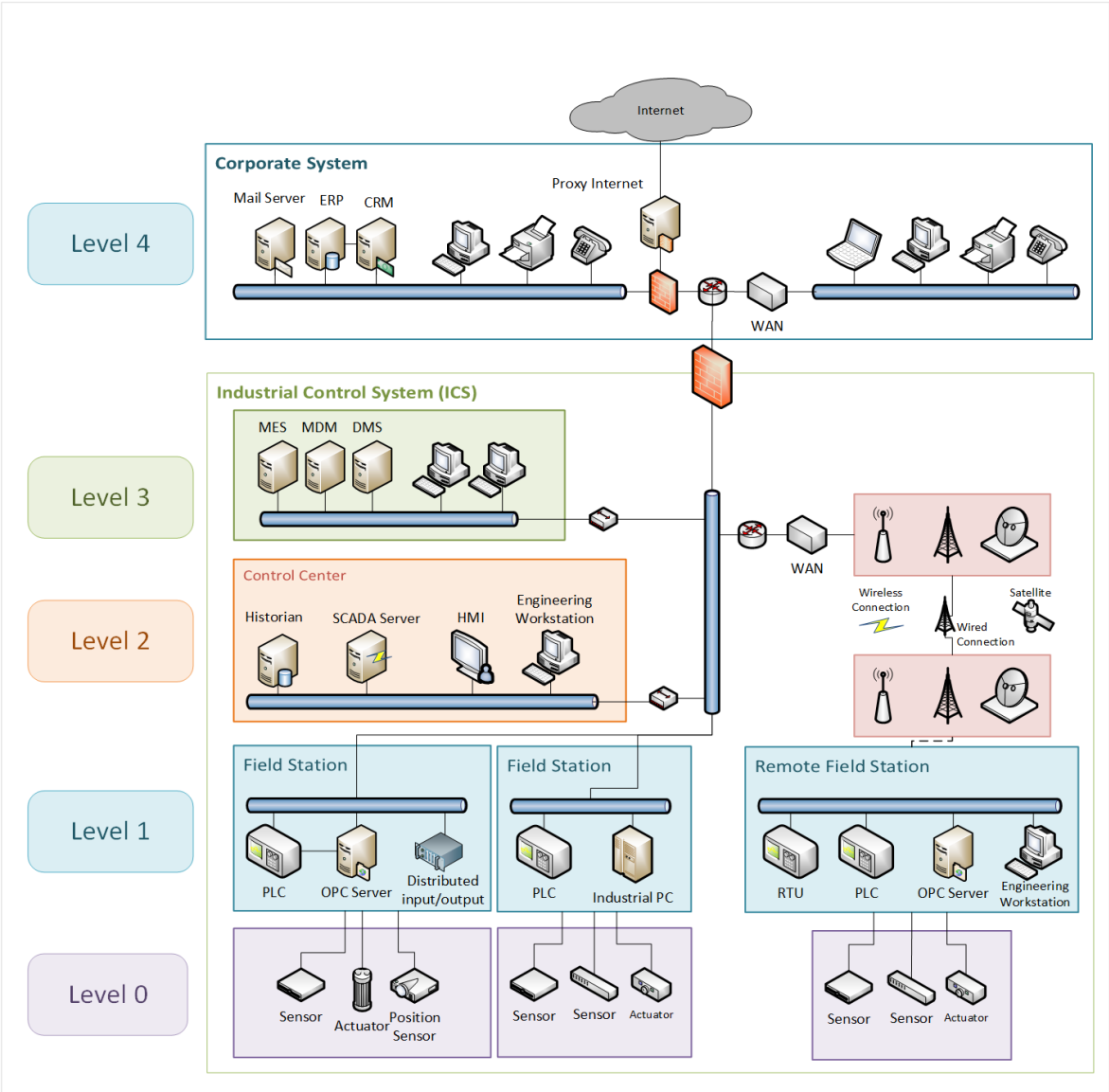

Figure 2.4 – IICS Reference Architecture.

IICS functions involved in the 5 levels listed above, are implemented using multiple software and hardware components. Figure 2.4 provides a quite complete list of these components relating them to the hierarchical model.

2.3.1 Level 4: Enterprise and business system

This level includes the functions involved in the business-related activities as well as management functions. It is the Corporate system zone where lie all the enterprise's components such as IT applications, email servers, ERP systems...

- **CRM:** CRMs are software applications that allow the processing of the sales plan with customers as well as the marketing management. They are generally "front-office" solutions, in opposition to "back-office" tools such as Enterprise Resource Planning solutions (ERP).
- **ERP:** is a category of business-management software, typically a suite of integrated applications that an organization can use to collect, store, manage and interpret data from many business activities (including: product planning, cost, manufacturing or service delivery, marketing and sales, inventory management and shipping and payment).

2.3.2 Level 3: Operational Management

This level includes the functions involved in managing the workflows to produce the desired end products. The main components of this level are:

- **MES:** Manufacturing Execution System (or MOM - Manufacturing Operations Management), is a computerized system used in manufacturing, to track and document a manufacturing process. The aim of an MES is to make the value-adding processes transparent [Kletti 2007]. MES might be seen as an intermediate between an ERP system, and a SCADA or a process control system.
- **MDM:** Meter Data Management is a software system that performs long-term storage, management and processing for the great amount of data delivered by smart metering systems.[Niyato and Wang 2012]
- **DMS:** A Distribution Management System is a collection of applications to monitor and control the entire distribution network in a safe and efficient way. It also serves as an operations platform, automating tasks and filtering information for the operator.[Thierry Godart 2012] DMSs use real-time data and provide all information on a single console at the control centre in an integrated way.

2.3.3 Level 2 : Supervisory Control

This level includes the functions involved in monitoring and controlling the physical process. The main components of this level are:

- **SCADA:** (Supervisory Control and Data Acquisition): It integrates data acquisition systems with data transmission systems and HMI software to provide a centralized monitoring and control system for multiple process inputs and outputs. They are designed to collect field data, transfer them to central computer facility, and display information to the operator graphically or textually. This allows the operator to monitor or control an entire system from a central location in near real time [Boyer 2009]. Supervisory control layer contains the top level components of SCADA to which we refer as control centers.
- **Control Centers:** A Control center is the central part of a SCADA system. It collects and logs information received from other SCADA components and may generate actions based on detected events. It is also responsible of centralized alarming, trend analyses and reporting [Keith Stouffer and Hahn 2015]. It is composed of the following elements:
  - **SCADA control Server:** (Usually called the master): It is a software service which connects with field devices using industrial protocols, exposes acquired supervision data, and sends controls.
  - **HMI**: Used by operators to monitor and control other SCADA components. It is a GUI (Graphical User Interface) that retrieves data from the SCADA server to create visual reports and perform alarming.
  - **Historian**: A data storage server that is used to store history data.
  - **Engineering workstations**: It is a computing unit, generally an ordinary computer, that industrial engineers mainly use to configure industrial control components (especially PLCs and RTUs...).
  - **OPC Classic**: It is a software interface standard that allows Windows programs to communicate with industrial hardware devices. OPC is implemented in server/client pairs.
    - **The OPC server:** It is a software program that converts the hardware communication protocol used by a PLC into the OPC protocol.
    - **The OPC client:** It is any program that needs to connect to an industrial hardware component. It uses the OPC server to get data from or send commands to the hardware.

2.3.4 Level 1: Local or Basic Control

Level 1 includes the functions involved in sensing and manipulating the physical process. It is mainly composed of field sites where a set of controllers are directly connected to the sensors and actuators of the process. This level also includes process monitoring equipment.

- **Field Sites:** Field sites are local or remote and are composed of devices directly responsible of data acquisition, logical operations and controls. a field site contains generally:
  - One or more **PLC** or **RTU** which are central sophisticated devices that interact with sensors and actuators in the site (more details about PLCs and RTUs are provided below).
  - Sometimes, a local computer connected to RTU/PLC for configuration.
  - **PLCs** (Programmable Logic Controller) are digital devices used for automation of industrial electro-mechanical processes. They connect to sensors in the process and convert their signals to digital data.
  - **RTUs** (Remote Terminal Unit) are microprocessor-controlled electronic devices that interface sensors and actuators by transmitting telemetry data to the SCADA Server, and by using messages from the master supervisory system to control connected objects.
  - **Differences between PLC and RTU:**
    * RTUs are considered more suitable for wider geographical telemetry, because RTUs are usually equipped with wireless communication; whereas PLCs are more suitable for local control (in building industry) and are especially designed for output arrangements and multiple inputs.
    * IEC 61131-3 is used more by PLCs, and RTUs use other alternative proprietary tools [Tiegelkamp and John 1995].
      IEC 61131-3 is a part of the open international standard IEC 61131 for programmable logic controllers, and was first published in December 1993 by the IEC. The current (third) edition was published in February 2013. Part 3 of IEC 61131 deals with basic software architecture and programming languages of the control program within PLC. It defines two graphical and two textual programming language standards.

2.3.5 Level 0: Industrial Process

Level 0 is the actual industrial physical process. It includes sensors and actuators directly connected to the process.

2.4 Communication flows

Communication between components is also a very important key aspect to be considered. It especially focuses on physical and logical interconnections between components and on the way they communicate (protocols).

Field data acquisition requires using protocols adapted for real-time communication such as: ModBus, DNP3 and Profinet. Physical communication in SCADA systems is usually based on Ethernet or Serial links. As for communication between ICS and Corporate system components, it depends on the technologies used on both sides. Most commonly, web services, FTP, and SQL are used for business components while other protocols such as SMTP are used for technical needs. Table 2.5 below lists the most common communication flows as well as the most used protocols in an IICS system.

2.5 Conclusion

In order to delimit the scope of our study, we defined a reference architecture to be the basis of our work. This architecture will help us to focus on a single type of ICS architecture, trying to study its security issues and provide some solutions. Studying all ICS architectures as part of a single project is not conceivable because they are very different in terms of functionality, operation and infrastructure. We decided to work with Manufacturing industries under a local industrial control systems, because on one hand, they are widely used, and on the other hand, they are easier to simulate. However, security requirements of manufacturing systems are quite different from other critical infrastructures, despite the similarities they share with them. Manufacturing systems can be attacked at different stages, from early design to the final inspection, anywhere in the supply chain because they are highly integrated into the product's life cycle. The development of effective security solutions for these systems requires specific research [Rosinger and Uslar 2013].

Our reference architecture has been defined in accordance with the standardized hierarchical functional model. We have defined examples of components at each functional level, and we have also set up a grid of communications. This architecture is only

	ERP	Mail Server	MES	Historian	SCADA Server	OPC-Server	Workstations
PLC/RTU	-	-	ModBus RTU ModBus TCP, DNP3 Profibus TCP IP Ethernet IEEE 802.3 Profibus PROFINET (industrial Ethernet)		ModBus RTU ModBus TCP, DNP3 Profibus TCP IP Ethernet IEEE 802.3 Profibus PROFINET (industrial Ethernet)	HTTP XML ModbusTCP TCP IP Ethernet IEEE 802.3 Profibus PROFINET (industrial Ethernet)	Profibus DeviceNet Modbus+ BACnet Arcnet TCP IP Ethernet IEEE 802.3 Profibus PROFINET (industrial Ethernet)
MES	JCA/ web services Specific protocols	SMTP HTTP	-		Specific protocols		-
Historian	Web Services	-	Specific protocols SQL Web Services	-	Specific protocols SQL Web Services		-
SCADA Server	Web Services		Specific protocols	Specific protocols SQL Web Services	-		
Workstations	-	SMTP, HTTP	-	Specific protocols SQL Web Services	Specific protocols Web Services	RPC/DCOM TCP IP Ethernet IEEE 802.3 Profibus PROFINET (industrial Ethernet)	
HMI				Specific protocols SQL Web Services	HTTP Specific protocols		

	Corporate Sysetm - ICS
	Level 3 – Level 2
	Level 2 – Level 1 (SCADA)

Figure 2.5 – Examples of IICS data flows.

a reference “template” that is not necessarily intended to be used in its current form for all our work and tests. It mainly provides a foundation to study generic problems and suggest generic solutions.

CHAPTER 3 Problem & State of the Art

The integration of ICS and Corporate systems raises many security issues if no countermeasures are taken. According to several research works and security guides [Keith Stouffer and Hahn 2015, ISA 2013, of France 2013], Integrated ICS systems may be exposed to a wide range of vulnerabilities. We have studied these vulnerabilities in order to assess the state of the art and identify security issues that are not (or not completely) addressed yet. We are most interested in the vulnerabilities that are directly related to the integration of the ICS.

3.1 Existing ICS systems security problems

ICS and Corporate systems integration introduces multiple security problems. Unlike Corporate systems that were designed to be protected against malevolence, ICS systems were essentially designed to protect against failure [Keith Stouffer and Hahn 2015, ISA 2013]. Cyber-security was definitely not an aspect taken into account in ICS systems because they have mostly been based on private isolated unique networks that used proprietary communication protocols. The only security topics that might have been addressed would be related to physical security and safety [Cherdantseva et al. 2016]. Security was primarily achieved by controlling physical access to system components [DeSmit et al. 2017a, Cruz et al. 2015]. Therefore, existing ICS systems are very predisposed to security problems. Predisposing conditions include human and organizational problems such as lack of staff training or lack of security policy, infrastructure and architectural problems such as the use of unsecured protocols, lack of consideration of security in architecture and design [Keith Stouffer and Hahn 2015, Cruz et al. 2015, Kim 2012].

3.1.1 Architectural and technological security problems

ICS systems have multiple technical and architectural security problems. First, most industrial equipment has no security capabilities (authentication and encryption ...) at all [Cruz et al. 2015]. They sometimes come with inadequate security properties such as hard coded passwords on their firmware [Johari and Sharma 2012, Nicholson et al. 2012]. They thus cannot be efficiently secured. Besides, most protocols used in industrial systems (Modbus/TCP [Drias et al. 2015], Ethernet/IP, DNP3 [Fovino et al. 2010, Drias et al. 2015] ...) are not designed with security in mind and, worse, the most vulnerable among them are sometimes employed despite their known vulnerabilities. For example, DCOM, a protocol used for OPC, uses RPC which opens multiple ports to establish communication making firewalls configuration difficult [Galloway and Hancke 2013]. Furthermore, industrial control systems are increasingly using wireless communications which can introduce additional vulnerabilities [Leith and Piper 2013].

In addition, most of ICS architectures do not make use of segmentation which means that all the components in the system are on the same low level of security [ANSSI 2013]. Authentication, encryption of exchanged and stored data, logging and traceability mechanisms are mostly absent [Obregon 2015]. Even for the most carefully designed ICS systems, cyber-security is not seriously applied. For example, proprietary protocols are mistakenly assumed to be secure and architectural choices tend to be made without taking security aspects into account [DeSmit et al. 2017b].

Technical support and maintenance are more often provided remotely by vendors, eliminating the need for an internal support team. However, this creates a significant angle of attack, especially when vendors' end-users do not comply with the minimal security best practices. For example, vendors sometimes provide systems with dial-up modems to allow remote access in order to reduce the "maintenance burden" of technical support in the field. In many cases, cyber-security controls are not activated by end users simply for practical reasons. In other cases, remote access is provided to support staff with administrator access to the ICS. Some passwords used for remote access are sometimes the same for all the clients and too frequently are not changed by the end users. Password cracking "freeware" can be used to gain access to such systems by exploiting remote access vulnerabilities [Leith and Piper 2013].

Furthermore, with the recent trend of using commercial off the shell (COTS) technologies (especially open protocols such as TCP/IP protocols stack and ordinary windows computers) and Internet of Things (IoT) [Cherdantseva et al. 2016, Evans 2011], ICS systems are more vulnerable than ever before because these technologies are very

well known by attackers. Popular automated software tools used to analyze networks and vulnerabilities, that are of minimal impact on corporate networks, can, in contrast, cause huge damage to ICS networks [Hildick-Smith 2006]. For example, [Leverett 2011] identified 3,920 ICS devices in the United States that were accessible via the Internet in a recent study. ICS devices are therefore subject not only to targeted attacks, but also to inadvertent attacks [Larkin et al. 2014a]. Figure 3.1 illustrates the growth of the number of recorded attacks in relation to the number of exposed devices. Cyber-attacks have drastically increased since the early 1980's. As the number of attacks grows, their visibility decreases and maliciousness increases. Over the past decades, this has been seen in various industrial sectors.

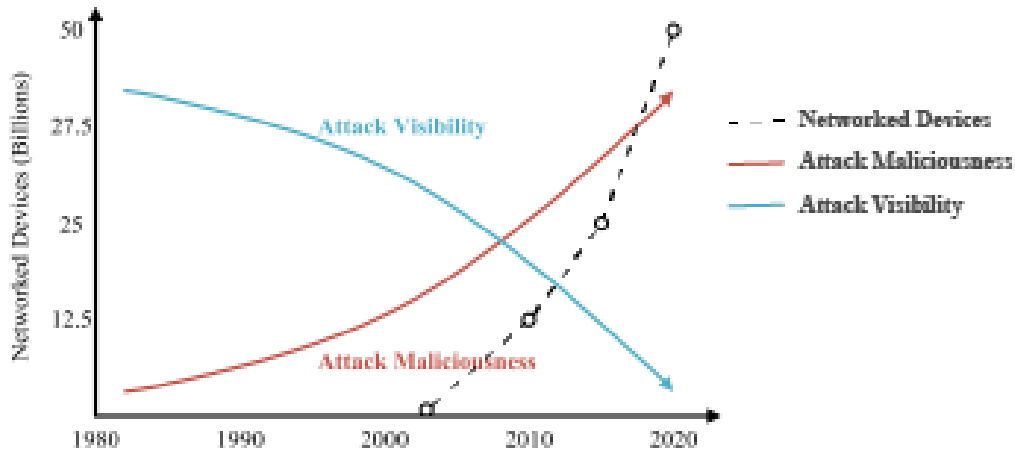

Figure 3.1 – Growth of networked devices [Evans 2011] and cyber-attack visibility and maliciousness trends [Bayuk et al. 2011, Watin-Augouard et al. 2011]

In addition, internet-based Computer Aided Engineering (CAE) tools, such as cloud computing software as a service (SaaS) are being adopted introducing new vulnerabilities [DeSmit et al. 2017b]. And in some cases, there also may be some physical security issues such as unprotected easy to access physical points that can be exploited by malicious persons.

3.1.2 Human and Policy related security problems

ICS security problems are not limited to architectural and technological issues. Human errors are an other important source of vulnerabilities. They may result in unintended attacks, intended internal and external social engineering attacks. Attacks by internal agents are more frequent than attacks by external ones [Henrie 2013, Sacramento 2007, Poulsen 2009].

Human errors are the most exploited angle of attack of most known cyber-security attacks achieved on industrial systems so far [CSSP 2009]. Therefore, even with architectural and technical vulnerabilities addressed, human imprudence remains one of the most threatening source of vulnerabilities.

Actually, the current ICS systems human related security problems are direct consequences of two factors.

Lack of training

There is a serious lack of training and sensitisation among ICS personnel. Training for people working with ICS systems is often limited to industrial practices and promotes misconception about tools and their fallibility [Nicholson et al. 2012] and does not raise engineers and designers'awareness of the threats of cyber-attacks on ICS systems [Wells et al. 2014].

Lack of security policy

ICS generally lack well-defined globally applied security policies that establish suitable security procedures and constrains human resources to adopt convenient security practices. Unlike Corporate systems that are governed by very well established security standards [ISA 2013, Force and Initiative 2013, ANSSI 2013, of France 2013] and controlled by well defined entities (ISD: IT System Department), ICS systems may be managed and maintained by different departments (automation, maintenance, industrial processing, Information Systems Department(ISD)...) and lack standardisation. This heavily contributes to the persisting of human related security vulnerabilities. As a result, the definition of security policy, enforcement procedures and vulnerability checks, risk assessment and system security audit are not carried out. Below some examples of human related issues:

- Using common passwords, [Leith and Piper 2013]
- Using default passwords, [Leith and Piper 2013]
- Using USB sticks passwords,
- Connecting external devices to the ICS network [Leith and Piper 2013]
- Keeping temporary accesses open because of the absence of security supervision [Leith and Piper 2013]
- No screensaver or mandatory log off requirements [Leith and Piper 2013].
- No access rights management giving users the highest level of access. For example, in one large industrial plant, more than 100 technical employees had high-level

access, while after a risk assessment, this number was reduced to 10 employees who really needed that high-level access for their work [Leith and Piper 2013].

- Remote vendors maintenance users access rights. They often are granted high level of access regardless their tasks' requirements [Leith and Piper 2013].

More alarming, as a result of the non-existence of routinely scheduled security checks and attack detection procedures, the median number of days between the onset of a cyber-attack was reported and its detection in an organization was over 200 days [FireEye 2015]. Besides, 69% of the attacks recorded on ICS systems were not discovered by the victims themselves, but by third parties such as law enforcement entities and clients [FireEye 2015].

In summary, current ICS systems combine classical technology vulnerabilities, COTS vulnerabilities, industrial protocols and more importantly human related vulnerabilities. While the situation has changed over the last decade, and a number of standards and directives dealing with the cyber security of SCADA systems have emerged [Cherdantseva et al. 2016], the threat of cyber attacks on ICS systems is not being fully addressed, leaving facilities and entire supply chains vulnerable [DeSmit et al. 2017a].

3.1.3 Impact of ICS security issues

An attack can alter design files or process parameters to bring some parts out of specification. It could also modify the quality control (QC) system to avoid proper quality assessment. Such attacks can disrupt the product, the design process and adversely affect a product's design intent, performance, or quality. The consequences of a security incident, whether related to an attack or an error, may include compliance and legal issues, financial and physical damage. An incident can also result in defective products that do not meet the design specifications. This can result in delays in product launch, equipment failure, increasing warranty costs, loss of clients trust [Wells et al. 2014]. More importantly, such incidents constitute a threat to the human safety of operators and consumers [DeSmit et al. 2017b]. Recent case studies at Virginia Tech have shown the ease of executing such cyber-physical attacks. In the first case study [Wells et al. 2014], the tool path files were modified in a subtractive manufacturing operation, while the design files for an additive manufacturing process were modified in the second case study [Sturm et al. 2014].

Miller and Rowe's [Miller and Rowe 2012] analysis states that the number of cyber attacks against ICS systems increases over time. In 2010, the Industrial Security Inci-

dent Inventory (ISI) identified 161 incidents, with an additional 10 new incidents each quarter. In 2013, the RISI database already contained 240 incidents recorded between 2001 and the end of 2012 [RISI 2013]. In addition, an in-depth study of the current state of cyber-security of ICS systems, based on a series of interviews with a large number of experts, confirmed that cyber threats are really increasing [Henrie 2013]. In addition, the critical manufacturing sector accounted for the most security incidents reported to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in 2015 [ICS-CERT 2015].

Examples of cyber-attacks are quite numerous, expanding across a variety of fields.

In 1982, The "logic bomb" was reportedly inserted in the Trans-Siberian pipeline's control software. This attack changed pump and valve settings, causing a massive explosion [Miller and Rowe 2012].

In 2003, a slammer worm penetrated a network at the Davies-Besse nuclear plant in Ohio [Guan et al. 2011, Patel et al. 2005] and a computer virus named Sobig shut down train signalling systems in Florida [Miller and Rowe 2012].

In 2006, a hacker penetrated the operation system of a water treatment facility in Harrisburg, USA [Guan et al. 2011, Patel et al. 2005] and the Browns Ferry nuclear plant in Alabama was manually shut down due to the overload of network traffic [Nicholson et al. 2012].

In 2007, a dismissed employee installed unauthorised software on the SCADA system of the Tehama Colusa Canal Authority [Miller and Rowe 2012].

In 2010, the Stuxnet computer worm struck the Iranian nuclear facility causing the failure of almost one-fifth of all centrifuges [Miller and Rowe 2012]. Stuxnet allegedly destroyed as many as 1000 Iranian high speed centrifuges used for uranium enrichment. Specifically, the life-spans of these centrifuges were significantly reduced by periodically changing their rotational speeds [Albright et al. 2010, Vincent et al. 2015]. This attack was successful because it was able to display misleading equipment readings (readings indicated no problems) to operators [Cherry and Constantine 2011]. Stuxnet was a game-changer, it attracted the world's attention to cyber threats to ICS systems by drawing a vivid and horrifying picture of the consequences of a cyber attack on industrial systems.

In 2016, there was an attack on a power grid which cut power to over 100,000 people [Tuptuk and Hailes 2016].

These examples demonstrate that no system is beyond the reach of cyber-attackers, and ICS systems are no exception.

3.2 Integration security challenges

Achieving integration, from a security point of view, is laborious because securing ICS with using only known security techniques and solutions is fairly challenging. Integration relies on efforts of both ICS and Corporate systems engineers. However, ICS teams have unfortunately no knowledge about cyber-security and IT security specialists have insufficient knowledge about industrial systems. In addition, addressing the integrated system security needs cannot be accomplished using only known IT security skills because ICS and Corporate systems have very different nature and requirements [(NDIA) 2014, Vincent et al. 2015].

3.2.1 ICS and Corporate systems have different security expectations

ICS and Corporate systems are very different by their nature and have different security properties and expectations. ICS security focuses on availability, plant protection, plant operation, control complexity and time-critical components response while Corporate security mainly focuses on protecting information. In other words, in ICS systems, availability outweighs integrity and confidentiality while these two properties are more important in Corporate systems.

3.2.2 Technical security challenges

ICS OT and enterprise IT systems have always been regarded as totally two separate areas. They have always been using different mechanisms, different technologies, different protocols... and are, more importantly, not designed to integrate with each other from a security standpoint.

While Corporate system remains protectable thanks to the expertise we have in IT technologies security, ICS system can not profit from this knowledge because IT security measures are not directly applicable to industrial systems. ICS systems security expectations are different from Corporate systems and industrial heterogeneous equipment and protocols particularities are not supported by the existing security solutions [Drias et al. 2015, Sicard et al. 2018]. In addition, ICS systems have neither testing nor staging environments to test security measures and perform audit without disturbing "production" industrial processes [DeSmit et al. 2017b]. Unfortunately, duplicating an ICS system for the purpose of testing security solutions is significantly expensive and

technically complicated due to sector inter-dependencies, customized system configurations, and massive use of proprietary protocols still in use [Larkin et al. 2014b].

ICS systems are, also, very demanding in terms of timing requirements since they heavily implement real-time critical exchanges. Because of these very resource-consuming timing requirements and because of the oldness of ICS equipment, industrial control devices usually have very limited memory and computing capabilities to execute security processing such as anti-virus and firewalls. Industrial systems are moreover structurally and operationally constraining for the security updates deployment [Etigowni et al. 2016, Huda et al. 2018a]. Applications and drivers inter-compatibility requires keeping them on very precise not up to date versions which makes security patches installation very complicated. Furthermore, life time of system components is usually 3-4 times longer [Keith Stouffer and Hahn 2015, Cheminod et al. 2013] and equipment renewal has a quite long periodicity (sometimes around 20 years [Obregon 2015, Cheminod et al. 2013, Nicholson et al. 2012, Cherdantseva et al. 2016]) and is relatively expensive which makes industrial systems modernization a difficult decision to make. Even when system modernization is accepted, it is still necessary that industrial equipment manufacturers add security capabilities to their products without altering their nominal operation. On the other side, existing security solutions (firewalls, IDS ...) and techniques (segregation, segmentation, authentication mechanisms...) must also be adapted to industrial systems context [Patel et al. 2005, Cherdantseva et al. 2016].

3.2.3 Policy security challenges

ICS and Corporate systems have always formed two separate entities managed by different teams. Corporate systems security policies are significantly more mature than ICS's ones when they exist. The main difficulty is to define a common security policy that takes into account Corporate and ICS specificity. Corporate security management teams are more qualified to define this common security policy but they do not have enough experience with ICS networks. Defining a concise efficient global IICS security policy is hence far from being straightforward.

In ICS systems, security is often preceded by safety, reliability, robustness and maintainability leaving little or no resources for security goals. In [Park and Lee 2014], the authors discuss a need for an update of well established international security standards such as NIST SP 800-53 and ISO 27001 in order to bring the safety and security requirements together in the context of ICS systems.

3.3 Existing solutions

We conducted an extensive study of integrated ICS systems vulnerabilities as well as the solutions proposed by numerous guides and research works to protect against these vulnerabilities. We tried to evaluate their maturity, their implementability and their efficiency. Our objective was to identify topics and issues that are not yet fully addressed to work on them.

The proposed security solutions and countermeasures can be grouped into three families [ISA 2013] as illustrated in Figure 3.2:

Figure 3.2 – Countermeasures families.

- **Measures on "People":** Assuring personnel awareness and training,
- **Measures on "Process":** Defining security policies and procedures as well as identifying the real security needs,
- **Measures on "Technology":** Securing equipment and technologies.

3.3.1 Policy measures

A range of standards and normative documents attending ICS systems security has been produced over the years. In 2007, the US President's Critical Infrastructure Protection Board and the Department of Energy outlined the steps an organisation must undertake to improve the security of its ICS networks in a booklet named "21 Steps to Improve Cyber Security of SCADA Networks" [of Energy et al. 2007] which provides guidelines to setup security procedures in order to protect critical systems. In 2008, the Centre for Protection of National Infrastructure (CPNI) produced a

Good Practice Guide for Process Control and SCADA Security (CPNI) encapsulating best security practices especially in terms of procedures. In 2008, NIST released a quite complete guide on a wide range of security issues, and technical, operational and management security controls for ICS systems. The guide was updated in 2011 [Stouffer et al. 2011]. In 2013, the European Union Agency for Network and Information Security (ENISA) released the recommendations for Europe on SCADA patching (ENISA, 2013) while in 2014, the North American Electric Reliability Corporation (NERC) developed a wide range of standards covering many aspects of ICS cyber security (NERG, 2014). A more extensive overview of SCADA-related security standards is provided in [Miller and Rowe 2012, Igure et al. 2006, Nicholson et al. 2012] .

According to [Force and Initiative 2013, ISA 2013], effort should be put on defining an IICS security policy that satisfy two main conditions:

- The global IICS security policy should be globally applicable.
- The global security policy should remedy the ICS system security policy problems.

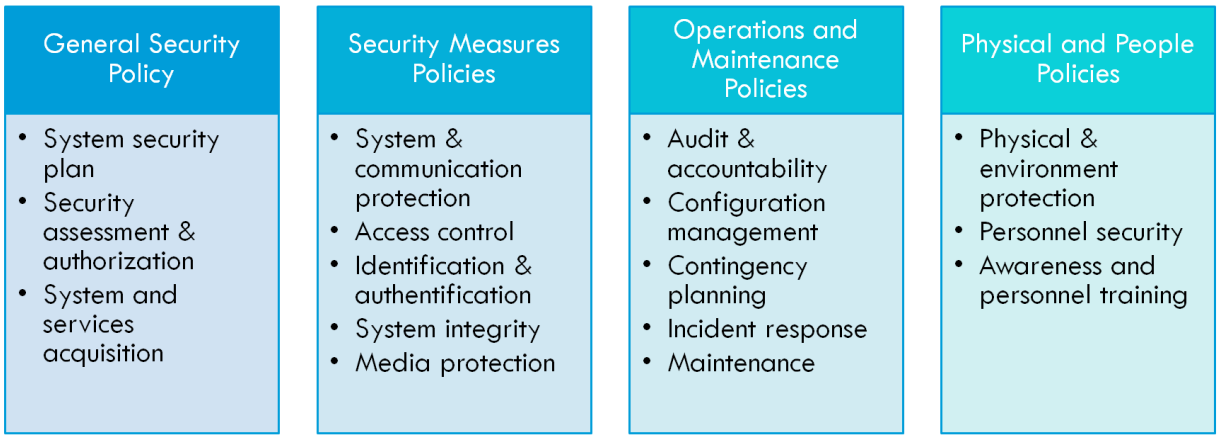

Figure 3.3 – Policy Measures Categories.

ICS security policy and procedures should be established to ensure effective implementation and application of security measures. Policy and procedures reflect applicable federal laws, executive orders, directives, regulations, policies, standards, and guidance" [Force and Initiative 2013]. IICS security policies and procedures should be set up in accordance with the organizational risk management strategy. They can be categorized into four categories (Figure 3.3) depending on the organization's area and the level in which they are applied:

- **General Security Policy**
  The first policy category to establish is the general organization's security policy and procedures. This type of policies should fundamentally address "system security plan" to define security requirements and describe the system, "security assessment and authorization" to define assessment procedures and responsibilities and "system and service acquisition" to manage resources allocation and funding. This category of policies is necessary for integrated ICS as they help to correctly define and validate the security scope.

- **Security Measures Policies**
  The second category is the security measures policies and procedures. This type addresses system and communication protection, access control, identification and authentication, system and information integrity and media protection to regulate architectural and technical security controls. These policies facilitate security solutions design and implementation.

- **Operations and Maintenance Policy**
  As for the third category, it manages operations and maintenance aspects. Policies from this category address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of "audit and accountability", "configuration management", "contingency planning", "incident response" and "maintenance" facets of the system. Integrated ICS systems have to take these policies into account at the design and build time in order to ensure facilitate monitoring and maintenance.

- **Physical and People Policies**
  The last category consists of physical and people policies. This set of policies should focus on "physical and environment protection", "personnel security" and importantly "awareness and personnel training".

Research works and standards that address the issue of Integrated ICS security, generally cover very well "people" and "process" security aspects. Multiple groups of measures are proposed for which important guidance on security policies and procedures is provided. At least, they can be used as a check list that helps to select adequate "people" and "policy" measures for the system to be secured.

3.3.2 Technological measures

Integrated ICS system include both cyber and physical processes. The technological security problems of ICS are related to different levels of the system. They can be associated with low-level elements such as the electronic implementation of devices, or with the protocols design, as well as with the architectural choices and the applicative logic of the components. Many research studies on ICS security have been conducted and many of them have come up with a wide range of solutions that address these different types of problems. The proposed solutions sometimes are generic and at other times very specific. These solutions can be grouped into two groups:

Low level security solutions

ICS communication security

ICS networks are subject to various security problems and can be quite easily attacked [Ashibani and Mahmoud 2017]. Most of the protocols and network equipment used within these systems do not provide an appropriate level of security. For example, most industrial protocols do not provide basic security features such as encryption and authentication.

Therefore, many research projects have been focusing on the security of communications and networks within industrial systems trying to design new solutions that address some of these issues. These studies mainly propose solutions to strengthen the integrity and confidentiality of the communications as well as access controls usually by using low level authentication and authorization mechanisms, but with strong focus on availability and timing requirements.

Some studies such as [Keith Stouffer and Hahn 2015, Shahzad et al. 2015, Diovu and Agee 2017, Diovu and Agee 2017] propose secure industrial protocols often as new versions of the most commonly used industrial protocols. Many others [Premnath and Haas 2015, Vegh and Miclea 2014] propose new authentication mechanisms and key agreement solutions. Attack detection and network access control mechanisms also are very important subjects that are addressed by many research studies [Cheminod et al. 2016, Zvabva et al. 2018, Parra et al. 2019, Li et al. 2018] that propose new firewalls and IDS/IPS solutions. More detailed presentation and discussion of ICS networks security solutions will be provided in section 3.5 as a part of our study of the state of the art on Integrated ICS segregation solutions.

