The Challenges of the Internet of Things Considering Industrial Control Systems

Kim Smith and Ian Wilson

1 Introduction

1.1 Internet of Things

There are many authors who have described what the Internet of Things (IoT) is. Author Greengard (2015) introduces the subject of IoT along with multiple articles (Madakam et al., 2015; Khan & Salah, 2018). They present an introduction to the concept of IoT. Authors Madakam, Ramaswamy, and Tripathi (2015) reviewed literature on the IoT concept with the conclusion that there is no common definition of the term. Authors have tried to identify the origins of the terminology. The suggestion by sources (Greengard, 2015; Postscapes, 2020) is that Kevin Ashton, the Executive Director of Auto-ID Labs in MIT in 1999, was the first person to make use of the term IoT. He was at the time working on a presentation for Procter & Gamble in the context of RFID supply chains.

The definition adopted throughout this article will be that provided by the Centre for the Protection of National Infrastructure (CPNI) (Centre for the Protection of National Infrastructure, 2021) which offers a definition that presents a network of devices with autonomous functions which are part of everyday life.

The IoT as described is something that exists everywhere that a connection to the Internet is possible. The connection mechanism does not concern the IoT. As in Miller (2015) any device that can be uniquely identifiable (normally by an IP address) can be considered as a part of the IoT. This is not just devices we consider as digital such as laptops or smart phones but also includes those domestic devices such as washing machines, lights, and heating that can be controlled remotely.

K. Smith (✉) · I. Wilson
University of South Wales, Treforest, UK
e-mail: kim.smith@southwales.ac.uk; Ian.Wilson@southwales.ac.uk

R. Montasari et al. (eds.), *Privacy, Security And Forensics in The Internet of Things (IoT)*, https://doi.org/10.1007/978-3-030-91218-5_4

1.2 Industrial Control System

Multiple authors have described Industrial Control Systems (ICS) in peer-reviewed articles as well as in academic materials. Authors (National Institute of Standards and Technology, 2011; Simon, 2017; Assenza & Setola, 2019; National Institute of Standards and Technology, 2008; Hayden et al., 2014; Bodungen et al., 2017) introduce the modern concept of ICS; however, ICS was first identified in Greek and Arabian societies. The literature sources surrounding ICS use a different terminology that leads to confusion. One form of terminology used to describe an ICS is a Process Control System (PCS). Another terminology used is Supervisory Control and Data Acquisition (SCADA). This describes one of the topologies of ICS. The different topologies of ICS are PCS, SCADA, Distributed Control System (DCS), SMART, or Industrial Automation and Control Systems (IACS).

The definition to be adopted throughout this article will be that provided by the National Institute of Standards and Technology in their Glossary of Terms in NIST SP-800 (National Institute of Standards and Technology, 2011) that describes information systems that control remote assets and local assets utilized in industrial processes including manufacturing, distribution, and other production processes.

2 Industrial Control Systems

ICS are different from IoT, but they are also similar. This section is aimed at providing a more in-depth introduction to ICS and how they are similar to IoT. An ICS is different because it is based on industry and will have a combination of operational and information technology. An IoT will tend to be more based on a residential setting and be based on information technology only. However, current development is presenting the Industrial Internet of Things (IIoT). In his report (Simon, 2017) the author describes the IIoT in terms of the communication that occurs between machines and the immense volumes of data that are generated that can support the development of efficient industry processes.

2.1 Operational Technology

Operational technology (OT) is only relevant in an industry setting. In their article (Assenza & Setola, 2019) the authors define OT as a system with assets that are linked together to monitor and control automated processes through information communication technology.

2.2 Information Technology

Information technology (IT) is a supporting structure for both industry and the citizens of the world. It consists of a diverse range of digital devices from computers to IoT devices such as smart washing machines and heating controls. The other element of IT is the communication media that is used. There are also many forms of media, but they all provide a connection to the Internet whether through Bluetooth, wireless, or Ethernet technology.

2.3 Functions of ICS

A typical ICS operation is described by NIST (National Institute of Standards and Technology, 2008), and the fundamental structure is a closed-loop control system also known as a feedback loop. A closed-loop control system has the primary aim of processing information in the following manner:

- Accept an item of data usually from a sensor.
- Feed the data to a process.
- Perform a process using the data and the feedback data.
- Output an item of data.
- Feed the output data (feedback data) into the process.

This is performed in a cyclic manner as shown in Fig. 1.

