

A new Segmentation Method for Integrated ICS

Khaoula Es-Salhi, David Espes, Nora Cuppens

▶ **To cite this version:**

Khaoula Es-Salhi, David Espes, Nora Cuppens. A new Segmentation Method for Integrated ICS. PST 2017 : 15th International Conference on Privacy, Security and Trust, Aug 2017, Calgary, Canada. 10.1109/PST.2017.00020 . hal-01872432

HAL Id: hal-01872432
https://hal.science/hal-01872432

Submitted on 12 Sep 2018

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.

A new Segmentation Method for Integrated ICS

Khaoula ES-SALHI
IMT Atlantique
Cesson Sevigne, France 35576
Email: khaoula.es-salhi@imt-atlantique.fr

David Espes
University of Western Brittany
Brest, France, 29238
Email: david.espes@univ-brest.fr

Nora Cuppens
IMT Atlantique
Cesson Sevigne, France, 35576
Email: nora.cuppens@imt-atlantique.fr

***Abstract*—The paper presents a new segmentation method for Integrated ICS (*Industrial Control Systems*) with *Corporate system*. This new method aims at simplifying security zones identification by focusing only on the system's aspects that are really relevant for segmentation taking into account the system's constraints. Multiple research works have studied IICS (*Integrated ICS*) segmentation but their solutions are unfortunately not generic enough and do not sufficiently take into account all of the Integrated ICS specificity. Our new method tries to address the problem more efficiently by providing realistic and pragmatic answers to the issue while remaining sufficiently generic to be applied to different types of Integrated ICS.**

I. Introduction

One of the most important orientations of the current industrial business world is Industrial Control Systems (ICS) and Corporate Systems Integration [1]. This has numerous benefits. For example, it increases visibility of industrial control system activities and allows to use business analysis to optimize production processes. This ensures more responsiveness to business requirements and more business competitiveness [2]. However, the integration introduces multiple security problems because industrial systems have been designed without security in mind because they have usually been isolated [3], [4], [5], [6], [7]. Defense-in-depth is one of the most recommended security measures that should be applied to IICS (*Integrated ICS*) [3], [5]. It consists of implementing multiple layers of defense to protect against security issues [5] by dividing the IICS into multiple encapsulated security zones. It is mainly implemented using Segmentation and Segregation. Segmentation is segmenting a system into multiple security zones that can be separately controlled, monitored and protected [8]. A security zone is a set of *Components* or sub-systems connected within one sub-network governed by a single authority and one security policy [9]. The security zones must be created with clearly defined boundaries and policy. *Components* within them respect the same policy [9] and inter-zones communications are filtered in accordance with their policies.

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 [5], [8] have suggested some zoning solutions, but these solutions are unfortunately not generic enough and do not sufficiently take into account all of the IICS specificity. Besides, the system's elements characteristics 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?

Therefore, we suggest a new IICS segmentation method that aims to simplify IICS segmentation. This new method is based on a meta-model of IICS that allows to describe systems elements by focusing only on aspects that are really meaningful for segmentation. The method uses this meta-model to identify new potential security zones throughout its cycles. The new identified zones are kept or not depending on a constraints analysis.

The rest of the paper is organized as follows. Section II states the IICS segmentation problem. Section III depicts our new IICS segmentation method. We will present our IICS meta-model (III-A), the system's constraints that our Segmentation method takes into account (III-C) and explain how new potential zones are identified and how the decision to keep them or not should be made (III-D).

II. Problem statement

IICS segmentation is not a simple task. IICS configurations are heavily functionally and technically heterogeneous. Besides, IICS integrate two systems (ICS and Corporate systems) that have always formed two separate entities managed by different teams. IICS segmentation may be based on various types of characteristics such as functional characteristics, business impact, risk levels, or other requirements defined by the organization. However, there is currently no precise method that structures the segmentation operation.

Furthermore, segmenting large-scale networks is a complicated task for administrators and security experts. It is all the more complicated in systems with frequently changing configuration and topology. Performing segmentation in large-scale networks taking into account architecture changes and configuration updates is also another issue with IICS segmentation.