Smart objects and automation tools security

Devices with smart capabilities such as PLCs, actuators, intelligent electronic devices (IEDs) are increasingly being used in modern industrial control systems and are connected over IoT (Internet of Things) platform [Huda et al. 2018b].

Such devices mainly are in charge of collecting and processing data and issuing commands in order to monitor physical industrial processes [Ashibani and Mahmoud 2017]. They sometimes implement quite complex decision making logic to perform supervision, monitoring and control functions to ensure that industrial processes are correctly and optimally executed. For such type of devices, availability, integrity, confidentiality and trust management are important security properties to ensure. However, with small computing capabilities [Li and Da Xu 2017, Lu and Da Xu 2019], theses devices lack important security features such as authentication and encryption which results in serious vulnerabilities as they are connected by Internet and sometimes over wireless networks [Ashibani and Mahmoud 2017].

Many research works have been studying smart industrial objects trying to find solutions for their security issues. A large part of these works propose new lightweight encryption, access control and authentication mechanisms specifically designed to correctly perform despite the limited resources of the smart industrial objects. For example, [Premnath and Haas 2015] presents a new solution to use small cryptographic keys in asymmetric encryption for WSN. [Trappe et al. 2015] propose a lightweight authentication protocol for RFID tags to protect against Electronic Product Key sniffing.

Some other works suggest new mechanisms to implement security for IoTs [Badra and Zeadally 2014, Yan et al. 2017]. For example, [Yang et al. 2017] proposes a Gaussian-mixture model-based detection scheme to mitigate the data integrity attacks. [Hu and Gharavi 2014] propose a new solution based on Merkle-tree based handshaking scheme, while [Saxena et al. 2016] proposes a new authentication and authorisation scheme. Some other research focus on security attacks, such as Denial of Service (DoS) attack [Liu et al. 2013], Man-In-The-Middle attack [Liu et al. 2015] and data integrity attacks [Giani et al. 2013].

High level security solutions

Some studies have opted to address the security issues of IICS with a more high level way by focusing on one or more security aspects over an entire system or subsystem trying to propose new architectures, new methods and new frameworks instead of targeting low level issues and solving specific technical problems in very specific contexts such as securing a protocol, protecting against a type of attack or adding a security feature to some device type. As far as we are concerned, our research works belong to

this type of studies. They consist of proposing new models and mechanisms to improve IICS security.

As examples of this type of research findings, [Sani et al. 2019] proposes a cyber-security framework for IoT-based Energy systems which includes an identity-based security mechanism, a secure communication protocol and an intelligent security system for energy management in order to ensure a suitable level of security. In [Vegh and Miclea 2014], a method of designing a secure cyber-physical system model by combining both cryptography and steganography is proposed. A trust-based approach to create a reliable and secure ICS is proposed in [Saqib et al. 2015]. [Xie and Wang 2014] presents a mutual trust model for inter-system security based on an item-level access-control framework. [Wang et al. 2010] proposes a context-aware security framework for ICS.

Security guides and standards such as such as NIST [Keith Stouffer and Hahn 2015] ISA [ISA 2013, ISA 2001, ISA 2004, ISA 1999] and ANSSI [ANSSI 2013, of France 2013] guides also address high level security topics and propose multiple frameworks and methodologies. They often recommend to combine multiple generic security measures such as authentication and authorization mechanisms, secure protocols, monitoring and logging mechanisms, single point of failure and redundancy techniques [Keith Stouffer and Hahn 2015, Force and Initiative 2013]. They always propose generic security architectures that can be used to strengthen Integrated ICS systems. Defense-in-Depth is one of the their most important recommendations. It is an architectural security technique that consists of implementing multiple layers of defense to protect against security issues [CSSP 2009]. It is implemented by dividing the IICS system into multiple encapsulated security zones to create multiple layers of defense. Defense-in-depth leverages best practices by making use of firewalls, routers with Access Control Lists (ACLs), configured switches, routing configuration and dedicated communications media.

Defense-in-depth is mainly implemented using segmentation and segregation. Segmentation consists of segmenting a system into multiple security zones that can be separately controlled, monitored and protected [WUL 2016]. A security zone (or security segment) is a set of components or sub-systems connected within one sub-network governed by a single authority and one security policy [Mahan et al. 2011]. Any zone can be divided into sub-zones when required for some organizational, technical or security reasons [Jens-Tobias ZERBST 2009]. The security zones must be created with clearly defined boundaries and policy. Components within them must be governed by the same policy [Mahan et al. 2011] and communication between zones must be filtered in accordance with their policies. Segmenting the IICS system into multiple security

zones really assists organizations in creating clear boundaries in order to effectively apply multiple layers of defense to protect against malicious and accidental actions [CSSP 2009]. In general, the system should be closed-looped or air-gapped, and connect the ICS network to Internet only if necessary [Larkin et al. 2014b]. However, researches state that many ICS networks are connected to the Internet, sometimes without the system owner's approval [Leverett 2011]. When connecting the ICS systems to Internet is really needed, defense-in-depth through segmentation and segregation is required.

Unfortunately, we could not find enough details on how to efficiently implement segmentation and segregation in an IICS context. There are still several questions that remain unanswered [CSSP 2009, Keith Stouffer and Hahn 2015]. First, no precise explanation was given on how to partition IICS networks into segments. Should the segmentation be based on the components' physical characteristics, on their functions or on their geographical localization? In addition, although segregation rule-sets definition is not trivial, no sufficient explanation was provided.

We believe that IICS segmentation and segregation are major IICS security topics that need more study. This is why, for our research works, we mainly focused on these two techniques trying to create new models and mechanisms that appropriately meet the actual security needs of integrated ICS systems. A more deep state of the art study of segregation and segmentation will be provided in the next sections.

3.4 IICS segmentation

3.4.1 Problem statement

IICS are heavily functionally and technically heterogeneous. The segmentation of an IICS may be based on various types of characteristics such as functional characteristics, business impact, risk levels, or other requirements defined by the organization. Although many research works [CSSP 2009, WUL 2016] have suggested some zoning solutions, but these solutions are unfortunately not generic enough and do not sufficiently take into account all of the IICS specificities such as their heterogeneous technical and functional nature. Besides, the system's aspects that should be considered for segmentation are not obvious. Should the segmentation be based on the *Components* physical characteristics, their functions or their geographical location? Should we combine more than one characteristic type to achieve segmentation? There is unfortunately currently no method that straightforwardly drives this operation to get accurate results.

Moreover, engineering expertise is not enough to perform IICS segmentation because it may be error-prone and produce inaccurate results. The work may take more time than necessary while some important aspects may be neglected. Using a framework or a working method is always very useful because it guarantees more valuable results more quickly. Although some segmentation solutions have been suggested by some research works [CSSP 2009, WUL 2016], they still are not generic enough. Integrated ICS systems really need a new generic segmentation method that fills all these gaps. This would be a valuable contribution on which we decided to work.

3.4.2 Existing segmentation methods and models

Multiple research works have studied IICS systems segmentation. They can be classified into three categories regarding the approach they take to deal with the segmentation issues as well as the aspects they take into account.

General Security Guides

The first category of the studied documents mainly includes general security guides such as NIST [Keith Stouffer and Hahn 2015] and ISA [ISA 2013, ISA 2001, ISA 2004, ISA 1999] guides and also ANSSI [ANSSI 2013, of France 2013]. They are very valuable resources for initiation to the subject as they present the concepts and provide the needed definitions in a fairly simple way. They all agree that implementing segmentation should be done on a case by case basis based on a risk assessment of the system [Ralston et al. 2007].

To perform IICS segmentation, the first step is to divide the system into proper security zones with clearly defined boundaries and policy. A security zone must have a well-specified boundary, and communication between zones must be filtered in accordance with their policies. The segmentation should be based on functional characteristics, business impact, risk levels, or other requirements defined by the organization.

Direct connection of ICS system to either the Corporate IT system or the Internet can expose the ICS system to additional threats. Therefore, it's necessary to separate the two systems. A new neutral security zone that is in its own DMZ (De-Militarized Zone) should be created [Pollet 2006] as illustrated in Figure 3.4. A demilitarized zone (or DMZ) is a separate security zone that contains components that communicate with "untrusted" networks. This new neutral DMZ will create a security stage between the corporate IT network and the ICS system.

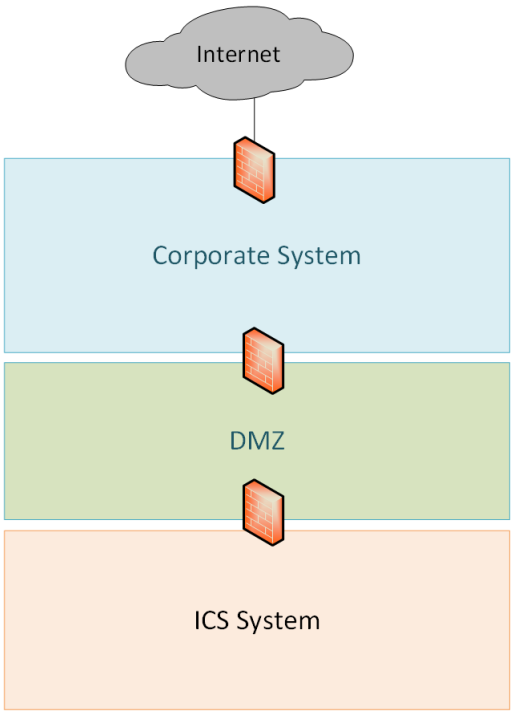

Figure 3.4 – General security guides segmentation

The main benefit of this new zone is that exchanges between the Corporate system and the ICS system can be staged. It avoids multiple direct connections from Corporate system to the ICS system [Pollet 2006]. This DMZ can also be used as a relay zone that can securely forward on mandatory flows from the Corporate side to ICS side such as operating systems and antivirus update patches. Two firewalls are used to protect this DMZ zone. The first firewall inspects traffic into and out of the DMZ to protect against security threats destined to the ICS system. The second firewall protect against security problems originated inside the ICS network [Obregon 2015].

Components within the ICS network such as SCADA server, HMI, PLCs and RTUs that control the industrial processes should be in a separate security zone in order to mitigate the risks and prohibit industrial and corporate interference and unauthorized communication [Pires and Oliveira 2006].

Further considerations should be taken into account to properly perform IICS segmentation:

- No direct connections should exist between the Internet and the ICS network.
- Access from the enterprise network to the control network must be restricted.
- If a component's criticality is high within a security zone, it is recommended to enforce this zone's protection.

- ICS industrial protocols should be filtered using industrial firewalls. Unfortunately, there are not many choices out there. Tofino Firewall [Tof 2014, Cereia et al. 2014a] and StormShield SNI40 [Sto] are some of the few existing solutions.
- Using two firewalls from different vendors at a zone boundary instead of only one firewall is an excellent technique. The two vendor firewalls should match in rules set and configuration [CSSP 2009, Pires and Oliveira 2006].
- A firewall should be added between any wireless network and the network it connects to [CSSP 2009].

To summarize, security guides firmly recommend at least three defense layers as illustrated in Figure 3.4:

- A first layer where the system's boundaries are protected by segregating exchanges with external systems.
- A second layer where the Industrial Control System and the Corporate system should be logically separated into two security zones.
- Finally, the components that need to communicate from these two security zones, should be connected through a demilitarized zone. A demilitarized zone (or DMZ) is a separate security zone that contains components that communicate with "untrusted" networks. They should be used to create a security stage between the corporate IT network and the ICS system.

Furthermore, they notably underline the constraints and issues related to segmentation such as the possible additional delay engendered by controlling the system communications, as well as, the technical experience needed to correctly implement this security measure.

Nonetheless, these documents recommendations remain quite shallow because most of the work must be done on a case by case basis while no precise information is provided on how to proceed. Many questions remain without answers, especially when it comes to the aspects that should be taken into account to achieve segmentation.

Example Based Solution

The second category of documents [CSSP 2009] deals the subject with a more concrete approach since they implement their solutions using a well defined reference architecture. They suggest to implement multiple layers of defense by creating multiple security zones. They mainly suggest to use the Purdue Model for control hierarchy logical framework (Figure 3.5), developed by the International Society of Automation ISA-99 [ISA 2013] that we presented earlier.

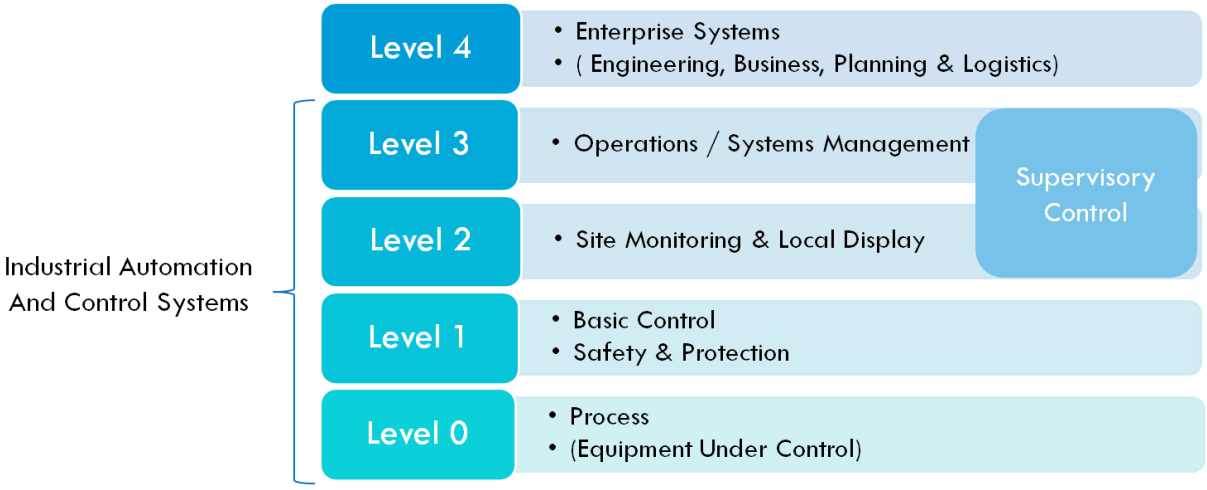

Figure 3.5 – Functional Hierarchical model [ISA 2013].

The five functional levels are used, by this second category of documents, as the primary criterion for security zones delimitation. In other words, according to these studies, IICS systems should be segmented, at least, into five security zones that correspond to the ISA95 five functional levels with some DMZs especially between ICS and Corporate system.

The approach of these research works is rather precise, however it has two drawbacks:

- Basing the segmentation solution on a settled reference architecture makes the solution rigid and inappropriate for a large number of ICS systems. The solution can, thus, only be adopted for systems similar to the reference system or, at best, for learning.
- The suggested solutions restrain themselves to the ISA95 functional model which is usually not really enough to model the IICS system.

Generic segmentation solutions

The third category of studied research works try to solve the problem in a more generic way. This category's solutions, while still based on the ISA95 hierarchical model, are in the form of generic rules and guidance where security zones are abstractly defined. We believe that this approach can lead to great results if conducted with deep focus on the aspects that are really relevant for IICS segmentation. This is an important ingredient that these research works do not unfortunately ensure because:

- Only the functional aspect, via the ISA95 model, is taken into account. This is definitely not enough to cover most of the IICS systems.
- IICS (technical, functional ...) constraints highlighted by the first category of studies, are not taken into account by the proposed models.

3.4.3 Discussion

The studied solutions suggest to create more than one layer of defense and separate the ICS system from Corporate system. They all make use of DMZs to stage communication between the different security zones, but do not explain when creating a DMZ becomes necessary. Most of them agree on the usefulness of the ISA95 model, but do not take into account other types of characteristics of IICS systems elements that may be very significant for segmentation. Finally, none of the studied solutions models the IICS systems real conditions and constraints that may impact security zones. Therefore, we set up about designing a new generic IICS segmentation method to fill these gaps. It will be presented, in detail, in the coming sections.

3.5 IICS segregation

The goal of networks segregation is to minimize access to sensitive information for systems and people who do not need it, while ensuring that the organization can continue to operate effectively. Therefore, granular network traffic inspection and access control is necessary to properly secure the conduits. This can be achieved using network segregation techniques that control communications through the segments' boundaries based on a predefined rules set. Rules are typically based on source and destination identity and the type or content of the data being transferred. This is essentially performed using firewalls.

Segregation should be implemented by respecting general best segregation practices. The most important one is the "least privilege principle" [Obregon 2015]. This principle dictates that a component, a system or a person that needs to communicate through a zone boundary should be only able to access the information or resources that are strictly necessary for its legitimate purpose. This implies that the base rule should be "DENY ALL, PERMIT NONE". Permissions should only be on demand respecting a well defined procedure for granting permissions. For example, permission requests for each incoming or outgoing data flow should be recorded and validated only by authorised persons. All "PERMIT" rules should be both IP address and TCP/UDP port specific. The rules should consider both directions through the firewall. Besides, any communication between two zones must be filtered in accordance with policy. Services, protocols, and applications that are not necessary inside a zone must be disabled. Any boundary-crossing traffic carrying those services, protocols, or applications should be blocked at the boundary. For example, industrial traffic that involves only ICS components should only be allowed within the ICS network. Accordingly, MODBUS/TCP [Huitsing et al. 2008] and DNP3[Fovino et al. 2010] are examples of protocols that should not cross neither the integration layer nor the edges of the system. If an exchange is allowed between the control network and the DMZ, then it should explicitly not be allowed between the DMZ and corporate network. Similarly, traffic that concerns only corporate components must not reach the ICS network. If this is not possible, compensating measures have then to be taken to protect the networks against attacks and misuse from outside the ICS.

While conventional segregation solutions could work in some IICS contexts, they are not always fully compatible with IICS. In fact, ICS systems usually are very demanding in terms of timing requirements while conventional firewalls may introduce significant latency. For example, firewalls are generally deployed on the boundaries of the security zones to control all outgoing and incoming flows which creates a significant load. The Deep inspection mechanism introduces a processing time that, however negligible it may be, becomes, by a mass effect, significant enough to challenge the use of firewalls in a context with very high timing requirements such as industrial systems [Cheminod et al. 2016, Zvabva et al. 2018, Parra et al. 2019, Li et al. 2018]. IDS/IPS and authentication mechanisms could also have the same side effect on industrial flows. Segregation inside ICS may thus constitute an angle of denial-of-service attack if its timing impact is not taken into account. Besides, many of the existing access control commercial solutions such as firewalls, IDS and authentication mechanisms do not fully support industrial protocols [Cereia et al. 2014b, Cereia et al. 2014a, Li et al. 2018] or, for the best, support only some industrial protocols such as ModBus and DNP3 ([Tof 2014]).

Many research studies have been carried out to address the issue of flows segregation and access control in industrial systems. The proposed solutions are diverse and usually strongly focus on the timing and infrastructural constraints of industrial systems. Proposed solutions include new access control mechanisms, new industrial firewalls and secure protocols.

3.5.1 Industrial access control solutions

Some commercial products such as SEL 3620 [Laboratories b] and SEL 3021 [Laboratories a] from Schweitzer Engineering Laboratories ensure some level of security for industrial equipment. The SEL 3620 is a secure Ethernet gateway that handles Ethernet and serial communications. The SEL 3620 secures all the field communication with link level encryption using IPsec while providing access control capabilities. There have also been some efforts for applying RBAC to industrial systems. [Rosic et al. 2013, Wang et al. 2008, Wei et al. 2013, Wei et al. 2011, Nagarajan and Jensen 2010] propose different RBAC models for ICS systems.

3.5.2 New industrial secure protocols

Many important protocols used in the industrial world, such as OPC/D-COM [Galloway and Hancke 2013], Industrial Ethernet/IP, and MODBUS/TCP, and sometimes HTTP and FTP, have significant security vulnerabilities [Keith Stouffer and Hahn 2015]. As a general rule, insecure protocols (e.g., HTTP, Telnet, FTP) should be replaced by their secure equivalent (e.g., HTTPS, SSH, SFTP) to ensure integrity, confidentiality and authenticity [ANSSI 2013, Keith Stouffer and Hahn 2015]. For protocols that cannot be secured for technical or operational reasons, compensatory measures should be implemented [Keith Stouffer and Hahn 2015]. Insecure protocols that cross the integration layer between ICS and Corporate system should be encapsulated in VPNs such as IPsec VPNs.

Some research works propose to use crypto-enabled SCADA protocols with authentication and encryption features to secure communication between industrial devices while ensuring inherent access control. [Shahzad et al. 2015] proposes a new security design that uses cryptography for MODBUS protocol. [Hayes and El-Khatib 2013] proposes a new Modbus alternative called ModbusSec that uses stream control transmission protocol and hash-based message authentication to ensure availability and integrity of Modbus messages while providing mutual authentication mechanism.

[Gilchrist 2008] presents a security mechanism called secure authentication for DNP3 protocol. [Majdalawieh et al. 2006] proposes DNP3Sec.

Protocol based solutions pay considerable attention to industrial performance requirements but are very specific and do not cover all protocols leaving unprotected a large number of communications in multiple systems.

3.5.3 Industrial firewalls

Firewalls are very important to control communication across different networks especially between external and internal networks and ICS and Corporate systems. To the best of our knowledge, there is unfortunately no firewall fully adapted for all industrial systems configurations [CSSP 2009, Keith Stouffer and Hahn 2015]. Most of existing firewalls only support protocols commonly used in Corporate systems especially TCP/IP and, for the best, some industrial protocols such as ModBus and DNP3 (see Tofino Industrial Security Solution [Tof 2014, Cereia et al. 2014b, Cereia et al. 2014a]. IICS systems really need industrial firewalls that can be used with different industrial systems configurations (distributed, located, wired, wireless...) taking into account industrial technologies and protocols and more importantly industrial timing requirements.

Besides the commercial industrial firewalls such as Modbus DPI (Deep Packet Inspection) Firewall from Tofino [Tof 2015], SCADA Firewall from Bayshore Network, and Eagle mGuard from Innominate [inn 2015], some studies propose new firewalls to address the problem of inspection of industrial protocols. [Nivethan and Papa 2016] proposes to use Linux Iptables. [Hachana et al. 2016] shows through experimental study how conventional firewalls can be tuned to fit ICS requirements using stateful filtering. [Salah et al. 2012] proposes a simple Markov model to describe the behavior of an iptables-based software firewall for industrial access control. Unfortunately, the proposed firewalls do not consider how the deep packet inspection can impact latency.

Some other research works propose very specific firewall solutions. [Khosroshahi and Shahinzadeh 2016] introduces a firewall system for the energy sector focusing on the Distributed Network Protocol 3 (DNP3). Their implementation is based on the iptables firewall. [H. Eslava and Pineda 2015] presents a firewall system for IEC 61850 protocol. [W. Shang and Zeng 2016] introduces a novel firewall system for Modbus protocol. [Diovu and Agee 2017, Diovu and Agee 2017] propose new firewalls designed specifically for smart grid systems. The results of these studies are interesting but are unfortunately only applicable in their specific context.

[Li et al. 2018] proposes a new firewall model to increase the efficiency of controls in terms of resource consumption by using Comprehensive Packet Inspection (CPI) to inspect packets more deeply and efficiently. Their solution, however, lacks extensibility.

[Force and Initiative 2013, ISA 2013, CSSP 2009] give some guidelines, but their recommendations should be put into practice to evaluate their efficiency to answer to the request "How can we use firewalls with different industrial systems (distributed, located) taking into account industrial technologies and protocols?"

Industrial IDS/IPS

IDS/IPS are also common solution to implement flows access control. Unfortunately, there is no commercial IDS/IPS solution that is fully adapted to IICS systems. This is because existing IDS/IPS commercial solutions do not support most of the industrial protocols, and are not designed to respect ICS requirements. Besides, no precision is given on where to place IDS within an ICS system. Campbell and Rrushi [Campbell and Rrushi 2011] present research on an anomaly detection model for nuclear power plants. The methodology consists in examining the detection of a potential attack that attempts to send faulty data from a field device to the HMI. The work demonstrates that it is possible to extend anomaly detection models to the ICS environment [Larkin et al. 2014a]. However, without developing custom solutions, current IDS solutions also work poorly in a ICS environments as stated by [Verba and Milvich 2008, Larkin et al. 2014a]. [D'Antonio et al. 2006] developed a new IDS for ICS systems to detect real time intrusion by extracting user behavior from the network traffic and comparing it to a set of predefined behavior model. [Rrushi and Campbell 2008] created a model to identify anomalies based on MODBUS payload data units (PDU). [Düssel et al. 2010] propose a protocol independent IDS using n-grams that takes the similarity of the communication layer messages. Recently, [Yun et al. 2018] proposed an IDS that uses a nearest neighbor approach to learn patterns of normal activities and identify anomalies. Similarly, [Lin et al. 2017] proposed a machine learning-based scheme to develop an IDS which learn normal behavior patterns to be able to detect unwanted intrusion events.

While IDS/IPS can be used to detect abnormal flows and prevent them, they are not always as deterministic as it could be needed. Besides, most of the proposed solutions need significant effort to model normal behaviours for non supported protocols or for specific systems.

3.5.4 DTE

[Bradetich and Oman 2007] investigated the use of DTE techniques on IICS systems. Although their findings are interesting, they are limited to securing flows between ICS and Corporate system. Interested in developing new generic models and mechanisms for IICS security, we believe that such a technique can be transformed into a generic model that can be applied to different IICS systems. Our objective is to generalize DTE controls to the whole system by providing a generic model that provides simple and consistent concepts that allow control rules to be defined in a straightforward and homogeneous way across the system, but with more focus on ICS systems. Our study will be presented in chapter 6.

3.6 Conclusion

This chapter provides a summarized overview of ICS security problems, the integration challenges and an analysis of countermeasures evaluating their maturity for Integrated ICS systems. A lot of work has been done on IICS security. Multiple vulnerabilities have been identified and a lot of countermeasures have been proposed. However, ICS and Corporate systems integration remains very challenging from a security standpoint. Most of the existing IICS security measures are borrowed from the IT world and are not redesigned to take into account industrial system specificities. We argue that there are still many security topics that need more work to complete the existing solutions panel in order to secure IICS more efficiently. This is especially the case for segmentation and segregation, where authentication and authorization mechanisms, firewalls and IDS/IPS still need adaptation for industrial systems.

We decided to work on the problem of segmentation and segregation of IICS. The results of our work will be detailed in the next chapters.

CHAPTER 4 SONICS segmentation method

4.1 Introduction

Integrated ICS segmentation is not easy because they are heavily heterogeneous. Characteristics on which security zones identification should be based may include functional characteristics, business impact, risk levels, or other requirements defined by the organization, but they remain complex and ambiguous. Besides, performing segmentation in large-scale networks taking into account architecture changes and configuration updates is another difficulty with Integrated ICS segmentation. Engineering expertise are not enough to perform segmentation because it may be error-prone and produce inaccurate results. The work may take more time than necessary while some important aspects may be neglected. Using a framework or a working method is always very useful because it guarantees more accurate results more quickly. Unfortunately, there is currently no method that straightforwardly drives this operation.

As explained in chapter 3, several research works have studied IICS segmentation. For most of them (NIST [Keith Stouffer and Hahn 2015], ISA [ISA 2013, ISA 2004, ISA 1999] and ANSSI [of France 2013] guides ...), segmentation should be done on a case by case basis. However, they do not provide sufficient guidance. Some others [CSSP 2009] have an example oriented approach and try to perform segmentation on a well defined reference architecture. They recommend adopting the Purdue Model for Control Hierarchy logical framework (IEC 62264) [ISA 2013] to delineate the security zones.

Few research [CSSP 2009, WUL 2016] works propose a generic solution to the problem. They provide generic rules and guidance to identify security zones while still adopting the IEC 62264 (ISA95) hierarchical model. We believe that this approach can lead to great results if conducted with deep focus on aspects that are relevant for IICS segmentation. Therefore, we propose SONICS, a new generic IICS segmentation

method that aims at simplifying IICS security zones identification by focusing on relevant aspects and taking industrial specificity into account. This method uses a simple meta-model to describe IICS systems and allows to identify potential security zones throughout multiple steps. The new identified potential zones are kept or not based on a constraints analysis.

In the next sections, we present SONICS, our new IICS segmentation method. We explain the method's meta-model (4.2.2), the system's constraints taken into account by SONICS (4.2.3) and the potential zones identification the constraints analysis process (4.2.4). Next, we present our test plan for validating the method. We will explain the test methodology and present the results we obtained. The latest section discusses the tests results as well as possible improvements.

4.2 SONICS: the IICS segmentation method

4.2.1 The principle

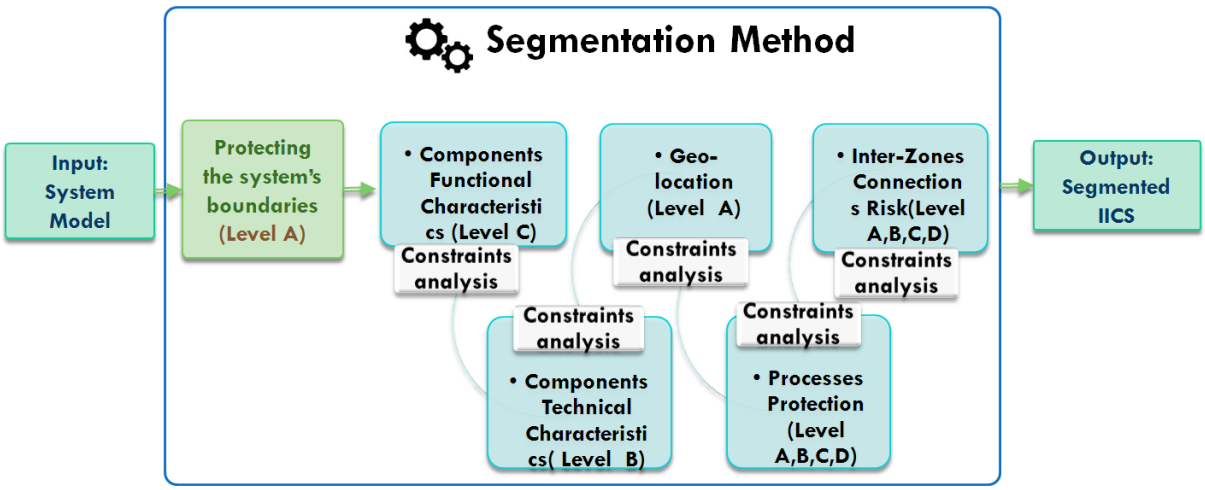

Figure 4.1 – The Segmentation method

With SONICS, the segmentation is done in two phases as illustrated in Figure 4.1. The first phase consists of modeling the system to be segmented using the meta-model (Figure 4.2) presented in 4.2.2. The system's model is the main input of the second phase. The later consists of segmenting the system through six cycles. At the first cycle, the system's boundaries are protected. This is the first security zone of the system. Next the system's *Components* are grouped cycle after cycle based on only one aspect (Functional, Technical, Geographical, Processes, and Inter-Zones Connections

Risk) per cycle to constitute potential security zones.[Khaoula et al. 2017] More details about *Components* grouping are provided in the next sections. The identified security zones at each cycle, are kept according to a constraints analysis conducted on the *Components* involved in the new identified zones. Constraints analysis is explained in section 4.2.3.

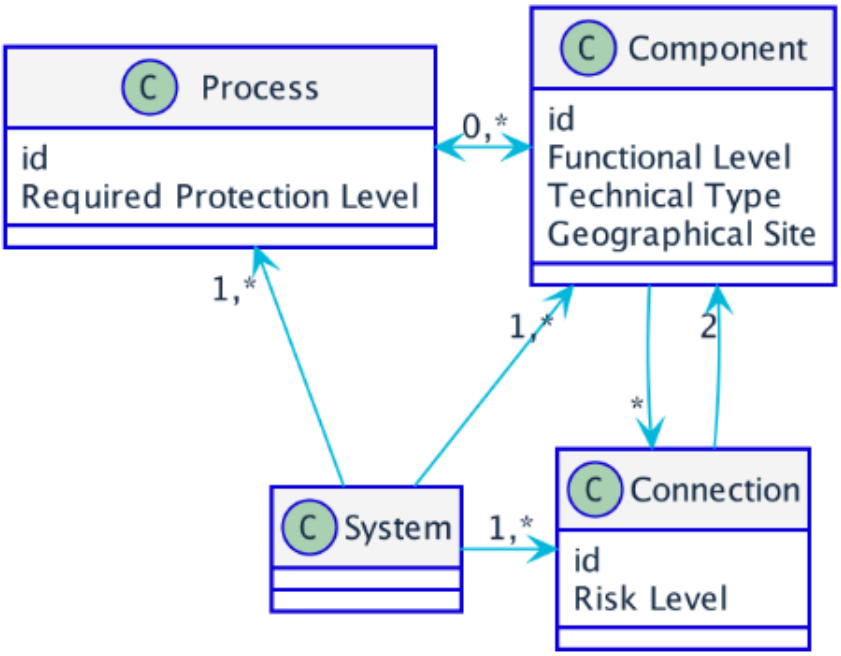

Figure 4.2 – IICS Meta-Model

4.2.2 The IICS Meta-Model

Our IICS meta-model (Figure 4.2) allows to model an IICS as a set of "*Components*", "*Connections*" and "*Processes*".

Components

A ***Component*** is any device capable of communicating through the network of the system regardless its functions and technologies. A *Component* is characterized by its functional level, its technical type and the geographical site to which it belongs.

- **Functional levels**
  Components can be grouped according to their function in the system

[ISA 2001, Obregon 2015]. We use an extended model of the IEC 62264 functional hierarchical model (ISA 95) that defines the different functional levels within IICS (see Table 4.1). Each component of the system belongs to only one functional group. Segmentation based on this aspect is recommended by multiple research studies [CSSP 2009, WUL 2016, ISA 2013] because *Components* with different functions usually have different security characteristics.

Table 4.1 – Functional Levels

Group	Name	Definition
FL-0	Process	This level includes sensors and actuators directly connected to the production process
FL-1	Local or Basic Control	It includes the functions involved in collecting data and manipulating the physical processes
FL-2	Supervisory Control	It includes the functions involved in monitoring and controlling the physical process
FL-3	Operations Management	This level includes the functions involved in managing and optimizing the production work flows
FL-4	Enterprise Business Systems	It includes the functions involved in the business-related activities
FL-ST	Support	It includes *Components* that do not belong to any of the other levels

- **Technical Types**

  The technical nature of the *Components* is another key aspect to consider for segmentation. There are many security guides and standards [Keith Stouffer and Hahn 2015, ISA 2013, ISA 2004, ISA 1999, of France 2013, Jens-Tobias ZERBST 2009] that state that components of different technical nature must be separated into different security zones because they have different security requirements (see Table 4.2). A *Component* can be an Information Technology (IT), Operation Technology (OT) *Component*[IOT 2014].

IT *Components*

- Are "Enterprise data centric": Cover the spectrum of systems that support corporate functions;
- Focus on higher level processes and transactions that manipulate data;
- Focus on data confidentiality and integrity.
- The main humans role is manipulating (reading, creating and updating) the data.

OT *Components*

- Are "Thing (product) centric": Deal with the physical transformation of products and services;
- Focus on physical industrial processes. They are mission-critical task-specific systems where controlling the physical equipment should be done with great precision;
- Focus on safety and availability.
- The main humans role is supervising and controlling the industrial processes.

A *Component* can, otherwise, be an IT-OT *Component*. We introduced this new type to distinguish *Components* that are designed to use both types of technologies IT and OT such as workstations.

