Summer 7-19-2017

Security for Complex Cyber-Physical and Industrial Control Systems: Current Trends, Limitations, and Challenges

Dabeeruddin Syed
Masdar Institute, UAE, dsyed@masdar.ac.ae

Tao-Hung Chang
Masdar Institute, UAE, tchang@masdar.ac.ae

Davor Svetinovic
Masdar Institute, UAE, dsvetinovic@masdar.ac.ae

Talal Rahwan
Masdar Institute, UAE, trahwan@masdar.ac.ae

Zeyar Aung
Institute Center for Smart and Sustainable Systems (iSmart) Masdar Institute of Science and Technology, zaung@masdar.ac.ae

Security for Complex Cyber-Physical and Industrial Control Systems: Current Trends, Limitations, and Challenges

Completed Research Paper

Dabeeruddin Syed
Khalifa University of Science and Technology, Masdar Institute
Block 1A Masdar City, Abu Dhabi, UAE
dsyed@masdar.ac.ae

Tao-Hung Chang
Khalifa University of Science and Technology, Masdar Institute
Block 1A Masdar City, Abu Dhabi, UAE
tchang@masdar.ac.ae

Davor Svetinovic
Khalifa University of Science and Technology, Masdar Institute
Block 1A Masdar City, Abu Dhabi, UAE
dsvetinovic@masdar.ac.ae

Talal Rahwan
Khalifa University of Science and Technology, Masdar Institute
Block 1A Masdar City, Abu Dhabi, UAE
trahwan@masdar.ac.ae

Zeyar Aung
Khalifa University of Science and Technology, Masdar Institute
Block 1A Masdar City, Abu Dhabi, UAE
zaung@masdar.ac.ae

Abstract

Today's society relies upon the smooth and secure functioning of the mission-critical infrastructures and their services. Much of this critical infrastructure relies on the complex cyber-physical systems and the industrial control systems. In recent years, securing these two types of systems has been a top priority due to a significant increase in number of attacks. Most of these systems are often several decades old, and they were developed without significant consideration of the security requirements. As such, there is an urgent need to protect these cyber-physical and industrial systems from external vulnerabilities. In this paper, we present a survey of the cyber-physical and industrial control systems, and explore the possibility and necessity for security of such systems. We discuss the various types of cyber-physical and industrial control systems currently being used, assess the vulnerabilities of such systems, discuss the literature on the cyber-physical and industrial control systems, and examine some works that propose security standards and models for these types of systems.

Keywords: Security, cyber-physical systems, industrial control systems

Introduction

Industrial control systems are control systems used in industrial production, which include supervisory control and data acquisition systems (SCADA), distributed control systems (DCS) and programmable logic controllers (PLC). Such systems are deployed in the operation and control of critical infrastructures (Creery and Byres 2005). Due to the increased reliance on the information technology (IT) in these systems, they are becoming increasingly related to *Cyber-physical systems* (cyberphysicalsystems.org 2015), i.e., the systems in which physical processes are merged with computational and networking elements, whereby operations are monitored, coordinated, controlled and integrated by a computing and communication core (Rajkumar et al. 2010). Securing critical computer systems – such as industrial control systems and cyber-physical systems – is becoming increasingly important, especially when they are used in applications with huge impacts on public safety, health, social life, and economy, or when they collect sensitive and private information about the physical environment (Lu et al. 2014).

One of the first prominent cyberattacks on an industrial control system took place before the Internet era. CIA added a Trojan horse to gas pipeline control software that the Soviet Union obtained from a company in Canada. It caused a huge explosion in the Soviet Union's Trans-Siberian gas pipeline in 1982 (Mazanec 2015). A more recent high profile attack was by a worm called "Stuxnet" in 2010 (Langner 2011). It targeted industrial computer systems and caused substantial damage to Iran's nuclear program. The industrial control system at the nuclear facility was not connected to the Internet; but the worm infected the system via a compromised USB flash drive.

Recently, there has been an increasing number of cyberattacks on the oil and gas sector in the Middle East (Cherrayil 2016). So far those attacks have not made any substantial damages yet. However, in the event of successful widespread attacks, this can result in a major economic damage to the victim country, and can even possibly lead to a global energy crisis.

Cyberattack on Ukraine power grid took place on 23 December 2015. It is a regarded to be the first known successful cyberattack on a power grid (Lee et al. 2016). Hackers were able to successfully compromise information systems of three energy distribution companies in Ukraine and temporarily disrupt electricity supply to the end consumers up to 6 hours.

