Master Thesis

Master's Programme in Network Forensics, 60 credits

Industrial Control System (ICS) Network Asset Identification and Risk Management

Digital Forensics, 15 credits

Halmstad 2018-08-05
Mohammed Abdulrazzaq, Yuan Wei
Abstract

Setting against the significant background of Industrial 4.0, the Industrial Control System (ICS) accelerates and enriches the upgrade the existing production infrastructure. To make the infrastructures “smart”, huge parts of manual operations have been automated in this upgrade and more importantly, the isolated controlled processes have been connected through ICS. This has also raised the issues in asset management and security concerns. Being the starting point of securing the ICS, the asset identification is, nevertheless, first dealt by exploring the definition of assets in the ICS domain due to insufficient documentation and followed by the introduction of ICS constituents and their statuses in the whole network. When the definition is clear, a well-received categorization of assets in the ICS domain is introduced, while mapping out their important attributes and their significance relating the core of service they perform. To effectively tackle the ever-increasing amount of assets, identification approaches are compared and a case study was performed to test the effectiveness of two open source software. Apart from the identification part, this thesis describes a framework for efficient asset management from CRR. The four cyclic modules proposed give an overview on how the asset management should be managed according the dynamics of the assets in the production environment.
Acknowledgements

We would like to express our gratitude to our supervisor, Professor Alexey Vinel, for insightful comments, remarks, and engagements through the preparation process of this master thesis together with Pavel Isachenkov. We also appreciate it a lot for the instructions and help from Assoc. Professor Stefan Axelsson who is the mentor and examiner of this thesis.

Moreover, we would like to thank Jens Jakobsen and Mattias Svensson from HMS Industrial Networks for introducing us to the subject as well for the support of providing the necessary equipment. Furthermore, we would like to extend our thanks to Shooresh Sufiye, who has willingly shared his precious time during the process of surveying.

We would also express our sincere thanks to the teachers and instructors from this programme for their generous knowledge sharing and support on the subjects and our studies at Halmstad University.

Finally, we own our thanks to our loved ones, who have supported us throughout the entire process, both by keeping our harmony and helping us in putting pieces together.
## Contents

1 Introduction ........................................ 1
   1.1 Background ....................................... 1
   1.2 Contribution ...................................... 2

2 Methodology ....................................... 5
   2.1 Research Goals and Objectives ..................... 5
   2.2 Research Questions ................................. 5
   2.3 Research Approach ................................ 6

3 Literature Review: Challenges ....................... 9

4 Industrial Control System (ICS) ..................... 13
   4.1 Definition of ICS .................................. 13
   4.2 Components of ICS ................................ 14
   4.3 Network Components ............................... 17
   4.4 ICS Types ......................................... 18
   4.5 ICS Security Issues ............................... 19
      4.5.1 ICS Characteristics ......................... 20
      4.5.2 ICS Potential Vulnerabilities ............... 20

5 Asset Detection .................................. 23
   5.1 Importance of the Asset ........................... 23
   5.2 Vulnerability and Asset ........................... 24
   5.3 Definition of Asset in the ICS Domain .......... 25
   5.4 Asset Inventory in the ICS Domain .............. 26
      5.4.1 People Assets ................................. 26
      5.4.2 Information Assets ........................... 27
      5.4.3 Technology Assets ............................ 27
      5.4.4 Facility Assets ............................... 27
   5.5 Asset Attribute in the Scope of its Service .. 28

6 Case Study ....................................... 31
   6.1 The Physical Setup ................................ 31
   6.2 Introduction of the Software ...................... 33
   6.3 Asset Identification Results ...................... 34
   6.4 Case Study Summary ................................ 37

7 Asset Management .................................. 39
   7.1 Modules of Asset Management ..................... 39
   7.2 Prerequisites for Asset Management ............. 40
      7.2.1 Asset Inventory ............................... 41
      7.2.2 Management of Assets ....................... 41

8 Conclusion and Limitation ......................... 43
List of Tables

5.1 People Asset ......................................................... 27
5.2 Facility Asset ......................................................... 28
List of Figures

4.1 Field Device Examples .................................................. 15
4.2 RTU Example ................................................................. 16
4.3 PLC Example ................................................................. 16
4.4 DCS Example ................................................................. 19
4.5 SCADA Layout ............................................................... 19
4.6 Exploiting Buffer Overflow Vulnerability ......................... 21
6.1 Configure The RTU Devices ............................................ 32
6.2 Grassmarlin Software ..................................................... 35
6.3 Nmap -sP ................................................................. 35
6.4 Nmap -o ................................................................. 36
6.5 Nmap -sU ................................................................. 36
6.6 ISF run Verbose .......................................................... 37
6.7 Use Exploits ............................................................... 37
7.1 CRR Asset Management Flow ....................................... 40
List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSF</td>
<td>Cyber Security Framework</td>
</tr>
<tr>
<td>CVE</td>
<td>Common Vulnerabilities Exposures</td>
</tr>
<tr>
<td>DCS</td>
<td>Distribution Control System</td>
</tr>
<tr>
<td>DHS</td>
<td>Department Homeland Security</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Device</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet Of Things</td>
</tr>
<tr>
<td>IIoT</td>
<td>Industrial Internet Of Thing</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>CPS</td>
<td>Cyber Physical System</td>
</tr>
<tr>
<td>MTU</td>
<td>Master Terminal Unit</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute Standards Technology</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>OT</td>
<td>Operation Technology</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control And Data Acquisition</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

1.1 Background

With the advancement of technologies and the worldwide Industrial 4.0, there has been a growing trend of exploring the capabilities and benefits. This concept originated from Germany due to its strong industrial history and innovation in this field in 2011. In the year 2012, the concept of Industrial Internet was brought up by General Electric company, and it depicted a blueprint of a connected manufacturing facility. Then following the trend, the concept ‘Industrie du futur’ was raised in France and was described as the future French industrial policy. The latest state industrial road map was Created by China. The China Ministry of Industry and Information Technology launched the “Made in China 2025” campaign in 2015. It aims to upgrade its manufacturing capabilities and overtake other international competitors.

One of the keys in Industrial 4.0 is to combine the IT technology with Operational Technology (OT), opening a new arena of productivity. This combination is partially a result of Cyber-physical System (CPS), one of the fundamental building blocks in Industrial 4.0 (Industry 4.0: the fourth industrial revolution - guide to Industrie 4.0, 2018), and an accelerator of CPS as well. The CPS is a complex category, and it includes the Industrial Control System (ICS) which is the major focus of this thesis. Another important block in this transformation is the Industrial Internet of Thing (IIoT). Together, these two applications in the industry, especially in manufacturing, constitute the basic elements of being “smart” in the definition of Industrial 4.0. This trend gains speed since it was suggested in 2011 at the Hannover Fair (Industry 4.0, 2018) Without doubts, this trend is changing the whole industrial landscape, either horizontally or vertically.

While the whole professional world is embracing the prosperity of Industrial 4.0, the cybersecurity starts to plague this great inquiry. The security aspect was not brought into the public’s attention until the incidence of Stuxnet. This malicious worm targets the Supervisory Control and Data Acquisition (SCADA), which is the key segment of ICS. The Stuxnet attacked Iran’s nuclear facilities and crippled the SCADAs and Programmable Logic Controllers (PLC). As matter of fact, the cybersecurity issue has been considered as one of the fundamental elements in the Industrial 4.0. (Rüßmann et al., 2015) It acknowledges that the once closed or semi-closed production systems are connected using standard communication protocols and protecting these critical facilities from cybersecurity threats increases dramatically. The technology makes it possible to access the production from the enterprise level or other segments of the ICS, and it could be also accessed remotely according to mobile requirements. This accessibility not only increases the flexibility of working but also leaves the room for adversaries. With the easiness of all kinds of the hacking framework being developed, there have been growing incidents targeting the ICS. Therefore, attentive concerns about the cybersecurity of ICS have raised from both the
Chapter 1. Introduction

academic and professional sides. For example, the National Institute of Standards and Technology which affiliates to the U.S. Department of Commerce has released the Guide to Industrial Control Systems (ICS) Security. Another example is that the Siemens PLC S-300 has a vulnerability which has been exploited and the Siemens Step7 has also been exploited by Stuxnet.

The cybersecurity measures already adopted or during this transition period are not capable enough to protect those critical infrastructures. The usually adopted “security through obscurity” sometimes work well for those physical facilities which are separated from external connections. However, the implementation of mature IT technologies in these environments and the integrations among different segments of the network often expose those critical ICS to the outside. The exposed vulnerabilities are soon targeted and exploited by intruders. Due to the impossibility of a perfect secure environment, the mission seems to find a viable approach to maintain the stability within a given environment so that the production can be carried on.