It would be less complicated if a framework that helps to perform IICS segmentation existed. More precisely, it would be very helpful if we had an IICS segmentation method. One can argue that engineering expertise and intuition are

978-1-5386-2487-6/17/$31.00 2017 European Union

enough to perform IICS segmentation. However, this approach is error-prone and is likely to lead to insufficient results. Some important aspects may be neglected and the work may take more time than it should be. Using a framework or a working method is always beneficial because it guarantees more valuable results more quickly.

Multiple research works have studied IICS segmentation. Most of them (such as NIST [3], ISA [6], [7], [10] and ANSSI [4] guides ...) recommend to perform segmentation on a case by case basis but provide only shallow guidance. Some others [5] treat the subject with a more concrete approach trying to perform segmentation using a well defined reference architecture. They mainly suggest to use the Purdue Model for Control Hierarchy logical framework (IEC 62264) [6] to delineate security zones. On the other hand, few research works try to solve the problem in a generic way. Their solutions, while still based on the IEC 62264 (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 relevant for IICS segmentation. Moreover, all the research works communally suggest to create more than one layer of defense and separate ICS 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 IEC 62264 model, but do not take into account other types of IICS characteristics that may be very significant for Segmentation. Finally, none of the studied solutions models IICS real conditions and constraints that may impact security zones. Therefore, we defined a new generic IICS Segmentation method that fills these gaps.

III. The segmentation method

The principle of our segmentation method is depicted in Figure 1. It consists of multiple cycles where new potential security zones are progressively identified based on one aspect of the system at a time. The new identified zones are kept or not depending on the constraints analysis performed on IICS elements that are involved in the new potential zones. The system to be segmented must be modeled before we can apply the segmentation method. This should be done using the meta-model that will be presented in the next section.

A. The IICS Meta-Model

Our IICS meta-model (Figure 2) simplifies IICS description and assists in characterizing and grouping IICS elements keeping the focus on elements and characteristics that are really meaningful for segmentation. It allows to model an IICS as a simple set of "*Components*", "*Connections*" and "*Processes*".

- A **"*Component*"** is any device capable of communicating through the system network regardless its functions or the technologies it uses. A Component is characterized by its functional level, its technical type as well as the geographical site it belongs to.
- 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.
- A **"*Process*"** is a set of interrelated or interacting activities, which transforms inputs into outputs". A system is organized into multiple processes. Each *component* belongs to one or more process. Each Process is characterized by its required protection level. Systems processes identification requires an organization work by the company. In general, an organization standard such as ISO9001 is applied to partition the system into multiple processes.

1) Components meta-characteristics:

- **Functional levels** Functional grouping is relevant for segmentation. It allows to separate *Components* based on their function within the system [11], [12]. We use an extended model of the IEC 62264 (ISA 95) functional hierarchical model that defines multiple functional levels for IICS (see Table I). Each *Component* of the system only belongs to one functional group.

TABLE I
FUNCTIONAL LEVELS

Group	Name	Definition
FL-0	Process	This levels 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 *Components* is also decisive for segmentation [13]. In an IICS, there are two very different families of technologies: Information Technology (IT) and Operation Technology (OT). These two types of technologies have different nature and focus on dissimilar objectives especially regarding security. A third technical type of *Components* should be distinguished: the IT-OT *Components*. These are *Components* that are designed to use both types of technologies IT and OT such as workstations.
- **Geographical location** *Components*'location is another key aspect to be taken into account for segmentation [3]. Two physically distant sites systematically lead to two