This basic principle is embedded into all ICS and is further defined by authors discussing the main functions of ICS. In their SANS whitepaper, Hayden et al. (2014) offer four main functions of an ICS as measure, compare, compute, and correct. NIST supports this in their description of the ICS components and operations (National Institute of Standards and Technology, 2008) in which they define four elements as measure, compare, compute, and correct. In their book Bodungen et al. (2017) consider only three functions of ICS as view, monitor, and control.

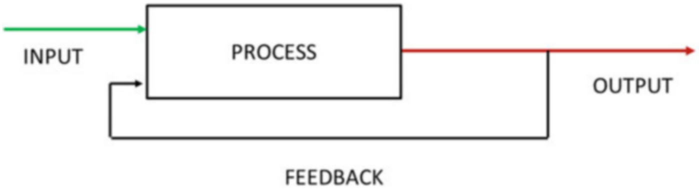

Fig. 1 A closed-loop control system

2.4 Physical Components of Industrial Control Systems

The ICS systems are found in all environments in support of everyday life. The functions as described above are performed by the components of the ICS system. The components are varied and depend partially on the topologies of ICS and the industry sector that they are applied to. The topologies are:

- DCS is used in process-based industry such as agriculture, chemical plants, and automobile manufacturing.
- SCADA is used to monitor and control industries such as oil and gas pipelines and electric power grids.
- PLC is a part of a larger configuration within a SCADA or DCS system.
- SMART is used in residential and industry environment.
- Industrial Automation and Control Systems (IACS) is in a small geographic location such as a manufacturing plant.

Authors Knapp and Langill (2015) describe the components of an ICS in a system-wide context. Others take a physical approach such as the one described by Hayden et al. (2014) in their SANS whitepaper. In their paper they identified the following components of ICS:

- Sensors that perform a measurement task
- Transducers that convert a measurement into an electrical signal
- Transmitters that convert and then send the signal
- Controllers that perform processes on input and provides an output
- Final control elements that make a change based on the signal sent to them

2.5 Commonalities Between ICS and IOT

This mixture of definitions of IoT means that it can be interpreted in many ways. In defining how an ICS is a form of IoT, it is necessary to analyze the definitions to identify the common elements. The result of comparing the definitions is the identification of the following commonality:

- Multiple intelligent devices
- Interconnectivity of devices through the Internet
- Enabling the sharing of big data
- Contained within a closed-loop control system
- Autonomous
- Self-monitoring capability

2.6 Other Components of Industrial Control Systems

As a part of an ICS system, the term socio-technical system (STS) is used to describe components including the physical. An STS consists of complex interactions between humans and technical systems. This term was derived from studies undertaken by Trist (1981) on the effects of technology on workers. The results did not always indicate an improvement in efficiency or productivity, linking these to other factors in the working environment not the technology. The original model of STS consisting of the social and technical systems was presented by Bostrom and Heinen (1977). This model develops the concept around four elements, technology, structure, people, and tasks, and is used to indicate the complexity of the interactions between humans and technology. They describe the system as:

- The technical system is concerned with the processes, tasks, and technology needed to transform inputs to outputs.
- The social system is concerned with the attributes of people (e.g., attitudes, skills, values), the relationships among people, reward systems, and authority structures.

This original model was further developed in 2016 by Oosthuizen and Pretorius in their article (Oosthuizen & Pretorius, 2016) where they add an additional environmental dimension. The environment dimension encircles the STS which contains the elements described by Bostrom and Heinen (1977). This additional element was included to represent the concept that the STS was an open system. Open systems are susceptible to external inputs from the environment, thus increasing the complexity. Other authors offer alternative views of STS. Wu et al. (2015) offer a hierarchy to represent the elements of the STS system. The hierarchy is subdivided into three parts:

- Social
- Technical
- Environment

Each of the subdivisions of the hierarchy is scoped individually, and it is not possible to combine them to attain a holistic view. Authors such as Malatji, Von Solms, and Marnewick (2019) in their paper continue to work within the STS model presented by Oosthuizen and Pretorius (2016)) and in their research identified the people element as the weakest link. They identify that there are many reasons why this is the situation. Their emphasis is to try to uncover gaps and to focus on the effectiveness of current security controls to optimize them.

3 Challenges in Industrial Control Systems

There are many challenges relating to ICS, and to explain these, they have been categorized into the following:

- People
- Physical
- Security
- Organization structure

Challenges in ICS are based on the concept of risk. Managing risk is a very important task within any organization. There are many types of business risk; however, this report is concerned with the risk surrounding the use of ICS and concentrates on the element of cyber risk. Cyber risk is a major concern of the board of an organization, and such things as awareness, budget, culture, and priorities may affect the level at which an organization deals with risk. Supporting the board, employees should have an awareness of cybersecurity, but this will be at different knowledge and skills levels. With a lack of knowledge come mistakes and errors which can increase risk. The statistics from Ernst and Young survey (Fig. 2) show that employees are accepted as the most likely cause of risk in a business (Ernst and Young Global Limited, 2020).