The first line of building a secure system in Industrial 4.0 is to systematically find all the vulnerabilities of the assets so that the risks could be investigated and foreseen. This will first give an overview of the structure of ICS which lays an overall structure for the scope and background within which thesis works on. In chapter four, the characteristics of ICS and the segmentation of it are explored so that the security aspects could be built on. Chapter five starts with the focus of the thesis, the investigation of asset detection in ICS and its significance in ICS security. Then a case study is presented to illustrate two possible ways to conduct asset detection. Some comparisons are made to direct attention on when to adopt appropriate approach.

The final chapter explores the risk management against the vulnerabilities from assets identified in the previous chapter. This thesis is jointly carried out with support and supervision from HMS, which is an industrial networking device company, and Halmstad University. Some of the data are sensitive and will be not released according to the agreement made between the authors and HMS.

1.2 Contribution

This paper tries to put the asset identification in the framework of security and well-defined assets in the security scope. Assets are vital to an organization for the fact that steady service and productions should be provided without interruptions. However, the increasing incidences of cyber-attacks aiming at industrial network put the security issues in the industrial network security lens. While the industrial circle and the academia have been aware of this issue and more organizations are willing to invest in this area, the progress and implementation are slow. The difficulties lie in not only the financial factors but also the complexity when implementing security measures. To make a systematic scheme for securing the industrial network is time-consuming and requires the efforts all over one organization. It is also true that all the measures put forward are all stemming from the assets. Therefore, this paper investigates the role of assets in the industrial network from a security perspective.

Tightly related to the work is how to plan an efficient asset identification and inventory. Clearly, a working definition of assets has to be defined so that they can be identified and managed in the following steps. This definition needs at least organization-wide recognition so that they can be materialized or stored in an information database to be managed. Apart from that, different assets could be identified using different techniques due to their natures. Some of them can be acquired from
1.2. Contribution

other units within the organization, while others could be detected with automated software. This paper compares open source software to detect technology assets to see how they perform either in the active way or passive way.
Chapter 2

Methodology

2.1 Research Goals and Objectives

The critical task of this thesis is to investigate the definition of asset identification and use the existing methods to accomplish acquiring assets in an ICS environment using chosen techniques. The task of investigating the definition of assets is the core of the first task. Although there are some existing definitions of assets from various domains, there are more or less inadequate in address nature or attributes in the scope in the ICS domain and security aspect. More work is needed to align these existing definitions into our framework and discover new attributes of assets in our perspective. Another task requires some empirical procedures to yield a solid conclusion about the methods of building an asset inventory. Some of the frameworks have already subsumed this part as one of its modules, and some techniques aim at doing this task in an automated way. To achieve a feasible result, a case study is designed to see how these approaches work in our framework.

2.2 Research Questions

To Align with the necessities and challenges outlined in the introduction part, the asset identification in the ICS context means significant. The rationales have been established in the background introduction. Then what questions or aspects of the questions consider the efforts of investigation and explorations?

The first question is what is the status of asset identification in the ICS? The significance of assets is clearly understood by many stakeholders. Many of the studies and standards are from the traditional industries which might linger in the previous industrial stage. The new changes in the combination of IT and OT require a close look at the asset identification and management. Since many industrial networks are in critical infrastructures, this investigation of the status of asset identification and management demands a close examination. One of the tasks of this work is to have a survey of this aspect in the context of ICS.

The second question is what the definition of an asset is in the scope of ICS. The concept of an asset is obviously loaned from economics. The definition of it is not so valid because the definition of these assets in the ICS should be defined with the consideration of security rather than just the economic sense. However, it is still valid in that many of the assets in ICS are closely related to the function of the whole organization and the service or production they involve. Another aspect to consider is that the definition may vary according to different stakeholders. A common agreement needs to be reached so that the definition could be attained. What needs to be
investigated for those aspects are required to explore the question.

The third question is how to relate the assets to security schema according to its attributes. For the financial units, what interests to them is the economic value of the asset. Issues such as the budget for purchasing and maintaining these assets are the priority of their task. The assets could have many attributes which make them unique in the production line or service they perform. Therefore, what attributes should we identify and how to align them in the security scheme is another task of this research.

The fourth question is what tools could be employed to perform the time-daunting task of asset identification. It might not be a big problem for a small organization, but when the scale of the organization grows the task becomes difficult to handle. Some of the asset types are difficult to be performed with an automated software due to the nature of the assets. It is now possible to be identified with software, for instance, the technical assets. Once all of these assets are stored in a sort of database, it is easy to be managed with the help of software. These automated identifications could be carried out in a passive way in order not to interrupt the live production process due to the nature of the ICS. However, some assets cannot be detected unless an active approach should be adopted. Then the sub-questions should also be considered in comparing different open source asset identification software.

The fifth question is how to manage the identified assets. Since the assets could have different priorities based on their attributes and roles in the security scheme, then the management of the assets should be performed accordingly. Before this, it is important to have a strategy to figure out what should be done to manage these assets. A good asset management plan benefits the normal function of the business and provides uninterrupted service even though the organization faces security risks or threats.

2.3 Research Approach

To yield a complete and fit definition of asset identification requires through a survey of the literature in this aspect. This approach will help the authors see not only the significance of the work but also the status of an asset in the scope of ICS and security. The literature from two domains are going to be surveyed: Industrial Control Network (ICS) and defense in depth security approach. The angle of this research is to combine the security into ICS when the unwell parties have already targeted the ICS. The ICS has its fundamental and critical status in our society, and the critical and infrastructural services must not be interrupted. Therefore, the literature review will be carried out to explore the significance of ICS and its important nodes which need security attention. While the critical assets in the ICS have been spotted, the defense in depth approach should be applied to secure them. Then it’s worthwhile discussing this approach to help achieve one of the goals of this thesis.

An empirical approach is also employed to validate what has been discovered in asset identification. The previous approach will yield a comprehensive assets definition in security concern, but not the tangible result. The second approach will demonstrate a mini case study to utilize the definition comparing various open source software to yield an asset inventory. This inventory is a tangible result which
2.3. *Research Approach*

can validate the previous discussion. One of the advantages of using a case study is that it shows how the theory and practice relate. Through comparison, different profiles of assets could be tangibly mapped, and an effective tool could be promoted.
Chapter 3

Literature Review: Challenges

This section attempts to give a short review of asset identification and asset management in the hope of giving a solid ground for conducting this research. The idea of performing this research is initialized with the help of HMS which hopes to automate the process of detecting elements in the ICS domain using an efficient approach. With this goal in mind, the query for discovering the technical assets in an ICS domain is just one part of this thesis. The concept of performing asset identification has more to explore, especially when fewer literature resources have been available. This deficiency of documentation of this subject strongly triggers the motivation to consider it in a detailed and thoughtful way in the hope of contributing to the repertoire of asset identification.

The literature of giving informed resources are limited. Neither from the quantity scale of researching this topic nor the quality of the research is producing a satisfactory result in this subject area. It is the fact that when performing a simple search using a combination of asset identification and ICS, highly relevant results are rather limited. Apart from some commercial software advertisements, useful and qualified academic research articles are hard to obtain. To make the search more challenging is to find qualified articles or research papers addressing the subject matter. According to (Shostack, 2014), they provide a working definition of assets within the ICS security domain. The identified assets are mainly hardware assets within the SCADA system and its related network elements, though the whole article provides a good view of securing ICS assets on that level. The most comprehensive work which dedicated to the discussion of asset identification and management is from CRR. It establishes both a theoretical and practical view of how assets should be defined and what should be done for asset management. Unfortunately, most of the asset identification often falls into a tiny portion in most research articles which merely announce the criticality of this issue. Another disturbing aspect is that there is no coherent definition of asset identification and what attributes of assets should be counted when making an inventory of assets. In most of the cases, the so-called “logical” approach of tackling assets is selected and relies on the individual expertise of the assessor.

The asset identification is most likely to be subsumed under more general subjects, for instance, information security risk management, while there are very few resources dedicated to the study of asset identification and management. One of the strong motivations of performing asset identification is to lay a foundation to outline the potential vulnerabilities and potential risks. Undoubtedly, the importance of asset identification, especially the management of critical infrastructures, is generally recognized from different perspectives. The critical infrastructure prevails in vital industries that are now equipped with ICS. The American Department of Homeland Security has commissioned a guideline for the task of performing nation-wide asset identification in critical infrastructures. The National Infrastructure Protection
Plan is the federal guide for risk management of critical infrastructures (Izuakor and White, 2016). The importance has been acknowledged not only for the American, but the European Programme for Critical Infrastructure Protection has also been introduced. There are some competitions for asset identification, for example, S4X18 is an event which holds every year to challenge the new approaches of discovering assets in ICS. Its leading sponsors including CISCO and many others, which shows the status of its influence in the field. It is unfortunate that the results and approaches are not published for access.