In 2015, ISIS (Islamic State of Iraq and Syria) terrorists tried to hack into the United State's energy grid system – but were not successful (Pagliery 2015).

In the book "*Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*", Koppel (2015) described a hypothetical event in which one of the Untied State's three electric power grids was successfully cyberattacked by an advanced adversary. The author stated that the United State was currently (as of 2015) so unprepared for such an attack, and the consequences would be unprecedented. He speculated that:

> "Imagine a blackout lasting not days, but weeks or months. Tens of millions of people over several states are affected. For those without access to a generator, there is no running water, no sewage, no refrigeration or light. Food and medical supplies are dwindling. Devices we rely on have gone dark. Banks no longer function, looting is widespread, and law and order are being tested as never before."

The author also suggested some disaster preparation and planning for such a catastrophic cyberattack.

All the above examples emphasize the importance of security of the industrial control and cyber-physical systems on whose services we rely more and more and eventually become integral parts of our daily lives in a modern society.

The remainder of this paper is structured as follows. Section "Background" provides some necessary background on cyber-physical systems and industrial control systems. Section "Security Threats" discusses some of the potential security threats that need to be addressed when handling such systems. Section "Impacts and Limitations" outlines the strengths and weaknesses of each type of systems. Section "Research Challenges" discusses some of the security-related research challenges that need to be overcome. Finally, Section "Conclusion" concludes the paper.

Background

This section provides the necessary background information on cyber-physical systems and industrial control systems.

Cyber-Physical Systems

Due to the recent advancements in the technology of sensors and small computing devices (Gungor and Hancke 2009) the cost of producing advanced technical devices, such as those used in information and network systems, has dropped significantly. Furthermore, the capabilities of those devices have increased significantly in recent years. These advancements, as well as the increasing availability and reliability of wireless communication and internet bandwidth, have led to the advent of Cyber-Physical Systems (cyberphysicalsystems.org 2015). These are usually comprised of networked agents such as, e.g., sensors, actuators, control units and communication devices. Typically, such systems possess (some of) the following characteristics (Neuman 2009):

1. Input (and possibly also feedback) from physical surroundings;
2. Distributed control and management;
3. Uncertainty in terms of status and readings;
4. Real-time performance requirements;
5. Wide geographical distribution over locations with potentially limited physical security; and
6. Multi-scale and so-called *system-of-systems* control characteristics.

The main structure of a cyber-physical system is illustrated in Figure 1. In short, the system communicates with the physical devices and sends the control commands for those devices to work safely and efficiently in real-time (Rajkumar et al. 2010). The information flow of a cyber-physical system is illustrated in Figure 2. Here, the process of collecting data from sensors, and sending that data to the controllers, is called “estimation”. On the other hand, the signals coming from the controllers to the physical system are called “control commands.” Such a system is widely applied across a variety of industries, including smart grid, medical care, aerospace systems, autonomous vehicles, defense systems and industrial automation.