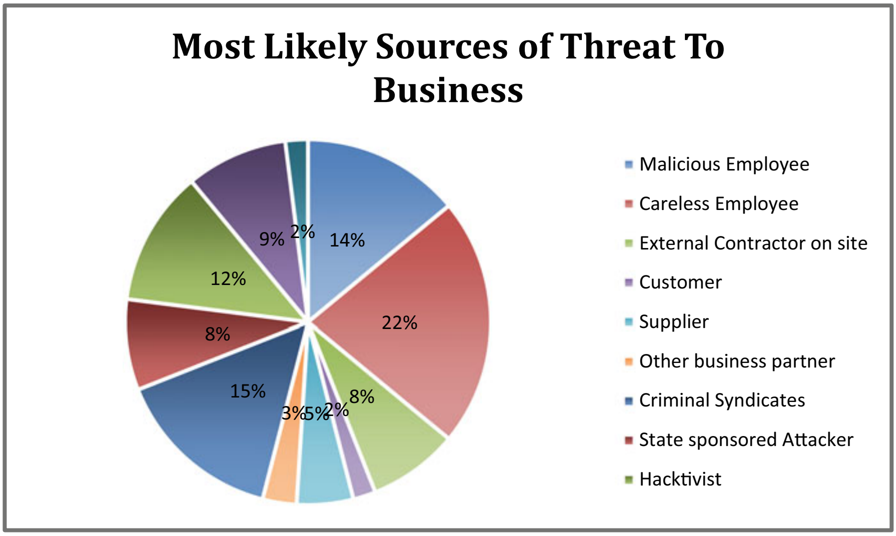

Fig. 2 Most likely sources of threat

3.1 People

People are a key element of an ICS, but they are often ignored in the recognition of the risk level that they give. When considering the human as a part of risk, an important subject is psychology. In terms of ICS and IoT, exploring the area of psychology can help identify certain characteristics and traits that make a person more vulnerable to an attack from social engineering. Three general concepts are:

- Susceptibility
- Awareness
- Motivation

The concept of risk associated with humans relates to different aspects, and authors such as Mouton, Leenen, and Venter (2016) have developed an extensive ontology of attacks, techniques, and other key areas around social engineering. In his book Hadnagy (2011) introduces the concept of social engineering and references definitions from multiple sources. He offers a simple definition in an individual performing an action through the maneuvering by another.

There are many sources of definitions of social engineering. The Oxford University Press states that this is deception by an individual to gather confidential information from another through manipulation.

Developing this along with information from Babu et al. (2017), National Institute of Standards and Technology (2021), and Doan (2006)), the diagrams identifying an ontology of social engineering in Fig. 3 and Fig. 4 demonstrate the complexity of the subject.

Susceptibility

This is concerned with the characteristics and traits of an individual. Individuals develop these traits over time, and a person involved in social engineering is observing in the hope of identifying these traits in support of the development

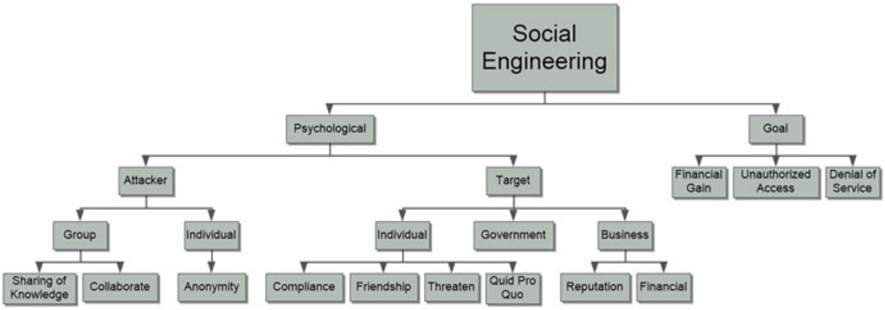

Fig. 3 Social engineering ontology part 1

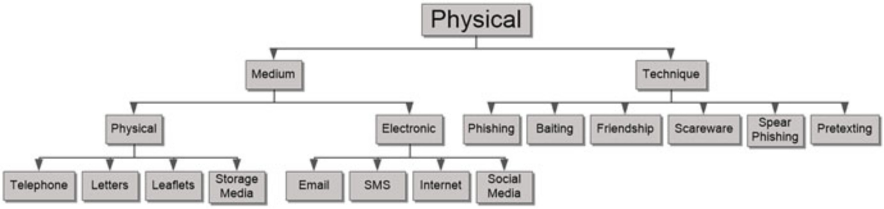

Fig. 4 Social engineering ontology part 2

of an attack. They will watch and observe individuals looking for their habits, routines, and personal behaviors. The Collins dictionary (2016) presents the word susceptibility as the link to the degree to which an individual can be affected by or influenced by another. The habits, routines, and behaviors make individuals a target.