The deficiency in asset coverage is an challenge in the current status of asset identification studies. There are three approaches when it comes to assessing the asset identification framework. They are function-based, network-based, and logic-based. According to (Izuakor and White, 2016), the function-based approach refers to identify assets according its criticality to the mission of the organization and evaluate against defined criteria. The network-based approach identifies all the nodes and relationships in one system and evaluates it against their statuses in the system. The logical-based approach, which seems to have some sort of subjective sense, is the selection of assets according to the assessors’ value. The framework with the function-based approach highlights the relationship between the assents and their performing services and grasps the key to this task of asset identification while neglecting other minor or supporting parts and yields incomplete results. The network approach seems to be very complete, but it often does not include external assets which also should be included. Finally, the logical approach is the most incomplete one since the task of asset identification rests on the assessor’s expertise. Nonetheless, when we look at the functions of most commercialized software of asset identification, the bragging benefits of using them often yields one of the most salient identifications of technical assets. Another example is the S4X18 event; the competition requirement is to see which team can be the best to identify the technical assets, like mapping the network topology, hardware type, maker, version number, IP, protocol, etc. The deficiency in performing the task of asset identifications and management using handy tools makes the course time-consuming and difficult to achieve. This deficiency is partly caused by the diverse nature of assets. According to the categorization of CRR, the people asset, information asset, technology asset, and the facility asset are the four integral elements in a well-structured management system. From a technical perspective, the readiest part which is possible to be identified using automated technique is the technology asset. (Wedgbury and Jones, 2015) They conducted a survey on the automated asset discovery in the ICS. Although some tool sets can be utilized to perform the task of asset identification in ICS domain, they point out that the limited functionality of the different tool sets, the fragility of legacy equipment in the existing ICS perimeter, and the flaws of identification approaches need future development to meet the demands of such task. Lastly, there is also a disagreement over the identification approaches for detecting technical assets. The automated method is usually fit for identifying the technical asset, one of the four types which shall be discussed more later. However, there are two competing approaches: passive and active. According to (Adams; M.), the active scanning “requires probing the network for a response from nodes.” By using verities of protocols, for example, TCP, ARP, ICMP, etc., probe traffic is injected into the ICS and elicits the response from various ICS elements. This method offers the possibility of identifying the nodes which connect in the network yet are not equipped with the mechanism of providing information passively. The active scanning or solicitation help collecting nodes information. However, the active has more
disadvantages. The active scanning will intrude the network and introduce disturbing traffic which has huge impacts on the determinism nature of ICS. This negative impact will not only disturb the normal production traffic but also can cause physical harms to the system. Then the other approach is the passive approach. This approach doesn’t actively pool the devices or collect asset information by listening passively the traffic traversing the ICS domain. Compared with the active scanning, the passive scanning will not disturb the normal operation of the ICS nodes and strain the determinism feature of the ICS network. Adams et al. lists a few tool kits which can be used to deploy this approach, like tenable network security passive vulnerability scanner, pass asset detection system, netdiscover, etc. Apart from either active or passive scanning approach, the hybrid of the two which tries to eliminate the disadvantages is also possible in the asset identification task. In their research,(Bantseev and Labbé, 2003) they conducted structured testing of different techniques. They selected two tools implementing passive techniques and six hybrid techniques. The study finally concluded that “a tool does for all” implementation does not exit.
Chapter 4

Industrial Control System (ICS)

4.1 Definition of ICS

The automation of industry has never ceased to evolve, and the various factors make it possible for today’s modern automation. The history of control system dates to 1800s and is considered as part of the factory process. The control system is a combination of engineering and mathematics producing the single-input and single-output in the classical control theory and the multi-input and multi-output system (GICSP, Assante, and Conway, 2014). The consequences and benefits of this evolution are that it reduces human labor, materials resources, improves the accuracy of the process, and precision, and makes the whole manufacturing process more controllable at ease. One other hand, the mentioned aims continuing to push the development of ICS through the recent years via the joint of IT technology to accelerate this process. The maturity of the IT technology, its availability, and the cost-effectiveness have helped the industry integrate it to the OT side.

But, what is Industrial Control System? If we look at this term concordantly, rather than historically, this is the scope of this thesis. It does not conduct a historical survey of this term, but rather the ICS emerged from the 1950s and integrated with IT technologies. The followings are three typical definitions quoted from authorities:

ICS “refers to a variety of systems comprised of computers, electrical and mechanical devices, and manual processes overseen by humans; they perform automated or partially automated control of equipment in manufacturing and chemical plants, electric utilities, distribution, and transportation systems and many other industries” (Cyber-security of SCADA and Other Industrial Control Systems; 2016).

The industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures (Stouffer, Falco, and Scarfone, 2011).

ICS is a term used to encompass the many applications and uses of industrial and facility control and automation systems. ISA-99/IEC 62443 is using Industrial Automation and Control Systems (ISA62443.01.01) with one proposed definition being “a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.” (GICSP, Assante, and Conway, 2014)

For the above quotes, a few similarities can be found. First, all of them define ICS as a system and integrate itself into the industrial process. Indeed, the ICS is a typical setup of a control system which fulfills the functions of measure, compare, compute, and correct. While having these features, the realizations of them often depend on some specific devices. For instance, the sensors help measure different values of the set objects, like temperature, level, etc. After the values of the target are collected,
they are used to compare with the predefined ones. Accord to the design, the controllers and the actuators perform the actual actions to modify the physical states. They are realized in some common types of automation, for instance, the feedback control and sequence control.

The second similarity is that they include the constituents of the ICS, though the constituents vary, and they differ in the inclusion of elements in ICS. Since the ICS is a system which impacts the certain process, there are lots of key elements which function together to yield the designed processor products. The definition from NIST is more specific and outlines the key components of ICS, including SCADA, DCS, and PLC. These elements are most common and key elements in this process. They are also very prevailing in most ICS. The first definition from Colbert and it adopts an abstract description of components, ranging from IT to OT sectors. It also mentions the functions of the ICS in various industrial processes. The third one which is quoted form SANS and it seems adopts an abstract summary of the ICS elements. It distinguishes the hardware, software and human elements involved in this control process. One of the differences is that adds an extra element which is not included in the other two definitions, the human element.

However, despite some minor differences, the definitions listed above do outline the key concepts of ICS in the profile of the industry perimeter. The crucial components are named with their designated functions. They also outline some structures which are helpful for categorizing the segments of ICS. These segments are crucial and fundamental when considering and applying security measures against risks or threats targeting the ICS. The next chapter is going to list a detailed overview of ICS types and structures.

### 4.2 Components of ICS

An ICS consists of many types of components which function together to accomplish the controls over the process. It is the fact that individual components in ICS domain are connected via a network, then it’s a good practice of categorizing the ICS components into two categorizations, namely, the control component and the network component. The control components are standalone parts which function discretely in a pre-defined point of the process in an ICS domain. The network domain connects them to accomplish the process and to some extent, it is the conduit where data and control commands are issued via this medium. A communication approach is adopted in the illustrating and listing the components in this system, and some key components are introduced in this chapter. The logical fashion of the introduction is arranged in the definition of component, how it works in the system, and what status of it in the general picture.

- **ICS Field Devices**
  Field devices are sensors, transducers, actuators, and machinery which are connected with their upper controllers using either digital or analog I/O model and perform the instructions from the controllers. The communication between the field devices and controllers are often industrial protocols and instructions are then communicated. The field devices are often the lowest level of an ICS and directly connected with the physical world and perform the designated tasks. One example is the sensor. As the definition outlined, the sensor is used to collect different information about the physical conditions of the certain process. The elements collected could be temperature, pressure, vibration, sound, humidity, current, and other many physical caricaturists. Once these
data are collected, they are sent back to a controller, most likely a PLC, and they are compared to the set points. After the comparison, a specific instruction is given to determine a certain action in the process. The figure 4.1 (Modbus, 2018) shows some common field devices:

- **Remote Terminal Unit**
  A Remote Terminal Unit (RTU) is “a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) the system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.” (Remote terminal unit, 2018)
  An RTU with computational capabilities monitors the intended data, for instance, parameters, and transmits those data to upper controllers. The RTU first acts like a polling device to collect and store the data from field devices. Then upon the request of the higher control center, it will release the stored data. An RTU usually sits directly above the field devices from which they poll data. Figure 4.2 (RTU - Remote Terminal Unit, 2018) depicts a TRU in the control chain of an ICS.
  The RTU could be further divided into two types, station RTU and field RTU. The working logic between these two is very similar. Both collect the data from various sensors and execute programmed login with these inputs. The significant difference is that the field RTU may be considered as a sub-node of station RTU and feed data to it.