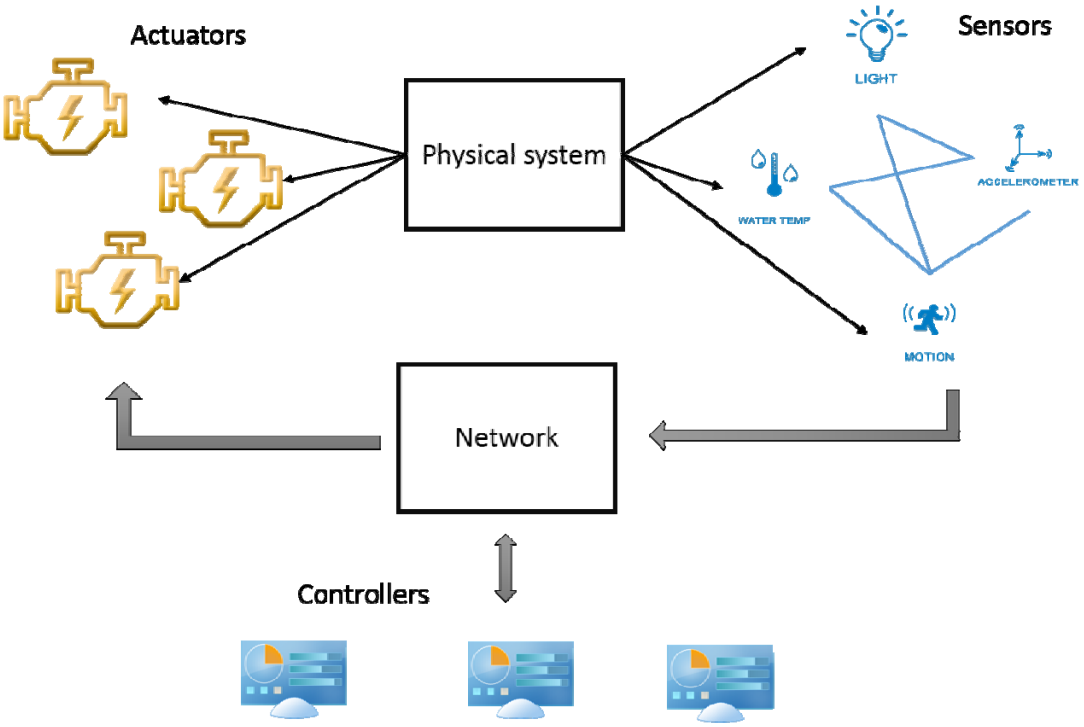

Figure 1. Cyber-physical system structure

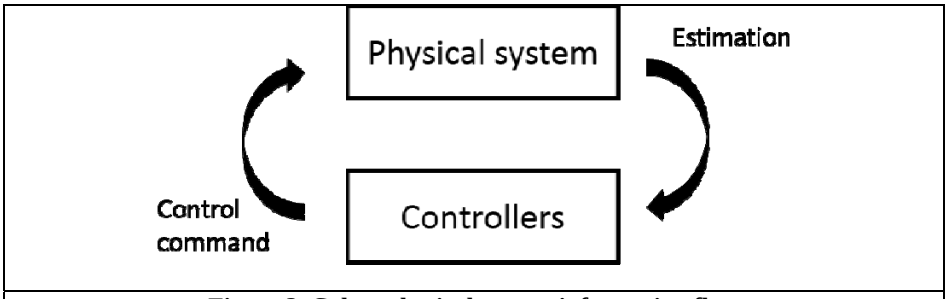

Figure 2. Cyber-physical system information flow

Industrial Control Systems

The industrial control systems are developed to control the industrial production and distribution process (Falco et al. 2004). They are designed to meet performance, reliability, safety and flexibility requirements. They are also increasingly incorporating connectivity features and remote access control. Their networks contain computers that provide critical services and perform essential tasks for the critical infrastructure. For example, this infrastructure could include the followings (Sivaraman 2015):

1. Power generation and distribution centers;
2. Nuclear reactors;
3. Dam control and hydro power stations;
4. Oil and gas refineries;
5. Large scale manufacturing process industries;

6. Water treatment and distribution plants; and
7. Telecommunications and information technology.

A typical architecture of a networked industrial control system is illustrated in Figure 3.