Table 4.2 – Technical Types

Group	**Definition**
OT	Operational Technology Component
IT	Information Technology Component
IT-OT	Components that are designed to use both types of technologies (IT/OT)

- **Geographical location**
  Components' geographical location is also relevant for segmentation [Keith Stouffer and Hahn 2015]. Two physically distant sites systematically constitute two different security zones. "Physically distant" sites are sites that are either connected by wireless *Connection* or non physically protected wired *Connection*.

Processes

Segmentation should also take into account the organisational aspects of the organisation. This can be achieved with system business and industrial processes.

A **"*Process*"** is a set of interrelated interacting activities that transform inputs into outputs. A system is organized into multiple business and industrial processes. Each component belongs to one or more processes. Process identification should be done by the company. In general, an organizational standard such as ISO9001 is applied to organize the system into processes.

Each process is characterized by its "required protection level" and represents a potential security zone. The "required protection level" of a process can have one of the following values:

- **Level A**: Ultimate protection level
- **Level B**: High protection level
- **Level C**: Medium protection level
- **Level D**: Weak protection level

The level of protection required depends on the risk level of the process and should be evaluated based on a risk analysis. We propose a simple risk analysis method based on EBIOS [de la Défense Nationale 2010] and adapted to the specificity of IICS. The risk level is a function of the gravity of the feared events and their likelihood. It can be evaluated as follows:

1. **Identify the feared events and estimate their gravity:** Feared events gravity is the extent of their impact on one or more of the organization's assets. It can have one of the gravity scale values from Table 4.3. Estimating the gravity is performed through a qualitative approach that requires a good knowledge of the system and the organization's activity. It should therefore be done in collaboration with the organization's staff. In case a feared event has more than one gravity level from the Table (for example, significant gravity in terms of security aspects but critical financial loss), the worst case is assumed.
2. **Analyze Threat Sources and estimate the likelihood of the attack:** There is one threat source that can affect an IICS process security: the compromise of one of its components or a component that is connected to it. In this case, the

Table 4.3 – The gravity scale

1. Low	**Safety:** No threat to safety **Regulatory/Legal:** Internal sanction at the most **Company's image:** No impact
	Financial: Low potential financial low (e.g., few dozens of dollars) **Business:** Loss of some few prospects
2. Considerable	**Safety:** Small material damage
	Regulatory/Legal: Small Contractual penalties with some small clients **Company's image:** Local impact, limited number of actors **Financial:** e.g., some thousands of dollars **Business:** Loss of small clients
3. Critical	**Safety:** Considerable material damage **Regulatory/Legal:** Strong contractual penalties with major clients, civil or criminal cases, non-compliance with law or regulation **Company's image:** Wide perimeter impact **Financial:** Dozens of thousands of dollars annually **Business:** Loss of important clients
4. Major	**Safety:** Big material damage, Danger on Human safety **Regulatory/Legal:** Major non-compliance with the law or regulation, massive invasion of privacy, criminal conviction, contractual penalties with multiple actors. **Company's image:** Scandal **Financial:** Hundreds of thousands of dollars annually **Business:** Loss of partnership, Massive loss of clients

whole process can be compromised. The likelihood of such an attack should be estimated using the qualitative scale presented in Table 4.4, taking into account the system's technical and organizational context, the attack's difficulty as well as the existing solutions.

3. **Evaluate the risk level:** The risk level associated to the process is calculated based on the related gravity and the likelihood of the attack. The risk levels grid in Figure 4.3 assists in calculating it.

Table 4.4 – The likelihood scale

Liklihood	Definition
1. Low	This is unlikely to happen
2. Probable	This may happen
3. Significant	There is a significant risk that this will occur
4. Strong	This should happen one day

Table 4.5 – Risk level / Required protection level

Risk level	Required protection level
Extreme risk	Level A (Ultimate)
Critical risk	Level B (High)
Considerable risk	Level C (Medium)
Negligible risk	Level D (Low)

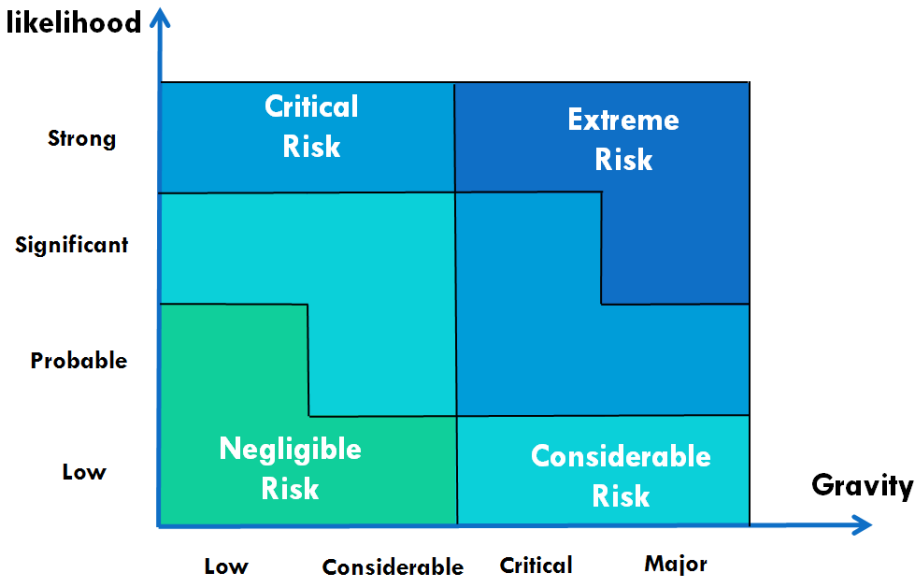

Figure 4.3 – Risk levels grid

The required protection level of a process is proportional to its risk level. Table 4.5 presents how risk levels match “required protection levels”.

Connections

A "***Connection***" is any channel that can be used by two (or more) *Components* to communicate with each others. It can be physical, where the *Components* are directly linked by a physical (wired or a wireless) connection, or logical, where the *Components* are linked through a succession of physical *Connections*. A Connection may be characterized by its risk level. *Connections* impact segmentation especially when they connect *Components* from different zones. This is why we pay special attention to inter-zones *Connections*. These connections emerge at the end of each cycle of the segmentation method, as we progressively create new security zones. Therefore, they can only be modeled when all the *Components* security zones are identified.

Inter-zones *Connections* may connect security zones that have different security levels or contain *Components* of different risk levels. This can introduce security issues. Therefore, these zones should be protected by introducing a new security zone [Obregon 2015] that stages and secure communication through their boundaries.

For example, when connecting two *Components* X and Y from two different zones A and B, where the risk on the zone A is high while the security level on the zone B is low, it is necessary to protect zone A against potential issues lead by this *Connection* (see Figure 4.4). This can be done by introducing a new security zone that stages communications between the two zones A and B.

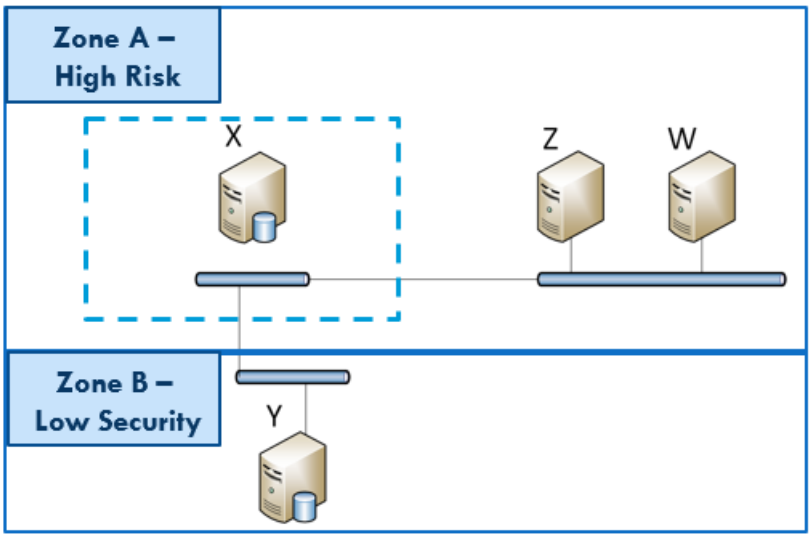

Figure 4.4 – Inter-zone connection's security zone

The risk level of each inter-zone connection of the system should be evaluated based on a risk analysis of the *Connections* and *Components* they connect. We use the same

risk analysis method presented in section 4.2.2. For a given inter-zone connection, all the **Services** exposed by the Components of the zones it connects as well as all the manipulated **Data** should be analyzed in order to perform a more accurate qualitative assessment of the risk associated to these components.

Note that each inter-zone connection is bidirectional. This implies that the risk analysis should be performed on the two interconnected zones components.

4.2.3 IICS Segmentation Constraints

The addition of a new security zone can sometimes be subject to difficulties related to the state of the system or its specific requirements. Our segmentation method takes this into account by requiring a constraints analysis at the end of each cycle. The constraints analysis helps to decide whether the identified zones are to be retained or not. There are two generic types of IICS constraints that we focus on:

Functional Constraints

Introducing a new security zone must not adversely affect the expected functioning of the system. Functional requirements that may be sensitive to segmentation should be identified and studied on a case-by-case basis. For example, special attention should be paid to the timing requirements of the critical components of the IICS to ensure that they will not be affected by the flows filtering across security zones boundaries. This task will have to be taken care of by the security administrators.

Functional constraints are not all on the same level of importance. Therefore, we defined three Constraints Levels:

- **Constraint Level A**: Some mandatory requirements can not be satisfied if the new boundary is created. A mandatory requirement is a requirement that can not be dropped out. For example: in a very critical industrial infrastructure, timing requirements of the communication between a PLC and the physical process it controls can be so strict that the response time must not be beyond some milliseconds. This is a mandatory requirement that should not be impacted by the creation of a new security zone. When such a requirement can not be respected, the constraint level is then at Level A.
- **Constraint Level B**: Some important requirements can not be satisfied if the new boundary is created. An important requirement is a requirement that can hardly be dropped out.

- **Constraint Level C**: Some optional requirements can not be satisfied if the new boundary is created. An optional requirement is a requirement that should preferably be satisfied but can be dropped out.

The system administrators have to do a qualitative evaluation of the constraint's level of all the constraints he/she identifies in the system.

Technical Constraints

Creating new security zones and filtering communication through their boundaries can sometimes be very difficult when the system's technologies (protocols, servers, techniques...) lack adapted zoning and filtering (firewalls, IDS,...) security solutions. This is a common issue of industrial systems where legacy and proprietary industrial technologies continue to exist whereas no segmentation product support them. It is all a matter of cost. Theoretically, it is always possible to build custom solutions on demand to meet the specific needs. However, cost can be so high that the return on investment is not interesting. In such a case, adding a new security boundary is simply not worth it. Technical constraints can have one of the following Constraint Levels:

- **Constraint Level A**: Adding the new security boundary has a Very High Cost.
- **Constraint Level B**: Adding the new security boundary has a High Cost.
- **Constraint Level C**: Adding the new security boundary has a Medium Cost.

4.2.4 Selecting the potential zones to keep

The potential security zones that are progressively identified are kept or not based on a constraints analysis performed on those new zones. Retaining a new identified potential zone is a decision to make by comparing the **Necessity** of this new zone to the **Constraint level** of its elements. We defined, therefore, a **Grading System** that helps to evaluate the **Necessity** of adding a new zone, evaluate the **Constraint's Level** of its elements and compare these two "grades" in order to decide whether or not to keep the new zone. It is composed of the two Necessity and Constraints scales (Tables 4.6 and 4.7).

Table 4.6 – Segmentation Necessity Levels

Necessity Level	**Definition**
Level A	Non-Negotiable
Level B	Necessary
Level C	Mildly Necessary
Level D	Optional

Table 4.7 – Constraints Level Scale

Constraint Level	**Definition**
Level A	Zoning is inconceivable
Level B	Zoning is almost inconceivable
Level C	Zoning is conceivable with difficulty

Segmentation Necessity Grading System

The **Necessity** of a zone represents how important this zone is. This depends on the cycle (Functional, Technical ...) in which the zone was identified. For example, functional based zones are not as necessary as geo-location based zones. We therefore estimated the **Necessity** associated to each cycle. All the **Necessity** levels are listed by Table 4.8. These values were preset based on our knowledge of IICS systems.

Segmentation Constraints Grading System

The level of a given constraint is its impact on the feasibility of adding a new potential security zone. Each known constraint must be assigned a grade from Table 4.7. The company has to evaluate the system's constraint's impact based on their knowledge of the technical and functional context of the system. Constraints levels for functional and technical constraints were presented in sections 4.2.3 and 4.2.3.

Grades Comparison

The ultimate objective of our two grading systems is to compare a new zone's necessity to its constraints in order to decide if the new zone should be created or rejected. The comparison should be done as follows: Let us assume that we identified a new potential zone based on a given meta-characteristic. We will call this zone **Zone A** for simplicity. Let us also assume that:

Table 4.8 – Segmentation Necessity Level Scale

Meta-Characteristic	**Segmentation Necessity**
Functional Grouping	Level C
Technical Grouping	Level B
Geographical Grouping	Level A
Process Grouping	Equals the required protection level (A, B, C, D)
Inter-zone Staging	Equals the connection risk level (A, B, C, D)

- L_{seg}: is the **Necessity Level** of creating the **Zone A**.
- L_{cs}: is the greatest grade of the grades assigned to the constraints that are relevant for **Zone A**.

Then:

- if $L_{seg} \geq L_{cs}$: Creating the new zone is conceivable and it is as necessary as its necessity level grade is great.
- if $L_{seg} < L_{cs}$: Creating the new zone is inconceivable.

4.2.5 Formalization

The formalization below of the SONICS method using mathematical objects summarizes the method and provides a useful starting point for the implementation.

Preliminary: Let S an IICS system, S = <C,X,P,Ge> where:- C is the set of components of S, - X is the set of connections of S, where : $\forall x \in X$, $\exists$ $c_1, c_2 \in C$ *where* $x =< c_1, c_2 >$. - P is the set of processes of S. - Ge is the set of all the geographical sites of S.

Notations:

- $\forall c \in C$,
  - $fl_c \in \{FL0, FL1, FL2, FL3, FL4, FLST\}$ is the functional level of c.

- $tt_c \in \{TI, TO, TIO\}$ is the technical type of c.
- $site_c \in Ge$ is the site to which c belongs.
- $proc_c \subset P$ is the set of processes to which c belongs.

- $\forall x \in X$,
  - $cl_x \in \{LEVEL_A, LEVEL_B, LEVEL_C, LEVEL_D\}$ is the constraint level of x.
  - $risk_x \in \{LEVEL_A, LEVEL_B, LEVEL_C, LEVEL_D, \emptyset\}$ is the risk level of x.

<u>Definitions</u>:

1. The function constraints level cl is defined as follows:

$$\begin{array}{rcccl} cl & : & X & \rightarrow & \{LEVEL_A, LEVEL_B, LEVEL_C, LEVEL_D\} \\ & & x & \mapsto & cl(x) = cl_x \end{array}$$

2. The function risk level $risk$ is defined as follows:

$$\begin{array}{rcccl} \text{risk} & : & X & \rightarrow & \{LEVEL_A, LEVEL_B, LEVEL_C, LEVEL_D, \emptyset\} \\ & & x & \mapsto & risk(x) = risk_x \end{array}$$

3. We define the inter-components connection function as:

$$\begin{array}{rcccl} cx & : & C \times C & \rightarrow & X \cup \{\emptyset\} \\ & & (c,d) & \mapsto & cx(c,d) = \begin{cases} < c, d > : \text{if } c \text{ and } d \text{ are connected} \\ \end{cases} \end{array}$$

   when c and d are not connected, $cx(c,d) = \emptyset$.

4. *Let* $\Sigma_{(S)}$ the set of all possible segmentations of the system S,
   $\Sigma_{(S)} = \{ \ \sigma \ / \ \sigma$ is a partition of C $\}$

   σ is a partition of C if:

   - $\emptyset \notin \sigma$
   - $\bigcup_{A \in \sigma} A = C$

- $\forall A, B \in \sigma,\ A \neq B \Rightarrow$A $\cap B = \emptyset$

5. For each cycle of the method, we define the cycle's processor function as:

$$\begin{array}{rcccl} Pr_g & : & \Sigma_{(S)} & \rightarrow & \Sigma_{(S)} \\ & & \sigma & \mapsto & Pr_g(\sigma) \end{array}$$

$$\begin{array}{l} Pr_g(\sigma) = \\ \{ \\ \quad \text{A'} \subset C / \forall c, d \in A', \\ \quad\quad (\exists A \in \sigma \ where\ c, d \in A\ and \\ \quad (\\ \quad\quad\quad g(c) = g(d) \\ \quad\quad\quad or \\ \quad\quad\quad cl(cx(c,d)) > necessity_g(c,d) \\ \quad)) \\ \} \end{array}$$

where $necessity_g$ is the cycle's necessity function of creating a boundary between two components, and g is the cycle's grouping function. The definition of grouping functions is:

$$\begin{array}{rcccl} g & : & C & \rightarrow & G \\ & & c & \mapsto & g(c) \end{array}$$

G is a set of grouping values (such as functional levels, technical types ...). Thus:

- The functional grouping function is:

$$\begin{array}{rcccl} func & : & C & \rightarrow & \{FL0, FL1, FL2, FL3, FL4, FLST\} \\ & & c & \mapsto & func(c) = fl_c \end{array}$$

- The technical grouping function is:

$$\begin{array}{rcccl} tech & : & C & \rightarrow & \{TI, TO, TIO\} \\ & & c & \mapsto & tech(c) = tt_c \end{array}$$

- The geolocation grouping function is:

$$\begin{array}{rcccc} geo & : & C & \rightarrow & Ge \\ & & c & \mapsto & geo(c) = site_c \end{array}$$

- The processes grouping function is:

$$\begin{array}{rcccc} proc & : & C & \rightarrow & P \\ & & c & \mapsto & proc(c) = proc_c \end{array}$$

6. The intern-connection-risk grouping function is:

$$\begin{array}{rcccc} IZX & : & \Sigma_{(S)} & \rightarrow & \Sigma_{(S)} \\ & & c & \mapsto & IZX(\sigma) \end{array}$$

$IZX(\sigma) =$

$\{$

A' $\subset C / \forall\ c \in A', \exists A, B \in \sigma, \exists d \in B$ where :

$($

$A \neq B$ *and*

$c \in A$ *and*

$cx(c,d) \neq \emptyset$ *and*

$cl(cx(c,d)) \leq risk(cx(c,d))$

$)$

$\}$

7. We finally define SONICS as:

$$\begin{array}{rcccc} SONICS_{(S)} & : & \Sigma_{(S)} & \rightarrow & \Sigma_{(S)} \\ & & \sigma & \mapsto & IZX \circ Pr_{proc} \circ Pr_{geo} \circ Pr_{tech} \circ Pr_{func}(\sigma) \end{array}$$

Let us assume that $\sigma_{initial}$, is the initial segmentation of the system S, $\sigma_{result} = \text{SONICS}_{(S)}(\sigma_{initial})$, is the result of the application of SONICS on the system S.

4.2.6 SONICS Tool

We have developed a tool that implements our method (Figure 4.5). This tool allows to create system models and run the segmentation steps on a model to obtain a segmented system.

Creating a model using the tool is fairly simple but requires good knowledge and prior preparation. It is necessary that the tool's user knows sufficiently well the architecture of the system, its processes, its risks, and its constraints. The system's modeling consists, as depicted in Figure 4.5, of creating components, specifying their characteristics and adding connections and processes.

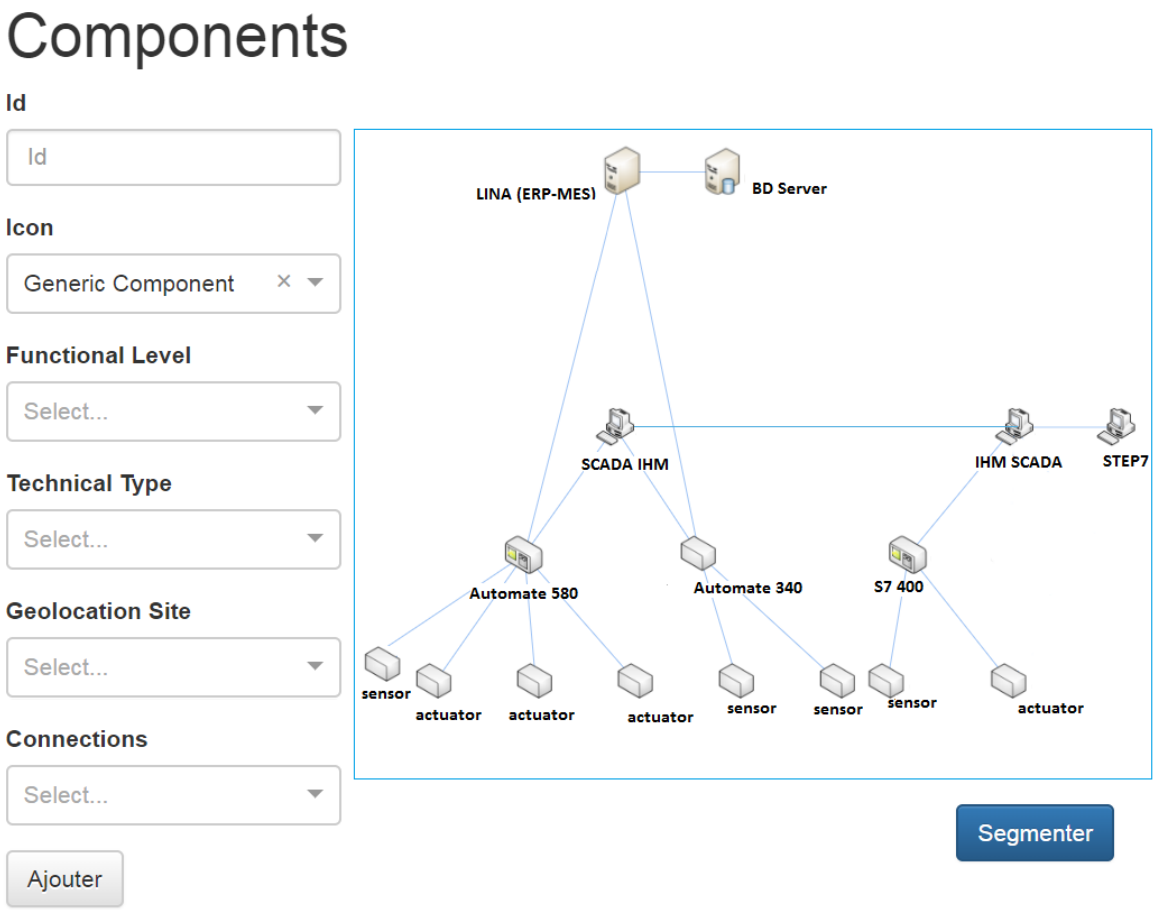

Figure 4.5 – SONICS Tool - Modeling step

Once the model is created, the tool allows to roll out the steps of the method one after another allowing to assign constraint levels to inter-zones connections. For example, for the first segmentation step, namely functional segmentation, the tools calculates the cycle's new potential zones (differentiating them using different colors) as illustrated by Figure 4.6. It outlines the inter-zones connections of these potential zones allowing to set their constraints levels (Figure 4.7). The security zones are then recalculated based on the newly set constraints levels values. The next cycles are processed (by pressing the "Next Step" button) in a similar way until we get the final result.

Moreover, the tool is completely recursive. Any value set by the user, no matter whether it is a characteristic of a component, of a connection, or of a process, is

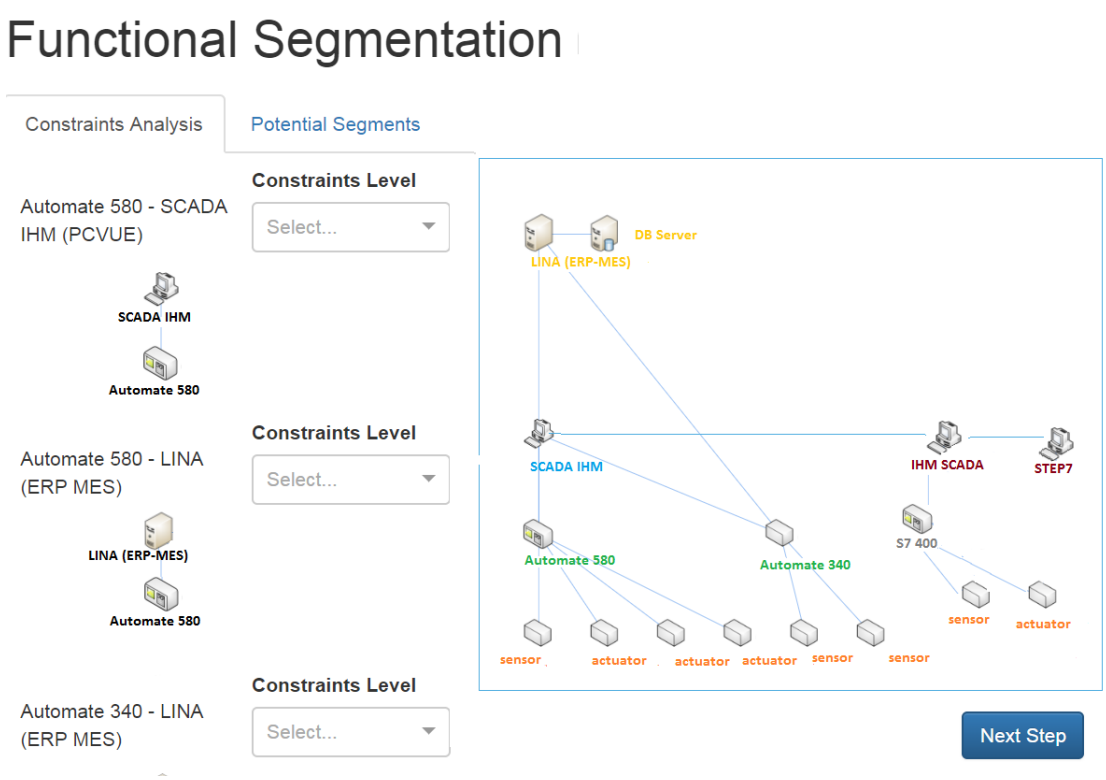

Figure 4.6 – SONICS Tool - Functional potential zones

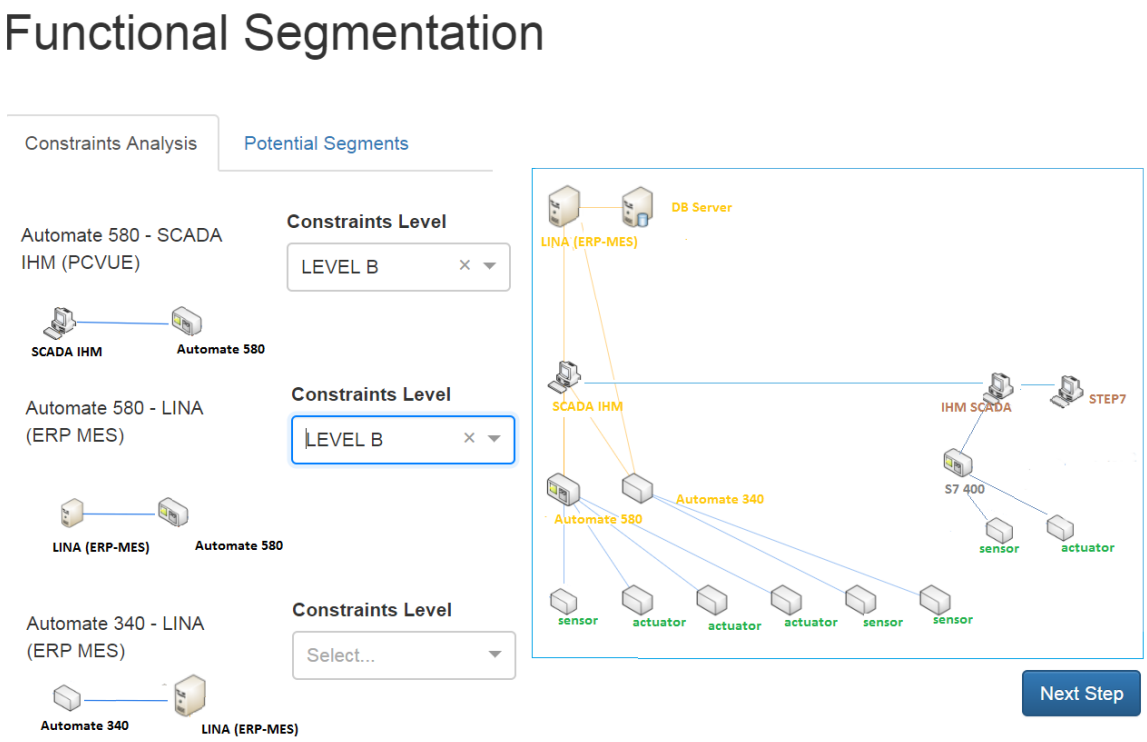

Figure 4.7 – SONICS Tool - Constraints levels attribution

included in the system's model and reused through the various steps. For example, if a connection's constraint level is set during some cycle, is does not need to be reset at other cycles as it becomes a characteristic of that connection. This ensures that the segmentation result is automatically recalculated any time the system's model evolves by adding, modifying or deleting components, connections or processes.

4.3 Application and Results

4.3.1 Test methodology

SONICS is the result of a rather deep and complex analysis of the segmentation problem. Our approach to design SONICS is completely based on our understanding of industrial systems, and the aspects recommended for segmentation by the standards and research works we have studied. It is very difficult to explain how the different parts of this method were built because it is the result of a very complex process of brainstorming, improvement, refinement and reworking that took a long time. This is not very important in determining the value of our method. The only important thing is to prove that the results of the method are correct. Most, if not all, paradigms and methods introduce new theoretical concepts to try to model a problem or phenomenon without explaining the why and how. They are nonetheless approved when they prove their accuracy. This is done in perfect respect of the modern scientific experimental approach.

Therefore, we designed a validation test method in order to evaluate our segmentation method. This test method is based on the comparison of the result of SONICS to segmentations that are made over time by expertise (without a method) and are assumed to be accurate. Given a test system with an existing accurate segmentation, the validation test consists of applying SONICS on this system and comparing the results with the existing segmentation as explained in Figure 4.8. For more readability, we will use the term *Ex-Segmentation* to refer to any "existing accurate segmentation".

The comparison of SONICS result with an *Ex-Segmentation* is done using the new concept of segmentation efficiency and accuracy presented below.

Segmentation efficiency and accuracy

We define the efficiency of a method on a set of test systems as the mean of the accuracy of the results obtained for each system. A result's accuracy depends on how

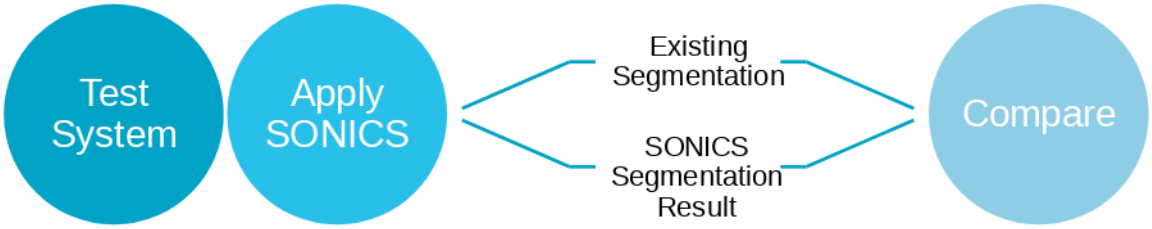

Figure 4.8 – Test Methodology

much the result is similar to the expected one. In our case, a segmentation's result's accuracy is a function of the distance between the segmentation obtained using SONICS and the *Ex-Segmentation*. The distance between two segmentations of a same system is the minimum cost to transform a segmentation into the other one by performing a set of only the following actions:

- Move only one component at a time from one segment to another.
- Remove one segment
- Merge two segments

Each action has a cost of 1. For example, the distance between two segmentations, where it is necessary to move two components of their segments, is equal to 2. Accuracy is calculated based on the distance using the following formula:

$$accuracy = \frac{1}{1 + distance}$$

When two segmentations are the same, the distance between them equals 0, the accuracy then equals 1 (the maximum value). On the other hand, when the distance increases, the accuracy decreases towards 0.

4.3.2 Test systems

A test system can only be used in our validation test if it incorporates an *Ex-Segmentation* that has been verified over time. This allows to validate segmentation results on real systems with effective segmentation under real conditions and on a long term basis. However, this approach has the disadvantage of being very expensive and

inflexible because creating a good test system is time-consuming and finding existing test systems is not easy.

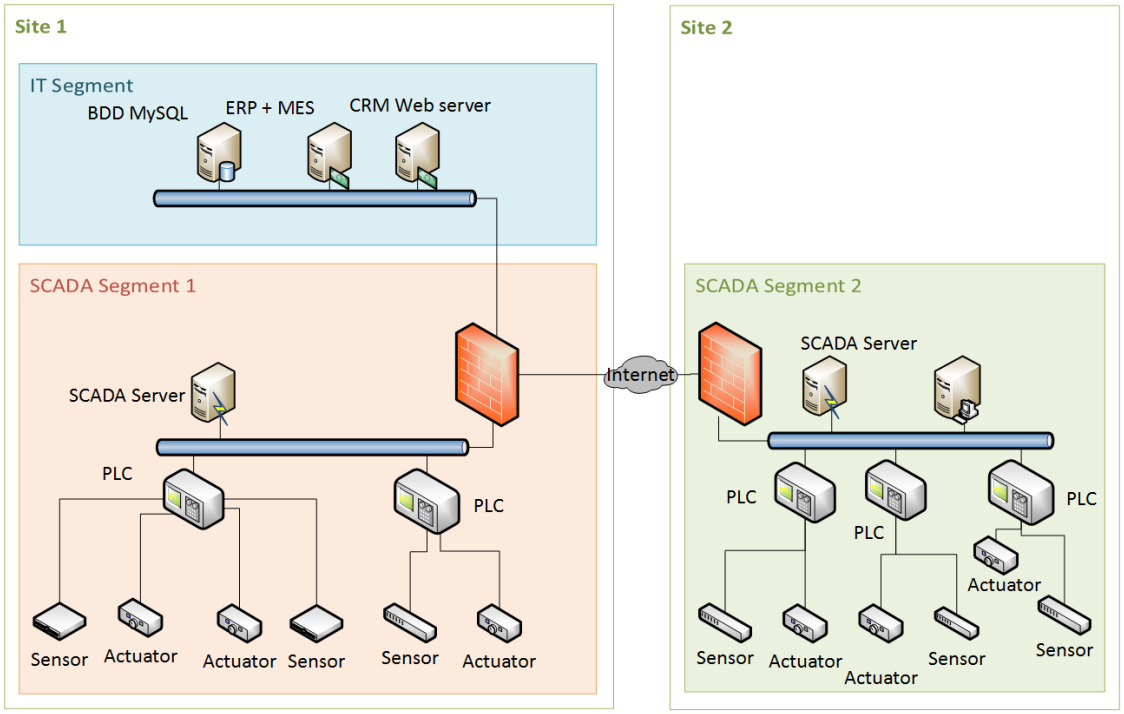

Figure 4.9 – The IIC test System

We have tested our method on only one test system (Figure 4.9). This is the only system available to us that fulfills the criteria of test systems selection. It is based on a real system in production with an *Ex-Segmentation*. It consists of two geographically separate sites and includes the following components :

- An ERP / MES - LINA: that manages all the company's resources.
- A CRM Web server: that manages orders, validates them, and launches industrial processes.
- MySQL database: that Contains all the business data. It is shared by the CRM and the ERP-MES.
- SCADA (PCView and WinCC): that controls PLCs, such as loading new programs, retrieving and displaying information...
- The ICS part of the system consists of two field sites.
    1. A main field site where a SCADA network and a set of industrial production devices are deployed.