- **Programmable Logic Controller**
  A Programmable Logic Controller (PLC) is a small industrial computer which reads the inputs from lower devices, executes predefined actions using the inputs or orders from higher level controllers, and sends out the signal to lower devices of performing certain actions. The PLC has a key role in the ICS system and is the boundary between the connected area and the physical process. It is an essential part of varying ICS system and is running a real-time system which is quite different from other ordinary operating systems. This is due to the deterministic nature of PLC. The time of a PLC processing inputs, outputs,
and executing logic is counted by millisecond, while other systems’ time constraint is measured using the second. Figure 4.3 (Siemens S7, 2018) is a typical PLC manufactured by Siemens.

- **Intelligent Electronic Device**
The Intelligent Electronic Device (IED) is another type of controller in the hierarchy of ICS. An IED is “any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multi-function meters, digital relays, controllers)” (McDonald, 2003). In an ICS environment, the IED can be polled by either a controller from the control center or by an RTU which locates at the field level. It provides functions like protection, control, monitoring, metering, and communications.

- **Historian**
The historian is also called Data Historian or Operational Historian. It is a software application and deployed in a server. It collects real-time data from the
automation process, stores and sorts them according to certain pre-set rules for future analysis. The deployment of this software could be in a common commercially available server situated in the ICS domain. However, the deterministic nature of ICS requires that this application and deployment must be fast and efficient enough to handle the huge amount of process data.

- **Human Machine Interface**
  The Human Machine Interface (HMI) is an interaction interface from which the current status of an automation process could be viewed, and an operator could manually interfere the process by giving orders from it. The most common type of an HMI is a touchable panel where the parameters and status of the process are displayed, and the operators could override the process by certain actions.

- **Communication Gateways**
  The communication Gateway is a bridging device to translate different protocols between ICS devices. Due to the fact that many ICS products are developed by different vendors and protocols. Sometimes, there might be more than one protocols running in an ICS domain. This creates the needs of converting protocols so that the data or commands could be collected and performed.

- **Engineering Workstation**
  The engineering workstation is a typical workstation which has been installed with related software so that the configurations could be done to a PLC, RTU, etc.

### 4.3 Network Components

The network component is an essential element in the automation process. The network connects different levels of devices so that data can traverse, and configurations could be implemented. With the accessibility of modern IT technologies, it is much easier to combine it into the industrial perimeter. An enterprise has different integration strategies and in turn the influence of how the network is designed. No matter how complicated the network might be, the following maps out some major network components of an ICS. The following hardware provides the infrastructures to connect control components in an ICS domain:

- **Router and switch**
  The router connects the data transferring between different networks. It could be the case that routers are implemented between two different ICS levels, for instance, the enterprise and control level. On the other hand, the switch connects devices within the same network. For instance, the data historian and HMI are connected by a switch within the control network.

- **Firewall**
  The firewall is a protective device on a network using pre-configured policies to filter out harmful traffic, and it also provides data to display accumulated report for analysis.

- **Modems**
  The modem is a connecting device via a public telephone line. It can be implemented between the SCADA and a remote site.
Remote Access Points
The remote access point is a device enables the operator connects facilities remotely.

Apart from the above hardware and infrastructures, there are two important network needs to be distinguished:

- Control Network
  It is the network which connects the supervisory control level to lower-level modules.

- Fieldbus Network
  The Fieldbus network connects the sensors, curators, etc. to a PLC or other controller. This network eliminates the disadvantages of point-to-point wiring among the controller and its controlled devices.

4.4 ICS Types

An ICS could be categorized into different types according to the function and geographical location of key components. Some of the common types are Process Control System, Safety Instrumented System, Distributed Control System, Building Automation System, Supervisory Control, and Data Acquisition, Energy Management System. As the scope of this thesis is the manufacturing domain, what matters in this scope would be the Process Control System, Distributed Control System and Supervisory Control, and Data Acquisition. What follows is the general introduction of these three systems.

The Process Control System in industrial sectors implemented is often either the continuous manufacturing process or the batch manufacturing process. The former features the non-stop and continuously running nature. Typical examples are fuel refinery and streamflow in a power plant. The products could be distinguished at certain grades in the process. On the other hand, the latter has a distinct stage. We can find a typical example is the assembling line in the car factory.

The Distribution Control System (DCS) controls multiple automation processes which may be part of the site or the whole site. A DCS uses a centralized supervisory control loop to mediate a group of localized controllers that share the overall tasks of carrying out an entire production process. (Stouffer, Falco, and Scarfone, 2011) The example shown in figure 4.4 depicts an example of such a system. There are four control loops in the field level, namely the machine controller, PLC, process controller, and the single loop controller. The PLC has interconnected all other filed devices through Fieldbus, which avoids route traffic back the PLC all the time and brings extra benefits.

The Supervisory Control and Data Acquisition (SCADA) system is a subsystem within the ICS and consists of Master Terminal Unit (MTU), RTU, or PLC. The MTU communicates and stores the data from an RTU or PLC, and the software takes actions as what to do against the collated real-time data. The SCADA is often combined with a DCS and controls geographically scattered sites. It offers centralized control and monitoring system by integrating data collection and transferring, and HMI software. Figure 4.5 depicts a general SCADA layout.
4.5 ICS Security Issues

The evolution of ICS has witnessed the fusion of IT technologies with OT. This brings a new age for industry and the march toward the Industrial 4.0 is under its way. The security aspects of the new field of ICS is not only drawing attention from the positive side, but also others are trying to compromise the system for various purposes. As one of the fundamental elements in the Industrial 4.0, the security measures must be implemented so that the industry can be freed from malicious intentions. This implementation could not be accomplished without the investigation of the unique characteristics of the ICS itself and the inherent flaws which can be exploited as vulnerabilities.
4.5.1 ICS Characteristics

In the early days, the ICS adopted a concept of “security of obscurity” because the industrial boundary was well protected by separating it from the network. The readiness and low cost of IT technologies gradually merge with the OT and the control part of ICS is more and more connected via a network. This combination has the old flaws inherited from the IT and new ones of its own. The following summarizes some of the major characteristics of an ICS.

- Deterministic requirement
  The ICS in most of the cases is time sensitive and the system requires deterministic responses. Frequent jitters or long delays are not acceptable in this system.

- Constant availability
  Either a process control system or distributed control system has no tolerance for system failure due to the fact that the services provided by these systems are critical to a community or nation. Even the maintenance of the system has to be carefully scheduled. The system has to be heavily tested before the deployment to ensure the availability.

- High-reliability
  The ICS is designed to be fault tolerant. When designing an ICS, the design is proved to be free from faults. In the testing of the system, the aim is to make sure that faults are exposed and eliminated. After the implementation of the design, hardware and software fault tolerance are configured so that the system can still function even when there are some faults present.

- Safety
  The ICS connects the virtual world with the physical world. The abnormal function of the ICS would cause damage to personal injuries. It can also damage properties, and the damage would cause the system failure which will make services unavailable to customers.

- Resource Constraints
  Most of the devices in the ICS domain are task-specific. They are designed to perform the time-critical tasks in the control domain and often have little extra computational capabilities to handle other functions. The field devices do not have the ability to do cryptographical function to check the identity or integrity of the traffic. The underlying assumption is that they trust each other and there is no need to invest resource in performing such a function.

4.5.2 ICS Potential Vulnerabilities

The vulnerabilities in the ICS domain arise from the various flaws. These flaws result from inherent hardware or software design faults or unforeseen consequences, lack of proper configurations, or inadequate administration of networks. These vulnerabilities can be categorized into two types: tangible or intangible. The tangible vulnerabilities are often found in hardware or software configurations. The vulnerabilities result from the hardware design faults, improper software configurations, or OS vulnerabilities where the software are installed. Some concrete examples are inadequate testing before implementation, insecure remote access on ICS components, use of clear text, buffer overflow, week network security architecture,
etc. According to Common Vulnerabilities and Exposures (CVE), which provides publicly collected known cybersecurity vulnerabilities, there are 76 incidents registered in their database for the attacks against the PLC exploiting buffer overflow vulnerability shown in figure 4.6. When the query is conducted with the keyword SCADA, there are 126 indexes matched. Among these examples, the products from ABB, Schneider Electric, Unitronics VisiLogic, etc. are located. These vulnerabilities are caused by the inherent in the hardware or software vulnerabilities. The inquiries conducted above are based on the data from the latest CEV list, and it is publicly available to download.