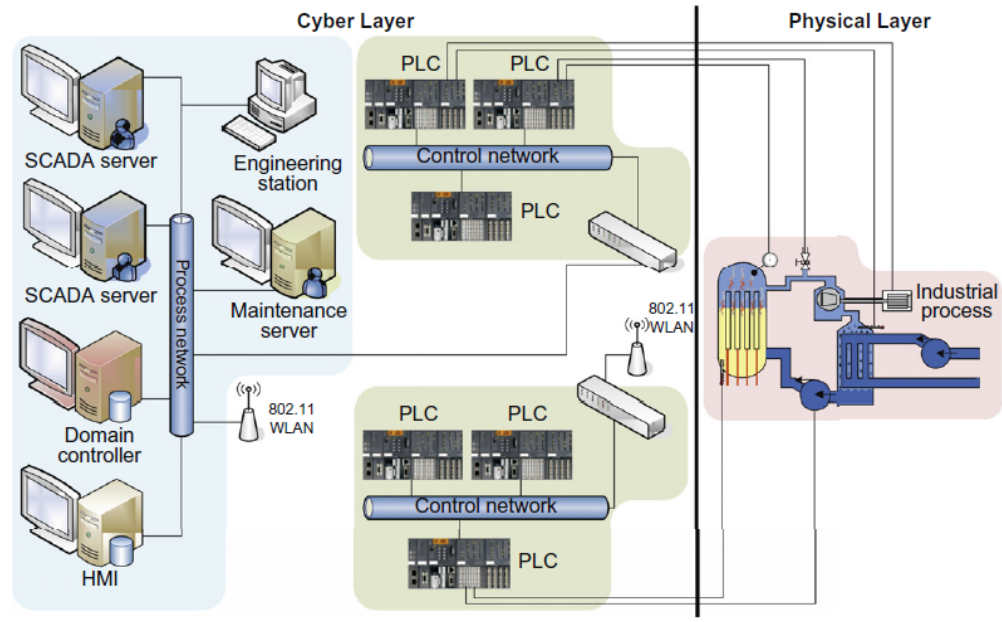

Figure 3. Typical architecture of a networked industrial control system

Due to the increased connectivity and openness of the above critical infrastructure framework, the industrial control systems are exposed to the threats of security breaches and vulnerabilities. Since the industrial production may deal with oil, electricity, gas, water distribution, or treatment of industrial wastes, cyber attacks on the industrial control systems may pose serious threats to the public health and safety, and may invoke significant damage to the environment. They may also negatively affect the production, generation or distribution of products, thus leading to substantial financial losses.

Security Threats

This sections discusses the potential security threats that need to be taken into consideration. This discussion is divided into two subsections, the first subsection focuses on the cyber-physical systems, whereas the second subsection focuses on the industrial control systems.

Cyber-Physical Systems

When discussing the characteristics of cyber-physical systems, Neuman (2009) emphasized the need to take security into account right from the start of the design process. To this end, he suggested a design approach that integrates the security into the core design of such systems. He also presented a research roadmap that highlights some requirements needed to enable such a secure design approach.

Cardenas et al. (2008a) identified a number of security-related issues with cyber-physical systems that need to be addressed, and highlighted a number of challenges that need to be overcome in order to address those issues. To this end, the authors focused on two major security goals of information security, namely *integrity* and *availability*. The authors also pointed out where attacks might take place. Among the many possible types of attacks, the authors focused on two types, namely *deception attacks*, and *denial of service* (DoS) attacks. Specifically, deception attacks are those where the adversary sends false information to the controllers; these can compromise the integrity of the system, as they lead to wrong control commands from controllers. In contrast, DoS attacks focus on disrupting the availability of the cyber component; these clearly compromise the availability of the system, especially for a cyber-physical system that is time sensitive such as, e.g., a medical care system.

Xu et al. (2008) argued that due to the nature of cyber-physical systems, many implementations need to be installed on computing devices, and need to communicate through *mobile and ad hoc network* (MANETs). However, there are some security issues with MANETs, where the attackers can have an access point to the system. These security challenges stem from the fact that MANETs lack infrastructure, and face dynamic topology changes. Previous studies proposed the public key infrastructure and identity-based public key cryptography (Deng et al. 2004; Zhou and Haas 1999). However, those require a complex certificate management process. After that a certificateless public key cryptography (CLS) was proposed; while these resolved the certificate management issue, their drawback is the need for high computational power (Al-Riyami and Paterson 2003). Consequently, the author presented the McCLS scheme, which resolved the computational overhead problem, and improved the system's resistance against certain types of attacks, such as *black hole* attacks and *rushing* attacks.

Singh and Sprintson (2010) focused on *reliability assurance*. More specifically, they surveyed alternative techniques from the literature on electric power grid system, and discussing how these can be applied to cyber-physical systems. To this end, the authors mentioned that a power grid system mainly consists of three parts: (1) a current carrying part, (2) a protection system, and (3) a cyber part. However, existing reliability techniques focus on the current carrying part, with a few exceptions that also consider the protection system. As such, these techniques cannot readily be applied to the cyber-physical system, mainly due to the inherent dimensionality and complexity of the system. In fact, as the authors pointed out, the literature on the reliability of the cyber part is practically non-existent. Finally, the paper suggested that future studies on reliability should focus on local, degrading and catastrophic failures.

Gamage et al. (2010) proposed an information flow security enforcement mechanism for cyber-physical systems. More specifically, they argued that the two main parts of such a system – the cyber part and the physical part – should not be considered separately, or else there could be an unintended information flow. As such, cyber-physcial security should be considered at the system level. The authors also compared two main kinds of system security mechanisms, namely *access control*-based, and *information flow*-based mechanisms. As for the first mechanism, i.e., access control, is not sufficient to control the information or data propagation. If certain parts of the physical devices are compromised, the attacker can still gain access to sensitive information. Accordingly, the authors suggested using the information flow-based mechanisms instead. Finally, the authors presented an *event compensation*-based framework to enhance the information flow properties in the cyber-physical system.