The behaviors that are a clue to a person's susceptibility would be a demonstration of their trust in people. Another could be their integrity; this can be tested by those who are involved in social engineering. Other clues would be a person identifying with their social worth; much of this information can be gathered from social media such as Facebook and Twitter. Other signs will relate to their working environment. The primary needs of an individual as identified by Maslow (2013) should be met particularly the basic needs such as shelter, food, water, and security for them to be less vulnerable.

Awareness

When considering awareness as a contributing factor to social engineering, there are different and conflicting opinions. Awareness can be separated into two key elements. The first is the employee awareness of cybersecurity and the risks and consequences to the organization. This awareness would be a part of a training package for all employees. The second is the awareness of employees of the standard working practices and policies in place to protect the organization from cyber-attacks. These should reduce the risk to the organization. This question of awareness was addressed by (Aldawood et al., 2020) in their article. The article links the security state of a system and the vulnerability of employees. They link people using the most secure systems as often being the most vulnerable to social engineering attacks. This is borne from the false idea that security procedures exist, and employees are aware that they will use them. The reality is that employees will try to find the quickest way to perform a task which could entail the bypassing of the security measures. For example, an employee may receive a USB storage device from a supplier. Procedure should say load into a clean (standalone) pc first; however, the employee trusts the supplier and loads straight onto the network causing malware to be loaded onto the network.

Motivation

Already mentioned is the challenge that employees in a business can be susceptible to a social engineering attack. One consideration is the motivation of the individual in terms of two things, their home life and work life. Employees who are dissatisfied at work have an increased susceptibility to attack. This can be from multiple sources, if an employee has been passed over for promotion or they feel that they are being blamed for things going wrong or even that they did not get a pay rise. These all affect a human's psychological state, and this can be manipulated. The use of social media to vent an individual's frustration is an open door for a social engineer. With motivational factors it is important to remember that this is a person's perspective and may not be true. To enable better security from cyber-attacks, managers must be aware of the human emotional factors of their work force. An article that undertakes a comparison of factors (Alblabi & Weir, 2018) for social engineering provides an analysis of the personal email and social environment which can be crossed into the work environment.

3.2 Physical

The physical challenges of ICS are concerned with the physical components of the ICS. This can be a primary element as described or the communication media of the interconnection between the elements. This chapter will not be used to consider the challenges that relate to the security of such elements as sites as these would be covered under a site management policy. The challenges of the physical components of ICS can be categorized as:

- Legacy
- Maintenance
- Cost
- Commercial off the shelf
- Mitigation of risk

Legacy

ICS are referred to as legacy systems by some authors (Ernst and Young Global Limited, 2020; Kriaa et al., 2019; Ginter, 2016); this happens for several reasons: the age of the system, the lack of vendor support, the older hardware, and an increased cost of maintenance. A simple explanation is provided in Techopedia (2021) defining the system as consisting of outdated components that could be the software, device, or programming language. An important point is that these types of systems were originally in place with the priority to ensure the safety of the system and protection of people and business not the security from attack.

Maintenance

One of the key issues for legacy systems is the subject of maintenance which includes upgrades and patches to software. Kilman and Stamp (2005) identify that many devices in ICS have never been updated with anti-virus or firmware since their installation. There are many reasons why organizations feel that they are unable to perform much-needed maintenance:

- Availability issue and disruption
- Lack of vendor support
- If it is not broken do not fix it attitude
- Too costly
- Not enough skills
- Concerned about the impact to other elements of the system

Babu et al. (2017) support (Kilman & Stamp, 2005) in that a lot of ICS systems have been operational for a long time and therefore are legacy systems. These systems have not been maintained, and the age of the technology implemented means new security options cannot be implemented.

Cost

Cost to a business must be considered for both long term and short term. There could be short-term costs that may give quick results in terms of risk mitigation. However, it is generally considered that the long-term cost is substantial given that devices may have to be upgraded in some way. Cost can also include the mitigation actions. A company may just decide to have devices on standby in case they are attacked. This can be a very expensive option but may be the only possible solution. Having redundant equipment around needs storage and needs to be maintained. The life of the device is a big factor in deciding the cost and the replacement plan.