2. A remote secondary field site where a remote production unit is deployed.

For simplicity, we suppose that the system does not have any specific legal, organizational or responsibilities grouping requirements.

The system is segmented into 3 segments as illustrated by the figure. This is the *Ex-Segmentation* for our test. It has been made only by skills and security knowledge but has also proven its effectiveness over time. It is also reliable because the test system is not very complex.

4.3.3 Results and Discussion

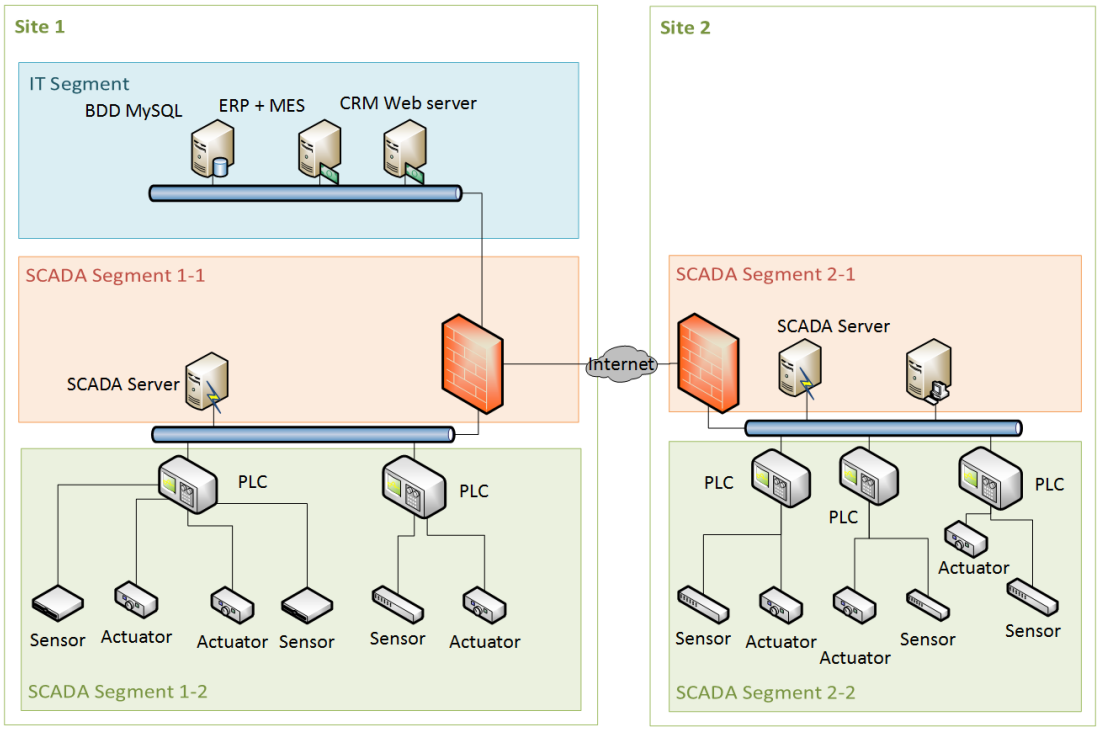

Figure 4.10 – The Segmented IIC test system

The application of our segmentation method on our test system has resulted in the segmented system illustrated by Figure 4.10.

By comparing the segmentation result with the *Ex-Segmentation*, the method allowed us to obtain a segmentation rather close to the *Ex-Segmentation*. The distance between the two segmentations remains quite small (equal to 3). We noticed that this distance was mainly due to the division of existing segments into several segments. This means that the method generated a segmentation that are too restrictive and too

demanding in terms of securing inter-component flows. This impacted the accuracy but does not mean that the result is completely incorrect. In fact, two unnecessary security zones was added introducing a gap with the *Ex-Segmentation*.

The study of the causes that led to the identification of these additional segments revealed that these segments were useful for flows controls without needing firewalls. That led us to an important conclusion that all the new identified zones do not necessarily have to represent a network segment with a firewall. Other segregation techniques may be used as appropriate to the security characteristics of the identified zone. Incorporating these segregation techniques into the method would be a possible improvement to our method. On the other hand, the method takes into account industrial systems specificities. Nevertheless, we believe that it may also be possible to rely the method a little more on security characteristics (such as Risk and Security Level).

In general, the first results support our conviction that SONICS is a valuable solution that provides satisfying and realistic answers to an unresolved problem namely IICS systems segmentation. It is a generic solution that can be applied to different types of IICS. It supplies efficient guidance and allows to be focused only on aspects that are significant for segmentation by using a simple meta-model. It considers multiple aspects in order to ensure that IICS systems heterogeneity is taken into account. Another advantage of our method is its constraints based zoning decision making. This makes the method very pragmatic and ensures more accurate results. In addition, the application of the method remains affordable, especially when using the tool we developed.

4.4 Conclusion

SONICS is a new IICS segmentation method that aims at ensuring efficient zoning to meet actual security needs of IICS. It is based on a meta-model that helps to model systems. System models are used by the method to identify potential security zones. These are kept or dropped out based on a constraints analysis.

We designed and carried out a validation test to evaluate the method. This helped us to identify the limitations and difficulties associated with the method and to identify possible improvements. The first test results were acceptable. However, we admit that the method's application is not simple enough without using the tool we developed. That said, our test method is by itself a standalone scientific contribution that can be reused or adapted for other scientific works.

SONICS has a lot of advantages. It is a generic solution that can be applied to different types of IICS. It keeps the focus only on aspects that are relevant for segmentation. It is a fairly pragmatic method that takes into account IICS constraints and specificity. Note that the method uses industrial systems concepts (Operation functional levels, IT and OT technical types), but it can be applied to a non integrated Corporate system (IT) as well as to a non integrated ICS. This should be guaranteed any way by our method because both systems are subsystems of an integrated ICS.

However, we agree that the method could be improved by taking more security aspects (such as Risk and Security Level) into account. The method could also incorporate more segregation concepts to provide more guidance for inter-zones flows protection in order to optimize the Segmentation/Segregation cost. These improvements will be addressed in the next chapters.

CHAPTER 5 RIICS: Risk based IICS segmentation Method

5.1 Introduction

SONICS method tries to take into account the most important aspects for IICS segmentation according to multiple security standards. Technical and functional specificities are well covered by the method via components' characteristics as well as with technical and functional constraints. This ensures that components of different technical or functional natures are separated unless there are constraints to do so. The method also involves separating components that belong to different remote sites in order to comply with common security recommendations. However, the security aspect of components is not adequately addressed. Only processes are segmented according to their risks. We have therefore decided to make more use of the concept of risk in order for our method to take more security aspects into account. We believe that the concept of components risk is one of the best ways to characterize components from a security angle. The risk associated with data, components or processes is based on the probability and gravity of the applicable attacks. Risk analysis requires a strong focus on the study of the context, and involves implementation of rational and optimal measures, especially in terms of cost. For example, it is not necessary to apply very strong and costly measures to protect against an attack that is unlikely to happen and for which the impact is not very significant.

On the other hand, SONICS segments according to both functional and technical characteristics. We realized, after the application of SONICS several times, that technical groups are actually a subset of functional groups:

- The IT group is equivalent to the FL4 group. All components of the FL4 levels are also considered as IT components, because they all are data centric.

- The ITOT group equals the FLST group in most cases. The most common support components are often ITOT components, and can be used in both IT and OT contexts.
- The OT group includes all functional groups FL0,1,2,2 and 3. All components of the FL0,1,2, and 3 groups are OT components because they are process centric.

We therefore initially thought of not using technical segmentation anymore. However, we also found that functional groups are very often not segmented because of functional and technical constraints (especially timing requirements and cost). We finally decided to keep the technical segmentation instead of functional segmentation because it gives, bearing in mind the constraints, the same results as the technical segmentation in most cases. We believe the elimination of functional segmentation will not only have little impact on the accuracy of the results, but it could also improve them.

Therefore, we propose RIICS (**R**isk based **IIC**S **S**egmentation), a new segmentation method for IICS systems that fills the gaps of SONICS and tries to simplify security zones identification by focusing on systems technical industrial specificities and risk. The RIICS method is presented in section 5.3. We explain the principle, the concepts and the main steps of the method. The next section presents the validation tests, and discusses the results.

5.2 Risk Analysis applied to IICS

Before we present the method, we have a say on risk assessment for IICS systems. We used risk analysis for the first time with SONICS, to segment business and industrial processes. At that stage, the risk is calculated in a fairly ordinary way by following specific instructions of the EBIOS method. We explored the subject of risk analysis a little further in order to study more closely the application of a risk analysis method such as EBIOS in an industrial context. We mainly aimed to verify the applicability of EBIOS to IICS and possibly propose an extension of the method to make it more compatible with industrial environments. The results of this study would be of benefit for the RIICS method to be improved.

5.2.1 EBIOS Method for IT risk assessment

EBIOS is a French acronym meaning Expression of Needs and Identification of Security Objectives (**E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **Sécurité**). It is a method for analysis, evaluation and action on Information Systems risk. The EBIOS method [de la Défense Nationale 2010] is an IT risk assessment method developed in 1995 by the Central Directorate for Information Systems Security (DCSSI) and maintained by the National Agency for Information Systems Security (ANSSI) since 2009.

It is used to assess the security risks of information systems and identify the necessary measures. For EBIOS, risk is a scenario that combines a feared events (a financial or physical damage for example) and one or more attack.

An EBIOS risk analysis applied to a given system or subsystem is carried out in 5 steps as illustrated in Figure 5.1.

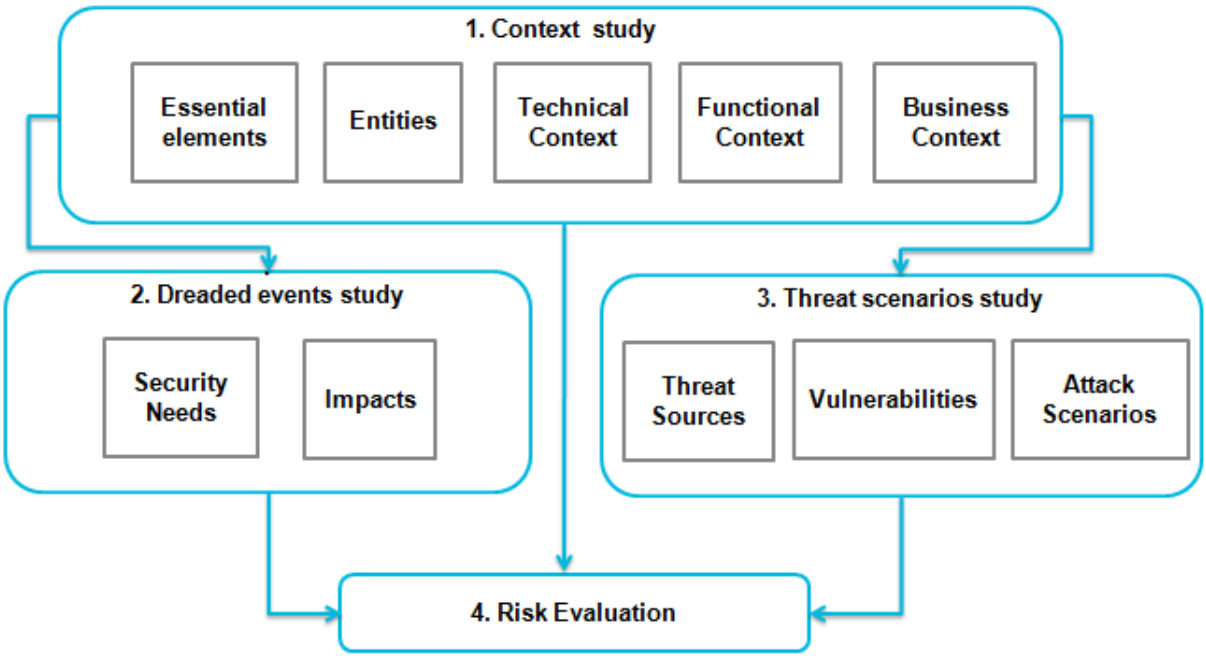

Figure 5.1 – EBIOS Steps

The Context Study

The goal of this key step is to define the scope of the risk analysis and to situate it in its context. It notably helps to specify the system's issues, its use context, its tasks and services.

This step is structured into three actions:

- **Studying the organization**: this involves defining the scope of the study where data should be collected on the organization and its information system.
- **Studying the target system**: this aims at specifying the context of use of the system to be analyzed.
- **Specifying the security study's target** : the purpose of this is to determine the entities (technical asset) on which the essential elements (essential assets) of the target system will be based.

Feared events study

This step provides a basis for estimating risks. It allows to express the organization's security needs. These security needs are expressed according to different security criteria such as availability, integrity and confidentiality. The expression of needs is based on the development and use of a scale of requirements and the identification of unacceptable impacts on the organization.

Threat scenarios study

This step consists of identifying scenarios that could affect the system's components. A threat is characterized by its type (natural, human or environmental) and/or by its cause (accidental or intentional).

Threats are formulated by identifying their components, methods of attack to which the organisation is exposed, the threat elements that can use them and the vulnerabilities that can be exploited on the entities of the system and their level.

This step is structured into three actions:

- **Investigation of the origins of threats**: This includes the identification of sources in the risk management process.
- **Vulnerabilities study**: The purpose of this activity is to determine the specific vulnerabilities of the target system.
- **Threat formulation**: aims to formulate an objective insight into the threats affecting the target system

Risks study

This step allows threats to be confronted with security needs. This confrontation helps to identify and prioritize the risks that are truly likely to affect the organization's important assets. It also makes it possible to set security objectives to cover risks and to determine the appropriate level of resistance to meet these objectives.

5.2.2 EBIOS Method for IICS risk assessment

We studied the feasibility and the necessity of extending the EBIOS risk analysis method to suit the industrial context. The objective is to create a fully IICS oriented version of the EBIOS method. Our starting point was the industrial specificities that make the difference between ICS and Corporate systems, especially from a security standpoint. The main points of difference lie in the characteristics of the system components:

- ICS components have different functions from IT components (different functional levels),
- They have different technical types (IT vs OT)
- Industrial processes are different from IT processes (Production centric vs Data centric).
- Their security requirements are also different

On the other hand, the main goal of a risk analysis is to evaluate the risk. Risk as defined by EBIOS is a function of the likelihood of a feared event and its gravity.

The industrial systems specificities mentioned below do not have any influence on the calculation of a risk because the concepts of feared event, its probability and its gravity remain very high level concepts that are applicable to any system whatever its nature. The only thing that changes in the EBIOS method usage, from one context to another, is the context itself.

We therefore came to the conclusion that creating a new EBIOS-based risk analysis method for industrial systems is not of much interest because EBIOS is already usable as is. The best we can do is to provide guidance elements and a knowledge database that assists in working with EBIOS in industrial contexts for users who are only used to information systems contexts. This was not something we were particularly interested

in for our study, but we have slightly customized EBIOS to make it more suitable for our segmentation method. We will see how this was achieved in the next sections.

5.3 Risk based IICS segmentation Method

5.3.1 The principle

RIICS is a new IICS segmentation method that aims to ensure efficient zoning to meet actual security needs of IICS. The principle of RIICS is illustrated in Figure 5.2. The segmentation is done in two phases. First, the system is analyzed and modeled to create the system's model that represents the main input of the segmentation phase.

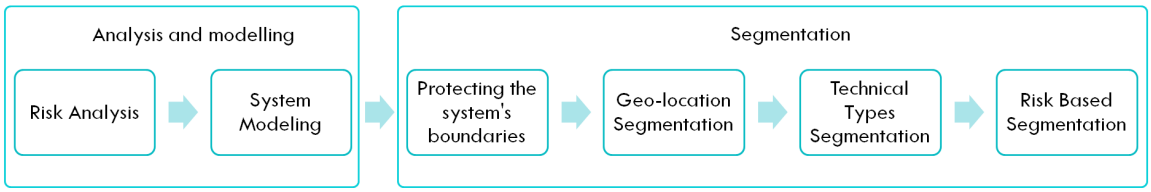

Figure 5.2 – RIICS principle

The system's modeling is based on the meta-model presented in section 5.3.2 and on a risk analysis of the whole system. An IICS model primarily focuses on system components and their interconnections. Risk analysis allows the evaluation and attribution of risk levels to the system's components (section 5.3.2).

At the second phase, the system should first have its boundaries protected before being segmented. The segmentation operation consists, next, of grouping the system's components according to their geo-location, technical type and risk level characteristics in three cycles. Simply stated, components that have the same geo-location, the same technical type and the same level of risk constitute together a single security zone.

5.3.2 Analysis and modelling

Risk Analysis

Components modeling requires the evaluation of their risk. This should be carried out using a risk analysis. We will use a somehow customized version of the EBIOS [de la Défense Nationale 2010] risk analysis method.

Risk analysis using EBIOS at the first phase of the method is done in 4 steps as illustrated in Figure 5.1.

Studying the organization's context

The first step of risk analysis is to study in depth the technical, functional and business context of the organization. For the study to be conducted properly, sufficient knowledge of the company's data, business processes, existing security policy and procedures, business model and competitors is required. The objective of this step is to:

- Model the company's assets
- Model the system architecture (components and connections)
- Acquire sufficient knowledge about technical, functional and business specificities of the company's assets.

Modeling the system relies on the meta-model of Figure 5.3. The system system modeling reuses almost the same modeling concepts introduced by SONICS. The system is still modeled as a set of components connected by connections and belonging to processes and geographical sites. However, it introduces the "risk" as a key characteristic for components. This meta-model also includes the SONICS meta-model but utilizes a lot of EBIOS concepts. It combines both SONICS and EBIOS meta-models to preserve the segmentation concepts and make use of the risk concepts. It creates a bridge between SONICS and risk analysis. This meta-model models a company as a set of assets. Assets are any valuable resource necessary to achieve the organization's objectives. There are two types of them: essential elements and entities. Essential elements are deployed, managed and protected by entities. Entities are assets such as sites, personnel, equipment, networks, software or systems. Essential elements potentially involve feared events that can occur as a result of an threat scenario operated by a threat source. Threat scenarios exploit entities vulnerabilities.

- **Essential elements**

  Essential elements of a company are its most important assets. They usually have many security requirements that should be analyzed and considered by the risk analysis. Processes and digital data are good examples of essential elements.

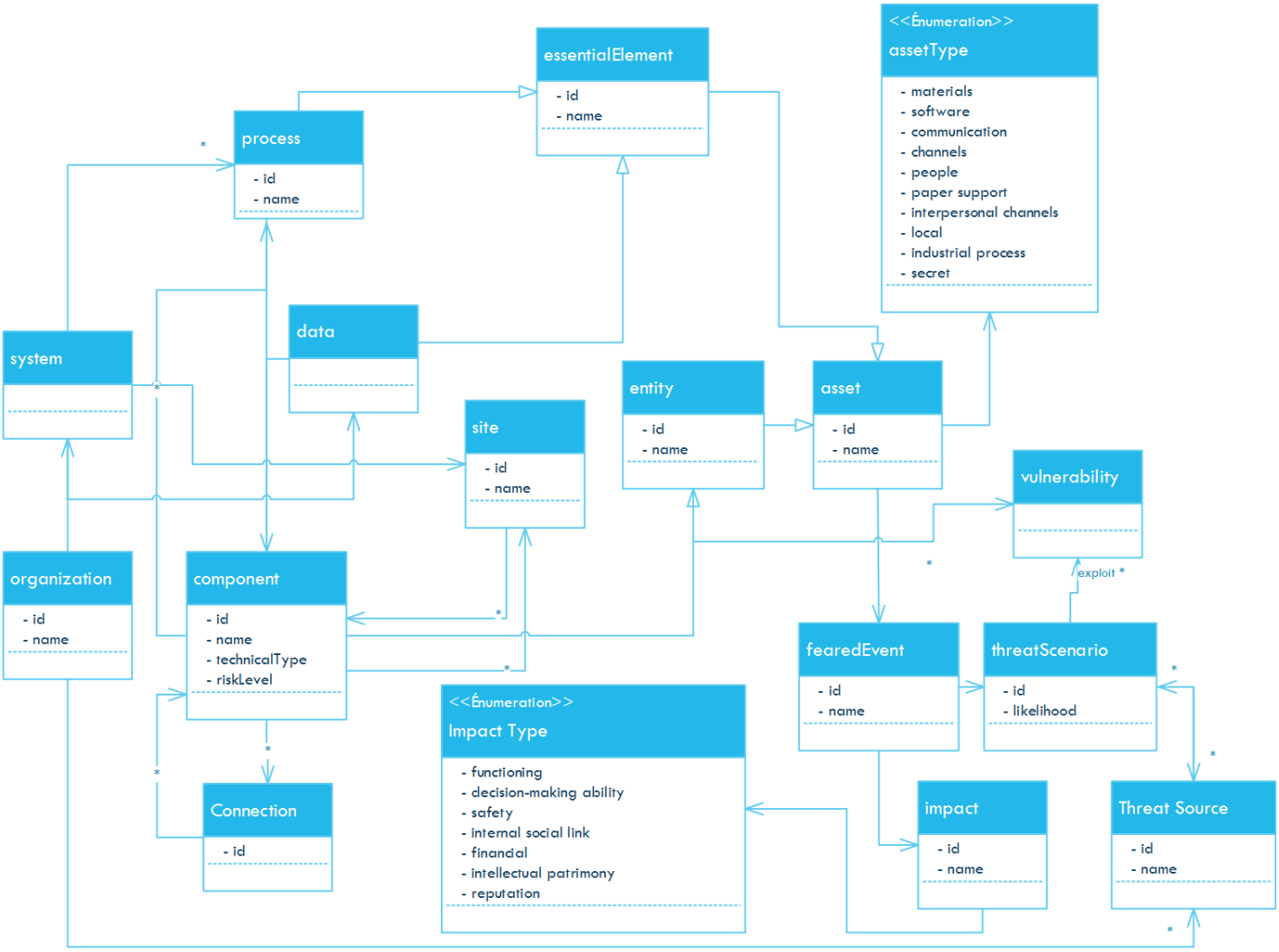

Figure 5.3 – EBIOS Meta-Model

- **Processes** A Process is a set of interrelated or interacting activities, which transforms input information into and output". A system is organized into multiple processes. Each process may contain one or more components. Processes identification should be done by the company. In general, an organization standard such as ISO9001 is applied to partition the system into multiple processes. Processes use one or more system components to ensure their operation. Order placement processes, billing processes, industrial control process, and secret recipe manufacturing processes are examples of essential elements processes. Special attention should be paid to confidentiality and integrity for IT processes and availability for industrial processes.
- **Digital Data** All data stored, manipulated or exchanged by components such as databases and file systems. They are highly valued by the company

and usually are critical assets. Clients personal data, invoices, orders and SCADA logs are examples of precious data.

- **Entities**

  Entities are assets of the system that perform core functions, process, store and transmit essential elements. These include physical locations, computing and human resources, networks, applications and software... As far as our method is concerned, we pay special attention to *Components* and *Connections* because they are the primary focus of the method.

  - **Components**

    Components were defined by the SONICS meta-model in section 4.2.2. However, for the RIICS method they are only characterized by their:

    * **Geographical Location**
    * **Technical Types**
    * **Risk Level**

      This is the novelty of RIICS. *Components* should also be characterized by their risk level. It can have one of the risk levels of Table 4.5. *Components* risk evaluation will be explained in section 5.3.2. Evaluating the risk levels of the *Components* is the main motivation for using a risk analysis method.

    Connections

    Connections were defined by the SONICS meta-model in section 4.2.2. They are modeled the same way by RIICS.

Identify the feared events and estimate their gravity

Feared events are security violations (in terms of confidentiality, integrity and availability) to one or more essential elements of the system under study. An example of feared events is the access to some essential elements (such as a clients database) by a non authorized external person. Each feared event is associated with a gravity level. Feared events gravity is the extent of its impact on one or more of the company's essential elements. It can have one of the gravity scale values from Table 4.3. Gravity estimation is done with a qualitative approach that needs good knowledge of the organization's system and business.

Analyze Threat scenarios and estimate the likelihood of the attack

Threat scenarios are operating mechanisms applied by threat sources (competitors, enemies, internal opponents, human error...) to violate security of entities (especially components) in order to achieve a feared event on one or more essential elements. A threat scenario can be either intentional or accidental. Basic threats typically involve exploiting system vulnerabilities at the organizational, functional, operational, or design level. Vulnerabilities are identified based on a security diagnosis. Special attention should be paid to potential threat scenarios and vulnerabilities in relation with components and their connections.

Each threat scenario is associated with a level of likelihood from Table 4.4. This depends on the attractiveness of the target for the threat source and how easily the attack can be achieved. Threat sources should be identified and qualified in terms of capacity and motivation.

Evaluate the risk level

The objective of this step is to assign a risk level value from Table 4.5 to each component of the system. This requires that the feared events of all the essential elements hold by the components are identified, their gravity estimated, all threat scenarios related to these feared events listed and their likelihood estimated.

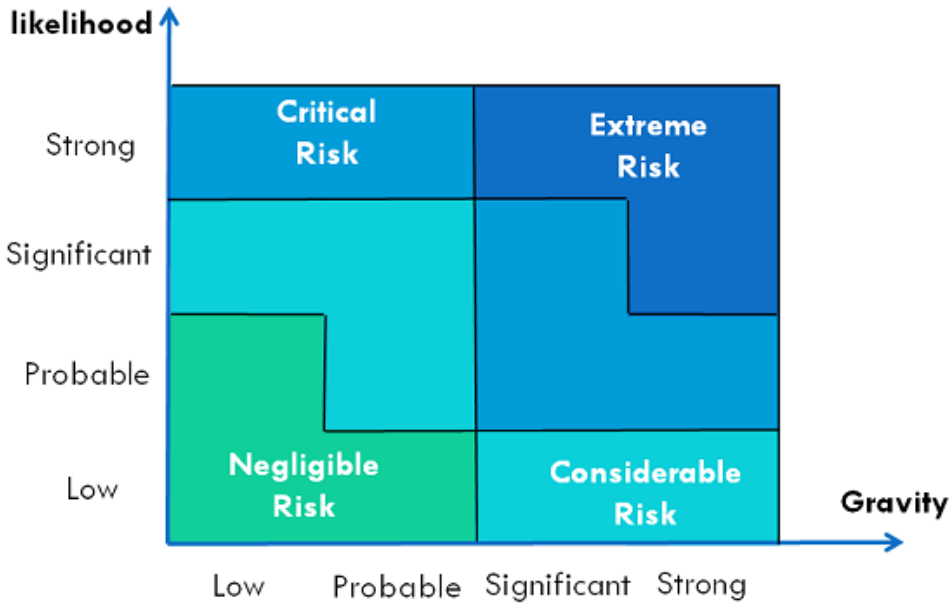

Figure 5.4 – Risk levels grid

The risk level of a *Component* is a function of feared events gravity and their likelihood. For one feared event and one threat scenario, the risk level is calculated using the the risk levels grid in Figure 5.4.

The risk level of a component should always be calculated assuming the worst case using the following formulas:

- The associated risk to an event and a scenario $Risk(event, scenario)$ is calculated using the risk levels grid.
- The risk associated to a feared event is calculated based on the most probable threat scenario:

$$Risk_{event} = Max_{scenarios}(Risk(event, scenario))$$

- The risk associated to an essential element equals the most important risk of its feared events:

$$Risk_{essential} = Max_{events}(Risk_{event})$$

- The risk associated to component is the most important risk associated to the essential assets it holds:

$$Risk_{component} = Max_{essentials}(Risk_{essential})$$

5.3.3 Segmentation

Once the components and connections are completely modeled, components are then straightforwardly grouped by their geo-location, technical types and risk levels. The segmentation can be formalized using mathematical objects as below to summarize the method and provides a useful starting point for implementation.

Preliminary:

Let S an IICS system, S = <C,Ge> where:

- C is the set of components of S,
- Ge is the set of all the geographical sites of S.
- $R = \{NEGLIGIBLE, CONSIDERABLE, CRITICAL, EXTREME\}$ is the set of all possible risks levels.

- $T = \{TI, TO, TIO\}$ is the set of all possible technical types.

Notations:

$\forall c \in C$,

- $tt_c \in T$ is the technical type of c.
- $site_c \in Ge$ is the site to which c belongs.
- $risk_c \in R$ is the risk level of c.

Definitions:

1. *Let* $\Sigma_{(S)}$ the set of all possible segmentations of the system S,
   $\Sigma_{(S)} = \{ \ \sigma \ / \ \sigma$ is a partition of C $\}$

   σ is a partition of C if:

   - $\emptyset \notin \sigma$
   - $\bigcup_{A \in \sigma} A = C$
   - $\forall A, B \in \sigma, \ A \neq B \Rightarrow$A $\cap B = \emptyset$

2. For each cycle of the method, we define the cycle's processor function as:

$$\begin{array}{rcccc} Pr_g & : & \Sigma_{(S)} & \rightarrow & \Sigma_{(S)} \\ & & \sigma & \mapsto & Pr_g(\sigma) \end{array}$$

   $Pr_g(\sigma) = \{A' \subset C / \forall c, d \in A', \exists A \in \sigma \ where \ c, d \in A \ and \ g(c) = g(d) \ \}$

   where g is the cycle's grouping function that depends on the cycle and respects the following definition:

$$\begin{array}{rcccc} g & : & C & \rightarrow & G \\ & & c & \mapsto & g(c) \end{array}$$

   G is a set of grouping values such as sites, technical types and risk levels. Thus:

   - The technical grouping function is:

$$\begin{array}{rcccc} tech & : & C & \rightarrow & T \\ & & c & \mapsto & tech(c) = tt_c \end{array}$$

- The geolocation grouping function is:

$$\begin{array}{rcl} geo & : & C \rightarrow Ge \\ & & c \mapsto geo(c) = site_c \end{array}$$

- The risk level grouping function is:

$$\begin{array}{rcl} risk & : & C \rightarrow R \\ & & c \mapsto risk(c) = risk_c \end{array}$$

3. We finally define RIICS as:

$$\begin{array}{rcl} RIICS_{(S)} & : & \Sigma_{(S)} \rightarrow \Sigma_{(S)} \\ & & \sigma \mapsto Pr_{risk} \circ Pr_{tech} \circ Pr_{geo} \end{array}$$

Let us assume that $\sigma_{initial}$, is the initial segmentation of the system S, $\sigma_{result} = RIICS_{(S)}(\sigma_{initial})$, is the result of the application of RIICS on the system S.

Application example

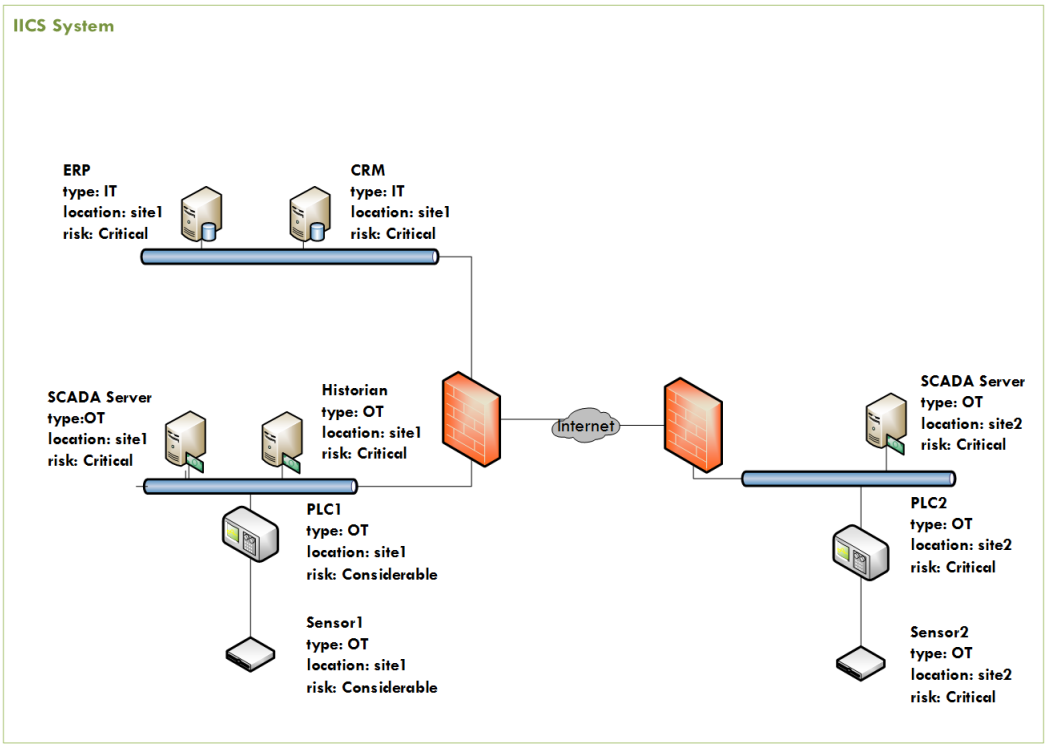

Figure 5.5 – Application example (1/4) - IICS System to segment

As an application example of the segmentation phase, let us assume that we have the modeled system of Figure 5.5. The example IICS system consists of a Corporate sub-

system and an industrial system geographically divided into two sites. The Corporate system belongs to the first site and only contains one ERP and one CRM. They are connected to the SCADA Server and historian from the ICS system of the first site. For simplicity, we assume that the components risks are already evaluated as depicted by the Figure. The technical types are assigned based on the definitions provided in section 5.3.2. For example, ERP and CRM are IT components, whereas, SCADA Servers, PLCs, sensors and actuators are OT components. The segmentation is then straightforwardly done in 3 steps as illustrated by Figures 5.6, 5.7 and 5.8.

1. The first step consists of grouping components by their geo-location. The system is composed of two geographical sites, therefore, we obtain two geographical segments (Figure 5.6).