Jiang et al. (2010) focused on the problem of time-critical messages in cyber-physical systems. Specifically, they pointed out that some of the messages in cyber-physical systems are time-sensitive, and if those messages are not delivered on time, they may lead to substantial financial losses, or even losses of lives. For instance, the cyber-physical system in a medical care system or an aircraft flight control system is extremely time sensitive. However, the present approaches expose the information in such systems to *confidentiality attacks*. The authors proposed a number of confidentiality-aware message scheduling policies for security in the cyber-physical environment. To this end, they proposed a heuristic algorithm, and demonstrated how it could enhance security give a set of messages. Furthermore, the algorithm achieved greater security gains compared to other alternative methods from the literature (e.g., 57.8% more than SV-RND, 18.5% more than SV-Greedy).

Industrial Control Systems

Byres and Lowe (2004) analyzed the *Industrial Security Incident Database* (ISID), and showed how even the supposedly immune systems of SCADA and process control, which are based on proprietary networks and hardware, can be compromised in terms of security. Further, they emphasized the fact that companies may need to reassess the security risk models for their industrial control systems. To this end, the authors proposed the following steps as an in-depth solution to the security issues in industrial control systems.

1. deploying of a greater number of internal zone defenses;
2. deploying of a greater number of intrusion detections;
3. re-evaluating boundary security, taking into consideration all possible intrusion points; and
4. security robustness design and testing before deployment.

Falco et al. (2004) explained the development of a laboratory scale testbed by the National Institute of Standards and Technology (NIST), which comprised of several implementations of typical industrial control and networking equipment as well as relevant sensors and actuators. The authors also highlighted the fact that the current industrial control systems are developed primarily to meet the needs of performance, reliability, safety and flexibility, while neglecting the security requirements. This lack of attention to the security requirements could lead to vulnerabilities from the operational system components' point of view. To curb this, the Process Control Security Requirements Forum (PCSRF) has put a number of efforts to address the security requirements of industrial control systems and components. To this end, the aforementioned testbed has been developed by the NIST, and work on this testbed has focused on and work on this testbed has focused thus far on testing the performance of industrial networking equipment, as well as the developing tests for measuring the effects of security implementations on the operation of industrial control systems. The testbed developed by the NIST is illustrated in the Figure 4 (Falco et al. 2004).

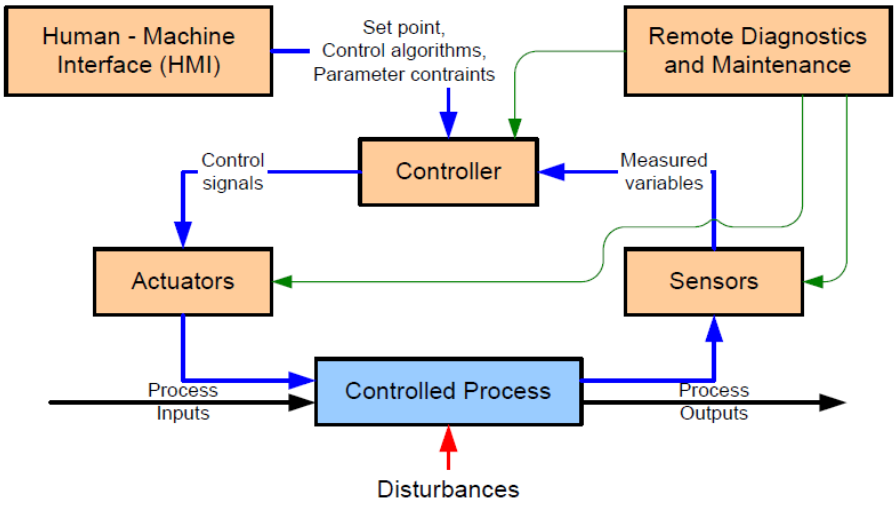

Figure 4. Generic industrial control system in the testbed by the National Institute of Standards and Technology (NIST)

Impacts and Limitations

In this section, we discuss the potential advantages and disadvantages of the systems under consideration. As with the previous sections, we divide this section into two subsections; the first focuses on cyber-physical systems, while the second focuses on industrial control systems.

Cyber-Physical Systems

The on-going development of cyber-physical systems could lead to new opportunities to our society. The system allows us to achieve goals that are otherwise very hard, if not impossible, to achieve. It not only brings opportunities to various new industries, but also refines and elevates the quality and efficiency of various traditional industries. For example, we can apply a cyber-physical concept to a power system to achieve a blackout-free electricity generation. We can even use a cyber-physical approach to increase the electricity efficiency in buildings by tightly integrating their physical and cyber connection.