Commercial Off the Shelf (COTS)

In the NIST glossary (National Institute of Standards and Technology, 2021) describing abbreviations throughout the vast library of NIST documentation, they define COTS as an abbreviation for commercial off the shelf. This means the range of existing software and hardware that is available from commercial outlets. For ICS systems this increases cyber risk which must be mitigated against to ensure minimum risk to life.

In his thesis Dung Doan (2006) introduces the advantages of using COTS items. The advantages are that it incorporates newer technology and newer standards. It can be updated faster than custom-built software. Maintenance cost is substantially reduced since COTS software is widely used by a large population. COTS items although they have advantages also have disadvantages, and the main concern relates to the security of using them. Some typical issues are that COTS software is not amendable, defaults will be in place, easy availability for an attacker, and configuration weaknesses.

COTS software is designed to not be changed and therefore cannot be customized to meet the needs of specific ICS. COTS vendors do not provide any guarantee that the items are secure. Lastly COTS items are designed with functionality as the highest priority; therefore less attention is spent on the security of the software. COTS items have security defaults in place such as administrator overrides. This immediately is a high risk to ICS systems, and all default passwords and user identifiers should be changed as soon as an installation is made. However, many vendors do not provide installers with the information, and so they are not aware of the risk. These provide excellent backdoors for hackers to attack an ICS system.

COTS items are widely available which increases the risk that users with malicious intent can attain them. These users therefore have the potential to uncover security flaws in the items as they take time to analyze how they work. If flaws are identified, there is an increase in risk to the item and the systems that they are embedded in.

The variety of potential risks is wide and putting this into a business context. A study was undertaken by Project SHodan INtelligence Extraction (SHINE) (2014) in 2014. This was a collaboration of organizations and individuals to demonstrate the vulnerability of SCADA systems. Their research demonstrated that there were over one million ICS/SCADA systems connected to the Internet with unique IP addresses. Having identified so many devices, it is easy to select those that are vulnerable and make an attack.

Mitigation of Risk

One type of mitigation of physical risk that is used is defense-in-depth as described by Melissa Tucker (2015) as a multi-layered defense approach. This approach makes use of different cyber-defense mechanism, and this should prevent a single point of failure in the system. This type of strategy is most often used by the military as a complex defense is more difficult and time-consuming to penetrate. This strategy is supported by NASA and other bodies such as the United States Nuclear Regulatory Commission (2016).

In the article written by Kupiers and Fabro (2006), they identify several key differences between traditional IT environments and control system environments and how they affect securing ICS systems. In the article they compare security elements and how they are different between IT and ICS. The comparison identifies the differences in applying patches and anti-virus, the requirements for availability and time criticality of the systems, as well as the lifetime of the components. They also included a comparison of the environment such as outsourcing and the physical situation in remoteness of systems.

The authors after the comparison discuss and identify what they consider as the five key security countermeasures for control systems:

1. Security policies
2. Blocking access to resources and services
3. Detecting malicious activity
4. Mitigating possible attacks
5. Fixing core problems

3.3 Security

ICS systems as well as IoT systems must be secure and safe. In terms of how important they are is based on the evolutional aspect of IT and ICS. Originally safety was the concern of developers of ICS systems minimizing any impact on the environment or ensuring no loss of life or injury. On the other hand, the developers and maintainers of IT systems were originally only concerned with the security. An issue for both areas is that there are different definitions for industry sectors. In their article the authors (Kriaa et al., 2019) define the difference between security and safety:

- Safety—the risk that is accidental but has unacceptable results
- Security—risk that is malicious

Another perspective was given by Andrew Ginter in his book (Ginter, 2016) where he defines cybersecurity as the prevention of attacks and that ICS security is the prevention of unauthorized operation of the system. Author Stig Johnson (Johnson, 2013) discusses resilience-based risk management and offers an alternative description of safety and security. He stated that safety was concerned with the accidental harm prevention, reduction, and reaction to systems. In comparison he stated that security was concerned with malicious harm prevention, reduction, and reaction to systems.

CIA/AIC Triad Model

The CIA triad model is a building block for security policies utilized by organizations. The model is a start point in the understanding of the security of ICS and is utilized by many different industries. There are three factors of the model: integrity, availability, and confidentiality.

- Confidentiality—is concerned with the protection of personal data, and its loss can have a huge impact on an organization both financially and reputationally.
- Integrity—is the ability to have confidence that the data within any system has not been altered and is original as it entered the system.
- Availability—is the ability to access information at any time as and when required.