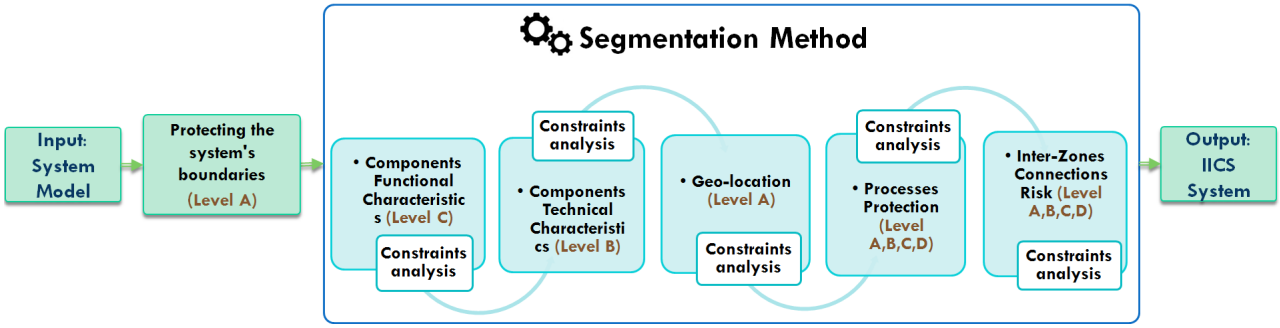


Fig. 1. The Segmentation method

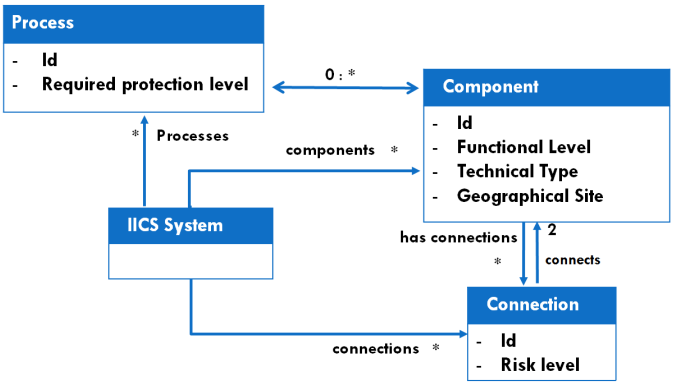


Fig. 2. IICS Meta-Model

different security zones. We mean by two "physically distant" sites: sites that are either connected by wireless *Connection* or non physically protected wired *Connection*.

2) Processes meta-characteristics: IICS should also be segmented based on Organizational aspects. This can be done in function of processes. Each process of the system represents a new potential security zone. Each process is characterized by its "required protection level". This represents the level of protection needed by a given process. 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 required protection level of a process depends on its risk level and should be evaluated using a risk analysis. We suggest a simple risk analysis method that was inspired by EBIOS and adapted to IICS specificity. This risk analysis method defines the risk as a function of dreaded events gravity and their likelihood. The steps that should be followed to evaluate the risk level of a given process are as follows:

1) **Identify the dreaded events and estimate their gravity** Dreaded events gravity can have one of the gravity scale values presented in Table II. It is a qualitative estimation that needs good knowledge of the organization's system and business. It is therefore to be done in collaboration with the organization's staff. If one dreaded event has different gravity levels (for example Considerable gravity regarding safety aspects but Critical financial loss), the worst case is assumed.

TABLE II
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

2) **Analyze Threat Sources and estimate the likelihood of the attack** As far as system processes are concerned, there is one threat source that can affect a IICS process security: the compromise of one of its components or a component that is connected to it. In this case, the whole process can be compromised. The likelihood of such an attack should be estimated using the qualitative

scale presented in Table III, taking into account the system's technical and organizational context, the attack's difficulty as well as the existing and possible solutions. .

TABLE III
THE LIKELIHOOD SCALE

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

3) **Evaluate the risk level:** The risk level associated to the process is a result of the related gravity and the likelihood of the attack. The risk levels grid in Figure 3 helps to calculate the risk level.

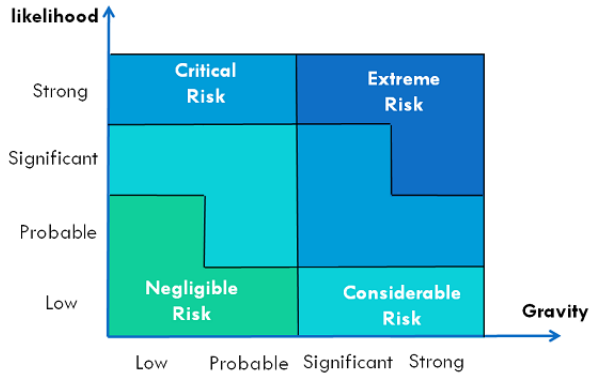


Fig. 3. Risk levels grid

The required protection level of a process is proportional to its risk level. Table VI presents how risk levels match "required protection levels".