The intangible vulnerabilities result from lack of adequate ICS documentation. To address the vulnerabilities is often the best practice to have needed documentation ready. Lack of these documentations will add the difficulties to address the problem and sometimes cause the incompetence of handling the risks or threats. These vulnerabilities can be found at the organizational level or the operational level. Some examples are inadequate security architecture and design, inadequate security audits on the ICS, lack of ICS specific configuration change management, etc.
Chapter 5

Asset Detection

Any security plan in the ICS domain is to protect the assets from malicious or accidental acts to ensure the normal function of the system. It is the assets in the domain where policies or strategies start. Since the modern ICS is a hybrid of IT and OT technologies, it has both features of those two and its own feature. After the assets’ definition is well-defined, it is also needed to find a framework where the asset could fit into a security strategy. There are many styles of security architecture which proves to be effective, but the one adopted in this thesis is the so-called Defense-In-Depth strategy. The nature of this strategy is to create multiple tires of security measures to counter-strike the malicious acts. Even though some tiers are compromised, it buys some time for the security team to cope with the situation. Therefore, this chapter starts with the definition of an asset and its status in the Defense-In-Depth strategy. The method of detecting these assets in the ICS domain are introduced, and a case study of detection is introduced as well.

5.1 Importance of the Asset

The importance of asset management is one of the fundamental controls in any business or organization. This practice has manifolds aims, for instance, financial management or production management. The scope in this thesis is to investigate the perspective of security of the control system in an ICS domain with inadequate or non-consensual definition of an asset.

To make the ICS able to stand malicious attacks is a paramount task for any business or organization having an ICS. It is impossible to make it immune to threats because the threats actors are always there and can hardly be eliminated. Therefore, the mindset of securing the system and making it strong enough to withstand attacks is the feasible and realistic approach. The security strategies also follow this approach.

In risk management, to identify what to protect is the first task to do when trying to secure the system. The task of the identification is to help owners establish a baseline understanding among comprehensive stakeholders within the ICS domain. This helps to set priorities in a security measure on what to monitor, what countermeasures could be applied according to each characteristic, and what backup plan could be deployed when the asset is compromised. On the other hand, the security response team in one business or organization finds it difficult to start the task when there is no asset inventory is available.

Another factor which makes this project meaningful is that there is no clear definition of asset available to implement what follows, though some working definitions
can be found (Shedden et al., 2016). They point out that there are three deficiencies in the traditional outcomes of asset identification. First, the traditional method defines it in a rough way and lacks granularity. Second, the traditional practice neglects the co-existing informal activities involved in this process. Third, it does not recognize the knowledge assets as distinct and important entities. The criticism is intended for information security management, but it is also valid in this context since the ICS is a hybrid of IT. Finally, through the literature review, it was difficult to find a comprehensive and clear explanation of the asset identification, though its status in security strategy has always been rated as important.

The rationales behind the investigation of asset identification are more than what has just contended. The aim is clear that the security of assets in an ICS is needed to be protected and a well-designed strategy is also needed. Consequently, to start this quest, it is always good to know what the asset identification is.

5.2 Vulnerability and Asset

The vulnerability, when it is used in the IT-related domain, refers to the “weaknesses in a system or its design that allow an intruder to execute commands, access unauthorized data, and/or conduct denial-of-service attacks” (Abomhara and Køien, 2015). This definition highlights the vulnerabilities in the IT domain and could not cover all the parts of an ICS domain. On the other hand, the Guide to Industrial Control Systems (ICS) Security (Stouffer, Falco, and Scarfone, 2011) defines the vulnerabilities as the “weaknesses in information systems, system procedures, controls, or implementations the can be exploited by a threat source.” Comparing it with the first one, we can see that the scope covers not only the information systems, but also the controls, procedures, or the implementations. Except this, it also adds the predisposing conditions of the likely vulnerabilities in the context.

The flaws either in the information system or the procedures are inherently existing in the entities, unlike the threats which pose themselves externally. The threat which is the external force is out of the scope of this thesis. The focus is on the assets which trigger the vulnerabilities. There are many types of vulnerabilities in the ICS domain. These potential vulnerabilities exist in different layers of business due to insufficient or unforeseeable designs. According to different dependencies, these vulnerabilities fall into three categories: business policy and procedure vulnerability, platform vulnerability, and network vulnerability. Although the ICS is becoming the trend in the business, lots of businesses which implemented the ICS have little or no investment in the design of a good security program. Lack of good security practices will lay the manufacturing facilities at risk. The affordable IT technologies find the way into the industry, but at the same time vulnerabilities introduced by them have not been properly addressed. The third type is the consequence of the fact that all the devices in the industry are more and more connected to the network. Poor design and management of the network leave the vulnerabilities to be exploited.

It is the high time that the industry should have a clear understanding of the asset inventory and baseline them. This created inventory is not only beneficial from the economic sense, but also the fundamental building block of any security strategy. The vulnerabilities can only be identified when this inventory is finished. Then the
whole security program could be made to counter the threats actors and minimize the risks so that its services and mission could be fulfilled.

5.3 Definition of Asset in the ICS Domain

Since assets are the crucial infrastructures for an organization, the necessity to create an asset inventory is a must. The first rationale behind this is that the security strategy starts from the asset. The strategy aims to protect the asset from malicious acts. If the asset is not clear to an organization, it is very difficult to build a secure or complete strategy to curb threats. Secondly, the ICS domain is much more complicated than traditional IT structure, and it contains more assets. The complexity comes from the deep structure and its nodes. There are usually five layers within an ICS, which is a lot more than the traditional IT structure. The devices in the ICS forms a pyramid with most of the field devices in the field level and few control devices up to the pyramid. Another factor making the ICS complicated is that an ICS is physically related and controls the actual production process. Any failure of its part will directly impact the safety or financial aspects. Finally, the concept of an asset in the ICS domain is not clear, and there is no explicit agreement on the definition of it. This causes lots of negative consequences. For instance, the security strategy architecture will be impacted, and no proper taxonomy has been defined, which will make it difficult for designing an automated detection software. Therefore, it is beneficial to invest some discussions on the definition from different perspectives.

The asset is an economic term which refers to “a resource with economic value that an individual, corporation or country owns or controls with the expectation that it will provide a future benefit”. (Investopedia - Asset, 2018) This definition of asset gives some clues on how the asset in the ICS should be counted. The key point needs to be noted is that the asset is a resource. The extension of the concept is vague and can apply to a vast number of entities. In this thesis, the asset will be directly or indirectly involved in the ICS process. Thus, those key components introduced in the previous chapter are all considered as assets. However, these assets are somewhat tangible entries which are physically real and make them sensible to become assets. Apart from these, the software or data transmitting between a PLC and sensor, for example, in the ICS should also be counted as assets. These assets are, to some extent, intangible, but in fact are critical to the production process.

The second definition of asset is taken from Shostack and he summaries five types of assets, a.k.a, computers as assets, people as assets, processes as assets, intangible assets, and stepping-stone assets (Shostack, 2014). Strictly speaking, it is not a definition but gives some clues on what to include. Another fact is that he is mainly concerned with program development and this categorization is intended for threat modeling. Anyway, it is still valid since many of these are common in IT and can find their roles in the ICS domain. In his summary, the computer assets are mainly referring to the computational hardware, like workstation, firewall, etc. The people assets involve the core development personnel, those who are dependent ones, and users form the other side of the program. The process assets are quite intensive and refer to various manufacturing process, etc. The intangible assets are somewhat “deviant” from programming development, like the stock price, but are relevant in a holistic perspective. The stepping-stone assets are the most interesting one because
it considers the entry or connection assets in this category. For instance, the authentication data, network access, and access to a particular computer.

The last definition is quoted from the CRR Supplemental Resource Guide: Asset Management. It defines the asset as “the raw material(s) that services need in order to operate” (“CRR Supplemental Resource Guide” 2016). Then it gives four types of assets in the definition regarding the services the assets support: people, information, technology, facilities. The people assets are those key employees who operate and monitor the organization’s services. The information assets are those required for the successful operation of the services. The technology assets cover the hardware, software, firmware, and physical interconnections. The facility assets are any physical plant where an organization relies on to deliver a service.