For many organizations, the business is governed by the requirement to ensure the confidentiality of their data for regulation purposes. However, this is where the main difference exists between IT systems and ICS. The three factors exist in both, but their importance differs and in ICS is referred to as the AIC triad. This change reflects the priority of these types of systems. Availability is the priority factor; the justification for this difference is that ICS requires immediate responses to be made to input data to prevent catastrophic events occurring, meaning that systems and their components need to be available 100% of the time. Integrity in ICS systems is the second priority because the processing in systems is real time which means that they must be able to respond and react to data immediately.

Challenges of OT Security

The problem is that the OT has several peculiarities that make the implementation of the protection measures that are usually adopted for the IT systems difficult and problematic. Systems support the critical infrastructure of the world, and a cyber-attack has the potential impact of loss of life which is more devastating than loss of an IT system. The links between OT and IT have increased during the period of development of the modern world of connectivity. This has increased the vulnerability of systems that could adversely affect communities and the environment.

Availability

The main challenge for OT is based on the availability priority of the AIC triad. OT systems will be operational on a 24-h basis every day of the week and normally 365 days a year. OT systems support the infrastructure of the nation and therefore need to be available. There have been attacks such as the 2000 Maroochy water system (Slay & Miller, 2007), the 2010 Stuxnet attack (Hagerott, 2014), and others that have caused major blackouts and water supply issues which are all effects of non-availability of OT systems. This requirement will lead to systems becoming more vulnerable overtime as they will not have current patches installed, and to apply such maintenance requires advanced complicated plans to ensure there is no disruption to system availability. Another consideration for availability is the real-time nature of these OT systems. The large amounts of data that are generated and analyzed are used instantaneously to alter the system state. The implementation of such security as firewalls and encryption would cause delays in communication and processing which would affect the response and sensitivity of such systems. This could compromise the system operation and ultimately cause loss of life.

There is an additional issue associated with availability, and that is the effects of implementing a patch. It is very difficult with OT systems to test that a patch works before it is implemented on the real system. This inherently increases the risk that a change may influence the operation of another element of the system.

Access Routes

As well as OT systems being at risk from the issues surrounding availability, they also suffer from the challenges of the routes of access provided for such systems. The IoT also have the challenges of access as multiple devices are linked together as a network and could use any one of the following communication media to communicate with other devices:

- Wi-Fi
- Ethernet
- Bluetooth
- Mobile network
- Satellite
- Fiber

The problems that the access route generates are varied and affect different industries who have different requirements. There are some common challenges which are identifiable. One is the ability to send a signal over either a short or long distance. Another is the reliability of the communication medium; if poor weather conditions affect the communication, then that cannot be implemented in an area where this type of weather is common. Other issues could be whether the media is shared by business and residential customers. This could influence the availability of slots to send messages as there could be bottleneck periods such as Christmas and New Year. The speed of communication is very important for ICS systems because of the real-time working environment; some media only offer slow speeds. Another is the potential for interference generated maliciously or unintentionally. Interference can affect all forms of communication and can cause catastrophic effects in ICS systems.

One challenge is the security of the media used to send information. This is an issue for all IT-based systems and is a constant source of development by engineers. It is not possible to make a system 100% secure if it is connected to the outside world. However, the aim of any organization is to provide the securest communication that they can. An area of particular concern for ICS and IoT are the protocols that are used for communication. The communication industry developed technology in an ad hoc manner and suffered from the wide variety of technology. The complexity of communication was due to the high number of different protocols that were available having to communicate with each other. To reduce this complexity, the communication industry formulated a plan to standardize the protocols. The first of these was adopted as a standard in 1984 and was known as the OSI Model. These common protocols are well known, and because of this, they are an area of weakness for any organization. Cybercriminals have been able to research these protocols in detail and have been able to identify flaws that will allow them to gain access to devices using the protocol.

Dependencies

ICS are complex in their nature because of the interlinks that have evolved as technology has been introduced and systems no longer work in isolation. This complexity is described in terms of the interdependency and dependency between components. The main risk is that this complexity has wide-reaching effects when failures occur and can include loss of life.

The key authors in the subject of complexity are Rinaldi et al. (2001) who were the initial presenters of the concept of dependencies and interdependencies. These definitions are frequently referred to and are in use in current literature such as the US Department of Energy (US DOE) report (Argonne National Laboratories, 2015) who quote Rinaldi et al. (2001) to ensure the consistency of the risk and resilience assessment methodology standards:

- Dependency—the reliance or influence of one infrastructure on another through a connection
- Interdependency—the reliance of influence of two infrastructure on each other with a bidirectional connection

Although the US Department of Energy (US DOE) in their report (Argonne National Laboratories, 2015) uses these isolated definitions, they agree with the view of others (European Union Agency for Cybersecurity, 2017; Lauge et al., 2015) that infrastructures cannot be taken into consideration in isolation of the dependencies and interdependencies that exist. The US DOE explanation is based around the interactions between environments. They take the description of a dependency back to the fundamental concept of a control system in having an input that is transformed and then supplies an output which acts as an input to another environment. They further develop the idea into three different types of dependency such as upstream, internal, and downstream.