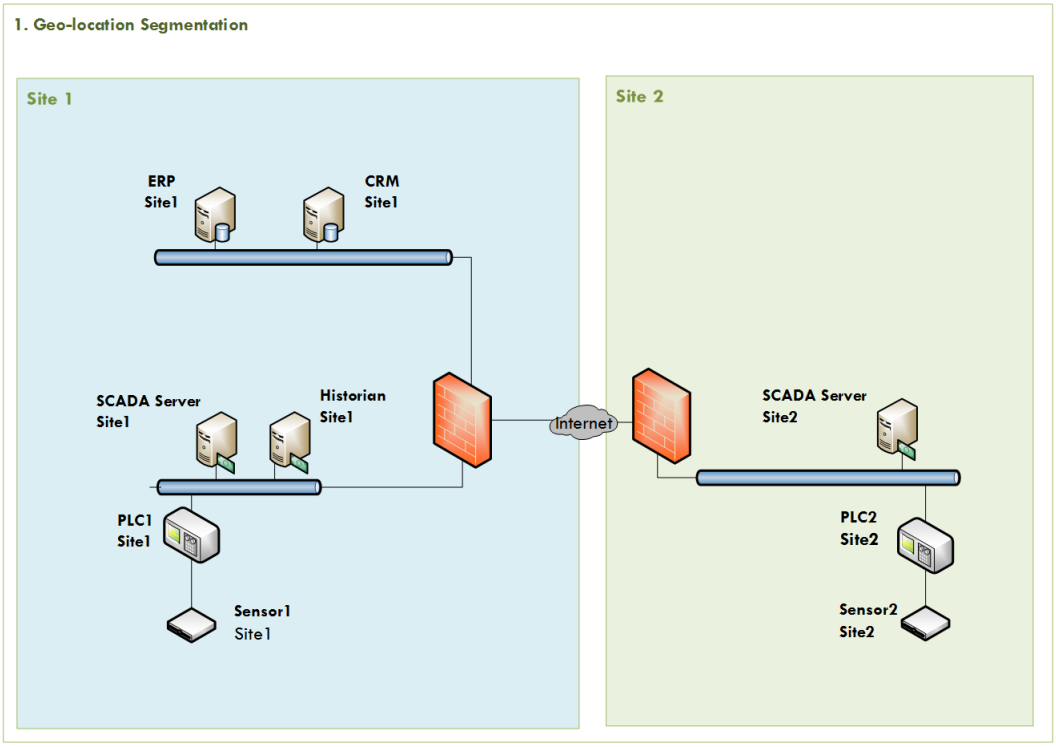

Figure 5.6 – Application example (2/4) - Geo-location Segmentation

2. Next, we group components according to their technical types inside the already identified geographical segments (Figure 5.7). The first geographical segment is then divided into two technical segments (one for IT components, and another for OT components). Whereas, the second geographical segment remains unchanged because it only contains OT components.

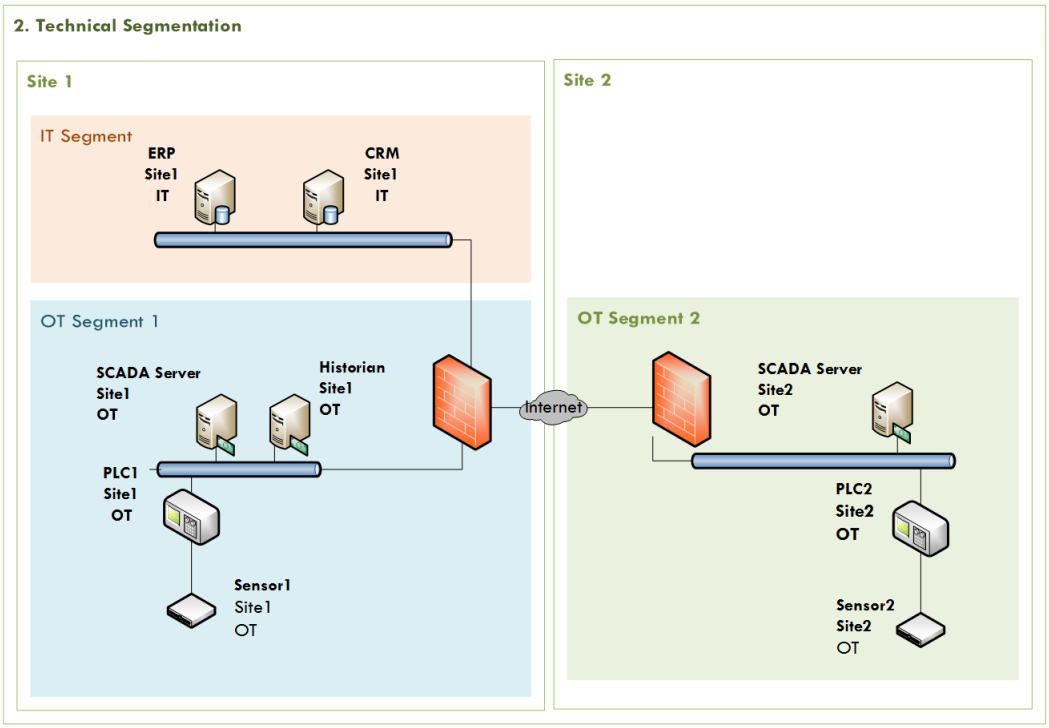

Figure 5.7 – Application example (3/4) - Technical Segmentation

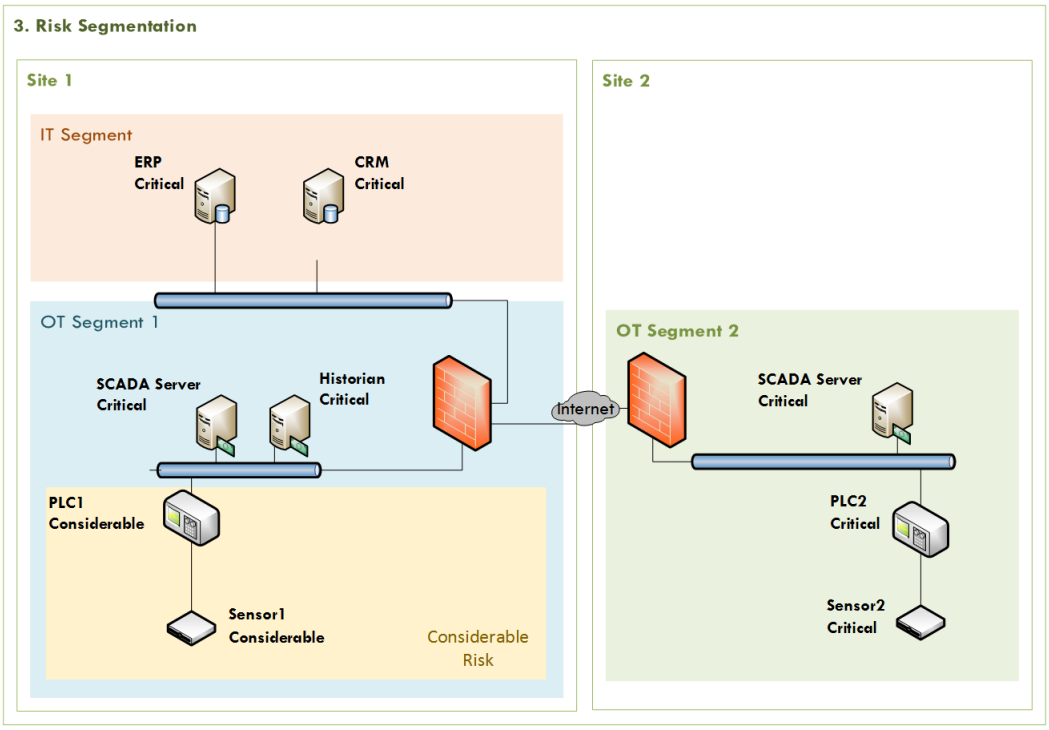

Figure 5.8 – Application example (4/4) - Risk based Segmentation

3. Finally, components are grouped based on their risk inside the already identified segments (Figure 5.8). Only one risk based segment is then added inside the "OT Segment 1". The other risk based segments are identical to the previously identified segments.

5.4 Tests and validation

For validation tests, we applied the same SONICS test methodology presented in section 4.3.1 to the same test system presented in 4.3.2.

5.4.1 Results and Discussion

The application of RIICS to the test system resulted in a segmentation similar to the *Ex-Segmentation* (Figure 4.9). The distance between the two segmentations is equal to zero. This result does not guarantee the efficiency of the method because it was obtained with only one system. The creation of several test systems with an Ex-Segmentation being very expensive, we have not yet been able to carry out all the tests necessary to validate the method. Nevertheless, initial results remain encouraging. Furthermore, the test system's risk analysis, is clearly not affordable for everyone. It requires a minimum level of knowledge and expertise in this type of practice. However, once the system model is created, the segmentation phase remains fairly quite simple.

5.5 Conclusion

This chapter presents RIICS, an IICS segmentation method that aims to fill the gaps of SONICS method to guarantee more accurate results that meet actual security needs of IICS. It is based on a risk analysis that helps to assess components risk. Systems models are used by the method to delineate security zones by grouping components with the same characteristics.

The first results of our validation test were rather accurate. However, we still have many more tests to do before we can confirm the effectiveness of the method. It is especially necessary to apply the method to a variety of systems with different configuration and various functional and business specificities. The cost of finding or creating test systems remains, however, significantly high.

Note that RIICS, just like SONICS, is also applicable to Information Systems (without any industrial system), because it is generic and because Corporate systems are subsystems of IICS.

However, segmentation is only about setting logical boundaries between security zones, and is not enough to apply a security policy or to implement a defense in depth strategy. Real physical boundaries have to be set up. This is achieved through segregation and access controls techniques.

The issue with ICS integration represents a new use case in terms of flow filtering mechanisms. The next chapter will present our study on improving flows controls of integrated ICS systems taking into account the IICS specificities. We propose to study using enhanced security techniques such as DTE for this purpose.

CHAPTER 6 DTE Access control model for IICS systems

6.1 Introduction

We designed RIICS method for segmentation of integrated ICS systems to simplify the identification of security segments by grouping components with the same security characteristics. A segment must be managed by the same security policy and maintained at the same level of protection. Segmentation is only about setting logical boundaries between segments, and is not enough to apply a security policy or to implement a defense in depth strategy. Real physical boundaries have to be set up. This is achieved through segregation and access controls techniques. They are used to control flows into and out of segments and flows between external and internal networks. This creates a defense barrier at segments boundaries to protect valuable resources. However, our study of the state of the art on segregation has revealed that no framework for segregation exists to date. All the resources we studied on segregation and access control provide either very specific solutions or good practices guidelines to implement segregation [Force and Initiative 2013, ISA 2013, ANSSI 2013].

Most of the proposed segregation solutions are firewall-based. While conventional firewalls perfectly work for Corporate systems, they are not always fully compatible with ICS. In fact, ICS systems usually are very demanding in terms of timing requirements while conventional firewalls may introduce significant latency. Firewalls are generally deployed on the boundaries of the segments to control all outgoing and incoming flows which creates a significant load. The deep inspection mechanism used by firewalls introduces a processing time that, however negligible it may be, becomes, by a mass effect, significant enough to challenge the use of firewalls in a context with very high timing requirements such as industrial systems [Cheminod et al. 2016, Zvabva et al. 2018, Li et al. 2018, Parra et al. 2019]. Firewalls inside ICS may thus constitute an angle of denial-of-service attack if their timing

impact is not seriously taken into account. Besides, most of existing firewalls only support protocols commonly used in Corporate systems especially TCP/IP and, for the best, some industrial protocols such as ModBus and DNP3 ([Tof 2014]) but with no possibility to define custom packet inspections to support more protocols [Cereia et al. 2014b, Cereia et al. 2014a, Li et al. 2018].

Therefore, we believe that a fundamentally more adapted access control mechanism is required to control flows within IICS with respect of the systems requirements. The new access control mechanism should:

- Apply strict controls on all flows, especially on communication with other networks
- Respect the timing requirements of industrial systems
- Allow to customize packet inspection to extend supported protocols. This will especially allow to support more industrial protocols.
- Simplify the definition of control rules to make it easier for administrators, especially industrial system administrators because they are less familiar with security concepts.

Domain and Type Enforcement (DTE) [Badger et al. 1995, Oostendorp et al. 2000] is an access control mechanism that holds promise to provide needed flexibility and strength while enforcing access controls. We suggest to study and explore whether security-enhanced control access, such as DTE, can be used to implement flow controls within IICS and replace the traditional IT firewalls.

There have been some studies investigating the use of DTE techniques on IICS systems such as the research work done by Schweitzer Engineering Laboratories [Bradetich and Oman 2007]. Although their findings are interesting, they are limited to securing integration flows with DTE techniques. Our objective in this study is to generalize DTE controls to the whole system by providing a generic model that provides simple and consistent concepts that allow control rules to be defined in a straightforward and homogeneous way across the system. Our work is a continuation of Trusted Information Systems, Inc.'s work on DTE Firewalls [Bradetich and Oman 2007, Bradetich and Oman 2008] that were the first to suggest using DTE for firewalls. However, our work is more focused on integrated ICS systems.

After reviewing the primary concepts of DTE, we will present the first phase of our study of using DTE for securing ICS and Corporate systems flows. We will present our generic ruleset based on the generic model provided by ISA95.

6.2 Data Type Enforcement concepts

6.2.1 DTE

DTE was originally proposed by Boebert and Kain [Oostendorp et al. 2000]. It is an enhanced form of table-oriented mandatory access control mechanism [Oostendorp et al. 2000, Hallyn and Kearns 2000a].

As with many access control schemes, type enforcement considers the system as a set of active entities (subjects) and a set of passive entities (objects).

- Active entities or subjects (usually processes). A domain and a DTE-protected user identifier (unchangeable even by the root user) is associated with each active entity, or subject
- Passive entities or objects (e.g., IPC messages, files or network packets). A type is associated with each passive entity, or object;

In DTE, two domain tables are considered:

- Domain Definition Table (DDT) represents allowed access modes between domains and types (e.g. read, lock, write, execute)
- Domain Interaction Table (DIT) represents allowed access modes between domains (e.g. signal, create)

Similarly to RBAC [Ferraiolo et al. 1995], all access attempts which are not authorised directly in the tables are denied. DTE policies can be specified in various languages (DTEL, SELinux TE language etc.). DTE policy should commonly implement the following components:

- **Type** declares one or more object types later used in the DDT
- **Domain** defines a restricted execution environment composed of three parts:
  - "Entry point" programs, identified by full pathname, that a process has to execute in order to enter the correct domain (e.g. /usr/sbin/sshd, /bin/login)
  - access rights to types of objects (e.g. read or append to /etc/password)
  - access rights to subjects in other domains (e.g. transition)

- Initial domain - defines the domain of the first process
- Assign - associates a type with one or more files

DTE has three main advantages. First, the security policy is specified in a high level language that reduces the burden of expressing, verifying, and maintaining security rules. Second, security attributes on objects are implicit, thereby allowing a file hierarchy to be typed concisely. Finally, DTE provides mechanisms for backward compatibility with existing software and with systems not running DTE.

6.2.2 DTE Firewalls

The DTE Firewalls were initially proposed by Trusted Information Systems, Inc. [Bradetich and Oman 2007, Bradetich and Oman 2008] to connect partner companies with a high level of security by extending limited trust to external entities, for example, suppliers, bankers, accountants, advisors, consultants, partners, customers, and allies [Oostendorp et al. 2000].

To extend DTE protection across networks, each network packet is regarded as an object (passive entity) with three associated attributes (carried in the IP option space of each datagram): the DTE type of the information, the domain (source domain) of the source process, and the DTE-protected UID of the source process. A process can send or receive a message object only if the process's domain has the appropriate access to the DTE type of the message. Communication with non-DTE systems also is mediated: when a message originates from a non-DTE host, the receiving DTE system assigns a type (and domain) to the message. Similarly, a DTE system mediates a message before sending it to a non-DTE system to ensure that the domain associated with the non-DTE system can read the messages. If the associated domain cannot read the message's type, the message is not sent.

6.3 DTE access control Model

We have created a generic access control model based on DTE. This new model, when implemented and applied to IICS, responds to the four requirements we presented before. The next sections provide the formal definition of the model and present the syntax to use to define the different DTE rules and concepts. We have created a DTEL language extension to represent the new concepts introduced by our model while remaining

compatible with the standard version of DTEL. Domains, objects and permissions are defined using almost the same syntax of the DTE language with a few new features.

6.3.1 Security policy definition

Entities

Unlike traditional access control approaches that define entities as hosts that send packets, entities for DTE consist of the processes that are running on the system.

- **Notation:**

  Let P the set of all the processes of a system S, C_i is a component that belongs to the system S and S_{Ci} is its operating system. We can define S such that:

$$S = \bigcup_{i=1}^{n} C_i$$

- **Property 1:**

  The set of entities of an operating system S_{Ci} on a component C_i is defined as $E(S_{Ci})$ where:

$$E(S_{Ci}) \subseteq P$$

An entity (a process) is defined as a pair of the component on which it runs and its runnable file on that component's system:

$$e = (parent_component, \quad file_path)$$

For example a process OpenERP that is run on an ERP_Server using the file $/bin/openerp$ is equal to:

$$OpenERP = (ERP_Server, /bin/openerp)$$

Services

Our new model allows to group processes into services. A service is a set of processes that are governed by the same access control rules. A service can group processes that are not on the same hosts. For example, an OpenERP and an SAP ERP processes can be grouped into one service $Serv_{ERP}$ if they have the same access control rules.

- **Property 2:**

  A service Serv is a set of processes (entities) such that:

$$\exists\ n \in \mathbb{N}^* / \exists P_0, ..., P_n \in P$$
$$Serv = \{P_0, ..., P_n\}$$

- **Property 3:**

  Any service Serv is a subset of P:

$$Serv \quad \subseteq \quad P$$

- **Property 4:**

  Let the *exec_serv* a function that returns the entities executed on a system S_{Ci} for a $Serv_j$ service:

$$exec_serv(S_{Ci}, Serv_j) \quad = \quad E(S_i) \cap Serv_j$$

A service is a set of component processes pairs. For example, provided the aforementioned $Serv_{ERP}$ can be defined as:

```
// define a service
component ERP_Server = 10.0.0.13;
component SAP_Server = 10.0.0.14;
Serv_ERP={(ERP_Server, /bin/openerp), (SAP_Server, /bin/sap),
    ...};
```

For example, assuming that the ERP OpenERP is running on a server with a linux operating system S_{SL} from the path /bin/openerp:

$$exec_serv(S_{SL}, Serv_{ERP}) = \{/bin/openerp\}.$$

The service view helps to abstract processes and define common access control rules. This is easier to handle for systems administrators with limited IT and security knowledge once processes are defined.

Objects

A DTE object is any system resource that can be accessed by an entity. In the context of DTE, objects are generally files, memory space... For network communication, objects

are the packets that are transmitted between entities. Our model will mainly focus on this type of object.

An object can be defined as a set of attributes that are transmitted as portions of the packet. Objects attributes are, for example, the source or destination IP address, the source or destination port, data from the application layer...

In order not to have to extend the syntax of the model with each new protocol, the attributes are defined by their position in the packet. This allows to model objects and their attributes in a generic way and ensures very loose coupling between the objects attributes and the underlying protocols that can be replaced or updated over time.

- **Property 5:**

  An attribute c is defined as a vector that indicates its position in the packet:

  $$c \quad = \quad < offset, \quad length >$$

  For example, we can represent the TCP port source within a packet that has a length of 2 bytes and is at position 0 of the TCP segment that is itself encapsulated in a 20-byte header IP packet that is itself encapsulated in a 14-byte header Ethernet frame as:

  $$TCP_{src-port} \quad = \quad < \quad 34, 2 \quad >$$

- **Property 6:**

  Let O_S the set of objects within a system S. An object is defined as a set of attributes with their associated values:

  $$\begin{gathered} \forall n \in \mathbb{N} \quad o =< ((c_1, valeur_1), ..., (c_n, valeur_n)) >\in O_S \\ \Rightarrow \forall i \in [1, ..., n] \\ c_i.offset \in [1, ..., packet_{max-size}] \\ and \quad c_i.length + c_i.offset \leq packet_{max-size} \end{gathered}$$

Below are some examples of object definitions:

- $o =< (< 36, 2 >, 80) >$ represents all packets with a destination port equal to 80. They are generally requests for a web server.

- $o =< (< 30, 4 >, 10.0.0.1), (< 36, 2 >, 502), (< 61, 1 >, 3) >$ represents all the packets of a Modbus TCP/IP connection to the machine with an IP address of 10.0.0.0.1. This represents a Modbus request to read a register.

By defining objects this way, it is easier to handle new protocols without having to modify the implementation of the rule engine and access control mechanism. In addition, for similar protocols in terms of payload such as SCTP/TCP, it is possible to reuse rules that include objects with identical attributes.

Types

Objects can be grouped into groups called types.

- **Property 7:**

  Let T_S the set of all the types within the system S, a type is defined as:

$$\forall t \in T \quad t = \{o_1, ..., o_n\} \quad \rightarrow \quad \forall i \in [1, ..., n], \quad o_i \in O_S$$

In order to remain compatible with DTE Languge (DTEL), we use exactly the same syntax to define types and assign them to objects except that the definition of objects is slightly different from DTEL.

```
type type_name;
assign type_name object;
```

For example:

```
type read_register;
assign read_register <(<30,4>,10.0.0.1),(<36,2>,502),(<61,1>,3)
   >;
```

Actions

In a DTE context, entities can perform actions on packet objects of a particular type. Three possible actions can be distinguished:

- **send:**

  this action represents the possibility to send a DTE object type by entities

- **receive:**

  represents the possibility to receive a DTE object type

- **send_state:**

  is used to support connection oriented protocols of the transport layer. That is, protocols where messages can be bi-directional once the connection is initiated by the sender that can then receive messages from the receiver if they comply with the protocol state machine.

Domains

A DTE domain is a list of tuples $(\{entities\}, (action \rightarrow object_type))$.

The initial DTEL allows to define inter-domain controls to define which domains are authorized to interact and the actions that can be performed. Only process-related interactions (sending signals, creating processes...) are supported.

Therefore, the initial DTEL has to be extended in order to:

- Support the new actions defined previously (send, receive, send_state) in order to allow processes from different domains to communicate (exchange objects) with each other.
- Limit access to some objects. When a domain is authorized to communicate with another domain, it is necessary to define which DTE objects are allowed to be exchanged between these two DTE domains.

We will use the following syntax:

A domain can be defined using the new DTEL syntax as follows:

```
type some_object_type_1;
type some_object_type_2;

domain some_domain = (
    /* first tuple */
    {
        (component_a_1, process_path_a_1),
        (component_a_2, process_path_a_2),
    ...
    },
```

```
    ( action_1 -> another_domain_1{some_object_type})

    /* second tuple */
    {
        (component_b, process_path_b_1),
        (component_2, process_path_2),
        ...
    },
    ( action_2 -> another_domain_2{some_object_type_2})

    /* more tuples */
    ...
);
```

where $(component_i, process_path_i)$ are entities, and $action_i$ can be "send", "receive" or "send_state".

For example:

```
type schedule_production;

domain erp_domain = (
    {(ERPServer, /bin/openerp)} ,
    (send -> manufactoring_domain{schedule_production})
);
```

Since services are themselves sets of processes, entities that belong to a domain can include individual processes or services as well. For example:

```
type schedule_production;

Serv_ERP={(ERP_Server, /bin/openerp), (SAP_Server, /bin/sap)};

domain erp_domain = (
    {Serv_ERP} ,
    (send -> manufactoring_domain{schedule_production})
);
```

This is only an extension of the DTEL syntax that remains compatible with the original syntax. If the authorized DTE objects are not specified, the behavior defined by initial DTEL is applied, which allows actions to be performed on the entire destination DTE domain.

- **Property 8:**

  Each entity belongs to one or multiple domains.

6.3.2 Domains communication

DTE domains are a logical grouping of entities. The system's flow control rules primarily rely on them such that:

- **Property 9:**

  Inter-domain flows are by default denied. An explicit rule should be added to authorize a communication between two domains.

- **Property 10:**

  Flows between entities that belong to a same domain are permitted.

Mediation

In a DTE context, some hosts (source or destination) may not be DTE compatible. In order to properly process objects sent by a non-DTE host, it is necessary to determine the domain of the sender. Mediation is a mechanism that associates DTE domains to non-DTE entities. It uses the packet headers to determine the DTE type of the packet and the DTE domain to which the sending or receiving entity belongs.

To perform the mediation, the DTEL language defines the inter_assign command with the following syntax:

```
inter_assign  object_definition  a_domain;
```

It is necessary to precisely determine the domains of processes executed on non-DTE hosts that may contain processes from different domains. It is important to wisely use objects'attributes that precisely identify the corresponding domain. It is possible to identify non-DTE processes based on hosts'source and destination IP addresses as well as ports, or application-level protocols.

For example, to assign the "web" domain to a non-DTE web server process running on host 10.0.0.13:

```
1 inter_assign  <(<30,4>,10.0.0.13),(<36,2>,80)>  web;
```

Segments

The system may be segmented into multiple segments. A segment is generally technically implemented a sub-network or a VPN [Andress and Leary 2017] in which all communications that respect the segment's security policy are allowed, but where access control equipment such as firewalls are placed at the segment's boundaries to control all incoming and outgoing flows.

For example, in TCP/IP systems, two important rules are applied in regard to segments:

- Components can determine whether another component belongs to the same segment, to decide whether it can directly communicate with it or if it must cross a gateway. This can be done for example using ip masking techniques.
- Components within the same sub-network communicate with each others to configure themselves using protocols such as ICMP, IGMP, ARP.

Using DTE in a segmented system is problematic. Flows between DTE domains are by default denied while intra-segment flows can be permitted by the security policy that governs the segment. If a segment contains components that run entities that belong to different domains, communication between these entities will be by default denied by the DTE controls.

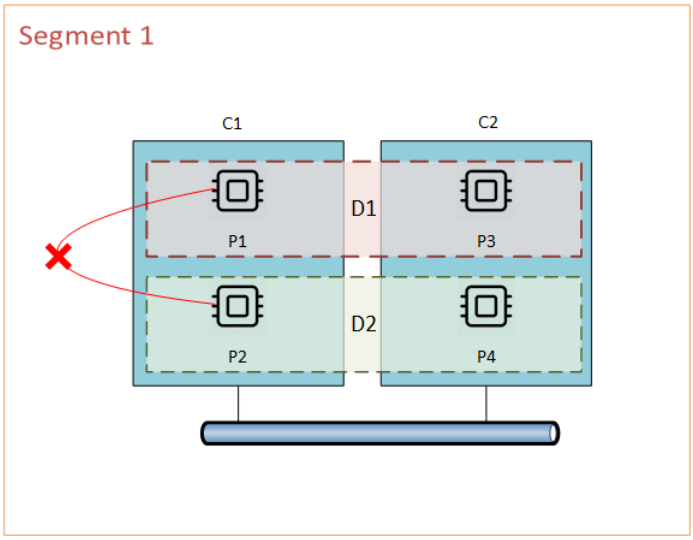

Figure 6.1 – Segmentation and multi-domain problem

For example, in Figure 6.1, components C1 and C2 belong to the same segment. C1 runs two processes P1 and P2 which belong to domains D1 and D2 respectively. C2

runs processes P3 and P4, which belong to domains D1 and D2 respectively. While P3 and P1 are authorized to communicate as they belong to the same domain D1, P2 and P1 are not authorized to communicate unless an explicit authorization rule is defined. This is an unwanted behavior inside a segment where P2 and P1 are authorized to communicate.

The reason for such an incompatibility is that inter-domain communication is DENY-ALL oriented while some communications within a segment should be authorized.

The first and most direct solution to this problem is to add rules to explicitly authorize entities inside the same segment to communicate with each others. However, this can quickly become a very burdensome task, especially when the system is composed of a large number of segments.

A more thoughtful solution is to use Properties 8 (6.3.1) and 10 (6.3.2) previously presented that assert that a process can belong to multiple domains and that the intra-domain flows are by default permitted. For each segment of the system, we will define a new domain to group all the processes of that segment that are authorized to communicate in order to allow communication between them.

Continuing with our previous example, the solution, as illustrated in Figure 6.2, is to create a new Dseg1 domain that includes all the processes that are authorized to communicate.

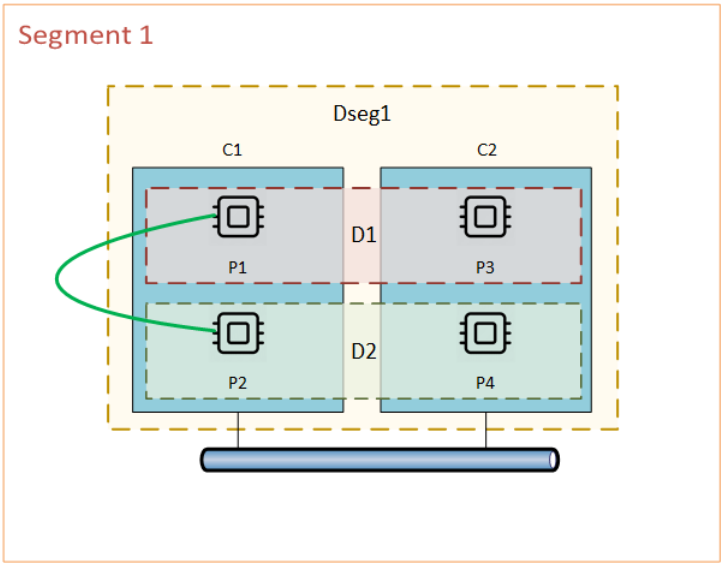

Figure 6.2 – Segmentation management with DTE

Note 1: Mitigate the risk of the intra-segments flow

Sometimes, some components, although within the same segment, are not allowed to communicate. For example, to protect a component against the compromise of another component that communicates with it. The segment domain should then not include the processes of that vulnerable component. Nevertheless, if a component is known to be vulnerable and to present a risk for the components within the same segment, the isolation of that vulnerable component into a separate segment should seriously be considered.

If the system segmentation is done with the RIICS method, it is unlikely to need to protect one component against the compromise of another component of the same segment. Provided the risk analysis is correctly performed, components of the same segment supposedly are on the same level of risk. The RIICS method separates components with a high impact, and a vulnerable components into different segments.

Therefore, by using the RIICS method for segmentation, the authorization of all intra-segment flows can be acceptable as all components of the same segment are on the same level of risk. If, in some cases, more controls on intra-segment flows are needed, this can be achieved by using additional access control mechanisms (other than DTE) for the concerned flows. However, this is not in the scope of our study.

Note 2: Inter-segments flows control

Inter-segments flows are also controlled. Controls are performed using DTE at the host level or at the DTE Firewalls deployed on the boundaries between the segments. More details about the flows control mechanism are provided in the next section. By creating a domain per segment, inter-segments flows will be controlled using DTE rules to authorize, for example, two processes from two different segments to communicate.

6.4 Access control

This section explains the operating procedure of our DTE model access controls.

6.4.1 DTE Hosts

While non DTE hosts rely on the mediation mechanism to be DTE-compatible, DTE hosts natively implement DTE access control inside their Operating System. Multiple DTE prototypes were developed [Hallyn and Kearns 2000b, Badger et al. 1996]. They all are based on UNIX. As for our model, a new prototype is needed. However, the operating procedure of the access control mechanism will be explained.

6.4.2 Operating procedure

On DTE hosts, access control is applied whenever a packet is sent or received by a process running on the DTE host. When a packet is sent, the rules defined regarding the sending domain will be verified. To achieve this, all rules that apply to the process that sends the packet will be checked. For each rule, the packet is compared to the object type of the rule trying to return only one rule at most. If a send action authorization rule matching the object type is found, the packet is allowed to be sent, otherwise it is rejected.

If the packet is authorized to be sent, the source domain is added to the packet header (in the option field of the IP header) by the sender (assumed DTE compatible) before the packet is sent.

When the receiver receives the packet, it identifies all the destination domains. For each destination domain, the control rules are checked to determine whether such a packet is allowed to be received. This is done by calculating the source domain and the type of the packet from the header. If a rule allows such a packet to be received, the destination process is then allowed to receive it.

6.4.3 DTE Hosts access control

DTE allows access control to be carried over to the edges of communications i.e., to hosts that support DTE. It is no longer necessary to process all the packets on the firewall as usual. This allows to define much more fine-grained control rules such as applying controls at the application level without worrying about the firewalls performance. Since firewalls are generally at the segment boundaries, they have to process all incoming and outgoing packets. Deep packet inspection can drastically reduce the firewall performance (processing time may reach several tens of milliseconds). However, when the objects are controlled locally on DTE hosts, where the traffic to be processed is much smaller, it is possible to apply more sophisticated controls without impacting the processing time of the objects and their latency. This ensures highly effective access control while respecting the real-time requirements of the system.

6.4.4 Firewall access controls

DTE firewalls should be deployed at the segments boundaries. They are in charge of ensuring that access controls are properly performed by the DTE hosts. Message processing by the firewall can affect the real-time performance of the system. However,

it does protect against the compromise of some hosts that may bypass the access control rules for which they are responsible.

In order to optimize the DTE firewall performance, it would be possible that it does not check the validity of communications of some DTE hosts depending on its level of trust in those hosts. The trust granted to DTE hosts by a DTE firewall will be defined by the administrator. This makes the verification process on some DTE objects more flexible depending on the reputation of the equipment sending the message. The reputation can be a value calculated based on the application of updates, the version of the operating system...

Controls on flows to and from hosts in a segment still remain as strict as they should be because communications from outside a segment are by default not allowed and must be explicitly authorized. This furthermore reduces the load on Firewalls.

The DTE firewall will also be responsible for mediation between non-DTE and DTE hosts. Two cases are to consider:

- **The source is a non-DTE host:**

  The firewall is then in charge of determining the host's source domain based on the content of the packet using the Mediation mechanism explained in section 6.3.2. Once the source domain is identified, the firewall applies the access right verification procedure explained in section 6.4.2 in order to verify that the packet (DTE object) can be transmitted to the destination DTE domain and that the destination DTE domain accepts to receive such an object.

- **The destination is a non-DTE host:**

  In this case, packet processing is relatively simple for the DTE firewall. The most important thing is to determine the source domain which is already known in the case of a DTE source host or determined as described before. When the source domain is known, it is simple to determine the destination domain based on the object type and the specified DTE rules before transmitting the packet to its destination.

6.4.5 Sharing definitions and rules

Definitions and rules must be reusable between DTE equipment, and must also be locally overwritable. We suggest a new security policy storage and processing strategy. DTE devices will apply access controls based on two security policies: global security policy and local security policy.

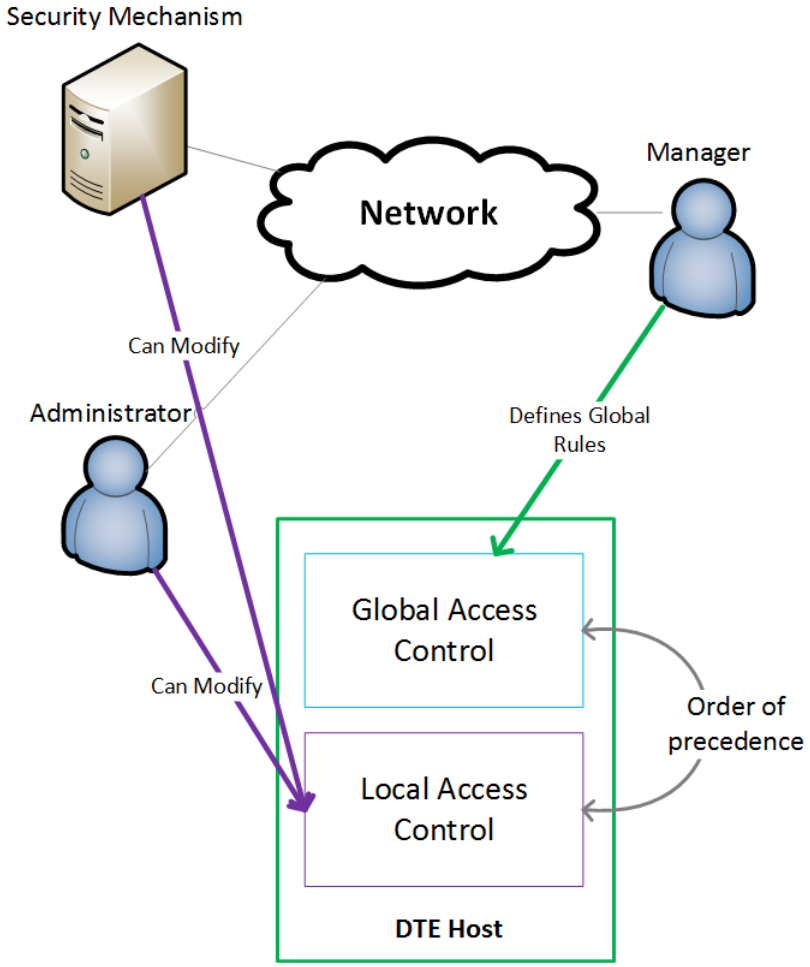

Figure 6.3 – DTE global rules management architecture

Global security policy

Global security policy is stored on a central server. It mainly consists of global access control rules, objects and domains definitions. It is managed by the system's security managers.