This thesis will adopt the following elements as the working definition. It contains the resources in the control system and includes the four elements mentioned above. Of course, the four types need to be more refined to fit into the ICS domain in the following chapters. All these resources are contributed to fulfilling the organization’s mission. The focuses are on the informational and technological types, while the rest are also introduced with the limited elaborations.

5.4 Asset Inventory in the ICS Domain

The following shows what each type of assets in the ICS domain should cover. Four different categorizations of assets are going to be listed. However, the list is not a complete one since the technology is advancing all the time. The items on the list could be added or deleted due to the retirement of the technology. Another factor should be taken into consideration is that the services could also come from a provider. Therefore, the assets could be further divided into the internal one and the external one if they exist.

5.4.1 People Assets

The people assets in an ICS domain refer to those who are the key roles within the control system. It is suggested to focus on the role of the post rather than the actual person. The person on the post in the control system is dynamic and could be replaced at any time. The role should always explicitly state what qualification the actual person should have to be able to be competent for the post. The following table lists the key roles within the ICS domain:
5.4. Asset Inventory in the ICS Domain

### Table 5.1: People Asset

<table>
<thead>
<tr>
<th>Internal People Asset</th>
<th>External People Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Architect</td>
<td>Service Contractors</td>
</tr>
<tr>
<td>System Tester</td>
<td>Service Contractors</td>
</tr>
<tr>
<td>System Security Designer</td>
<td>Service Contractors</td>
</tr>
<tr>
<td>Configuration Specialist</td>
<td>Service Contractors</td>
</tr>
<tr>
<td>Incident Response Team</td>
<td>Service Contractors</td>
</tr>
<tr>
<td>Human Resources</td>
<td></td>
</tr>
<tr>
<td>Media and Public Relations</td>
<td></td>
</tr>
<tr>
<td>Responsible Technicians</td>
<td>Service Contractors</td>
</tr>
<tr>
<td>Legal Enforcement</td>
<td></td>
</tr>
<tr>
<td>Equipment and Service Providers</td>
<td></td>
</tr>
</tbody>
</table>

5.4.2 Information Assets

The information assets within the ICS domain include any information data which are needed to make sure the successful operation of the organization. The information provides the necessary resources for understanding the structure of the business through which how the assets are implemented. The information can also be the output of the process, for example, the usual baseline of the network traffic within the field level which is useful to detect the abnormality of the field devices. The following lists some significant information assets within the ICS domain:

- Policies
- Personal
- structure
- Contact
- Data
  - Database
  - Documentation

5.4.3 Technology Assets

In the category, the core components of the ICS are covered, and it needs constant updating to make sure real-time changes are reflected. The vital role of this category makes it more complicated than others to map a clear structure of it. It contains more sub-categories of entities in this list. It is also possible to do an automated detection of these assets using certain applications.

5.4.4 Facility Assets

This category provides the lists of those dependencies with which the ICS operates. These assets are not directly involved in the controlling processes, but they are necessary to support the functions of them. It is different because most of these assets may be subject to external influences, but this does not affect the criticality of them and its role in security strategies. When counting them, it is always good to list the internal and external ones.
TABLE 5.2: Facility Asset

<table>
<thead>
<tr>
<th>Internal Facility Asset</th>
<th>External Facility Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Parameter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Power Supplier</td>
</tr>
<tr>
<td></td>
<td>Network Supplier</td>
</tr>
<tr>
<td></td>
<td>Water, heat Supplier</td>
</tr>
</tbody>
</table>

5.5 Asset Attribute in the Scope of its Service

In the previous chapter, the five types of assets are outlined at varying levels. The granularity of assets inventory depends on a few factors. The first factor is the size of an organization. The inventory is larger and more complicated for a bigger organization. For example, a large manufacturing plant has more RTUs, and these RTUs may be connected with different typologies using incompatible protocols. These elements will add to the complexity of the asset inventory. Another important factor which influences the complexity of the asset inventory is the service of the asset performing. Within the scope of one organization, it is vital to identify the service it provides and what are the dependencies with the assets. The importance of the asset derives from the service it provides related to the organization’s mission. For instance, a manufacturing plant places greater importance on the field level since the field level directly controls the production line and the production chain would be broken when some incidents disrupt the controlling systems. The third factor is that the new attributes would emerge and old ones might retire due to the fast development in the industrial 4.0. It would be an unrealistic approach to list every attribute, and this would cause redundancy without focuses. Therefore, it is essential to place the attributes of the assets under their service scope in the whole controlling system so that redundant or unnecessary attributes are filtered out.

The following attributes are generic and can apply to the many infrastructures. According to (Carali and Curtis, 2016), the following asset attributes should be collected:

- asset type (people, information, technology, or facilities)
- categorization of the asset by sensitivity (generally for information assets only)
- asset location (typically where the custodian is managing the asset)
- asset owners and custodians (particularly where this is external to the organization)
- the format or form of the asset (particularly for information assets that might exist on paper and electronically)
- location where backups or duplicates of this asset exist (particularly for information assets)
- the services that are dependent on the asset
- the value of the asset in either qualitative or quantitative terms

These asset attributes are on a more high level which provides an architectural view of the assets information. This is a macro view of how the asset attributes should look like, and it would be inspiring for the management level personnel. On the
hand, for the operational level, this is not so handy and contains less information they need to manage, monitor, or troubleshoot assets.
Chapter 6

Case Study

This part attempts to use selected open source ICS identification software to perform tests on some arranged ICS nodes. The design is to test two types of open source software which are designed by different approaches, namely the passive and the active. The test results are evaluated to see what kind of assets are identified in the controlled test bed. However, asset identification is conducted with the intention of identifying the technical assets, and other types are not in the scope of this case study. It is also true that the whole structure of an ICS network is not provided due to the lack of availability.

6.1 The Physical Setup

The ideal setup would include PLC, HMI, historian, RTUs, etc. in the typology so that the functionality of the software could be tested. However, this is not a viable plan due to the lack of ICS nodes. Combining the equipment provided by HMS, we have the following nodes:

- PLC X 1
- RTU X16
- Tap device mirroring ports X 1
- Switch X 1
- Windows OS Laptop with installed software X 1

For the security reasons, the brand and model of the above equipment are not revealed since it is one of the policies with HMS. The PLC is widely used in the industrial network and has all the functions needed for this case study. The 16 RTUs are used to collecting various information like temperature, pressure, heat, etc. The tap device with one port is reserved for taking in traffic so that the traffic can be picked up and analyzed by different software. The switch is a 5-port gigabyte switch, and one port is reserved for data injection. The laptop is pre-installed with Grassmarlin, Nmap, and Industrial Control System Exploitation Framework (ISF). The ISF is an exploitation framework which has the ability to map an ICS system.

- The physical topology:

  - The passive way of detection: The PLC is connected to RTU devices through an ethernet cable to the tap device. The reason behind using the tab device is to use the mirror port to map the network passively by connecting the PC with mirror port using Grassmarlin to capture the traffic.
• **The active way of detection:** The PLC must be connected to the Switch through the ethernet cable then to the tap device connecting the RTU devices to the PLC. By connecting the laptop with installed ISF software to the switch to configure the RTU devices.
6.2 Introduction of the Software

The section will give brief descriptions and introductions of the software which are going to be tested. GrassMarlin was originally developed for commercial purposes to sell to the National Security Agency (NSA). Its functionality has an awareness for the various types of ICS or SCADA environments of the available systems. GrassMarlin is developed using Java, which is a lightweight tool to run on various platforms and OSs. It is visible to sniffer and the traffic on an ICS/SCADA network to be able to make logical and physical graphs that are available for different functions in an interface, (Gilbert Schultz, 2011, 34).

As an interface software, GrassMarlin is able to run on various platforms and mostly it can run on both Windows and Linux operating systems to provide various functionalities at different times when there is the need. Grassmarlin can support multiple formats of traffic, for example, PCAP, Bro2Conn, Cisco Config, etc. One of the advantages is that the plugins it provides are custom Java code which gives the user power to expand formats. It also has the capability to passively listen on a network, which is helpful for passive asset identification, because it is designed not have any active network components.

Apart from various view functions, an impressive function of Grassmarlin is that it can export three types of reports from the traffic it observes. The reports can be available from the View menu and can be export to a CSV file which can be processed later by various analysis software. The first exports can be exported is the logical nodes. It provides a list of nodes contained in the logical graph. The list can be customized according the source, destination or both of the traffic. The second one is the logical connection report which identifies the traffic sent and received between an end-to-end host. The third report is the inter-group connection. It displays the connections existing between different groups according to geographical IPs or the subnets the hosts belong to.