Complexity

The nature of the size of ICS systems means that the understanding of the systems complexity may not be complete. This could be for various reasons; it is possible that an industry sector is unable to share information, e.g., the nuclear industry, and it is only during a crisis or failure that this crossover of information occurs. Another reason for misunderstanding complexity is that many of these systems have evolved and this evolution has not created a complete set of information on the systems that are in place. It is difficult to have knowledge of every single element in an ICS system which is the fundamental requirement to identify all the interdependencies and dependencies. Another problem is that there are a lot of legacy systems, and having been in place for maybe 50 years, the experience and in-depth knowledge have disappeared as staff have retired.

The complexity of such systems brings with them a higher level of risk. When working in isolation, control systems were protected. Now that they communicate with others, they do not have the same level of protection. Some industries are not able to share information, and this leaves those interconnected at an increased risk. Collaboration is important to be able to deal with complexity of the system of systems effectively.

3.4 Organization Structures

An organization can in the way that it is organized support and reduce the challenges in ICS security. The elements for an organization to consider are:

- Culture and structure
- Financial
- Policies and procedures

The culture of an organization is understood as the group goal and the working relationships. There are different ways to describe the culture of an organization, and the culture will support the leadership and management of the organization. Factors such as empowerment, formality, communication, goal orientation, and bureaucracy will define the culture, but the challenge is to create a working environment that supports the employees and allows them to feel that they can be honest and open about issues. This is important in ICS because a small mistake could be a disaster and employees must be able to flag these as early as possible to reduce the impact. This is known as a no-blame culture.

The physical structure of the organization is a companion of the culture of the organization. It can be rigid or flexible, and many organizations that are rigid are not able to adapt to new situations. In ICS new situations will be a result of the challenges of the working environment, and the organization structure needs to be flexible enough to be able to adapt quickly and continuously improve.

The financial structure of an organization can also be a challenge. Security is an issue that can need addressing in a reactive manner and not proactive. This means that budgets and formal financial processes must be flexible enough for security teams to be able to respond to challenges as early as possible.

The policies and procedures of an organization are important as they support the organization, the leadership, and the employees to undertake their work in a safe manner. ICS organizations must comply with certain regulations and will therefore have fundamental policies such as security in place. The fact that these are in place does not guarantee that they are being used. The challenge for the organization is to not just have these procedures and policies in place but to make sure that they are followed. As stated earlier it is not assured that an awareness of cybersecurity decreases the risk of a cyber-attack. One of the procedures that can support these challenges is the continuous development process. This allows organizations to learn from their experience and improve their processes.

4 Conclusion and Future Work

In this chapter we have reviewed the definitions of the IoT and ICS and compared them to identify the similarities that they have. The chapter has discussed the challenges surrounding these new environments taking into consideration the operation of Industrial Control Systems. The use of ICS too describes the challenges and identifies some of the issues surrounding the operation of real-time systems. The IoT is a system that operates in real time, and therefore the challenges are similar.

In the future this work is to be developed and evolved to not only identify the challenges but also to develop some solutions to these challenges that can be utilized across the residential and commercial environments.

References

Alblabi, S. M., & Weir, G. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human Centric Computing and Information Sciences, 8*(5).

Aldawood, H., Alashoor, T., & Skinner, G. (2020). Does awareness of social engineering make employees more secure? *International Journal of Computer Applications, 177*(38), 45–49.

Argonne National Laboratories. (2015). *Analysis of critical infrastructure dependencies and interdependencies*. US Department of Energy.

Assenza, G., & Setola, R. (2019). Operational technology cybersecurity: how vulnerable is our critical infrastructure? *Contemporary Macedonian Defence, 19*(37), 9–20.

Babu, B., Liyas, T., Muneer, P., & Varghese, J. (2017). Security issues in SCADA based industrial control systems. In *2nd International conference on anti-cyber crimes, Abha*.

Bodungen, C. E., Singer, B. L., Shbeeb, A., Hilt, S., & Wilhoit, K. (2017). *Hacking exposed industrial control systems* (1st ed.). McGraw-Hill.

Bostrom, R. P., & Heinen, S. J. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS Quarterly, 1*(3), 17–32.