In addition, cyber-physical systems have multiple applications in health care systems. First, the cyber-physical can potentially have a significant impact on biological research. For example, consider the development of automated approaches that use high throughput microscopes and robotic equipment to perform experiments in larger numbers and on a larger scale. Such approaches use controlled cyber-physical systems of highly sophisticated models and algorithms. The impact that such approaches bring to the biological research could potentially facilitate the development of new treatments and medicine. Second, cyber-physical system can also provide home care for seniors. This is especially important as the senior population in the U.S. is expected to reach 70 million by 2030, and the expense of health care for the country will continue to increase over time. By combining the cyber-physical infrastructure with the health care system, one can remotely monitor the essential parameters of patients and conduct any necessary procedures or treatment based on the available information. With the proper infrastructure, the patients with minor disabilities are more likely to have the ability to live independently.

To achieve the implementations above, it is crucial that the cyber-physical system is secure in every aspect. For example, electricity shutdown, especially in health care systems, could lead to substantial life or financial losses. However, there are many challenges that need to be addressed in the field of cyber-physical systems. These challenges will be discussed later on in Section “Research Challenges”.

Industrial Control Systems

Industrial Control Systems are IT systems that control the industrial production. Nonetheless, they still have some distinguishing features that make them hard to secure. Some of these features include the following (Luiijf, and te Paske 2015; Creery and Byres 2005):

1. The industrial control systems are typically used in the critical infrastructure to control and monitor the critical processes. As such, the prime priority becomes to ensure that these processes are monitored and controlled without interruptions. The fact that the continuity is of extreme importance to the industrial control systems causes a strong reluctance to apply or make any changes that could harm the continuity of control and performance in the system. Consequently, any updates such as, e.g., security upgrades or anti-virus updates, to the systems are considered highly risky to its continuous operation.
2. Another distinguishing characteristic of industrial control systems is their lifespan. In particular, the different system components have different and asynchronous lifespans and lifecycles. This fact makes it impractical to renew the entire industrial control system framework as a whole. Another concern in terms of upgrades is the high cost of migration. Consequently, a coherent security approach for the whole system should be implemented gradually, one step at a time, while taking into consideration the cost constraints.

Research Challenges

In this section, we discuss some of the security-related research challenges from the perspective of cyber-physical systems and the perspective of industrial control systems respectively.

Cyber-Physical Systems

A cyber-physical system is composed of many different components, ranging from physical to cyber, which provide many access points for the attackers. When studying the security of a cyber-physical system, there are many research directions that one can take. Two of the main such directions in the literature are: (1) cyber-physical operations in power systems, and (2) information flow within the cyber-physical system. As for the power systems, the study by Rajkumar et al. (2010) identified some of the challenges that are currently faced when dealing with such systems. In particular, a system must be able to handle the failure of distributed elements such as generators, and it has to be able to handle multiple time scale interaction of distributing control. Moreover, the system must be able to continue to function even when under attack. Overall, the major challenge of cyber-physical operations in power system stems from the large number of components and the interactions between them. This creates the need for an operation strategy that can organize those interactions.

The second challenge in a cyber-physical system is the security of information flow in it. Here, due to the large scale of a typical cyber-physical system, one has to consider the system as whole when attempting to prevent unintentional information flow. To date, there are mainly two types of methods that can handle this: (1) *access control*-based methods, and (2) *information flow*-based methods. In this context, one particularly relevant type of attack is the *denial of services* (DoS) attack, which hampers the system's ability to be accessible and usable upon demand. This is particularly relevant to the cyber-physical system as most interactions therein are time-sensitive, and signals have to be delivered and executed on time. Such DoS attacks can be handled by access control, which prevents attackers from gaining access to sensitive information within the system, and ensures that information is safely delivered to the proper components on time.

Overall, the research challenges faced when dealing with cyber-physical systems can be summarized as follows:

1. Reduce testing and integration time and costs;
2. Use of cyber-physical infrastructure for the evolution of energy-aware building and cities;
3. Physical critical infrastructure that calls for preventive maintenance; and
4. Self-healing cyber-physical systems for one-off applications.

Having discussed the main research challenges from the cyber-physical systems' perspective, in the following subsection we discuss the main challenges from the industrial control system's perspective.