TABLE IV
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)

B. Connections meta-characteristics

A *Connection* is mainly significant for segmentation if it connects *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. Thus, they can only be modeled when all the *Components* groups zones are identified.

Inter-zones *Connections* may connect security zones that have different security levels or contain *Components* of different risk levels. 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). This can be done by introducing a new security zone [12] that creates a security stage between the two zones by applying filters to control traffic.

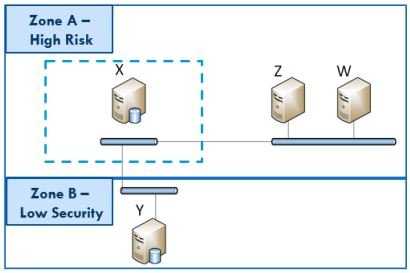


Fig. 4. Inter-zone connection's security zone

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 III-A2. For a given inter-zone connection, all the **Services** exposed by the Components of the zones it connects as well as all the **Data** manipulated by them should be analyzed. This ensure having a clear idea about the components 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.

C. IICS Segmentation Constraints

In some cases, we may be faced with some constraints that make new zone creation a difficult decision, if not unthinkable. Our segmentation method takes this into account by requiring a constraints analysis at each cycle. The constraints analysis helps to decide whether or not to keep the identified zones. We focus on two generic types of constraints that could dissuade from creating a potential security zone.

1) Functional Constraints: Introducing new security zones must not negatively affect the system's functionality and operation. Functional requirements that can be influenced by the security zoning are numerous. They should be identified and studied on a case by case basis. It is a task that the method's user will have to take on. As an example, the IICS timing requirements must not be impacted by the communication flows filtering across the security zones boundaries.

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

- **Constraint Level A**: Some mandatory requirements can not be respected if the new boundary is created. A mandatory requirement is a requirement that can not be dropped out.

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

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

2) Technical Constraints: Creating new security zones and filtering communication through their boundaries is technically not always simple. It sometimes requires a lot of technical skills, security expertise and knowledge of IT and OT operation specificity. Even having all the needed competence may not be enough. It is especially the case when the adopted technologies (protocols, *Components*, 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 solutions 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. Creating a new security boundary technical cost is constraining when it can be assigned 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.

D. Necessity and Constraint comparison

The potential security zones that are progressively identified are kept or not depending on the constraints analysis performed on IICS elements that are involved in the new potential zones. Preserving an identified zone is a decision to make by comparing the **Necessity** of this new zone to the **Constraint's Level** associated to 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 consists of two rating scales that contain a set of grades to evaluate zoning **Necessity** and **Constraints Level**.

1) Segmentation Necessity Grading System: The **Necessity Level** of keeping zones identified using a meta-characteristics is not the same for all the meta-characteristics. For example, functional based zones are not as necessary as geo-location related ones. Table VI lists all the grades of our necessity levels grading system. All our zoning meta-characteristics have been given preset grades as illustrated by table VI.

TABLE V
SEGMENTATION NECESSITY LEVELS

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

TABLE VI
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)

2) Segmentation Constraints Grading System: The level of a given constraint is its impact on the conceivability of a new potential zone creation. Each known constraint must be assigned a grade from Table VII. The method's user has to evaluate the system's constraint's impact based on his knowledge of the technical and functional context of the system. Constraints levels for functional and technical constraints were presented in sections III-C1 and III-C2.

TABLE VII
CONSTRAINTS LEVEL SCALE

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

3) Grades Comparison: The ultimate goal 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:

- L_{seg}: The **Necessity Level** of creating the **Zone A**.
- L_{cs}: 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.