The Industrial Exploitation Framework (ISF) is an exploitation framework based on Python, which is similar to the Metasploit framework. ISF is improved and built upon the project routersploit. This framework can be deployed to exploit the following PLCs, which are quite common on the market:

- S7_300_400_plc_control
- S7_1200_plc_control
- Vxworks_rpc_dos
- quantum_140_plc_control
- Crash_qnx_inetd_tcp_service
- Qconn_remote_exec
- Profinet_set_ip protocols

However, this study is not interested in the exploitation. What is interested in is the scan modules it contains. There are four scanner modules:

- Profinet_dcp_scan
- Vxworks_6_scan
- S7comm_scan
- Enip_scan

By deploying the framework, the expected protocol information of the targeted ICS nodes can be obtained by using these modules as long as the IPs are fed into the framework.

The Network Mapper (Nmap) is a free and open source tool specializing in network
discovery and security auditing. It utilizes raw IP packets to determine the availability of network hosts, services, operating systems, packet filters and firewalls, and many other functions. The availability of different platforms including Linux, Windows, and Mac OS X visions and the light weighted feature makes it an ideal network inventory and auditing tool. This software can run detection against a single host as well as large networks. The primary consideration of the selection of it is that it can generate packets in the system which makes it an active tool for network identification tool.

6.3 Asset Identification Results

- **Grassmarlin**
  The Grassmarlin is good at identifying assets which have been assigned IP addresses and displays multiple reports. According to the setup, all the nodes in the physical setup are mapped out in the Logical Graph, which can be seen in figure 6.1. After the live capture, all the IPs in the setup can be exported by selecting the source, destination or both to a CSV file in the View tab. Figure 6.1 displays the IPs in the setup. It can also export connection data from traffic using the Logical Connection Report. What is useful in the report is that it provides the data each node received or sent. These data can be used to compare with the baseline which has can be categorized as an information asset in the previous section to determine abnormal traffic. If malware exists in any of the nodes, it will introduce traffic and sometimes aims to introduce a DDoS attack. The abrupt increased amount of traffic can be picked up by Grassmarlin when the ICS network is monitored live. When this is transferred to another mechanism to alarm the administrator, the very easy phrase of the attack could be spotted and therefore be curbed in time. Figure 6.1 shows the Logical Connection Report from the setup. The Inter-group Connection Report give information according to network, country, MAC, Manufacturer, OS, SNMP category, etc. This offers the chance to see by what criteria those nodes interact. The fact is that the ICS nodes are supposed to exchange traffic within limited networks. If we scope in the level to the field device level, which is the case of our setup. The communication of traffic is only confined to one network. If any communication of traffic between the local network to another one, it is suspicious enough to raise the alarm to the administrator. Figure 6.2 shows the Inter-Group Connection Report according to the network criterion. Finally, figure 6.2 displays a snapshot of all nodes for the logical connection report in the CSV format in the setup.

- **Nmap**
  After the initial asset collection using the Grassmarlin, it is now known that the IP range of the test bed is within the 192.168.0.0/24. This passive identification functions as an intelligence collection method which shall not trigger any disturbances of the test bed by passively listening to the traffic. The Nmap is used as an active network probing tool. (Coffey et al., 2018) First, Nmap is instructed to actively scan the IP range to detect and list the hosts in that range without a port scan, using the -sP parameter. When a privileged user tries to scan targets on a local Ethernet network, ARP requests are used. The TCP SYN to port 443, TCP ACK to port 80, and an ICMP timestamp are requested.
6.3. Asset Identification Results

by default. This can allow light reconnaissance of a target network without
attracting much attention.

The quick scan confirms the hosts identified by Grassmarlin in the previous
step. Meanwhile, each note is additionally marked by the MAC address spec-
ifying the manufacturer. For example, the PLC is clearly marked and showing
the maker is Siemens. The RTUs are from HMS because the Nmap database
has been updated with MAC in Figure 6.3.

![Figure 6.2: Grassmarlin Software](image)

Next, by confirming the results from the previous stage, Nmap is used to probe
the network to display more about the test bed. With the flag -O, Nmap tries
to establish the OS of the target node. This active scan also lists open ports for
specific protocols, services, and network distance. As a result, the TCP 21 and
80 for FTP and HTTP protocol are open respectively. The report is generated
for each individual IP within the subnet in the following Figure 6.4.

![Figure 6.3: Nmap -sP](image)
To have a better understanding of the network, the UDP is scanned as it is often ignored by auditors, which usually leaves the room for attacks. The most common protocols are DNS, SNMP, and DHCP with registered ports 53, 161/162, and 67/68. Nmap scans by sending a UDP packet to every port. One service will respond with a UDP packet which proves that it is open. If no response is received after re-transmissions, the port is classified as open|filtered. This means that the port could be open, or perhaps packet filters are blocking the communication. The Figure 6.5 shows that all in all the RTUs the UDP port 161 is open for SNMP service which could be a security risk within the test bed.

**ISF (Industrial Control System Exploitation Framework)**

Another active ICS identification software is ISF which is an exploitation framework. This open source tool can also be applied to identify ICS assets actively. The difference from Nmap is that it can identify ICS assets based on the protocols the nodes run. Currently, the most common protocols like Modbus and PROFINET are supported. After deploying the software on the test bed, the Figure 6.5 shows identified assets using PROFINET.
Apart from the above functions of identifying the ICS assets, the testers try to see the functionality of this framework further. After the intelligence gathering using Grassmarlin, the target PLC is known to be from Siemens. Therefore, the exploit is tried against it. To be more exact, the

\texttt{s/_1200_plc\_control}

is deployed with the test bed. The function the framework contained can be used to start, stop, and rest the target PLC. The Figure 6.7 displays the deployment.

Generally speaking, the Grassmarlin is excellent software for providing logical topology of the ICS network. All the IP information can be obtained by using non-interfering approach. Meanwhile, it can also export various reports according to different criteria. The IP information obtained via Grassmarlin can be to feed further investigation. The reports shipped can be investigated traffic activities and compare with the baseline to detect potential risks. However, the functions of Grassmarlin cannot provide cluster information, and no hardware information could be obtained. This means an active identification should be introduced. The Nmap is active identification tool and can offer the functionalities, for example, MAC, Protocol, port, service, etc. For ISF, it can identify ICS assets according to their industrial network protocols and equipment information when the IP information is known. Hardware information can also be obtained by...
running the scanner modules. It even takes a step further by offering an exploitable module of modifying targeted PLCs. Due to the limitation of the design, the interference with the usual traffic is measured. Therefore, the impact the determinism can be observed in this study. The conclusion is that if the two types of software are combined, better results can be obtained.
Chapter 7

Asset Management

After the above elaborations of asset identification, the rationales have been established for assets in the whole process of an industrial network. The asset identification, however, is just one module in the cycle of asset management. Having good asset management is as important as the identification of assets in the industrial network. The asset management establishes a holistic picture of the managing assets in the business premises. Therefore, it’s quite worthwhile introducing the asset management in this essay to enrich the contents and benefits of asset identification. The readers should be reminded that this introduction only covers the fundamental concepts in asset management.

7.1 Modules of Asset Management

There are some versions on how to establish asset management in the literature and some are good for the theoretical understanding on undertaking the task of establishing the asset management in general settings. After comparisons were made among the literature, the modules suggested by CRR from Carnegie Mellon University are adopted in this section.

The selection of the modules from CRR has certain advantages. The first advantage is that the four modules are aligned with the Cybersecurity Framework (CSF) from the National Institute of Standards and Technology (NIST). The CSF aims to address the cybersecurity issues attempting to compromise the information technologies within industrial control systems, cyber-physical systems, and the Internet of Things. One of its prominent concerns is to address the issues for critical infrastructures. Therefore, the cores of aims align well with the security concerns for asset management. While coincides with the aims, the CSF also considers the asset management as one of its essential ingredients for securing the infrastructures. In the first core of the framework, the asset management tops the other five identification within a target entity. It laments the essential concept that the assets enable an organization to deliver critical services and the key role in security measures. Second, the CRR asset management modules are commissioned by the Department of Homeland Security’s (DHS) and conducted by Carnegie Mellon University. The validity and authority of the research institution can be trusted. So far, the version of CRR has been evolved to 1.1, the second version in 2016. This is also another proof that the modules and concepts in this research are updated and follow the trend both in the academia and industry. Lastly, the CRR provides a good elaboration on how to chain each module of asset management together and gives proper instructions on how to implement these modules. It establishes the rationales behind the imminent security issues facing critical infrastructure within the USA, which is also valid for the rest of the world.
According to the CRR, there are four modules in the process of asset management. The flow of this asset management is cyclic and needs constant maintenance. The logic of making a cohesion flow among the four modules is well preserved. However, the first module, plan for asset management, should not be considered as a fixed module in our perspective. It should rather be considered as some prerequisites before the asset management starts. The rest modules are well presented and fit the whole chain of asset management.