Industrial Control Systems

The main challenges and concerns that need to be overcome for securing the industrial control systems are as follows:

1. When industrial control systems were first deployed several years ago, security aspects were not a major concern, and so were not addressed adequately (Byres and Lowe 2004);
2. Current industrial systems are generally decades old (Sivaraman 2015);
3. Aggravating requirements (e.g., to communicate data between the enterprise, corporate and DCS networks) can lead to cyber-attack vulnerabilities (Gupta and Chow 2010);
4. Vulnerability to denial of service (DoS) attacks as service and continuity is of prime concern in the industrial control system framework (Cardenas et al. 2008a);
5. Current communication protocols were designed without addressing the various security aspects (Byres and Lowe 2004);
6. Widespread use of devices that lack adequate security features (Gungor and Hancke 2009);
7. Various database-related security vulnerabilities (Stouffer et al. 2011);
8. Lack of encryption and authentication (Byres and Lowe 2004);

9. Non-existent patching or security critical updates of software and/or firmware (Creery and Byres 2005).

Finally, the recent trend of the development and the integration with the Internet of Things (IoT) will even further exacerbate these security challenges. IoT poses a number of unique security threats and issues (Alqassem and Svetinovic 2014). In addition to a need for the early-stage security requirements modeling, the integration with IoT is creating a need for effective breakdown and analysis of requirements at the various abstraction levels, with a particular emphasis on the architecture security requirements (Svetinovic 2003). The early-stage requirements analysis and modeling should be combined with effective analysis of missing, outdated, or changed requirements for the legacy cyber-phisical and industrial control systems using semi- or fully-automated requirements data mining approaches, e.g., (Casagrande et al. 2014).

Conclusion

In this survey paper, we presented different aspects of security from the perspective of cyber-physical systems and the perspective of industrial control systems. We have covered several papers that discussed various security issues, and the areas of vulnerability that need to be handled. Moreover, various research challenges have been covered, such as the tradeoff between functionality and potential vulnerability, or the impact and limitation of the different systems and models. Suggestions to face those challenges have also been presented. As evident from the various works covered by our survey, the cyber-physical and industrial control systems need additional security requirements. This is primarily due to the integration of physical control, the real time requirements, and their common applications to the critical infrastructure. The goal of securing cyber-physical and industrial control systems can be achieved only if the security of the systems is taken into account at the very beginning of the design stage, by considering the information flow, control and availability requirements, to ensure that security is considered in all of the specifications and not just as a simple incorporation of existing add-on security mechanisms.

References

Al-Riyami, S. S. and Paterson, K. G. 2003. “Certificateless public key cryptography,” in *Advances in Cryptology-ASIACRYPT 2003*, pp. 452–473.

Alqassem, I. and Svetinovic, D. 2014. “A taxonomy of security and privacy requirements for the Internet of Things (IoT),” in *Proceedings of the 2014 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pp. 1244–1248.

Byres, E. and Lowe, J. 2004. “The myths and facts behind cyber security risks for industrial control systems,” in *Proceedings of the VDE Congress Volume 116*, pp. 213–218.

Cardenas, A. A., Amin, S., and Sastry, S. 2008. “Research challenges for the security of control systems,” in *Proceedings of the 3rd Conference on Hot Topics in Security (HotSec)*, article 6.

Cardenas, A. A., S. Amin, and Sastry, S. 2008. “Secure control: Towards survivable cyber-physical systems,” in *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops (ICDCS)*, pp. 495–500.

Casagrande, E., Woldeamlak, S., Woon, W. L., Zeineldin, H. H. and Svetinovic, D. 2014. “NLP-KAOS for Systems Goal Elicitation: Smart Metering System Case Study,” in *IEEE Transactions on Software Engineering* (40), pp. 941–956.

Cherrayil, N. K. 2016. “Mideast oil and gas sector faces wider cyberattacks,” *Gulf News*, June 30, 2016, http://gulfnews.com/business/sectors/technology/mideast-oil-and-gas-sector-faces-wider-cyberattacks-1.1854885, [Online; accessed 24-April-2017].

Creery, A. and Byres, E. J. 2005. “Industrial cybersecurity for power system and SCADA networks,” in *Proceedings of the Industry Applications Society 52nd Annual Petroleum and Chemical Industry Conference (PCIC)*, pp. 303–309.

cyberphysicalsystems.org, “Cyber-Physical Systems,” http://cyberphysicalsystems.org/, [Online; accessed 28-November-2015].