DTE devices retrieve this global security policy and store it locally in a "Global access control" module and apply it by default to perform access controls.

Local security policy

Global security policy can be overwritten locally by the device's administrators and authorized automated security mechanisms as illustrated in Figure 6.3. Local access rules are stored in a "Local access control" module. An order of precedence between

the two modules can be defined to determine whether or not local access control must override global access control.

Such an approach offers the advantage of being able to strengthen local access control without completely overriding global access control. For example, a security mechanism such as an IPS can operate locally on DTE devices to define new rules that block certain sensitive communications. It will thus be able, if authorized, to modify the local access control rules without affecting the global security policy.

Local security policy modification

Local security policy can be modified by authorized administrators and automated security mechanisms. The modification can be performed through a local process on the DTE host that receives policy modification requests from authorized entities and perform the requested modification. Access to this local security policy modification process is controlled using DTE rules.

For example, let's assume that the local security policy modification process is executed on the DTE device from $/bin/modif_acl$ as a daemon that listens on port 5000. This process can be used to modify the local access control file $/etc/local_acl$.

To authorize an IPS $/bin/snort$ process to use the $modif_acl$ process in order to make changes on the $local_acl$ file, the following rules are created :

```
type modif_acl;
type modif_acl_com;

component IPS_Server = 10.0.0.23;
component My_Host = 10.0.1.9;

domain ips =
    {(IPS_Server, /bin/snort)},
    (send_state -> host(modif_acl_com});

domain host =
    {(My_Host, /bin/modif_acl)}, (receive -> ips{modif_acl_com
   }), {(My_Host, /bin/modif_acl)}, (rw ->modif_acl);

assign /etc/local_acl modif_acl;
assign <(<36,2>, 5000)> modif_acl_com;
```

Thus, Snort process will be authorized to send policy modification requests to the DTE Host on port 5000. When such a request is received, the $/bin/modif_acl$ process is authorized to accept it and process it. The $/bin/modif_acl$ process is, on the other hand, authorized to read and modify (rw) the $/etc/local_acl$ file. However, it is not allowed to read or write the global access control file.

6.5 Application of DTE access control to IICS

Our control access model divides the system into multiple logical domains that include the different entities. The definition of domains and control rules are to be defined on a case-by-case basis depending on the system, however a large part of the access control policies is totally generic and can be applied to all IICS. This generic part is based on the functional integration model defined by ISA [ISA 1999] which defines the functions of an enterprise involved with manufacturing as well as the information flows between the functions that cross the Corporate/ICS interface.

6.5.1 Functional Model

The ISA [ISA 1999] functional model represents IICS as a set of functions, external entities and communication flows between them. It focuses on manufacturing IICS.

For this model, functions are a set of tasks with a common objective and are represented by a marked ellipses in the Figure. External entities are entities that exchanges data with the functions from outside the system. They are represented as a labelled rectangle. A solid line with an arrow represents data flows between functions, or external entities. A dotted line with an arrow represents a groups of data flows. The heavy dotted line illustrates the integration layer between the Corporate and ICS systems. It intersects functions that have sub-functions that may belong to the ICS system, or to the Corporate system depending on the system. This line is equivalent to the Level 3 - Level 4 interface defined in Chapter 2.

The ICS side of the integration layer includes Production Control functions and some of the Quality, Maintenance, Production Scheduling and Product Control functions. Whereas, the Corporate side includes business functions such as Order Processing, Product Cost Accounting, etc. However, the model structure does not reflect an organizational structure within a company, but an organizational structure of functions. Different companies will place the functions in different organizational groups. Functions and flows are out of scope.

6.5.2 Generic policy

We will use the generic functional model to create a generic part of the DTE security policy that should be deployed on an IICS system. The used functions represent DTE domains, and the flows between the functions represent the flows to be controlled. They represent the objects types.

This generic policy is intended to simplify the deployment of DTE access control and provide a good introduction to the concepts of domains and types of packets for administrators. However it remains, of course, extensible. The creation of new types, domains and control rules will be possible globally and locally.

Domains and Objects

For each functional domain, a DTE domain is defined. The interactions between these domains correspond to the DTE objects exchanged by the domains. Each domain contains a list of services.

Services

Besides the domains, our generic policy also includes definitions of some generic services. These were identified based on our reference architecture. They are:

- **ERP Services**

  This service includes all processes that can be grouped under the name of ERP. These are the different ERP software solutions that are deployed in the Corporate System. ERP services generally perform functions of “Order Processing”, “Production Scheduling”, “Material and Energy Control” and “Procurement”.

- **CRM Services** Includes all CRM processes of the Corporate System. They generally carry out the functions of “Order Processing”, “Product shiping admin” and “Product Cost Accounting”.

- **MES Services** Contains the MES processes of the ICS. They generally perform the functions of “Product inventory”, “Quality Assurance” and “Production Scheduling”.

- **Industrial Control Services** Includes ICS SCADA processes. They generally perform the “Production Control” functions.

- **Maintenance Services** Includes all entities involved in "Maintenance Management" functions such as maintenance tools installed on workstations.
- **Support Services** includes all cross-functional entities that handle other transversal functions of the system such as printing, emailing....

A summary of these services is provided in the table below 6.1.

Table 6.1 – Generic IICS Services

	CRM Services	ERP Services	MES Services	Industrial Control Services	Maintenance Services
Production Control				X	
Product Shipping Admin	X				
Product Cost Accounting	X				
Order Processing	X	X			
Production Scheduling		X	X		
Material and Energy Control		X	X		
Procurement		X			
Quality Assurance			X		
Product Inventory Control			X		
Maintenance Management					X

Access control rules

- **Property 11:** Any DTE equipment in an IICS will have at least the following DTE rules:

```
/*
The services below should be defined by manager
Exp: define ERP_SERVICES = (/bin/openerp), (/bin/sap)
*/
/*
define ERP_SERVICES,
CRM_SERVICES,
MES_SERVICES,
INDUSTRIAL_CONTROL_SERVICES,
MAINTENANCE_SERVICES,
SUPPORT_SERVICES;
*/

domain Order_Processing =
    {CRM_SERVICES,ERP_SERVICES}, (receive->
   Production_Cost_Accounting
    {cost_availability}),
    {CRM_SERVICES,ERP_SERVICES}, (receive->
   Production_Scheduling{availability}),
    {CRM_SERVICES,ERP_SERVICES}, (send_state->
   Product_Cost_Accounting
    {production_orders_acc}),
    {CRM_SERVICES,ERP_SERVICES}, (send_state->Quality_Assurance
   {finished_good_waiver});

domain Production_Scheduling =
    {ERP_SERVICES,MES_SERVICES}, (receive->Order_Processing{
   production_orders}),
    {ERP_SERVICES,MES_SERVICES}, (receive->Production_Control{
   production_capacity,
    production_from_plan}),
    {ERP_SERVICES,MES_SERVICES}, (receive->
   Product_Inventory_Control),
    {ERP_SERVICES,MES_SERVICES}, (send_state->Order_Processing{
   availability}),
```

```
    {ERP_SERVICES,MES_SERVICES}, (send_state->
   Product_Inventory_Control
    {pack_out_schedule}),
    {ERP_SERVICES,MES_SERVICES}, (send_state->
   Production_Control{schedule}),
    {ERP_SERVICES,MES_SERVICES}, (send_state->
   Material_and_Energy_Control
    {LTME_requirements});

domain Production_Cost_Accounting =
    {CRM_SERVICES}, (receive-> Product_Shipping_Admin
    {cost_availability}),
    {CRM_SERVICES}, (receive->Order_Processing{availability}),
    {CRM_SERVICES}, (send_state->Product_Shipping_Admin
    {production_orders_acc}),
    {CRM_SERVICES}, (receive->Order_Processing{
   production_orders_acc}),
    {CRM_SERVICES}, (send_state->Production_Control{
   production_cost_objectives}),
    {CRM_SERVICES}, (receive_state->Production_Control{
   production_performance_and_cost}),
    {CRM_SERVICES}, (receive->Material_and_Energy_Control{
    incm_material_and_energy_receipt});


domain Product_Shipping_Admin=
    {CRM_SERVICES}, (receive-> Product_Cost_Accounting
    {cost_availability}),
    {CRM_SERVICES}, (receive->Product_Inventory_Control{
   availability}),
    {CRM_SERVICES}, (send_state->Product_Cost_Accounting
    {}),
    {CRM_SERVICES}, (send_state->Product_Inventory_Control{}),
});

domain Procurement=
    {ERP_SERVICES}, (receive-> Material_and_Energy_Control {
   incm_order_confirmation}),$
    {ERP_SERVICES}, (receive-> Material_and_Energy_Control {
   material_and_energy_order_req}),
```

```
60      {ERP_SERVICES}, (receive->Maintenance_Management{
    maint_purchase_order_req}),
});

63
domain Material_and_Energy_Control =
      {ERP_SERVICES},MES_SERVICES, (receive->Production_Control{
66    LT_material_and_energy_requirements}),
      {ERP_SERVICES},MES_SERVICES, (send_state->Procurement{
      material_and_energy_order_req}),
69    {ERP_SERVICES},MES_SERVICES, (send_state->Procurement{
    incoming_order_confirmation}),
      {ERP_SERVICES},MES_SERVICES, (send_state >
    Product_Cost_Accounting{
      incm_material_and_energy_receipt});
72
domain Quality_Assurance
      {MES_SERVICES},(send_state->Production_Control{
    standards_and_customer_requirements}),
75    {MES_SERVICES},(send_state>Production_Control{QA_results}),
      {MES_SERVICES},(receive->Production_Control{process_data}),
      {MES_SERVICES},(send_state->Product_Inventory_Control{
    QA_results}),
78    {MES_SERVICES},(receive->Order_Processing{
    finished_goods_waiver});

domain Product_Inventory_Control
81    {MES_SERVICES},(receive->Product_Shipping_Admin{}),
      {MES_SERVICES},(send_state>Product_Shipping_Admin{}),
      {MES_SERVICES},(receive->Quality_Assurance{QA_results}),
84    {MES_SERVICES},(receive->Production_Scheduling{
    back_out_schedule}),
      {MES_SERVICES},(send_state>Production_Scheduling{
    finished_goods_inventory}),
      {MES_SERVICES},(receive->Production_Control{process_data});
87

domain Maintenance_Management
90    {Maintenance_SERVICES},(receive->Production_Control{
    maint_standards_and_methods}),
```

```
    {Maintenance_SERVICES},(receive->Production_Control{
   maint_requests}),
    {Maintenance_SERVICES},(send_state->Production_Control{
   maint_responses}),
    {Maintenance_SERVICES},(send_state->Production_Control{
   maint_technical_feedback}),
    {Maintenance_SERVICES},(send_state>Procurement{
   maint_purchase_order_req});


/* The types below should be defined by the manager */
/*
type production_orders,
availability,
cost_availability,
finished_good_inventory,
finished_good_waiver,
incm_material_and_energy_receipt,
incm_order_confirmation,
LTME_requirements,
LT_material_and_energy_requirements,
standards_and_customer_requirements,
maint_purchase_order_req,
material_and_energy__order_requirements,
maint_requests,
maint_standards_and_methods,
maint_technical_feedback,
maint_responses,
production_orders_acc,
production_cost_objectives,
production_performance_and_cost,
production_orders,
production_capability,
production_from_plan,
process_data,
pack_out_schedule,
schedule,
QA_results;
/*
```

These rules are totally generic because they are based on generic domains, services and actions. Nevertheless, all the types of objects used by this generic policy as well as the processes belonging to the services are to be defined according to the system. For example, this generic policy defines an Order_Processing domain, the services that belong to it, and authorized actions such as sending and receiving certain types of packets like ("ProductionOrder_Acc"), however, it remains up to the administrators to define the object (ProductionOrder_Acc) and the processes that belong to CRM_SERVICES.

6.6 Discussion

6.6.1 Advantages

The advantages of using DTE to implement an access control mechanism in IICS systems are numerous:

A single language for access control

The first advantage of DTE access control is that it uses a single rule-setting language across all systems. This reduces the complexity of administering multiple access control solutions with their languages at the same time. In addition, the centralization of rules and definitions provides a main entry point for administration that will be used most often for changes. These rules can still be overloaded on the hosts with the same language.

Language for defining high-level security policies

The service view provides more independence regarding the location of access controls in the system. It can be used for network access control (as it is usually found on a firewall) as well as access control for an operating system. It is totally independent of the equipment on which these services are performed. This service vision cannot be achieved with traditional access control mechanisms.

We can see that it is very easy to define rules because it is similar to what administrators are familiar with, namely the interactions between services in their systems.

Compliance with industrial constraints

While our DTE model is not specifically designed for industrial systems, it fully responds to their requirements. Using a host-based control mechanism helps to reduce the need for firewalls to control communication between DTE components, which improves response times between them. At the same time, it reduces firewalls'workload, which, even with some flows filtering and DTE mediation, ensures faster response times and therefore responds better to the system timing requirements.

Support of different protocols

Objects definition method allows to support different protocols as long as the content of the packets is known. This allows to cover protocols that are not currently supported by commercial firewalls.

6.6.2 Possible improvements

Objects definition

DTE objects definition can be more modular in order to be able to define new objects from existing ones by composing or extending them. For example, all web packets can be an extension of the basic definition:

```
assign   <(<36,2>,80)> web
```

Specific web packets can be defined by extending the "web" object definition as follows:

```
assign <web, (<30,4>,10.0.0.1)> to_my_web_server
```

which defines web requests addressed to the server 10.0.0.1.

Reusable values

Similarly, the values used in objects definitions can be defined as constants to allow their reuse. For example:

```
const my_web_server_ip = 10.0.0.1
to_my_web_server  = <web, (<30,4>, my_web_server_ip)>
```

Loose object definitions

DTE objects can only be defined in accordance with the system. In order to simplify this task as much as possible, one or more objects will be defined for each DTE type. Depending on the trust you have in DTE hosts, it is possible to more or less finely define the access control rules. For example, if there is a high degree of trust in certain equipment, the definition of the objects that are used in the rules related to this equipment could be as broad as possible, for example without specifying all the attributes of objects (e.g. IP addresses). In such a case, any DTE equipment performing the desired service may accept or reject these objects. Such flexibility ensures independence from the machine on which the service is running. On the other hand, such flexibility can affect the security of the system. If a trusted DTE machine is compromised, such broad rules can be used to bypass security policy. In fact, if trust is limited in some machines, it will be preferred to define objects much more finely such as with the quadruplet (source IP address, source Port, destination IP address, destination Port).

Client VS Server processes

A process belonging to a service that itself is part of a domain is governed by the rules of that domain. However, a process can be a server, a client, or both. The generic rules we defined apply to processes in both cases. However, sometimes, the access controls to be done can be different for server processes and client processes. The manager is then responsible for adapting the generic rules to take this into account this differences based on the process.

6.7 Conclusion

This chapter presents our study of using DTE access control to secure IICS systems flows.

After reviewing the primary concepts of DTE Firewalls, we presented the first phase of our study of using DTE in IICS context. A large part of the access control policies is generic and can be applied to all IICS. Therefore we proposed a generic access control policy based on the generic functional model provided by ISA95. We have therefore extended the initial DTE model, and formalized it to define a generic model of flow controls for integrated systems. This generic policy is intended to simplify the deployment of DTE access control and provide a good introduction to the concepts of

domains and types of packets for managers. However, it remains extensible by creating new types, domains and control rules.

The advantages of using DTE acces control in IICS systems are numerous. First, DTE reduces the complexity of using multiple access control solutions by using a single centralized rule-setting language across all the system. Besides, access controls are applied locally on DTE enabled hosts which lightens Firewalls workload and allows to respect industrial timing requirements. In addition, our model introduces the new service view that provides more independence regarding the equipment processes are running on.

The next step of our study would be to implement and test the proposed model in order to confirm its usefulness in the context of ICS integration. This will not be covered by this report.

CHAPTER 7 Conclusions and Perspectives

To conclude, we give an overview on how the different research objectives presented in the introduction have been followed as well as the different contributions that have been made. Afterwards, we will discuss the possible perspectives that can be followed to improve or complete our work and provide new research directions.

This thesis highlights one of the major challenges of current industrial systems namely ICS and Corporate systems integration security. The main objective was to propose new approaches and models to ensure the security of Industrial Control systems integrated with Information Systems against attacks.

First, we had to define a reference architecture to be the basis of our work. This architecture would make it possible for us to focus on a single type of ICS architecture, trying to study its security issues and provide some solutions. Studying all ICS architectures as part of a single project is not conceivable because they are very different in terms of functionality, operation and infrastructure. Our reference architecture has been defined in accordance with the standardized hierarchical functional model. We defined examples of components at each functional level, and we also set up a communication flows table. This architecture has been, along with this thesis, the main basis of our studies 2.

Next, we studied the state of the art of our problem. We particularly studied security issues of industrial control systems and created a list of vulnerabilities targeting industrial installations. We provided a summarized overview of ICS security problems, the integration challenges and an analysis of countermeasures evaluating their maturity for Integrated ICS systems. Multiple countermeasures have been suggested, however, the integration remains very challenging as regards security. Most of the existing IICS security solutions are IT solutions and are not really appropriate, as they are, for industrial

context. This is especially the case of Authentication and Authorization mechanisms, Segmentation and Segregation, Firewalls and IDS/IPS.

Therefore, we decided to work on IICS segmentation and segregation. The results of our work were presented in Chapter 4. We defined a new segmentation method "SONICS". It is an IICS segmentation method that aims at ensuring efficient zoning. It is based on a meta-model that helps to model systems. System models are used by the method to identify potential security zones. These are kept or dropped out based on a constraints analysis.We designed and carried out a validation test to evaluate the method. This helped us to identify the limitations and difficulties associated with the method and to identify possible improvements. The first test results were acceptable. However, we admit that the method's application is not simple enough without using the tool we developed. That said, our test method is by itself a standalone scientific contribution that can be reused or adapted for other scientific works. SONICS has a lot of advantages. It is a generic solution that can be applied to different types of IICS. It keeps the focus only on aspects that are relevant for segmentation. It is a fairly pragmatic method that takes into account IICS constraints and specificity. Note that the method uses industrial systems concepts (Operation functional levels, IT and OT technical types).

However, the security aspect of components was not adequately addressed in SONICS. Only processes are segmented according to their risks. We have therefore decided to make more use of the concept of risk in order for our method to take more security aspects into account. We believe that the concept of components risk is one of the best ways to characterize components from a security angle. The risk associated with data, components or processes is based on the probability and gravity of the applicable attacks.

Therefore, we proposed RIICS (Risk based IICS Segmentation), a new segmentation method for IICS systems that fills the gaps of SONICS and tries to simplify security zones identification by focusing on systems technical industrial specificities and risk. The first results of our validation test were rather accurate. However, we still have many more tests to do before we can confirm the effectiveness of the method. It is especially necessary to apply the method to a variety of systems with different configuration and various functional and business specificities. The cost of finding or creating test systems remains, however, significantly high.

Segmentation is only about setting logical boundaries between security zones, and is not enough to apply a security policy or to implement a defense in depth strategy. Real physical boundaries have to be set up. This is achieved through segregation and access controls techniques.

Therefore, we designed a new DTE based access control model to address the issue of access control of IICS. The new model reduces the complexity of using multiple access control solutions by using a single centralized rule-setting language across all the system. It also optimises the access controls processing time by applying them locally on DTE enabled hosts and thus lightens the firewalls workload. This allows to respect industrial timing requirements. Besides, using flexible objects definitions, new protocols can be supported without extending the model.

We also proposed a generic security policy based on the generic functional model provided by ISA95. This generic policy is intended to simplify the deployment of DTE access control and provide a good introduction to the concepts of domains and types of packets for managers. However, it remains extensible by creating new types, domains and control rules.

Only the formal definition of the model was done. The next step of our study would be to implement and test the proposed model in order to confirm its usefulness in the context of ICS integration.

7.1 Perspectives

Our research works can be extended, completed and improved. Below are some potential lines of inquiry that might help to complete our studies.

7.1.1 Segmentation methods validation

We developed generic segmentation methods. We managed to conduct some validation tests using an existing segmented system. But, more testing is of course needed. Testing these methods, however, requires a lot of resources and time. The methods should be tested on multiple systems with different configurations and architectures. Although testing on real systems is preferable, the use of simulated systems can be helpful as long as the accuracy of their *Ex-Segmentation* is ensured. This would be a major task for any further work.

7.1.2 Implement and test DTE access control

The DTE model should be implemented and tested. The implementation includes the development of DTEL and control logic extensions, the mediation mechanism and the decentralised management of the security policy.

The preparation of an IICS test system that contains DTE and non-DTE components and at least one DTE firewall is also required. Simulation techniques can be used to create such a system. Validation tests must cover the requirements previously presented. It would especially be required to validate the following requirements:

- **Strict controls**: Controls effectiveness should be tested. Specific attacks can be designed in order to challenge the access control functions performed by DTE hosts and firewalls, as well as access control for non DTE hosts.
- **Respect the timing requirements**: This is one of the most important things to validate. Measures and statistics about the access controls latency should be produced by performing a series of performance tests.

7.1.3 Extend our segregation solution with VPN

In this thesis we focused the DTE access control. This is not the only segregation solution out there. It would be interesting to study the application of other segregation solutions to IICS. For example, we could work on Virtual Private Networks (VPNs) with strong multi-factor authentication. It would also be interesting to study the combination of such a technique with our DTE model.

7.1.4 Work on other security techniques

In this thesis, we focused on the defence-in-depth technique and proposed methods and models of segmentation and segregation. However, as explained in our state-of-the-art study, other techniques such as IDSs and authentication mechanisms may need to be redesigned to take into account industrial specificities. A potential long-term follow-up of our works would be to study the integration of such solutions into the models we proposed. For example, it would be interesting to use IDS alerts records as an input of our segmentation method to recalculate the segmentation on a regular basis in order to protect the system in a more sustainable way.

APPENDIX A Résumé en français

Ce chapitre présente un résumé des trois années de travaux de recherche effectués dans le cadre de cette thèse. Nous présentons le contexte et les motivations, ainsi que les problèmes que nous avons étudiés et finalement les principales contributions réalisées.

A.1 Introduction

Le monde industriel a de plus en plus un réel besoin d'intégrer les systèmes de contrôle industriel (ICS) aux systèmes d'entreprise. L'intégration de ces deux systèmes présente de nombreux avantages tels qu'une visibilité améliorée des activités industrielles, une capacité d'utiliser les techniques de Business Intelligence pour optimiser les processus de production et acquérir une plus grande réactivité aux exigences et aux décisions Business pour atteindre une plus grande compétitivité commerciale.

Cependant, cette intégration engendre de multiples problèmes de sécurité. En effet, les systèmes industriels ont été conçus sans aucune sécurité, car ils étaient généralement isolés. L'utilisation de protocoles et de technologies peu sécurisés et l'absence de politiques et de formation des ressources humaines sur les pratiques de cyber sécurité sont des exemples de problèmes de sécurité des systèmes industriels.

Par conséquent, l'intégration expose à la fois les ICS et les systèmes d'entreprise à des menaces majeures. Malheureusement, les pratiques connues en matière de sécurité des IT ne peuvent être appliquées directement aux systèmes ICS parce que les deux types de systèmes sont différents par nature et ont des exigences fonctionnelles et de sécurité différentes.

La sécurisation des systèmes industriels, et en particulier des systèmes intégrés, devient l'une des préoccupations les plus urgentes qui inquiètent non seulement tous les acteurs industriels mais les gouvernements aussi. Un nombre très important d'entités industrielles et d'infrastructures sont si critiques que toute cyber attaque réussie contre

ces entités peut causer d'énormes dégâts aux entreprises, à l'environnement et plus gravement à la sécurité nationale et à la sûreté des personnes.

Cette thèse étudie l'intégration des systèmes ICS avec les systèmes d'entreprise d'un point de vue sécurité. Notre objectif est d'étudier les vulnérabilités de sécurité des systèmes industriels intégrés et de proposer des modèles et des mécanismes pour améliorer leur sécurité et les protéger contre les attaques complexes.

A.2 Les Contributions

La première partie de notre travail a consisté à réaliser une étude sur les vulnérabilités des systèmes ICS intégrés (IICS) ainsi que les contre-mesures et solutions de sécurité existantes. Nous avons mis en place une architecture de référence des systèmes intégrés des ICS pour servir de base à notre travail et nous aider à identifier plus précisément les vulnérabilités et étudier les mécanismes et modèles de sécurité proposés.

La Défense en profondeur est l'une des techniques de sécurité les plus importantes qui sont fortement recommandées pour les systèmes ICS intégrés. Malheureusement, aucune méthode expliquant sa mise en œuvre pour les IICS n'existe. La défense en profondeur est principalement implémentée à l'aide de la segmentation et de la ségrégation. La segmentation consiste à segmenter un système en plusieurs zones de sécurité qui peuvent être contrôlées, surveillées et protégées séparément. La ségrégation consiste à contrôler la communication à travers les frontières des segments sur la base d'un ensemble de règles prédéfinies. La segmentation d'un IICS peut être fondée sur divers types de caractéristiques telles que les caractéristiques fonctionnelles, l'impact commercial, les niveaux de risque ou d'autres exigences définies par l'organisation. Bien que de nombreux travaux de recherche aient suggéré des solutions de segmentation, ces solutions ne sont malheureusement pas suffisamment génériques et ne prennent pas suffisamment en compte les spécificités des IICS, comme leur hétérogénéité technique et fonctionnelle, leurs contraintes et leurs conditions industrielles réelles. Les caractéristiques des éléments du système à prendre en compte pour la segmentation ne sont pas non plus évidentes.

Nous avons donc défini une nouvelle méthode générique de segmentation pour les IICS, "SONICS", qui permet de simplifier la segmentation des IICS. Cette nouvelle méthode est basée sur un méta-modèle simple définissant les systèmes IICS qui permet de décrire des éléments de systèmes en se concentrant uniquement sur les aspects qui sont réellement significatifs pour la segmentation. Certains aspects du méta-modèle nécessitent la réalisation d'une analyse de risque pour décrire plus précisément le sys-

tème. La méthode elle-même consiste en de multiples cycles où de nouveaux segments potentiels sont progressivement identifiés en fonction d'un aspect du méta-modèle à la fois. Les nouvelles zones identifiées sont conservées ou non en fonction d'une analyse des contraintes réalisée sur les éléments IICS impliqués dans les nouvelles zones potentielles. L'analyse des contraintes permet de vérifier que la création d'une nouvelle zone identifiée ne conduit pas à une violation des exigences fonctionnelles du système, ni à un dépassement des coûts techniques. Préserver une zone identifiée est une décision à prendre en comparant la Nécessité de cette nouvelle zone aux contraintes connues sur ces éléments. Nous avons défini un système de classement composé de deux échelles (échelle des niveaux de Nécessité et échelle des niveaux de Contraintes) pour aider à évaluer et comparer les niveaux de Nécessité et de Contraintes liés à une zone identifiée et ensuite décider si cette zone doit être maintenue ou pas. [Khaoula et al. 2017, Khaoula et al. 2018b]

L'étape suivante a consisté à étendre la méthode à d'autres aspects de la sécurité. Nous sommes convaincus que le concept de risque des composants est l'une des meilleures façons de caractériser les composants d'un point de vue sécurité. Nous avons donc créé RIICS (Risk based IICS Segmentation), une nouvelle méthode de segmentation pour les systèmes IICS qui comble les lacunes de SONICS et tente de simplifier l'identification des zones de sécurité en se concentrant sur les spécificités techniques des IICS et des risques auxquels ils sont exposés. Le risque associé aux données, aux composants ou aux processus est évalué à l'aide d'une version légèrement adaptée de la méthode d'évaluation des risques EBIOS pour laquelle le risque est basé sur la probabilité et la gravité des scénarios de menace possibles.[Khaoula et al. 2018a]

Par ailleurs, la défense en profondeur ne peut pas seulement être réalisée par la segmentation. L'identification des zones de sécurité est nécessaire mais insuffisante. Les flux de communication sortant ou entrant dans une zone doivent être filtrés. Nous sommes donc convaincus que notre méthode de segmentation doit être complétée par une méthode de ségrégation.

Pour compléter la méthode de segmentation, nous avons étudié les solutions de ségrégation. Le problème de l'intégration des ICS représente un nouveau cas d'utilisation en termes de mécanismes de filtrage des flux. Lors de l'intégration des deux systèmes, il est nécessaire de:

- Appliquer des contrôles stricts sur tous les flux, et en particulier sur la communication entre des réseaux différents.
- Respecter les exigences temporelles des systèmes industriels.

- Permettre de personnaliser l'inspection des paquets pour étendre les protocoles pris en charge. Cela permettra notamment de supporter davantage de protocoles industriels.
- Simplifier la définition des règles de contrôle pour faciliter la tâche des administrateurs, en particulier les administrateurs de systèmes industriels car ils sont moins familiers avec les mesures de sécurité.

Nous avons décidé d'étudier l'utilisation du contrôle d'accès DTE (Domain and Type Enfoncement) pour la ségrégation ICS intégrée. Le DTE est un mécanisme de contrôle d'accès qui offre la souplesse nécessaire pour répondre aux exigences présentées ci-dessus. Nous avons étendu le modèle initial de DTE et l'avons formalisé pour définir un nouveau modèle de contrôle des flux pour les systèmes ICS intégrés. Nous avons proposé une politique de contrôle d'accès générique mais extensible basée sur le modèle fonctionnel générique fourni par la norme ISA95. Cette politique générique vise à simplifier le déploiement du contrôle d'accès DTE et à fournir une bonne introduction aux concepts DTE.

A.3 SONICS: Une nouvelle méthode de segmentation

Plusieurs travaux de recherche ont étudié la segmentation des IICS. Pour la plupart d'entre eux, la segmentation doit se faire au cas par cas sans fournir plus d'explication sur comment la faire. D'autres ont une approche orientée par l'exemple et essaient d'effectuer une segmentation sur une architecture de référence bien définie. Ils recommandent d'adopter le cadre logique du modèle Purdue pour la hiérarchie de contrôle (CEI 62264) pour délimiter les zones de sécurité.

D'autres travaux de recherche proposent une solution générique au problème. Ils fournissent des règles et des instructions génériques pour identifier les zones de sécurité tout en adoptant le modèle hiérarchique de la norme CEI 62264 (ISA95). Nous croyons que cette approche peut mener à d'excellents résultats si elle est menée en mettant l'accent sur les aspects les plus pertinents pour la segmentation IICS. C'est pourquoi nous proposons SONICS, une nouvelle méthode générique de segmentation IICS qui vise à simplifier l'identification des zones de sécurité IICS en se concentrant sur des aspects pertinents pour la segmentation en tenant compte des spécificités industrielles. Cette méthode utilise un méta-modèle simple pour décrire les systèmes IICS et permet d'identifier les zones de sécurité potentielles à travers plusieurs étapes. Les nouvelles

zones potentielles identifiées sont conservées ou non sur la base d'une analyse de contraintes.

A.3.1 SONICS: Le principe

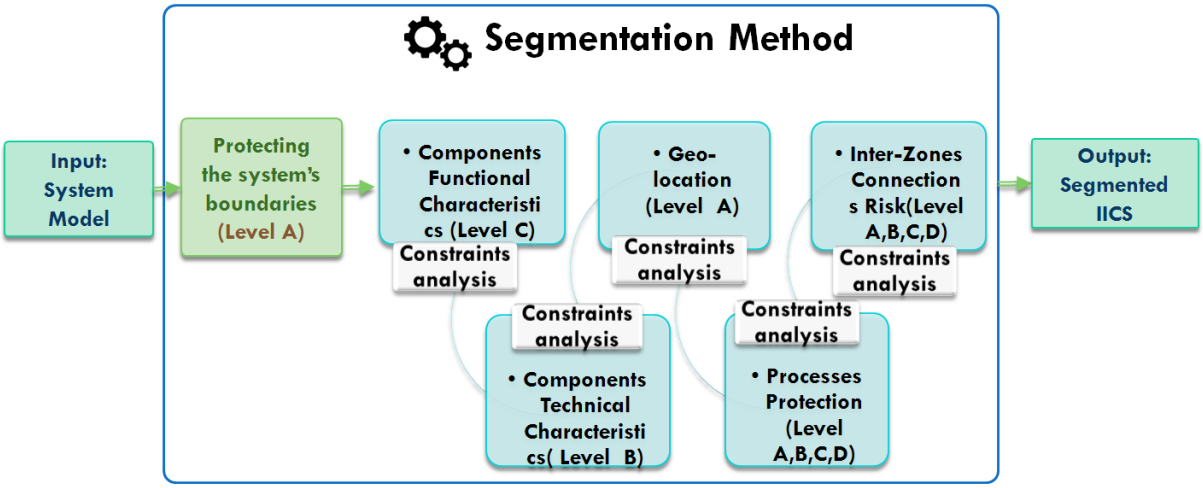

Figure A.1 – Etapes de la méthode de segmentation SONICS

Avec SONICS, la segmentation se fait en deux phases. La première phase consiste à modéliser le système à segmenter à l'aide du méta-modèle (Figure A.3). Le modèle du système est le principal input de la deuxième phase. Cette dernière consiste à segmenter le système à travers six cycles comme illustré sur la Figure A.1. Au premier cycle, les frontières du système sont protégées. C'est la première zone de sécurité du système. Ensuite, les composants du système sont groupés cycle après cycle en fonction d'un seul aspect (fonctionnel, technique, géographique, de processus, et le risque de connexions interzones) par cycle pour constituer des zones de sécurité potentielles. [Khaoula et al. 2017]

Plus de détails sur le groupement des composants sont fournies ci-dessous. Les zones de sécurité identifiées à chaque cycle, sont conservées en fonction d'une analyse de contraintes réalisée sur les composants impliqués dans les nouvelles zones identifiées (Figure A.2).

A.3.2 SONICS: Le méta-modèle

Notre méta-modèle IICS (Figure A.3) permet de modéliser un IICS comme un ensemble de Composants, Connections et Process.