![CRR Asset Management Flow](image)

**Figure 7.1: CRR Asset Management Flow**

### 7.2 Prerequisites for Asset Management

Apparently, lots of factors are there to be considered when an organization starts the quest of making asset management. The situation might be the case that not all organizations need to start this quest from scratch. Lots of units within one organization might have already compiled some lists or inventories. Then the job is to place them under a well-designed schema according to the specific need of the organization. However, two prerequisites have to be ensured so that a good asset management could be implemented. The first one is to have support within the organization. This very important due to the holistic nature of asset management. The managing level should know precisely the benefits it brings and grants the permission and support for the staff to carry out this quest. Each level of the asset owner should provide the necessary support for this quest and should also participate in this process. This is because the assets owners are usually those who know well the attributes of those assets and their dependencies among the services. The second is that an agreement on the definition of assets should be established before carrying out the task. It is true that the definition of the asset which is going to be identified and managed is hard to reach a unified standard, but a working agreement among the asset owner and the asset management team should be achieved. One issue that needs to be cautioned about is that the assets must be prioritized against the service the organization provides. The purpose of managing assets is to make sure the service or production of the target organization is not disrupted in the face of security threats. Therefore, the service or production flow must be identified
first, and then the assets which are utilized to provide them shall be managed under this schema.

**7.2.1 Asset Inventory**

This is the object and result of the previous chapter. After the assets are identified through systematic investigation, the product is the inventory of assets under the selected schema. This inventory contains all necessary assets which are directly related to the service they support and all the attributes which uniquely identify the assets. This connection between asset and service is a core concept when making the asset management. To ensure proper control for these assets, responsibilities should also be assigned to respective roles. Just as the difficulty of identifying assets, the larger an organization is, the more complex the task becomes. It is always essential to delegate the right responsibilities to the proper roles so that the management of them could be continued.

The inventory could either be a paper format or electronic format. It is, as matter as fact, the trend of using the IT technology to store it in a database. This format will make the queries and reports much easier. The Cybersecurity Framework provided by NIST is a good example to store the collected inventory. One of the reasons for this suggestion is that this framework uses collected data to evaluate the resilience based on the five cores, namely identify, protect, detect, respond, and recover. This database solution is open, and it can be downloaded at (NIST Cybersecurity Framework (CSF) Reference Tool, 2018) for either Windows or Apple OS X.

**7.2.2 Management of Assets**

The drives for managing assets are many, but to keep up with the dynamics of the business and reflect it on the management is the ultimately important factor. The dynamics of change and updates are due to the nature of assets. Conversely, the impacts of these changes have different impacts on the asset itself. Natural aging or structural dynamics can cause the changes or alterations of the assets. Most of the technological assets are changed due to the fact that they might reach the end of their life cycle or cannot cope with new requirements due to new risks arising from the external side of the business. Staff change might be caused by the fact that the responsible staff leaves the position. Facilities will also undergo this kind of dynamics, like the change of supplier, relocation of the business premise, or expanding manufacturing scope. All of the above dynamics require an organization having an understanding and preparation of integrating this dynamic into the asset management.

The impacts caused by the outlined dynamics are different for each asset type. The consequences reflected in the assets should be communicated promptly so that the concerned asset owners or custodians adopt appropriate measures. Sometimes the communication should be timely conducted and involves multiple units’ action. For instance, one of the key personnel leaves the position, and the HR should be able to appoint a competent candidate who has the capabilities required by the role. Otherwise, the service or production might be disrupted in the case of no appropriate responsible is appointed.
In this cycle of asset management, it is important to have an agreement on what the dynamic is or what should be counted as the criteria for change. Once the change criteria are established, they should be adopted consistently throughout the organization. These criteria should be promptly implemented when change happens in the target organization and should be reflected in the asset inventory.

Another important step in this section is that a change cycle should be outlined. The cyclic nature of the service or production needs the asset to function in sound performance. Distinct checkpoints of each stage of assets in the cycle should be noted and marked. This is especially true for the technology and information assets. There is a certain period of normal function for physical or technological assets. From initialization to retirement, the life cycle of them should be well traced and marked so that the asset management could have a better flow of them. For information assets, sensitive data undergo a life cycle regarding their confidentiality. The change of confidentiality requires different handling and the change impacts will determine the final process of these information.

Finally, the change of assets brings updates to the whole inventory, and it could introduce new needs for handling. These new requirements will impact the partial or entire management process. For instance, the introduction of new PLCs might not comply with the current asset management. Therefore, the changes should be reflected timely to align with other assets within the established status. The asset management is a cyclic process which means constant maintenance and management are required. The whole asset management should also be considered as one of the elements in the who chain of security, which is another aim of this work. The systematic view should be adopted when other elements could cause impacts on asset management. While other security modules could cause impacts on the asset, the vulnerabilities introduced by assets because of poor managements could also lead to risks in other parts. Then a holistic view is needed to ensure the sound functions of all assets.
Chapter 8
Conclusion and Limitation

The significance of asset identification and asset management has been recognized increasingly and is echoed in this thesis. The benefits of performing asset identification are manifolds. A systematic schema helps an organization run better asset management and gain financial rewards. The well-managed assets improve responsibilities internally and it highlights the focus of assets regarding its status within the function network. More importantly, a systemic and well-organized inventory could be obtained after the work. This work is of great significance when it comes to deal with security threats and risks. The attack against ICS is on the increase, and the first line of security starts from assets due to the fact that assets are bound with their vulnerabilities and improper management. The defense-in-depth security approach emphasizes each tier’s capability to guard the normal function of the system. It is also important that when a well-organized asset inventory is obtained, it is much easier and has much more value for the incident response team to deploy countermeasure in the face of security attacks against ICS system. The subject of asset identification and management should have their due role in the system of ICS security, and it is discussed in this thesis, though it has been subsumed in the overall ICS security strategy.

A well-defined asset matters and it is the starting point for all the work related to the performing a job of identify them. Although the definition of assets could be found in varied layers of details, a well-defined asset concept and its attributes are, in fact, hard to obtain. The function-based approach has its focus which associates the asset with its service. This approach prioritizes those assets with their vital roles in the system. On the other hand, the network-approach uses a systemic way to organize the assets and sees the inter-dependencies of assets and their roles in a holistic way. It is lamented that with either advantage they should be combined to fully incorporate the assets into the framework so that it can reflect both the priority and the connections within the network. The conflicts of adopting varied approaches result in the ill-defined assets. It is a convenient and irresponsible act of picking assets according to one’s expertise. However, a complete and excellent example of ICS asset inventory is difficult to locate, therefore the framework suggested by CRR is used instead. The CRR framework is aiming for critical infrastructure and provides sound theoretical and piratical guidance for establishing the asset identification and management schema. However, one thing should also be pointed out is that due to the nature of varied ICS, the attributes of the assets should be conditioned to reflect their own natures. The attempts of outlining all the attributes are impossible for this thesis to finish, then this attempt is discouraged after considerate discussions.

The actual procedure of performing the essential part of asset identification and management is illustrated in the thesis, but the choice of appropriate tool kits needs further investigation. The identification of four closely related assets and management cycles can be duplicated and should be used according to the specific needs of
the target ICS. The “one does for all” tool kit is not possible either for the commercially available or the open source software. It is also the fact that the identification approach using passive, active, or hybrid depends on the needs and ICS nodes. The passive scanning has more benefits than the active one since it will not disrupt the traffic of the actual production while collecting the necessary information of the assets. Due to its disruptive nature of the active scanning, it should be used after careful design. The hybrid approach combines the benefits of the previous two, attempting to eliminate the disadvantages. In a nutshell, the selection of automated software to conduct the asset identification should be designed carefully according to the nature of the target ICS.
Bibliography


Mohammed Abdulrazzaq received his B.Sc in Information Systems Computer Science from Alrafidain University College in 2008. His research interests are Network Design, Cybersecurity, Ethical Hacking, and Penetration Testing.

Yuan Wei a master student in Network Forensics. His research interests are industrial network design and security as well as commercial network routing and switch optimisation and security.