Deng, H., Mukherjee, A., and Agrawal, D. P. 2004. “Threshold and identity-based key management and authentication for wireless ad hoc networks,” in *Proceedings of the 2004 International Conference on Information Technology: Coding and Computing (ITCC) Volume 1*, pp. 107–111.

Falco, J. Gilsinn, J., and Stouffer, K. 2004. "IT security for industrial control systems: Requirements specification and performance testing," in *Proceedings of the 20th Annual NDIA Homeland Security Symposium and Exhibition*, pp. 1–15.

Gamage, T. T., McMillin, B. M., and Roth, T. P. 2010. "Enforcing information flow security properties in cyber-physical systems: A generalized framework based on compensation," in *Proceedings of the IEEE 34th Annual Computer Software and Applications Conference Workshops (COMPSACW)*, pp. 158–163.

Genge, B., Siaterlis, C., Fovino, I. N., and Masera, M. 2012. "A cyber-physical experimentation environment for the security analysis of networked industrial control systems," *Computers and Electrical Engineering* (38), pp. 1146–1161.

Gungor, V. C. and Hancke, G. P. 2009. "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Transactions on Industrial Electronics* (56), pp. 4258–4265.

Gupta, R. A. and Chow, M.-Y. 2010. "Networked control system: Overview and research trends," *IEEE Transactions on Industrial Electronics* (57), pp. 2527–2535.

Jiang, W., Guo, W., and Sang, N. 2010. "Periodic real-time message scheduling for confidentiality-aware cyber-physical system in wireless networks," in *Proceedings of the 2010 5th International Conference on Frontier of Computer Science and Technology (FCST)*, pp. 355–360.

Koppel, T. 2015. *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*, Broadway Books, New York City, NY, USA.

Langner, R. 2011. "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security and Privacy* (9), pp. 49–51.

Lee, R. M., Assante, M. J., and Conway, T. 2016. "Analysis of the cyber attack on the Ukrainian power grid. Defense use case," Technical Report, Electricity Information Sharing and Analysis Center, Washington, DC, USA.

Lu, T., Guo, X., Li, Y., Peng, Y., Zhang, X., Xie, F., and Gao, Y. 2014. "Cyberphysical security for industrial control systems based on wireless sensor networks," *International Journal of Distributed Sensor Networks* (2014), article ID 438350.

Luiijf, H. A. M. and te Paske, B. J. 2015. "Cyber security of industrial control systems," in *Proceedings of the 2015 Global Conference on CyberSpace (GCCS)*, pp. 1–59.

Mazanec, B. M. (2015). *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*. University of Nebraska Press, Lincoln, NE, USA.

Neuman, C. 2009, "Challenges in security for cyber-physical systems," in *Proceedings of the DHS Workshop on Future Directions in Cyber-Physical Systems Security*, 2009, pp. 1–4.

Pagliery, J. 2015. "ISIS is attacking the U.S. energy grid (and failing)," *CNN*, October 16, 2015, http://money.cnn.com/2015/10/15/technology/isis-energy-grid/, [Online; accessed 24-April-2017].

Rajkumar, R., Lee, I., Sha, L., and Stankovic. J. 2010. "Cyber-physical systems: The next computing revolution," in *Proceedings of the 2010 47th ACM/IEEE Design Automation Conference (DAC)*, pp. 731–736.

Singh, C. and Sprintson, A. 2010. "Reliability assurance of cyber-physical power systems," in *Proceedings of the IEEE 2010 Power and Energy Society General Meeting (PES)*, pp. 1–6.

Sivaraman, R. 2015. "Cyber security – ICS: Brief solution summary," Technical Report, S3tel. Integrated (i)ntelligence, Dubai, UAE.

Svetinovic, D. 2003. "Architecture-level requirements specification," in *Proceedings of the Second International Software Requirements to Architectures Workshop (STRAW)*, pp. 14–19.

Stouffer, K., Falco, J., and Scarfone, K. 2011. "Guide to industrial control systems (ICS) security," Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-82.

Z. Xu, X. Liu, G. Zhang, W. He, G. Dai, and W. Shu. 2008. "A certificateless signature scheme for mobile wireless cyber-physical systems," in *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops (ICDCS)*, pp. 489–494.

Zhou, L. and Haas, Z. J. 1999. "Securing ad hoc networks," *IEEE Network* (13), pp. 24–30.