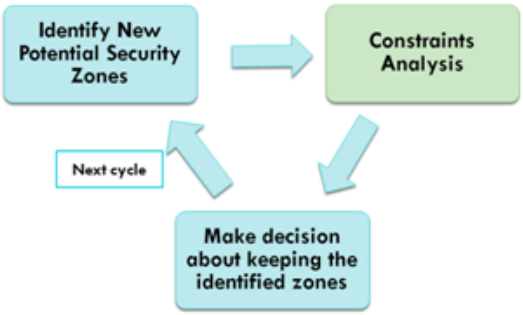

Figure A.2 – Cycle de segmentation

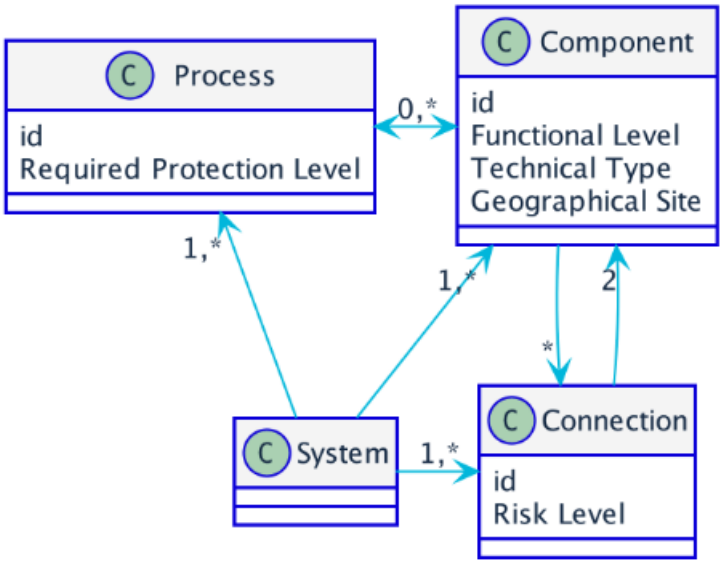

Figure A.3 – Méta-modèle SONICS

Les composants sont caractérisés par leur niveau fonctionnel du modèle CEI 62264 (ISA 95), leur type technique et leur géo-localisation.

Les composants sont connectés par des connexions. Une “Connexion” est un canal qui peut être utilisé par deux (ou plusieurs) composants pour communiquer entre eux. Il peut être physique, où les Composants sont directement liés par une connexion physique (filaire ou sans fil), ou logique, où les Composants sont liés par une succession de Connexions physiques. Une connexion peut être caractérisée par son niveau de risque, la segmentation de l’impact de la connexion, en particulier lorsqu’elle relie des composants de différentes zones. C’est pourquoi nous accordons une attention particulière aux Connections inter-zones. En effet, les “connexions inter-zones” peuvent connecter deux zones de deux niveaux de sécurité différents ou qui contiennent des composants de niveaux de risque différents. Cela pourrait introduire des problèmes

de sécurité. Le niveau de risque de chaque connexion inter-zone du système doit être évalué sur la base d'une analyse de risque des connexions et des composants qu'elles connectent. Pour évaluer le risque des connexions inter-zones, nous utilisons une version minimaliste de la méthode d'analyse de risques EBIOS. Pour une connexion inter-zone donnée, tous les Services exposés par les Composants des zones qu'elle connecte ainsi que toutes les Données manipulées doivent être analysées afin de réaliser une évaluation qualitative plus précise du risque associé à ces composantes.

Les process (les procédés métier ou industriels) sont des ensembles d'activités interdépendantes qui transforment des inputs en outputs. Un système est structuré en plusieurs processus. Chaque composant appartient à un ou plusieurs processus. Un process se caractérise par son "niveau de protection requis" et représente une zone de sécurité potentielle. Le "niveau de protection requis" est calculé en fonction de son niveau de risque qui est évalué à l'aide d'une analyse de risque.

A.3.3 Outil de segmentation

Nous avons développé un outil qui implémente notre méthode (Figure A.4). Cet outil permet de créer des modèles de systèmes et d'exécuter les étapes de segmentation dessus pour obtenir des systèmes segmentés. La création d'un modèle nécessite de bonnes connaissances et une préparation préalable. Il est nécessaire que l'utilisateur de l'outil connaisse suffisamment bien l'architecture du système, ses processus, ses risques et ses contraintes. La modélisation du système consiste, comme le montre la Figure A.4, à créer des composants, spécifier leurs caractéristiques et ajouter des connexions et des processus.

Une fois le modèle créé, l'outil permet de dérouler les étapes de la méthode l'une après l'autre en permettant d'attribuer des niveaux de contraintes aux connexions inter-zones. Par exemple, pour la première étape de segmentation, à savoir la segmentation fonctionnelle, les outils calculent les nouvelles zones potentielles du cycle (en les différenciant par des couleurs différentes) comme l'illustre la Figure 4.6. Il décrit les connexions inter-zones de ces zones potentielles permettant de définir leurs niveaux de contraintes (Figure 4.7). Les zones de sécurité sont ensuite recalculées en fonction des valeurs des niveaux de contraintes nouvellement définies. Les cycles suivants sont traités de la même manière (en appuyant sur le bouton "Next Step") jusqu'à l'obtention du résultat final.

De plus, l'outil est complètement récursif. Toute valeur fixée par l'utilisateur, qu'il s'agisse d'une caractéristique d'un composant, d'une connexion ou d'un processus, est incluse dans le modèle du système et réutilisée à travers les différentes étapes. Par

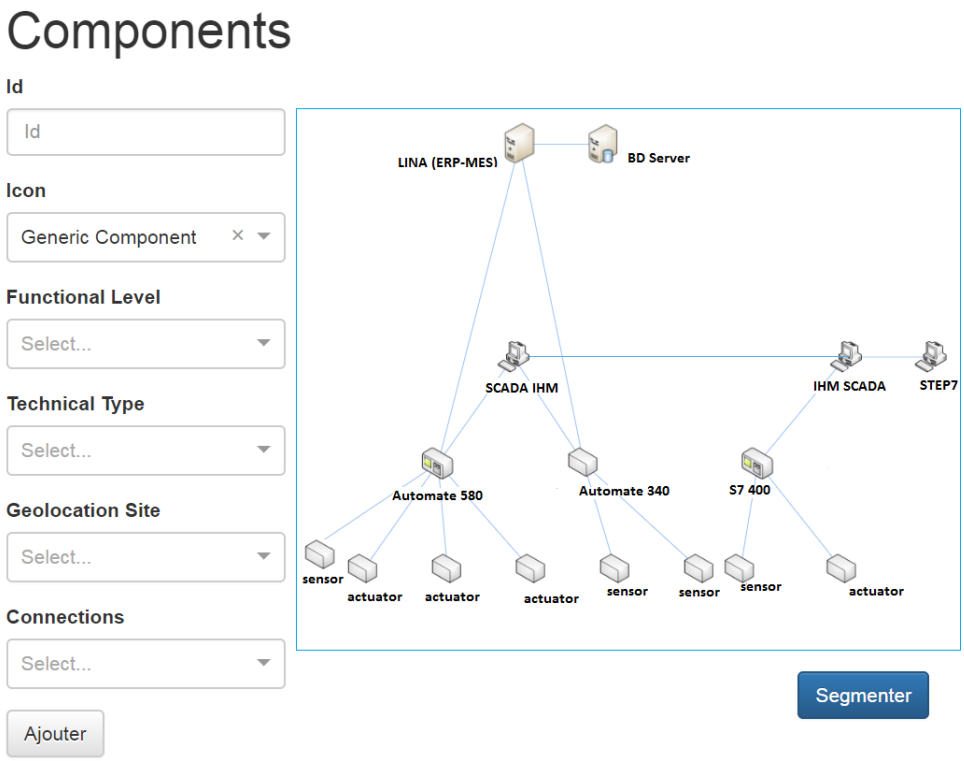

Figure A.4 – Outil de segmentation - capture 1

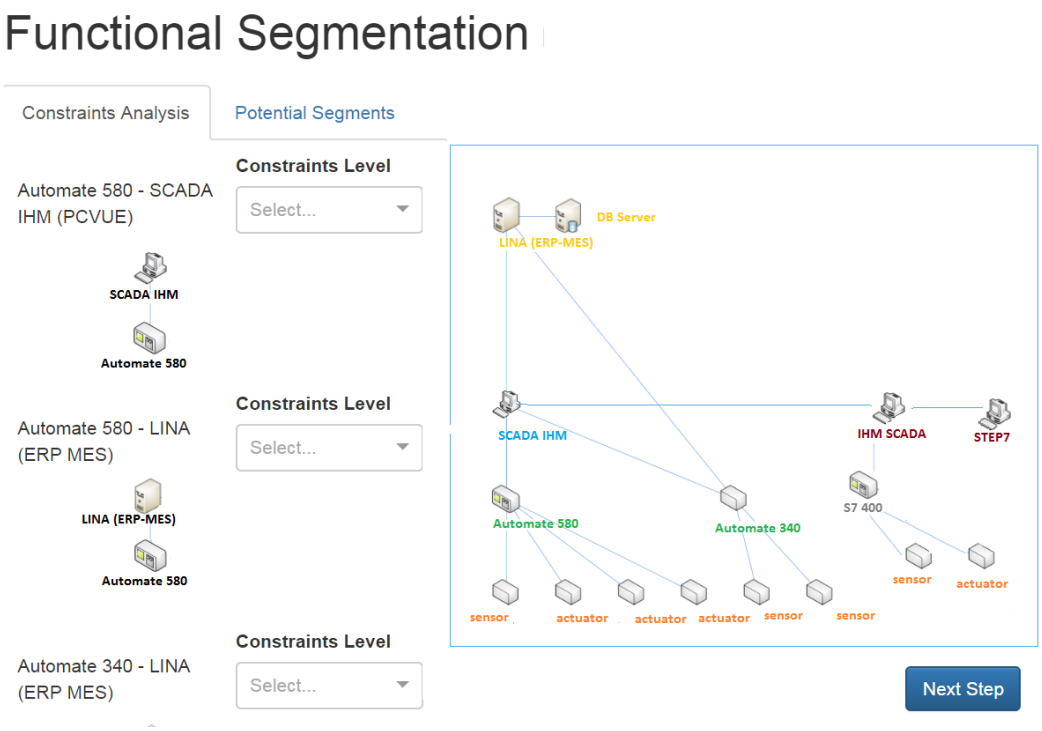

Figure A.5 – Outil de segmentation - capture 2

exemple, si le niveau de contrainte d'une connexion est défini pendant un cycle, il n'a pas besoin d'être réinitialisé à d'autres cycles car il devient une caractéristique de cette connexion. Ceci assure que le résultat de la segmentation est automatiquement recalculé chaque fois que le modèle du système évolue en ajoutant, modifiant ou supprimant des composants, des connexions ou des process.

A.3.4 Méthodologie de test

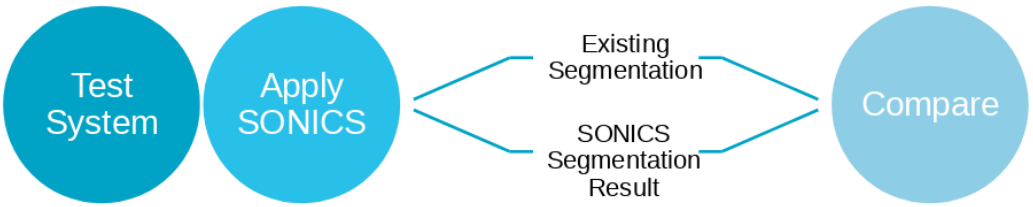

Figure A.6 – Méthodologie de test

Nous avons conçu une méthode de test et de validation afin d'évaluer notre méthode de segmentation SONICS. Cette méthode de test est basée sur la comparaison du résultat de SONICS à des segmentations qui sont faites au fil du temps par expertise. Nous nous référons à ces segmentations de références par "Ex-Segmentation" et nous les supposons correctes. Etant donné un système de test avec une segmentation existante (une "Ex-Segmentation"), le test de validation consiste à appliquer SONICS sur ce système et à comparer les résultats avec la "Ex-Segmentation" comme expliqué sur la Figure A.6.

La comparaison du résultat de SONICS se base sur le concept d'efficacité et de précision de la segmentation. Nous définissons l'efficacité d'une méthode sur un ensemble de systèmes de test comme la moyenne de l'exactitude des résultats obtenus pour chaque système. La précision d'un résultat dépend de la mesure dans laquelle le résultat est similaire à celui attendu. Dans notre cas, la précision du résultat d'une segmentation est fonction de la distance entre la segmentation obtenue par SONICS et la *Ex-Segmentation*. La distance entre deux segmentations d'un même système est le coût minimum pour transformer une segmentation en l'autre en effectuant un ensemble des seules actions suivantes :

- Déplacer un seul composant à la fois d'un segment à l'autre
- Enlever un segment

- Fusionner deux segments

La précision est calculée en fonction de la distance à l'aide de la formule suivante :

$$accuracy = \frac{1}{1 + distance}$$

Les premiers résultats des tests étaient acceptables. Cependant, nous admettons que l'application de la méthode n'est pas assez simple sans utiliser l'outil que nous avons développé. Cela dit, notre méthode de test est en soi une contribution scientifique qui peut être réutilisée ou adaptée pour d'autres travaux scientifiques.

A.4 RIICS: Une méthode de segmentation basée sur le risque

La méthode SONICS tente de prendre en compte les aspects les plus importants de la segmentation IICS selon de multiples standards de sécurité. Les spécificités techniques et fonctionnelles sont bien couvertes par la méthode via les caractéristiques des composants ainsi que les contraintes techniques et fonctionnelles. Cela permet de s'assurer que les composants de natures techniques ou fonctionnelles différentes sont séparés, à moins qu'il n'y ait des contraintes qui l'en empêchent. La méthode consiste également à séparer les composants qui appartiennent à des sites distants différents afin de se conformer aux recommandations de sécurité communes. Cependant, l'aspect sécurité des composants n'est pas suffisamment pris en compte. Seuls les processus sont segmentés en fonction de leurs risques. Nous avons donc décidé d'utiliser davantage la notion de risque afin que notre méthode prenne davantage en compte les aspects de sécurité. Nous croyons que le concept de risque des composants est l'une des meilleures façons de caractériser les composants du point de vue de la sécurité. Le risque associé aux données, composants ou processus est basé sur la probabilité et la gravité des attaques applicables. L'analyse des risques nécessite une forte concentration sur l'étude du contexte et implique la mise en œuvre de mesures rationnelles et optimales, notamment en termes de coûts.

Nous avons donc conçu une nouvelle méthode de segmentation RIICS (**R**isk based **IICS Segmentation**), qui vise à combler les lacunes de la méthode SONICS pour garantir des résultats plus précis qui répondent aux besoins réels de sécurité de l'IICS.

Elle repose sur une analyse des risques qui permet d'évaluer le risque des composants. Les modèles de systèmes sont utilisés par la méthode pour délimiter les zones de sécurité en regroupant des composants ayant les mêmes caractéristiques.

Figure A.7 – Les étapes de la méthode de segmentation RIICS

Tout comme SONICS, la segmentation se fait en deux phases. Tout d'abord, le système est analysé et modélisé pour créer le modèle du système qui représente l'entrée principale de la phase de segmentation. La modélisation du système est basée sur un méta-modèle plus complet qui inclut des éléments qui mettent en avant la notion de risque. Un modèle se concentre principalement sur les composants des systèmes et leurs inter-connexions. L'analyse de risque permet d'évaluer et d'attribuer les niveaux de risque aux composants du système. L'opération de segmentation consiste ensuite à grouper les composants du système selon leur géo-localisation, leur type technique et leur niveau de risque en trois cycles (Figure A.7). En termes simples, des composants ayant la même géo-localisation, le même type technique et le même niveau de risque constituent ensemble une seule zone de sécurité. L'évaluation des risques des composants est réalisée avec la méthode d'analyse de risque EBIOS.

Nous avons testé la méthode RIICS en utilisant la même méthodologie de test présentée précédemment. Les premiers résultats ont été positifs. Cependant, il nous reste encore beaucoup de tests à faire avant de pouvoir confirmer l'efficacité de la méthode. Il est particulièrement nécessaire d'appliquer la méthode à une variété de systèmes de configurations différentes et de spécificités fonctionnelles et techniques variées.

A noter que RIICS, tout comme SONICS, est également applicable aux systèmes d'information (sans aucun système industriel), car elle est générique et parce que les SI sont des sous-systèmes des IICS.

Nous convenons, toutefois, que l'analyse de risque exige un certain niveau d'expertise, mais la phase de segmentation est très simple.

A.5 Modèle de contrôle d'accès DTE

Les technologies de contrôle d'accès traditionnelles telles que les pare-feux sont très importantes pour les systèmes ICS intégrés afin de contrôler les communications entre les différents réseaux et de protéger les ressources importantes. Cependant, les pare-feux conventionnels ne sont pas toujours entièrement compatibles avec les systèmes de contrôle industriel. En effet, les pare-feux peuvent introduire une latence importante alors que les systèmes ICS sont généralement très exigeants en termes de temps de réponse. De plus, la plupart des pare-feux existants ne supportent pas tous les protocoles industriels.

Nous sommes convaincus qu'un mécanisme de contrôle d'accès fondamentalement plus adapté est nécessaire pour contrôler les flux au sein de l'IICS en ce qui concerne les exigences des systèmes. Le nouveau mécanisme de contrôle d'accès doit :

- Appliquer des contrôles stricts sur tous les flux, et en particulier sur la communication entre des réseaux différents.
- Respecter les exigences temporelles des systèmes industriels.
- Permettre de personnaliser l'inspection des paquets pour étendre les protocoles pris en charge. Cela permettra notamment de supporter davantage de protocoles industriels.
- Simplifier la définition des règles de contrôle pour faciliter la tâche des administrateurs, en particulier les administrateurs de systèmes industriels car ils sont moins familiers avec les mesures de sécurité.

Domain and Type Enforcement (DTE) est un mécanisme de contrôle d'accès prometteur qui permettrait de fournir la flexibilité et le renforcement nécessaires tout en appliquant les contrôles d'accès. Des études ont été menées sur l'utilisation des techniques de DTE dans les systèmes IICS. Bien que leurs conclusions soient intéressantes, elles se limitent à la sécurisation des flux d'intégration entre le ICS et le système d'entreprise. Notre objectif est de généraliser les contrôles de DTE à l'ensemble du système en fournissant un modèle générique qui fournit des concepts simples et cohérents permettant de définir des règles de contrôle d'une manière simple et homogène à travers le système. Ce nouveau modèle permet de définir et d'appliquer des contrôles d'accès renforcés dans le respect des exigences temporelles des ICS. La définition des contrôles d'accès est basée sur un langage de haut niveau qui peut être utilisé facilement par les administrateurs ICS. Nous proposons également un premier ensemble de

règles génériques basées sur le modèle fonctionnel de la norme ISA95. Ce jeu de règles génériques simplifie le déploiement des contrôles d'accès DTE et constitue une bonne introduction aux concepts DTE pour les administrateurs.

A.5.1 Le modèle DTE

Nous avons créé un modèle générique de contrôle d'accès basé sur DTE. Ce nouveau modèle répond aux quatre exigences que nous avons présentées précédemment. Nous avons également créé une extension du langage DTEL pour représenter les nouveaux concepts introduits par notre modèle tout en restant compatible avec la version standard de DTEL. Les domaines, objets et permissions sont définis en utilisant presque la même syntaxe que le langage DTE avec quelques nouvelles fonctionnalités.

Notre modèle est une extension du modèle DTE de base et permet de modéliser les process qui s'exécutent sur le système comme des entités. Celles-ci peuvent être groupées en des services. Un service est un ensemble de processus qui sont régis par les mêmes règles de contrôle d'accès. La vue service permet de faire abstraction des processus et de définir des règles de contrôle d'accès transverses communes. Pourvu que les processus sont définis, les services sont plus faciles à gérer pour les administrateurs de systèmes ayant des connaissances limitées en informatique et en sécurité.

Quant aux objets, ce sont les paquets qui sont transmis entre les entités. Un objet peut être défini comme un ensemble d'attributs basés sur l'emplacement des champs dans le paquet. Les attributs des objets sont, par exemple, l'adresse IP source ou destination, le port source ou destination, les données de la couche application.... Cela permet de définir des objets de différents protocoles sans avoir à étendre le modèle de contrôle d'accès.

Un exemple de définition d'objet est $< (< 36, 2 >, 80) >$. Cela représente un paquet dont la valeur du champs à la position 36 octets et d'une taille de 2 octets est égal à 80. Cette définition représente tous les paquets avec un port de destination égal à 80. Il s'agit généralement d'une requête à destination d'un serveur web.

Les objets sont typés et le entités sont associées à des domaines. Des règles peuvent être définie pour autoriser des domaines à exécuter des actions (comme l'envoi et la réception) sur des types d'objets. L'ensemble des définition et des règles constituent la politique de sécurité.

A.5.2 Mode opératoire

Le contrôle d'accès local

Les contrôles d'accès DTE sont réalisés localement sur les composants lorsque cela est possible. Sur les hôtes DTE, le contrôle d'accès est appliqué chaque fois qu'un paquet est envoyé ou reçu par un processus exécuté sur l'hôte DTE. Lorsqu'un paquet est envoyé, les règles définies concernant le domaine d'envoi sont vérifiées. Pour ce faire, toutes les règles qui s'appliquent au processus qui envoie le paquet seront vérifiées. Pour chaque règle, le paquet est comparé au type d'objet de la règle essayant de renvoyer une seule règle au maximum. Si une règle d'autorisation d'action d'envoi correspondant au type d'objet est trouvée, le paquet peut être envoyé, sinon il est refusé.

Il n'est donc plus nécessaire de traiter tous les paquets sur le pare-feu. Cela permet de définir des règles de contrôle beaucoup plus fines sans se soucier des performances car le traffic sur les composants est beaucoup moins important que sur les firewalls.

La médiation

L'avantage de DTE est qu'il fournisse des mécanismes de rétrocompatibilité avec les composants qui n'implémentent pas DTE.

La médiation est un mécanisme qui permet d'associer des domaines DTE à des entités exécutées sur des machines non-DTE. Il utilise les en-têtes de paquets pour déterminer le type DTE du paquet et le domaine DTE auquel appartient l'entité émettrice ou réceptrice.

Firewall access controls

Les pare-feux DTE sont déployés aux limites des segments et sont chargés de s'assurer que les contrôles d'accès sont correctement effectués par les hôtes DTE. Les communications provenant de l'extérieur d'un segment ne sont par défaut pas autorisées et doivent être explicitement autorisées. Les pare-feux DTE sont également responsables de la médiation entre les hôtes DTE et non DTE.

A.6 Application du modèle DTE aux IICS

Notre modèle de contrôle d'accès décompose le système en plusieurs domaines logiques qui incluent les différentes entités. La définition des domaines et des règles de contrôle doit être définie au cas par cas en fonction du système, mais une grande partie des politiques de contrôle d'accès est totalement générique et peut être appliquée à tous les IICS. Cette partie générique est basée sur le modèle d'intégration fonctionnel défini par la norme ISA 99 qui définit les fonctions d'une entreprise impliquée dans la fabrication ainsi que les flux d'information entre les fonctions qui traversent l'interface entreprise/ICS.

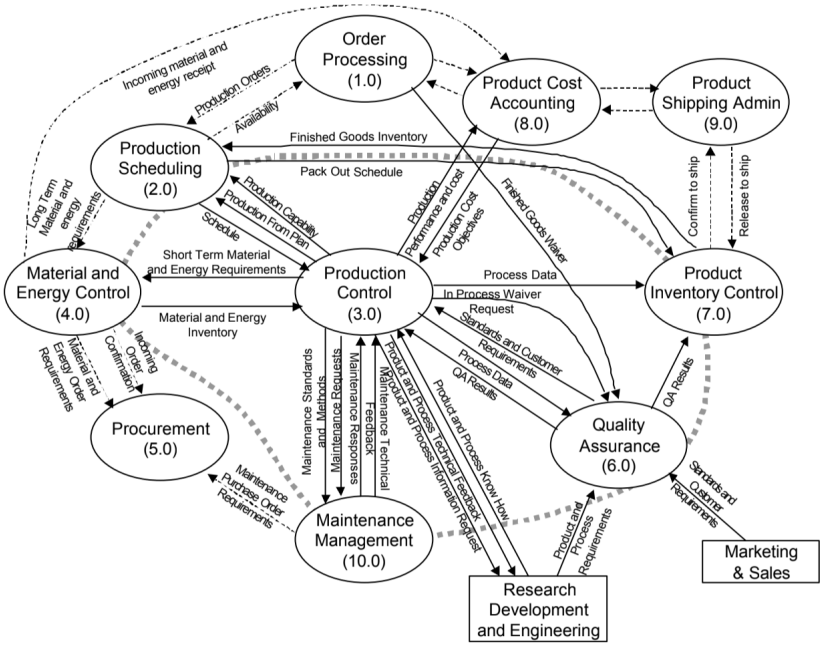

Figure A.8 – Modèle fonctionnel ISA95

Le modèle fonctionnel représente l'IICS comme un ensemble de fonctions, d'entités externes et de flux de communication entre elles. Il est illustré par la figure A.8.

Nous utiliserons le modèle fonctionnel générique pour créer une politique de sécurité DTE partielle générique. Les fonctions de la Figure A.8 représentent les domaines DTE, et les flux entre les fonctions représentent les flux à contrôler et les types d'objets. La politique générique que nous proposons a pour but de simplifier le déploiement du contrôle d'accès DTE et de fournir une bonne introduction aux concepts de domaines et de types de paquets pour les administrateurs. Cependant, elle reste, bien évidemment, extensible. La création de nouveaux types, domaines et règles de contrôle sera possible globalement et localement.

A.7 Conclusion

Cette thèse étudie l'une des problématiques majeures des systèmes industriels actuels, à savoir la sécurisation des systèmes ICS intégrés. L'objectif principal était de proposer de nouvelles approches et de nouveaux modèles pour assurer la sécurité de ces systèmes.

Nous avons travaillé sur la segmentation et la ségrégation des IICS. Nous avons défini une nouvelle méthode de segmentation "SONICS". Il s'agit d'une méthode de segmentation IICS qui a pour but d'assurer une segmentation efficace. Nous avons conçu et réalisé un test de validation pour évaluer la méthode. Cela nous a permis d'identifier les limites et les difficultés liées à la méthode et d'identifier les améliorations possibles. Les premiers résultats de tests étaient acceptables. Cependant, nous reconnaissons que l'application de la méthode n'est pas assez simple sans utiliser l'outil que nous avons développé.

Cependant, l'aspect sécurité des composants n'a pas été traité de manière adéquate dans SONICS. C'est pourquoi nous avons développé RIICS (Risk based IICS Segmentation), une nouvelle méthode de segmentation pour les systèmes IICS qui comble les manques de SONICS en mettant en avant les spécificités techniques et industrielles des systèmes et leurs risques. Les premiers résultats de notre test de validation ont été positifs. Cependant, il nous reste encore beaucoup de tests à faire avant de pouvoir confirmer l'efficacité de la méthode. Il est particulièrement nécessaire d'appliquer la méthode à une variété de systèmes de configurations différentes et de spécificités fonctionnelles et industrielles variées. Le coût de la recherche ou de la création de systèmes de test reste toutefois très élevé.

Pour compléter la méthode de segmentation, nous avons développé un nouveau modèle de contrôle d'accès à base de DTE. Le nouveau modèle réduirait la complexité de l'utilisation de plusieurs solutions de contrôle d'accès en utilisant un seul langage centralisé d'établissement de règles dans tout le système. Il permet également d'optimiser le temps de traitement des contrôles d'accès en les appliquant localement sur les hôtes DTE et d'alléger ainsi la charge des pare-feux. Cela permet de respecter les exigences temporelles industrielles. De plus, en utilisant des définitions d'objets flexibles, de nouveaux protocoles peuvent être supportés sans que le modèle ait besoin d'être étendu. Seule la définition formelle du modèle a été réalisée. L'étape suivante de notre étude consisterait à mettre en œuvre et à tester le modèle proposé afin de confirmer son utilité dans le contexte de l'intégration du ICS.

List of Publications

International Conferences

- K. Es-Salhi, N. Cuppens-Boulahia, and D. ESPES. **"Analysis of ICS and Corporate system Integration vulnerabilities"**. In the 14th International Conference on Embedded Systems, Cyber-physical Systems, and Applications, **ESCS 2016**, July 25-28, 2016, Las Vegas, USA.

- K. Es-Salhi, D. Espes, and N. Cuppens-Boulahia. **"A new Segmentation Method for Integrated ICS Systems"**. In the fifteenth International Conference on Privacy, Security and Trust, **PST 2017**, August 28-30, 2017, in Calgary, Alberta, Canada.

- K. Es-Salhi, D. Espes, and N. Cuppens-Boulahia. **"RIICS: Risk based IICS segmentation Method"**. In the 13th International Conference on Risks and Security of Internet and Systems, **CRISIS 2018**, 16st-18st October 2018, Arcachon, France.

- K. Es-Salhi, D. Espes, and N. Cuppens-Boulahia. **"SONICS: a segmentation method for integrated ICS and Corporate System"**. In the 14th International Conference on Information Systems Security, **ICISS 2018**, December 16-20 Bengaluru, India.

- K. Es-Salhi, D. Espes, and N. Cuppens-Boulahia. **"DTE Access Control Model for Integrated ICS Systems"**. In the 2nd International Workshop on Security Engineering for Cloud Computing, **IWSECC 2019**, August 26-29, 2019, University of Kent, Canterbury, UK.

List of Figures

2.1 The main industrial Sectors. 8

2.2 The types of ICS systems according to geographical distribution. 9

2.3 Functional Hierarchical model [ISA95] [ISA 2004]. 10

2.4 IICS Reference Architecture. 11

2.5 Examples of IICS data flows. 16

3.1 Growth of networked devices [Evans 2011] and cyber-attack visibility and maliciousness trends [Bayuk et al. 2011, Watin-Augouard et al. 2011] 21

3.2 Countermeasures families. 27

3.3 Policy Measures Categories. 28

3.4 General security guides segmentation 35

3.5 Functional Hierarchical model [ISA 2013]. 37

4.1 The Segmentation method 46

4.2 IICS Meta-Model 47

4.3 Risk levels grid 52

4.4 Inter-zone connection's security zone 53

4.5 SONICS Tool - Modeling step 61

4.6 SONICS Tool - Functional potential zones 62

4.7 SONICS Tool - Constraints levels attribution 62

4.8 Test Methodology 64

4.9 The IIC test System 65
4.10 The Segmented IIC test system 66

5.1 EBIOS Steps 71
5.2 RIICS principle 74
5.3 EBIOS Meta-Model 76
5.4 Risk levels grid 78
5.5 Application example (1/4) - IICS System to segment 81
5.6 Application example (2/4) - Geo-location Segmentation 82
5.7 Application example (3/4) - Technical Segmentation 83
5.8 Application example (4/4) - Risk based Segmentation 83

6.1 Segmentation and multi-domain problem 98
6.2 Segmentation management with DTE 99
6.3 DTE global rules management architecture 103

A.1 Etapes de la méthode de segmentation SONICS 125
A.2 Cycle de segmentation 126
A.3 Méta-modèle SONICS 126
A.4 Outil de segmentation - capture 1 128
A.5 Outil de segmentation - capture 2 128
A.6 Méthodologie de test 129
A.7 Les étapes de la méthode de segmentation RIICS 131
A.8 Modèle fonctionnel ISA95 135

List of Tables

4.1 Functional Levels 48
4.2 Technical Types 49
4.3 The gravity scale 51
4.4 The likelihood scale 52
4.5 Risk level / Required protection level 52
4.6 Segmentation Necessity Levels 56
4.7 Constraints Level Scale 56
4.8 Segmentation Necessity Level Scale 57

6.1 Generic IICS Services 107

Glossary

Authentication is the process of validating the identity of a third party before allowing access to the protected resource. i

Authorization is the process of validating that the authenticated user has been granted permission to access the requested resources. i

Commercial Off The Shell (COTS) is a term that references non-developmental items (NDI) sold in the commercial marketplace and used or obtained through government contracts. The set of rules for COTS is defined by the Federal Acquisition Regulation (FAR). A COTS product is usually a computer hardware or software product tailored for specific uses and made available to the general public. Such products are designed to be readily available and user friendlyl. i, 147

Corporate system is a group of "Enterprise data centric" components, connected together in a particular area, which are all owned by the same company or institutions and which cover and support corporate functions. i

Customer Relationship Management (CRM) The Customer Relationship Management is a type of business software for capturing, processing and analyzing information on customers and prospects in order to retain them by providing optimized services. i, 147

Distributed Component Object Model (DCOM) is a set of Microsoft concepts and program interfaces in which client program object s can request services from server program objects on other computers in a network. DCOM is based on the Component Object Model (COM), which provides a set of interfaces allowing clients and servers to communicate within the same computer. It's used for OPC, uses RPC which opens multiple ports to establish communication. i, 147

Distributed Network Protocol (DNP3) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies. i, 147

Distribution Management System (DMS) A Distribution Management System is a collection of applications to monitor and control the entire distribution network in a safe and efficient way. It also serves as an operations platform, automating tasks and filtering information for the operator. DMSs use real-time data and provide all information on a single console at the control centre in an integrated way. i, 147

Encryption Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key. i

Enterprise Resource Planning (ERP) is a category of business-management software i.e., typically a suite of integrated applications that an organization can use to collect, store, manage and interpret data from many business activities. i, 147

Ethernet Ethernet is the traditional technology for connecting wired local area networks (LANs), enabling devices to communicate with each other via a protocol – a set of rules or common network language. i

Firmware In a computer system, a firmware is a program integrated into computer hardware (computer, photocopier, PLC, APS, hard disk, router, digital camera, etc.) that allows it to operate. i

Global System for Mobile communication (GSM) is a digital mobile network that is widely used by mobile phone users in Europe and other parts of the world. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies: TDMA, GSM and code-division multiple access (CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. i, 147

Industrial Control System (ICS) is a general term that encompasses several types of control systems used in industrial production, including *Supervisory Control And Data Acquisition* (SCADA) *systems*, *Distributed Control Systems* (DCS), and other control system configurations often found in industrial sectors and critical infrastructures. i, 148

Internet of Things (IoT) is a computing concept that describes the idea of everyday physical objects being connected to the internet and being able to identify themselves to other devices. i, 148

Local Area Network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building. i, 148

Manufacturing Execution System (MES) Manufacturing Execution System (or MOM - Manufacturing Operations Management), is a computerized system used in manufacturing, to track and document a manufacturing process. The aim of an MES is to make the value-adding processes transparent. i, 148

Meter Data Management (MDM) Meter Data Management is a software system that performs long-term storage, management and processing for the great amount of data delivered by smart metering systems. i, 148

Modbus Modbus is a serial communications protocol originally published by Modicon (now Schneider Electric) in 1979 for use with its programmable logic controllers (PLCs). Modbus has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices. i

OLE for Process Control (OPC) It is a software interface standard that allows Windows programs to communicate with industrial hardware devices. OPC is implemented in server/client pairs. i, 148

OPC Classic is a software interface standard that allows Windows programs to communicate with industrial hardware devices. OPC is implemented in server/client pairs. i

Programmable Logic Controller (PLC) are digital devices used for automation of industrial electro-mechanical processes. They connect to sensors in the process and convert their signals to digital data. i, 148

Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details. A procedure call is also sometimes known as a function call or a subroutine call. i, 148

Remote Terminal Unit (RTU) are microprocessor-controlled electronic devices that interface sensors and actuators by transmitting telemetry data to the SCADA

Server, and by using messages from the master supervisory system to control connected objects. i, 148

Security policy A security policy specifies security requirements through permissions, prohibitions and obligations.. i

Segmentation the operation of dividing a system into multiple security zones that can be separately controlled, monitored and protected. i