Centre for the Protection of National Infrastructure. (2021). *Internet of things and industrial control systems.* Centre for the Protection of National Infrastructure [Online]. Retrieved April 1, 2021, from https://www.cpni.gov.uk/internet-things-and-industrial-control-systems.

Collins. (2016). *Collins English dictionary and thesaurus*. HarperCollins.

Doan, D. (2006). *Commercial Off the Shelf (COTS) security issues and approaches*. Naval Postgraduate School.

Ernst and Young Global Limited. (2020). *Global information security survey*. Ernst and Young Ltd.

European Union Agency for Cybersecurity. (2017). *Communication network dependencies for ICS/SCADA Systems*. European Union Agency for Cybersecurity.

S. I. Extraction. (2014). *Project SHINE findings report*. Creative Commons.

Ginter, A. (2016). *SCADA security what's broken and how to fix it* (1st ed.). Calgary.

Greengard, S. (2015). *The internet of things* (1st ed.). MIT Press.

Hadnagy, C. (2011). *Social Engineering The art of human hacking* (1st ed.). Wiley Publishing.

Hagerott, M. (2014). Stuxnet and the vital role of critical infrastructure operators and engineers. *International Journal of Critical Infrastructure Protection, 7*, 244–246.

Hayden, E., Assante, M., & Conway, T. (2014). *An abbreviated history of automation and industrial control systems and cybersecurity*. SANS Institute.

Johnson, S. (2013). Safety and security in SCADA systems must be improved through resilience based risk management. In C. Laing, A. Baddi, & P. Vickers (Eds.), *Securing critical infrastructures and critical control systems: Approaches for threat protection* (pp. 286–300). IGI Global.

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395–411.

Kilman, D., & Stamp, J. (2005). *Framework for SCADA security policy*. Department of Energy.

Knapp, E. D., & Langill, J. T. (2015). *Industrial network security: Securing critical infrastructure networks for smart grid, scada, and other industrial control systems* (1st ed.). Syngress.

Kriaa, S., Bouissou, M., & Laarouchi, Y. (2019). A new safety and security risk analysis framework for industrial control systems. *Institute of Mechanical Engineers, 233*(2), 151–174.

Kupiers, D., & Fabro, M. (2006). *Control systems cyber security: Defense in depth strategies*. Idaho National Laboratories.

Lauge, A., Hernantes, J., & Sarriegi, J. M. (2015). Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *International Journal of Critical Infrastructure Protection, 8*, 16–23.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of things: A literature review. *Journal of Computer and Communications, 3*(5), 164–173.

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security, 27*(2), 233–272.

Maslow, A. (2013). *A theory of human motivation* (1st ed.). Wilder Publications.

Miller, M. (2015). *The internet of things how smart TV's, smart cars, smart homes, and smart cities are changing the world* (1st ed.). Que.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers and Security, 59*, 186–209.

National Institute of Standards and Technology. (2008). *Guide to industrial control systems security*. NIST.

National Institute of Standards and Technology. (2011). *Managing information security risk*. US Department of Commerce.

National Institute of Standards and Technology. (2021, April 15). *COTS*, National Institute of Standards and Technology [Online]. Retrieved April 15, 2021, from https://csrc.nist.gov/glossary/term/commercial_off_the_shelf.

Oosthuizen, R., & Pretorius, L. (2016). Assessing the impact of new technology on complex sociotechnical systems. *South African Journal of Industrial Engineering, 27*(2), 15–29.

Postscapes. (2020, 1 January). *Internet of things (IoT) history* [Online]. Retrieved March 30, 2021 from https://www.postscapes.com/iot-history/.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. (2001). Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11–24.

Simon, T. (2017). *Critical infrastructure and the internet of things*. Centre for International Governance Innovation and Chatham House.

Slay, J., & Miller, M. (2007). Lessons learned from the Maroochy Water Breach. In *International conference on critical infrastructure protection* (Vol. 253, pp. 73–82). Springer.

Techopedia. (2021, April 1). *Legacy system. Janalta Interactive* [Online]. Retrieved April 15, 2021, from https://www.techopedia.com/definition/635/legacy-system.

Trist, E. (1981). The evolution of socio-technical systems a conceptual framework and an action research program. In *Perspectives on organizational design and behaviour* (pp. 19–75). Wiley & Sons.

Tucker, M. (2015). *TE framework: A framework for securing COTs applications*. SANDIA National Laboratories.

United States Nuclear Regulatory Commission. (2016). *Historical review and observations of defense-in-depth*. Brookhaven National Laboratory.

Wu, P. P.-y., Fookes, C., Pitchforth, J., & Mengersen, K. (2015). A framework for model integration and holistic modelling of socio-technical systems. *Decision Support Systems, 71*, 14–27.