E. The Segmentation Cycles

Potential security zones identification is done in three times. First we group the system's *Components* based on their meta-

characteristics to identify potential security zones. This is done through multiple cycles where only one *Components* meta-characteristic is used per cycle. Next, zones identification should be based on processes. Each process represents a new potential zone. New potential zones identified at each cycle, are kept according to the constraints analysis. Constraints analysis should be conducted on the *Elements* involved in the new identified zones. Functional requirements (e.g., timing requirements) must not be impacted by the new zones creation and Technical cost must be acceptable in comparison to the necessity level of the new zones. The grading system, we defined below, should then be used. Once the *Components* related zones are designated, only then can we model inter-zones *Connections* and identify related security zones.

1) First, the IICS should be modeled.
2) It is necessary to protect the system from external malevolence by creating the system's external boundaries. The **Necessity Level** of this step is **A**.
3) At the second cycle, the system's *Components* should be grouped according to their functional characteristics. Each functional group is a new potential zone. A constraints study should then be done to determine zones that should be kept. The **Necessity Level** of this step is the **C Level**.
4) For technical zoning, the system's *Components* should be grouped according to their technical nature. Each technical group represents a new potential zone.
5) Next, identify new zones based on the Geographical aspect. Every site represents a security zone.
6) Next, new security zones identification should be based on processes. Each process of the system represents a new potential zone. The necessity level of each process potential zone corresponds to its "required protection level".
7) Next, as all the security zones are now created, the inter-zone *Connections* risk should be analyzed in order to spot potential security zones. The necessity level of these potential zones depends on the *Connection*'s risk level as explained in section III-B. They should be preserved or rejected depending on the constraints analysis results.

IV. Conclusion

Despite the numerous benefits of integrating a Corporate System with an ICS, serious security problems arise especially on the ICS side because it is usually designed with very low, if not nonexistent, security. Defense-in-depth is recommended to apply multiple layers of security by creating new security segments. The segmentation of IICS is not trivial as they have heterogeneous configurations and much specificity. The solutions suggested by the research works curried out on the subject are not generic enough and do not take some important IICS aspects into account. This paper suggests an IICS segmentation method that ensures efficient zoning to meet the actual security needs of IICS. To segment an IICS, it is first necessary to study its *Elements* and their characteristics to be able to identify security zones. This should be done using our meta-model to create a model of the system. The identified potential zones should be kept or not depending on the constraints analysis results. The "Grading System" helps to make this decision.

Our segmentation method 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 really significant for segmentation. It is a fairly pragmatic method that takes into account IICS constraints and specificity. However we admit that the method's application is not simple enough. We are convinced that a tool that simplifies the system modeling and automates the zones identification would be necessary. 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 is mandatory and consistent because both are subsystems of an integrated ICS.

References

[1] 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*. IEEE, 2006, 2006.

[2] I. L. Nampuraja Enose Advanced Engineering Group Engineering Services, "Implementing an integrated security management framework to ensure a secure smart grid," *IEEE*, 2014.

[3] V. P. M. A. Keith Stouffer, Suzanne Lightman and A. Hahn, "Guide to industrial control systems (ics) security," *NIST special publication, vol. 800, no.82, 2015*, vol. 800, no. 82, pp. 16–16, 2015.

[4] "Detailed measures," ANSSI, 2013.

[5] D. CSSP, "Recommended proctice: Improving industrial control systems cybersecurity with defense-in-depth strategies," *US-CERT Defense In Depth, October 2009*, 2009.

[6] "Security for industrial automation and control systems: Terminology, concepts, and models." ISA-99 Standard 62443-1-1 (Draft2, Edit4), 2013.

[7] "Enterprise - control system integration part 3: Activity models of manufacturing operations management," ISA-95 Standard 95.00.03 (Draft 16), 2004.

[8] "Network segmentation for industrial control environments," *Wurldtech, A GE, March 2016*, March 2016.

[9] 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.

[10] "Enterprise - control system integration part 1: Models and terminology." ISA-dS95 Standard (Draft 14), 1999.

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

[12] L. Obregon, "Secure architecture for industrial control systems," *SANS Institute, InfoSec Reading Room, 2015*, 2015.

[13] I. R.-J. Jens-Tobias ZERBST, Erik HJELMVIK, "Zoning principles in electricity distribution and energy production environments," *20th International Conference on Electricity Distribution, 2009*, 2009.