Segregation the operation of controlling communication through the security zones boundaries based on a set of predefined rules. i

Serial cable is a cable used to transfer information between two devices using a serial communication protocol. The form of connectors depends on the particular serial port used.. i

Software as a Service (SaaS) is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet. SaaS is one of three main categories of cloud computing, alongside infrastructure as a service (IaaS) and platform as a service (PaaS). i, 148

Supervisory Control and Data Acquisition (SCADA) It integrates data acquisition systems with data transmission systems and HMI software to provide a centralized monitoring and control system for multiple process inputs and outputs. They are designed to collect field data, transfer them to central computer facility, and display information to the operator graphically or textually. This allows the operator to monitor or control an entire system from a central location in near real time. Supervisory control layer contains the top level components of SCADA to which we refer as control centers. i, 148

Wide Area Network (WAN) is a network that exists over a large-scale geographical area. i, 149

Acronymes

ARP Address Resolution Protocol. i

CAE Computer Aided Engineering. i

COTS Commercial Off The Shell. i, 147, *See:* Commercial Off The Shell

CRM Customer Relationship Management. i, 147, *See:* Customer Relationship Management

DCOM Distributed Component Object Model. i, 147, *See:* Distributed Component Object Model

DDT Domain Definition Table. i

DIT Domain Interaction Table. i

DMS Distribution Management System. i, 147, *See:* Distribution Management System

DNP3 Distributed Network Protocol. i, 147, *See:* Distributed Network Protocol

DTE Domain Type Enforcement. i

DTEL DTE Language. i

EBIOS Expression des Besoins et Identification des Objectifs de Sécurité. i

ERP Enterprise Resource Planning. i, 147, *See:* Enterprise Resource Planning

FTP File Transfer Protocol. i

GSM Global System for Mobile communication. i, 147, *See:* Global System for Mobile communication

GUI Graphical User Interface. i

ICMP Internet Control Message Protocol. i

ICS Industrial Control System. i, 1, 148, *See:* Industrial Control System

IDS Intrusion Detection System. i

IED Intelligent Electronic Devices. i

IGMP Internet Group Management Protocol. i

IoT Internet of Things. i, 148, *See:* Internet of Things

IP Internet Protocol. i

IPS Intrusion Prevention System. i

ISD Information Systems Department. i

IT Information Technologies. i

LAN Local Area Network. i, 148, *See:* Local Area Network

MDM Meter Data Management. i, 148, *See:* Meter Data Management

MES Manufacturing Execution System. i, 148, *See:* Manufacturing Execution System

OPC OLE for Process Control. i, 148, *See:* OLE for Process Control

OT Operation Technologies. i

PLC Programmable Logic Controller. i, 148, *See:* Programmable Logic Controller

RBAC Role Based Access Control. i

RIICS Risk based IICS Segmentation. i

RPC Remote Procedure Call. i, 148, *See:* Remote Procedure Call

RTU Remote Terminal Unit. i, 148, *See:* Remote Terminal Unit

SaaS Software as a Service. i, 148, *See:* Software as a Service

SCADA Supervisory Control and Data Acquisition. i, 148, *See:* Supervisory Control and Data Acquisition

SCTP Stream Control Transmission Protocol. i

SMTP Simple Mail Transfer Protocol. i

SONICS Segmentation On iNtegrated ICS system. i

SQL Structured Query Language. i

TCP Transmission Control Protocol. i

USB Universal Serial Bus. i

WAN Wide Area Network. i, 149, *See:* Wide Area Network

Bibliography

[Sto] Stormshield sni40. 36

[ISA 1999] Enterprise - control system integration part 1: Models and terminology. *ISA-dS95 Standard (Draft 14), 1999*, 1999. 11, 32, 34, 45, 48, 105

[ISA 2001] Enterprise - control system integration. part 2: Object model attributes. *ISA-95 Standard 95.00.02 (Draft 9), 2001*, 2001. 32, 34, 48

[ISA 2004] Enterprise - control system integration part 3: Activity models of manufacturing operations management. *ISA-95 Standard 95.00.03 (Draft 16), 2004*, 2004. 5, 10, 32, 34, 45, 48, 139

[JUN 2010] Architecture for secure scada and distributed control system networks. *2010, Juniper Networks,Inc*, 2010. 1

[ISA 2012] Security for industrial automation and control systems : Security technologies for industrial automation and control systems. *ISA TR62443-3-1 (99.03.01)(Draft1, Edit1), 2012*, 2012. 9

[ISA 2013] Security for industrial automation and control systems: Terminology, concepts, and models. *ISA-99 Standard 62443-1-1 (Draft2, Edit4), 2013*, 2013. 1, 9, 19, 22, 27, 28, 32, 34, 37, 42, 45, 48, 87, 139

[GSM 2014] Global mag security. *Global Security Mag, October 2014*, 2014. 1, 2, 7

[IOT 2014] It vs ot in manufacturing: How will convergence play out? 2014. 48

[Tof 2014] Tofino industrial security solutions. 2014. 36, 39, 41, 88

[inn 2015] The innominate security technologies mguard website. 2015. 41

[Tof 2015] The tofino security appliance website. 2015. 41

[WUL 2016] Network segmentation for industrial control environments. *Wurldtech, A GE, March 2016*, March 2016. 32, 33, 34, 45, 48

[Albright et al. 2010] D. Albright, P. Brannan, and C. Walrond. *Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant?* Institute for Science and International Security, 2010. 24

[Andress and Leary 2017] J. Andress and M. Leary. Chapter 6 - protect the data. In J. Andress and M. Leary, editors, *Building a Practical Information Security Program*, pages 103 – 123. Syngress, 2017. 98

[ANSSI 2013] N. C. A. o. F. ANSSI. Classification method and key measures. *ANSSI, 2013*, 2013. 1, 9, 20, 22, 32, 34, 40, 87

[Ashibani and Mahmoud 2017] Y. Ashibani and Q. H. Mahmoud. Cyber physical systems security: Analysis, challenges and solutions. *Computers Security*, 68:81 – 97, 2017. 30, 31

[Badger et al. 1995] L. Badger, D. F. Sterne, D. L. Sherman, K. M. Walker, and S. A. Haghighat. Practical domain and type enforcement for unix. In *Security and Privacy, 1995. Proceedings., 1995 IEEE Symposium on*, pages 66–77, 1995. IEEE. 88

[Badger et al. 1996] L. Badger, D. F. Sterne, D. L. Sherman, K. M. Walker, and S. A. Haghighat. A domain and type enforcement unix prototype. *Computing Systems*, 9(1):47–83, 1996. 100

[Badra and Zeadally 2014] M. Badra and S. Zeadally. Design and performance analysis of a virtual ring architecture for smart grid privacy. *IEEE Transactions on Information Forensics and Security*, 9(2):321–329, Feb 2014. 31

[Bayuk et al. 2011] J. Bayuk, D. Cavit, E. Guerrino, J. Mahony, B. McDowell, W. Nelson, R. Snevel, and P. Staarfanger. Malware risks and mitigation report. *Washington, DC: BITS Financial Services Roundtable*, 2011. 21, 139

[Boyer 2009] S. A. Boyer. *Scada: Supervisory Control And Data Acquisition*. International Society of Automation, USA, 4th edition, 2009. 7, 13

[Bradetich and Oman 2007] R. Bradetich and P. Oman. Connecting scada systems to corporate it networks using security-enhanced linux. In *Proceedings of 34th Annual Western Protective Relay Conference*, 2007. 43, 88, 90

[Bradetich and Oman 2008] R. Bradetich and P. Oman. Implementing scada security policies via security-enhanced linux. In *proceedings of the 10th Annual Western Power Delivery Automation Conference*, 2008. 88, 90

[Cai et al. 2008] N. Cai, J. Wang, and X. Yu. Scada system security: Complexity, history and new developments. In *2008 6th IEEE International Conference on Industrial Informatics*, pages 569–574, 2008. IEEE. 7

[Campbell and Rrushi 2011] R. Campbell and J. Rrushi. Detecting cyber attacks on nuclear power plants. *IFIP Advances in Information and Communication Technology (AICT)*, 290(290):1–54, 2011. 42

[Cereia et al. 2014a] M. Cereia, I. C. Bertolotti, L. Durante, and A. Valenzano. Latency evaluation of a firewall for industrial networks based on the tofino industrial security solution. In *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation, ETFA 2014, Barcelona, Spain, September 16-19, 2014*, pages 1–8, 2014. 36, 39, 41, 88

[Cereia et al. 2014b] M. Cereia, I. C. Bertolotti, L. Durante, and A. Valenzano. Latency evaluation of a firewall for industrial networks based on the tofino industrial security solution. In *Emerging Technology and Factory Automation (ETFA), 2014 IEEE*, pages 1–8, 2014. IEEE. 39, 41, 88

[Cheminod et al. 2013] M. Cheminod, L. Durante, and A. Valenzano. Review of security issues in industrial networks. *IEEE Transactions on Industrial Informatics*, 9(1):277–293, 2013. 26

[Cheminod et al. 2016] M. Cheminod, L. Durante, A. Valenzano, and C. Zunino. Performance impact of commercial industrial firewalls on networked control systems. In *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–8, Sep. 2016. 30, 39, 87

[Cherdantseva et al. 2016] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart. A review of cyber security risk assessment methods for scada systems. *Computers & security*, 56:1–27, 2016. 19, 20, 23, 26

[Cherry and Constantine 2011] S. Cherry and L. Constantine. Sons of stuxnet. *IEEE spectrum*, 14, 2011. 24

[Cruz et al. 2015] T. Cruz, J. Barrigas, J. Proença, A. Graziano, S. Panzieri, L. Lev, and P. Simões. Improving network security monitoring for in-

dustrial control systems. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 878–881, 2015. IEEE. 19, 20

[CSSP 2009] D. CSSP. Recommended proctice: Improving industrial control systems cybersecurity with defense-in-depth strategies. *US-CERT Defense In Depth, October 2009*, 2009. 2, 22, 32, 33, 34, 36, 37, 41, 42, 45, 48

[D'Antonio et al. 2006] S. D'Antonio, F. Oliviero, and R. Setola. High-speed intrusion detection in support of critical infrastructure protection. In J. Lopez, editor, *Critical Information Infrastructures Security*, pages 222–234, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. 42

[de la Défense Nationale 2010] de la S. G. Défense Nationale. Ebios-expression des besoins et identification des objectifs de sécurité, méthode de gestion des risques. 2010. 50, 71, 74

[DeSmit et al. 2017a] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio. An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. *Journal of Manufacturing Systems*, 43:339–351, 2017. 19, 23

[DeSmit et al. 2017b] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio. An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. *Journal of Manufacturing Systems*, 43:339–351, 2017. 20, 21, 23, 25

[Diovu and Agee 2017] R. C. Diovu and J. T. Agee. A cloud-based openflow firewall for mitigation against ddos attacks in smart grid ami networks. *2017 IEEE PES PowerAfrica*, 2017. 30, 41

[Diovu and Agee 2017] R. C. Diovu and J. T. Agee. Quantitative analysis of firewall security under ddos attacks in smart grid ami networks. In *2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON)*, Nov 2017. 30, 41

[Drias et al. 2015] Z. Drias, A. Serhrouchni, and O. Vogel. Analysis of cyber security for industrial control systems. In *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, pages 1–8, 2015. IEEE. 1, 20, 25

[Düssel et al. 2010] P. Düssel, C. Gehl, P. Laskov, J.-U. Busser, C. Störmann, and J. Kästner. Cyber-critical infrastructure protection using real-time

payload-based anomaly detection. In E. Rome and R. Bloomfield, editors, *Critical Information Infrastructures Security*, pages 85–97, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg. 42

[Etigowni et al. 2016] S. Etigowni, D. J. Tian, G. Hernandez, S. Zonouz, and K. Butler. Cpac: securing critical infrastructure with cyber-physical access control. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, pages 139–152, 2016. ACM. 26

[Evans 2011] D. Evans. The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper*, 1(2011):1–11, 2011. 20, 21, 139

[Ferraiolo et al. 1995] D. Ferraiolo, J. Cugini, and D. R. Kuhn. Role-based access control (rbac): Features and motivations. In *Proceedings of 11th annual computer security application conference*, pages 241–48, 1995. 89

[FireEye 2015] FireEye. M-trends 2015: a view from the front line. *Mandiant*, 2015. 23

[Force and Initiative 2013] J. T. Force and T. Initiative. Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, 800(53):8–13, 2013. 8, 22, 28, 32, 42, 87

[Fovino et al. 2010] I. N. Fovino, A. Carcano, T. D. L. Murel, A. Trombetta, and M. Masera. Modbus/dnp3 state-based intrusion detection system. In *24th IEEE International Conference on Advanced Information Networking and Applications, AINA 2010, Perth, Australia, 20-13 April 2010*, pages 729–736, 2010. 20, 39

[Galloway and Hancke 2013] B. Galloway and G. P. Hancke. Introduction to industrial control networks. *IEEE Communications Surveys and Tutorials*, 15(2):860–880, 2013. 20, 40

[Giani et al. 2013] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla. Smart grid data integrity attacks. *IEEE Transactions on Smart Grid*, 4(3):1244–1253, Sep. 2013. 31

[Gilchrist 2008] G. Gilchrist. Secure authentication for dnp3. In *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, July 2008. 41

[Guan et al. 2011] J. Guan, J. H. Graham, and J. L. Hieb. A digraph model for risk identification and mangement in scada systems. In *Proceedings of 2011 IEEE*

International Conference on Intelligence and Security Informatics, pages 150–155, 2011. IEEE. 24

[H. Eslava and Pineda 2015] L. A. R. H. Eslava and D. Pineda. An algorithm for optimal firewall placement. *iec61850 substations," Journal of Power and Energy Engineering*, 2015. 41

[Hachana et al. 2016] S. Hachana, F. Cuppens, and N. Cuppens-Boulahia. Towards a new generation of industrial firewalls: Operational-process aware filtering. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec 2016. 41

[Hallyn and Kearns 2000a] S. E. Hallyn and P. Kearns. Domain and type enforcement for linux. In *Annual Linux Showcase & Conference*, 2000. 89

[Hallyn and Kearns 2000b] S. E. Hallyn and P. Kearns. Domain and type enforcement for linux. In *Annual Linux Showcase & Conference*, 2000. 100

[Hayes and El-Khatib 2013] G. Hayes and K. El-Khatib. Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol. In *2013 Third International Conference on Communications and Information Technology (ICCIT)*, pages 179–184, June 2013. 40

[Henrie 2013] M. Henrie. Cyber security risk management in the scada critical infrastructure environment. *Engineering Management Journal*, 25(2):38–45, 2013. 21, 24

[Hildick-Smith 2006] A. Hildick-Smith. Security for critical infrastructure scada systems. *SANS Reading Room, GSEC Practical Assignment, Version*, 1:498–506, 2006. 21

[Hu and Gharavi 2014] B. Hu and H. Gharavi. Smart grid mesh network security using dynamic key distribution with merkle tree 4-way handshaking. *IEEE Transactions on Smart Grid*, 5(2):550–558, March 2014. 31

[Huang et al. 2009] Y.-L. Huang, A. A. Cárdenas, S. Amin, Z.-S. Lin, H.-Y. Tsai, and S. Sastry. Understanding the physical and economic consequences of attacks on control systems. *International Journal of Critical Infrastructure Protection*, 2(3):73–83, 2009. 2, 7

[Huda et al. 2018a] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren. Securing the operations in scada-iot platform based industrial control system using ensemble of deep belief networks. *Applied Soft Computing*, 71:66–77, 2018. 26

[Huda et al. 2018b] S. Huda, J. Yearwood, M. M. Hassan, and A. Almogren. Securing the operations in scada-iot platform based industrial control system using ensemble of deep belief networks. *Applied Soft Computing*, 71:66 – 77, 2018. 31

[Huitsing et al. 2008] P. Huitsing, R. Chandia, M. Papa, and S. Shenoi. Attack taxonomies for the modbus protocols. *IJCIP*, 1:37–44, 2008. 39

[ICS-CERT 2015] ICS-CERT. Ics-cert monitor newsletters november-december. 2015. 24

[Igure et al. 2006] V. M. Igure, S. A. Laughter, and R. D. Williams. Security issues in scada networks. *computers & security*, 25(7):498–506, 2006. 28

[Jens-Tobias ZERBST 2009] I. R.-J. ,Erik HJELMVIKJens-Tobias ZERBST. Zoning principles in electricity distribution and energy production environments. *20th International Conference on Electricity Distribution, 2009*, 2009. 32, 48

[Johari and Sharma 2012] R. Johari and P. Sharma. A survey on web application vulnerabilities (sqlia, xss) exploitation and security engine for sql injection. In *2012 International Conference on Communication Systems and Network Technologies*, pages 453–458, 2012. IEEE. 20

[Keith Stouffer and Hahn 2015] V. P. M. A. ,Suzanne LightmanKeith Stouffer and A. Hahn. Guide to industrial control systems (ics) security. *NIST special publication, vol. 800, no.82, 2015*, 800(82):16–16, 2015. 1, 2, 7, 9, 13, 19, 26, 30, 32, 33, 34, 40, 41, 45, 48, 49

[Khaoula et al. 2017] E.-S. Khaoula, D. Espes, and N. Cuppens. A new segmentation method for integrated ics. *15th International Conference International Conference on Privacy, Security and Trust (PST'2017)*, 2017. 3, 47

[Khaoula et al. 2018a] E.-S. Khaoula, D. Espes, and N. Cuppens. Risk based iics segmentation method. *13th International Conference on Risks and Security of Internet and Systems, (CRISIS'2018)*, 2018. 4

[Khaoula et al. 2018b] E.-S. Khaoula, D. Espes, and N. Cuppens. Sonics: a segmentation method for integrated ics and corporate system. *14th International Conference on Information Systems Security, (ICISS'2018)*, 2018. 3

[Khaoula et al. 2016] E.-S. Khaoula, C.-B. Nora, E. David, and C. Frederic. Analysis of ics and corporate system integration vulnerabilities. *14th International Conference on Embedded Systems, Cyber-physical Systems, and Applications (ESCS'2016)*, 2016. 3

[Khosroshahi and Shahinzadeh 2016] A. H. Khosroshahi and H. Shahinzadeh. Security technology by using firewall for smart grid. *Bulletin of Electrical Engineering and Informatics*, 2016. 41

[Kim 2012] H. Kim. Security and vulnerability of scada systems over ip-based wireless sensor networks. *International Journal of Distributed Sensor Networks*, 2012, 2012. 2, 19

[Kletti 2007] J. Kletti. *Manufacturing Execution System-MES*. Springer, 2007. 12

[Laboratories a] S. E. Laboratories. Sel-3021-1 serial encrypting transceiver. *Pullman, Washington*. 40

[Laboratories b] S. E. Laboratories. Sel-3620 ethernet security gateway. *Pullman, Washington*. 40

[Larkin et al. 2014a] R. D. Larkin, J. Lopez Jr, J. W. Butts, and M. R. Grimaila. Evaluation of security solutions in the scada environment. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 45(1):38–53, 2014. 21, 42

[Larkin et al. 2014b] R. D. Larkin, J. Lopez Jr, J. W. Butts, and M. R. Grimaila. Evaluation of security solutions in the scada environment. *ACM SIGMIS Database*, 45(1):38–53, 2014. 26, 33

[Leith and Piper 2013] H. Leith and J. W. Piper. Identification and application of security measures for petrochemical industrial control systems. *Journal of Loss Prevention in the Process Industries*, 26(6):982–993, 2013. 20, 22, 23

[Leverett 2011] E. P. Leverett. Quantitatively assessing and visualising industrial system attack surfaces. *University of Cambridge, Darwin College*, 7, 2011. 21, 33

[Li et al. 2018] D. Li, H. Guo, J. Zhou, L. Zhou, and J. Wen. Scadawall: A cpi-enabled firewall model for scada security. *Computers Security*, 80, 10 2018. 30, 39, 42, 87, 88

[Li and Da Xu 2017] S. Li and L. Da Xu. *Securing the internet of things*. Syngress, 2017. 31

[Lin et al. 2017] C. Lin, S. Wu, and M. Lee. Cyber attack and defense on industry control systems. In *2017 IEEE Conference on Dependable and Secure Computing*, pages 524–526, 2017. 42

[Liu et al. 2015] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage, and A. K. Srivastava. Analyzing the cyber-physical impact of cyber events on the power grid. *IEEE Transactions on Smart Grid*, 6(5):2444–2453, Sep. 2015. 31

[Liu et al. 2013] S. Liu, X. P. Liu, and A. El Saddik. Denial-of-service (dos) attacks on load frequency control in smart grids. In *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–6, 2013. IEEE. 31

[Lu and Da Xu 2019] Y. Lu and L. Da Xu. Internet of things (iot) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, pages 1–1, 2019. 31

[Mahan et al. 2011] R. E. Mahan, J. Burnette, J. Fluckiger, C. Goranson, S. Clements, H. Kirkham, and C. Tews. Secure data transfer guidance for industrial control and scada systems. *Report to US Department of Energy, PNNL-20776*, 2011. 32

[Majdalawieh et al. 2006] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera. Dnpsec: Distributed network protocol version 3 (dnp3) security framework. In K. Elleithy, T. Sobh, A. Mahmood, M. Iskander, and M. Karim, editors, *Advances in Computer, Information, and Systems Sciences, and Engineering*, 2006. Springer Netherlands. 41

[Miller and Rowe 2012] B. Miller and D. C. Rowe. A survey scada of and critical infrastructure incidents. *RIIT*, 12:51–56, 2012. 23, 24, 28

[Nagarajan and Jensen 2010] A. Nagarajan and C. D. Jensen. A generic role based access control model for wind power systems. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications - JoWUA*, 2010. 40

[(NDIA) 2014] N. D. I. A. (NDIA). Cybersecurity for advanced manufacturing. 2014. NDIA. 25

[Nicholson et al. 2012] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke. Scada security in the light of cyber-warfare. *Computers & Security*, 31(4):418–436, 2012. 20, 22, 24, 26, 28

[Nivethan and Papa 2016] J. Nivethan and M. Papa. A linux-based firewall for the dnp3 protocol. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, 2016. 41

[Niyato and Wang 2012] D. Niyato and P. Wang. Cooperative transmission for meter data collection in smart grid. 2012. 12

[Obregon 2015] L. Obregon. Secure architecture for industrial control systems. *SANS Institute, InfoSec Reading Room, 2015*, 2015. 20, 26, 35, 39, 48, 53

[of Energy et al. 2007] of U. D. Energy, I. Security, and Energy. 21 steps to improve cyber security of scada networks. 2007. 27

[of France 2013] of N. C. A. France. Detailed measures. *ANSSI, 2013*, 2013. 1, 19, 22, 32, 34, 45, 48

[Oostendorp et al. 2000] K. A. Oostendorp, L. Badger, C. D. Vance, W. G. Morrison, M. J. Petkac, D. L. Sherman, and D. F. Sterne. Domain and type enforcement firewalls. In *DARPA Information Survivability Conference and Exposition, 2000. DISCEX'00. Proceedings*, volume 1, pages 351–361, 2000. IEEE. 88, 89, 90

[Park and Lee 2014] S. Park and K. Lee. Advanced approach to information security management system model for industrial control system. *The Scientific World Journal*, 2014, 2014. 26

[Parra et al. 2019] G. D. L. T. Parra, P. Rad, and K.-K. R. Choo. Implementation of deep packet inspection in smart grids and industrial internet of things: Challenges and opportunities. 2019. 30, 39, 87

[Patel et al. 2005] S. Patel, R. Tantalean, P. Ralston, and J. Graham. Supervisory control and data acquisition remote terminal unit testbed. *Intelligent Systems Research Laboratory technical report TR-ISRL-05-01, Department of Computer Engineering and Computer Science. Louisville, Kentucky: University of Louisville*, 2005. 24, 26

[Pires and Oliveira 2006] P. S. M. Pires and L. A. H. Oliveira. Security aspects of scada and corporate network interconnection: An overview. In *IEEE International Conference on Dependability aof computer Systems, pp. 127-134*, 2006. IEEE, 2006. 35, 36

[Pollet 2006] J. Pollet. Innovative defense strategies for securing scada and control systems. *PlantData Technologies, 2006*, 2006. 34, 35

[Poulsen 2009] K. Poulsen. Ex-employee fingered in texas power company hack. *Retrieved August*, 9:2013, 2009. 21

[Premnath and Haas 2015] S. N. Premnath and Z. J. Haas. Security and privacy in the internet-of-things under time-and-budget-limited adversary model. *IEEE Wireless Communications Letters*, 4(3):277–280, June 2015. 30, 31

[Ralston et al. 2007] P. A. Ralston, J. H. Graham, and J. L. Hieb. Cyber security risk assessment for scada and dcs networks. *ISA transactions*, 46(4):583–594, 2007. 34

[RISI 2013] RISI. Industry attacks growing. october 14. In *<http://www.isssource.com/risi-industry-attacks-growing>*, 2013. 24

[Rosic et al. 2013] D. Rosic, U. Novak, and S. Vukmirovic. Role-based access control model supporting regional division in smart grid system. In *2013 Fifth International Conference on Computational Intelligence, Communication Systems and Networks*, June 2013. 40

[Rosinger and Uslar 2013] C. Rosinger and M. Uslar. Smart grid security: Iec 62351 and other relevant standards. In *Standardization in Smart Grids*, pages 129–146. Springer, 2013. 15

[Rrushi and Campbell 2008] J. Rrushi and R. Campbell. Detecting cyber attacks on nuclear power plants. In M. Papa and S. Shenoi, editors, *Critical Infrastructure Protection II*, pages 41–54, Boston, MA, 2008. Springer US. 42

[Sacramento 2007] S. M. Sacramento. Man pleads guilty to attempting to shut down california's power grid. In *United States Attorney: Eastern District of California, News Release*, 2007. 21

[Salah et al. 2012] K. Salah, K. Elbadawi, and R. Boutaba. Performance modeling and analysis of network firewalls. *IEEE Transactions on Network and Service Management*, March 2012. 41

[Sani et al. 2019] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong. Cyber security framework for internet of things-based energy internet. *Future Generation Computer Systems*, 93:849 – 859, 2019. 32

[Saqib et al. 2015] A. Saqib, R. W. Anwar, O. K. Hussain, M. Ahmad, M. A. Ngadi, M. M. Mohamad, Z. Malki, C. Noraini, B. A. Jnr, R. Nor, et al. Cyber security for cyber physcial systems: A trust-based approach. *J Theor Appl Inf Technol*, 71(2):144–152, 2015. 32

[Saxena et al. 2016] N. Saxena, B. J. Choi, and R. Lu. Authentication and authorization scheme for various user roles and devices in smart grid. *IEEE Transactions on Information Forensics and Security*, 11(5):907–921, May 2016. 31

[Shahzad et al. 2015] A. Shahzad, M. Lee, Y. K. Lee, S. Kim, N. Xiong, J. Y. Choi, and Y. Cho. Real time modbus transmissions and cryptography security designs and enhancements of protocol sensitive information. 2015. 30, 40

[Sicard et al. 2018] F. Sicard, C. Escudero, É. Zamaï, and J.-M. Flaus. From ics attacks' analysis to the safe approach: Implementation of filters based on behavioral models and critical state distance for ics cybersecurity. In *2nd Cyber Security In Networking Conference*, page 8, 2018. 25

[Stouffer et al. 2011] K. Stouffer, J. Falco, and K. Scarfone. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82):16–16, 2011. 28

[Sturm et al. 2014] L. Sturm, C. Williams, J. Camelio, J. White, and R. Parker. Cyber-physical vunerabilities in additive manufacturing systems. *Context*, 7(8), 2014. 23

[Ten et al. 2010] C.-W. Ten, G. Manimaran, and C.-C. Liu. Cybersecurity for critical infrastructures: attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 40(4):853–865, 2010. 7

[Thierry Godart 2012] J. W. ,Ken GeislerThierry Godart. How the distribution management system (dms) is becoming a core function of the smart grid. 2012. 12

[Tiegelkamp and John 1995] M. Tiegelkamp and K.-H. John. *IEC 61131-3: Programming industrial automation systems*. Springer, 1995. 14

[Trappe et al. 2015] W. Trappe, R. Howard, and R. S. Moore. Low-energy security: Limits and opportunities in the internet of things. *IEEE Security Privacy*, 13(1):14–21, Jan 2015. 31

[Tuptuk and Hailes 2016] N. Tuptuk and S. Hailes. The cyberattack on ukraine's power grid is a warning of what's to come. *The Conversation. Retrieved from http://theconversation. com/thecyberattack-on-ukraines-power-grid-is-a-warning-of-whats-tocome-52832*, pages 847–855, 2016. 24

[Vegh and Miclea 2014] L. Vegh and L. Miclea. Enhancing security in cyber-physical systems through cryptographic and steganographic techniques. In *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*, pages 1–6, 2014. IEEE. 30, 32

[Verba and Milvich 2008] J. Verba and M. Milvich. Idaho national laboratory supervisory control and data acquisition intrusion detection system (scada ids). In *2008 IEEE Conference on Technologies for Homeland Security*, pages 469–473, 2008. IEEE. 42

[Vincent et al. 2015] H. Vincent, L. Wells, P. Tarazaga, and J. Camelio. Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. *Procedia Manufacturing*, 1:77–85, 2015. 24, 25

[W. Shang and Zeng 2016] M. W. ,Q. QiaoW. Shang and P. Zeng. Design and implementation of industrial firewall for modbus/tcp. *JcP*, 2016. 41

[Wang et al. 2008] B. Wang, S. Zhang, and Z. Zhang. Drbac based access control method in substation automation system. In *2008 IEEE International Conference on Industrial Technology*, April 2008. 40

[Wang et al. 2010] E. K. Wang, Y. Ye, X. Xu, S.-M. Yiu, L. C. K. Hui, and K.-P. Chow. Security issues and challenges for cyber physical system. In *2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*, pages 733–738, 2010. IEEE. 32

[Watin-Augouard et al. 2011] M. Watin-Augouard et al. Prospective analysis on trends in cybercrime from 2011 to 2020. *National Gendarmerie*, 2011. 21, 139

[Wei et al. 2013] D. Wei, F. Darie, and L. Shen. Application layer security proxy for smart grid substation automation systems. In *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, Feb 2013. 40

[Wei et al. 2011] D. Wei, Y. Lu, M. Jafari, P. M. Skare, and K. Rohde. Protecting smart grid automation systems against cyberattacks. *IEEE Transactions on Smart Grid*, Dec 2011. 40

[Wells et al. 2014] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White. Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, 2(2):74–77, 2014. 22, 23

[Xie and Wang 2014] Y. Xie and D. Wang. An item-level access control framework for inter-system security in the internet of things. In *Applied mechanics and materials*, volume 548, pages 1430–1432, 2014. Trans Tech Publ. 32

[Yan et al. 2017] J. Yan, H. He, X. Zhong, and Y. Tang. Q-learning-based vulnerability analysis of smart grid against sequential topology attacks. *IEEE Transactions on Information Forensics and Security*, 12(1):200–210, Jan 2017. 31

[Yang et al. 2017] X. Yang, P. Zhao, X. Zhang, J. Lin, and W. Yu. Toward a gaussian-mixture model-based detection scheme against data integrity attacks in the smart grid. *IEEE Internet of Things Journal*, 4(1):147–161, 2017. 31

[Yun et al. 2018] J.-H. Yun, Y. Hwang, W. Lee, H.-K. Ahn, and S.-K. Kim. Statistical similarity of critical infrastructure network traffic based on nearest neighbor distances. In M. Bailey, T. Holz, M. Stamatogiannakis, and S. Ioannidis, editors, *Research in Attacks, Intrusions, and Defenses*, pages 577–599, Cham, 2018. Springer International Publishing. 42

[Zvabva et al. 2018] D. Zvabva, P. Zavarsky, S. Butakov, and J. Luswata. Evaluation of industrial firewall performance issues in automation and control networks. In *2018 29th Biennial Symposium on Communications (BSC)*, pages 1–5, 2018. IEEE. 30, 39, 87

Titre : Mécanismes et modèles de segmentation et de ségrégation pour sécuriser l'intégration des systèmes de contrôle industriel (ICS) avec les systèmes d'entreprise.

Mots clés : Systèmes de Contrôle Industriel, Segmentation, Ségrégation, Contrôle d'accès, Domain-Type Enforcement.

Résumé : Sécuriser des systèmes industriels, et en particulier des systèmes intégrés au système d'information, devient l'une des préoccupations les plus urgentes qui inquiètent non seulement tous les acteurs industriels mais aussi les gouvernements. Un nombre très important d'entités industrielles et d'infrastructures sont si critiques que toute cyber attaque réussie contre ces entités peut causer d'énormes dégâts aux entreprises, à l'environnement et plus gravement à la sécurité nationale et à la sûreté des personnes.

Cette thèse étudie l'intégration des systèmes ICS avec les systèmes d'entreprise d'un point de vue sécurité. Notre objectif est d'étudier les vulnérabilités de sécurité des systèmes industriels intégrés et de proposer des modèles et des mécanismes pour améliorer leur sécurité et les protéger contre les attaques complexes.

Après avoir réalisé une étude approfondie sur les vulnérabilités des systèmes ICS intégrés (IICS) et les solutions de sécurité existantes, nous nous sommes concentrés sur l'étude de la technique de défense en profondeur et son applicabilité aux systèmes ICS intégrés. Nous avons alors défini une nouvelle méthode générique de segmentation pour les IICS, SONICS, qui permet de simplifier la segmentation des IICS en se concentrant uniquement sur les aspects qui sont réellement significatifs pour la segmentation. Nous avons ensuite développé une version améliorée de SONICS, RIICS, une méthode de segmentation pour les systèmes IICS qui comble les lacunes de SONICS en se concentrant sur le risque en plus des spécificités techniques et industrielles.

Pour compléter la méthode de segmentation, nous avons étudié les solutions de ségrégation et de contrôle d'accès. Nous avons proposé un nouveau modèle de contrôle de flux basé sur DTE (Domain Type Enforcement) pour les systèmes ICS intégrés.

Title : Segmentation and Segregation mechanisms and models to secure the integration of Industrial Control system (ICS) with Corporate system.

Keywords : Integration, Industrial Control Systems, Segmentation, Segregation, Access control, Domain-Type Enforcement.

Abstract : Securing ICS systems, and especially integrated ones, is becoming one of the most urgent issues that disquiets not only all industrial actors but also governments. Very important number of industrial entities and infrastructures are so critical that any non contained cyber attack on these entities can cause huge damage to business, to environment and more gravely to national security and people safety.

This thesis studies the integration of ICS with Corporate systems from a security standpoint. Our goal is to study integrated ICS systems security vulnerabilities and suggest models and mechanisms to improve their security and protect them against ceyberattacks.

After conducting a study on the vulnerabilities of integrated ICS systems (IICS) and the existing security solutions, we focused on the study of defence in depth technique and its applicability to integrated ICS systems. We defined a new generic segmentation method for IICS, SONICS, which simplifies the segmentation of IICS by focusing only on spects that are really significant for segmentation. We next developed an improved version of SONICS, RIICS (Risk based IICS Segmentation), a segmentation method for IICS systems that fills the SONICS gaps by focusing on risk on top of technical and industrial specifications.

To complement the segmentation method, we studied segregation and access control solutions. We proposed a new DTE-based l (Domain Type Enforcement) flow control model for integrated ICS systems.