*Research Article*

# Security Algorithm Design and Development for Cyber-Physical Systems against Cyber-Attacks

**Amit Gupta**

Asst. Professor, Department of CSE (Computer sc)

GEHU-Dehradun Campus

**Abstract**:

The term "cyber physical system" (CPS) refers to the increasingly common practise of embedding internet connectivity and sensing/transmitting capabilities into everyday things. Think about a smart home app that uses CPS gadgets. Due to its many benefits, such as saving time and money and improving human comfort and energy efficiency, the IoT has been more popular in recent years. The cyber physical system relies heavily on the low-capacity sensor node. To function as clients or hosts on the internet, these diverse components communicate with one another across a wireless network. Due to resource limits including little storage capacity, restricted computing power, and limited energy backup, the well-known security methods employed in desktop computers cannot function on these systems. SecureAuthKey is a lightweight authentication and key agreement system. Security and privacy concerns in existing constraint-based CPS applications are the focus of the proposed method. The final product is supposed to be a simple method of authenticating cyber-physical systems. Trustworthy, private, and data-protecting security algorithm for cyber-physical systems that does not compromise their ability to learn and act autonomously

**Keywords**: Cyber Physical Systems (CPS), Internet of Things (IoT), lightweight key agreement, SecureAuthKey

## Introduction

From simple instruments to complex robotic systems, automation has resulted in a wide variety of artefacts. Work-saving equipment has been changing from mechanically controlled to computer systems since the 1940s, when computers became commonplace and the field of cybernetics was established. When applied to military settings, cybernetics aimed to provide robots with senses and controls formerly reserved for human hands. Robotics (machines able to control the physical environment in a semi-autonomous fashion) grew out of this study. The Internet, imagined in the 1960s, revolutionised humankind's ability to communicate on a worldwide scale via digital networks. The convergence of mechanical labour, data processing, and communications technology may have been inevitable, but its future directions and effects are unclear at this time. The present trend in automation is variously referred to as the "Internet of Things," "Cyber Physical System," "Ubiquitous Computing," and "Pervasive Computing." All of these expressions are shorthand for various forms of technology that contributed to the design and execution of the automated system. When it comes to automating processes, cyber physical systems are becoming more popular. CPS is an active system that uses technology and a set of instructions to convert a physical system into a computerised system. With CPS, even the most fundamental tools may perform as sophisticated electronic gadgets. These gadgets often have little computing power, use little energy, and have a restricted capacity for storage. Electronic systems are being upgraded to a new generation. It's a computational approach to integrating physical systems. Computational algorithms are programmes that may be run on computers to accomplish different operations. It uses computers connected to a network to keep tabs on and control all the machinery's many moving parts. As a result, it paves the way for automated technologies that need fewer operators. Failures in the system as a result of user error are reduced as a result. Examples include "smart" house and vehicle systems. When discussing CPS, the Internet of Things is the engine that propels the whole global economy. It is being put to use in the construction of "smart" houses and urban areas.

CPS was made possible by the widespread use of the internet and other forms of electronic communication, which have had an effect on every industry from manufacturing to the sciences. Automated mechanisms were common in earlier versions of electrical appliances. However, the incorporation of CPS into these frameworks increases their responsiveness and productivity. It also links up to the web, so you can stay in touch with your gadgets no matter where you are or what time it is. Take, for example, a smart home system in which the air conditioners function automatically based on the ambient temperature. In addition to measuring temperature, it can also identify human-made things and track human movement. After processing the information, it sets the thermostat to a pleasant temperature. Because of this, the system becomes more adaptive and can make choices on the go. "intelligent and transparent interactivity between things, the physical environment, and people in order to effortlessly transfer data and deliver new applications to users" is how the CPS is described. A few trillion dollars in income will be created across several industries as a result of the surge in the popularity of connected devices in India. These industries include automotive, utilities, grid computing, smart cities, healthcare, and transportation. Numerous nations have acknowledged CPS as a vital science and technology for their future economic growth. More than 100 million euros are being invested by the European Union (EU) through the Seventh EU Framework Programme in a wide variety of connected device projects that will see widespread deployment across a wide range of sectors, including healthcare, transport, grid modernization, city management, and utility provision. Commission of Europe (2016). Smart cities, a revamped healthcare system, and advanced transit are just a few of the CPS-based initiatives India has implemented recently. Broad Public Sector Modernization and Smart Cities Plan was recently unveiled by the government of India. Short-term and long-term targets for growth are outlined, along with potential strategies for reaching them. A schedule for implementation is also included in the plan.

## Components of Cyber Physical System

Figure 1 depicts the various CPS parts. The CPS implementation was specified by these parts in various contexts. There are three main components that make up the CPS layout:

1. Things or Objects

2. Infrastructure and processing

3. Analytics and software applications.

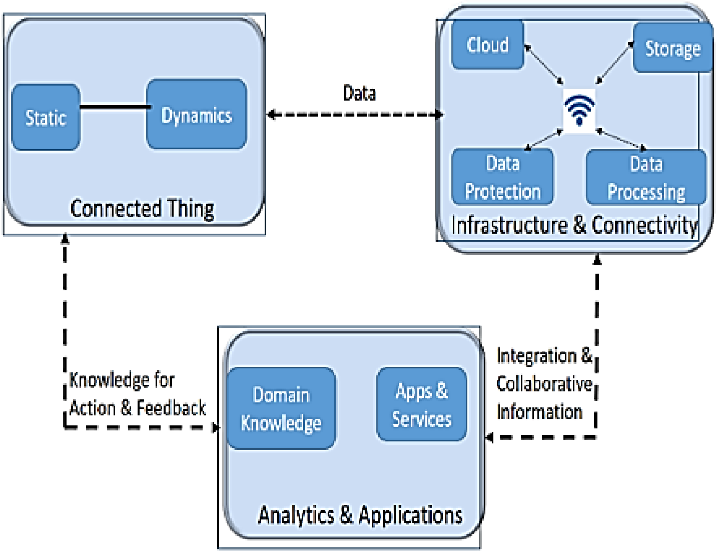


**Figure 1: Components of Cyber Physical System**

Data is gathered from the environment by artefacts or networked devices. It's possible to set up objects in either a changing or a fixed setting, depending on their characteristics. Unlike living things, inanimate objects don't adapt to their environments. They are programmed to always carry out the specified procedures. Things that can adapt to changing circumstances during execution are said to be "dynamic." In order to be useful, IoT devices need not only the capacity to gather data, but also the means to send that data to cloud-based processing service (CPS) applications. This part of the CPS offers space for data storage and processing power, as well as the means to include a wide range of intelligent processing technologies, including cloud computing, databases, and similar tools. Many Internet of Things databases are now hosted in the cloud and deployed in a variety of settings. Information is stored on a decentralised system and accessed as needed. Information is protected from many threats. Analytics and software apps employ CPS data to provide consumers additional capabilities or functions and help them make educated choices. Data gathered in a particular field will be transferred to the cloud using apps and accessed over the internet. CPS agricultural data is a good example. Sensors and CPS-based devices are used in agriculture data collection to gather information about individual plots of land and the crops grown there. This information is sent to the cloud through a mobile app developed for the agriculture industry. Information gathered online is examined and processed to provide useful recommendations for farmers and landowners. The advice will aid the farmer's crop's development.

The vast potential of CPS to enhance services in daily life is limited by many security issues that prevent its widespread use. Security methods must be implemented into CPS design and application development to avoid national-level catastrophes or data breaches. Seventy percent or more of a CPS application's data may be exploited in some way.The research utilised the top 10 devices detected in CPS infrastructure for testing purposes. On average, it found 25 security flaws in each of the test devices, for a grand total of 250 (Abusing IoT). Chaos, breakdowns. Further, Stakeouts. It's worrisome, because it highlights the need for further investigation into security procedures tailored specifically to CPS gadgets. The most prevalent security flaws were related to privacy issues, a lack of authentication techniques, insufficient authorization procedures, a lack of end-to-end security measures, exposed user interfaces, and a lack of security rules.

A smart home system is a network of interconnected electronic appliances (light bulbs, fans, locks, TVs, ovens, refrigerators, washing machines, and so on) that can be remotely controlled from a central location. Philips has introduced a connected light bulb for smart homes. The light bulb, which communicates with the home network, has had the necessary firmware installed. The ZigBee protocol is utilised as the means of connecting to the WiFi in the house. To get access to the light bulb and the rest of the home network, attackers focus on ZigBee. Using a Zigbee antenna, the attacker disconnected one of the lamps from the smart home device network before inserting malicious malware. The lightbulb will switch off if an unauthenticated person attempts to turn it on using the Philips Hue app. Once the virus enters a home network, it will infect any device that is linked to it. Constraint-based devices are utilised in a wide variety of contexts, including smart home systems, healthcare systems, and more. These gadgets don't do much of anything. Things like turning on and off, sending signals, and so forth fall under this category. Due to their restricted functionality, these gadgets feature low-powered hardware. Key features of such gadgets are processing power, storage space, and a backup power supply. The integrity in such an app is compromised. It has so little processing power, storage space, and energy backup that we couldn't even try to install and configure modern security methods in it. Many experts are focusing on developing lightweight methods that nevertheless guarantee the safety of constraint-based devices.

**Overview of Research work**

There has already been research done to solve problems and concerns with CPS security. The security of software has attracted the attention of many researchers. Some people have offered security procedures in an attempt to discover answers. Several of them are listed below. In order to implement, several current solutions provide a security framework. Communication protocols like CoAP and MQTT are employed in certain approaches.(Razetli, 2011) Researchers have developed a solution with a specific emphasis on "Smart home" technology. According to (Komninos, Philippou, & Pitsillides, 2014). In certain articles, researchers found that constraint-based devices have very rudimentary support for security mechanisms.As of 2013 (Guillet, Bouchard, & Bouzouane).Lightweight session key generation mechanisms were suggested by a select group of researchers for usage in resource-limited smart home devices. As reported by (Kim & Kumar, 2013).

**Problem Overview**

In certain CPS-based use cases, tiny and diverse physical devices are used. For heavily used CPS-based systems with improved hardware support, the existing security methods are adequate. Improved processing and memory support, as well as sufficient energy backup, are examples of such components of hardware. As a consequence, conventional safeguards work well in such a setup. Some CPS-based devices, however, may be too limited in hardware or software to use modern authentication or encryption protocols. The existing security technique cannot be applied due to hardware constraints. Existing research solutions and research projects concentrate on a single security attribute, such as authentication, privacy, or authorisation, rather than building a universal and adaptable framework that can serve the demands of a CPS-based application. Existing research solutions for CPS devices don't adhere to tried and true operating system concepts. Some security procedures did not even function at all on a distributed environment. In order to guarantee client device authentication, the vast majority of current approaches impose substantial computational complexity while ignoring other important security features. Furthermore, eavesdropping and other security issues are often overlooked during the system design process. Key distribution centre (KDC) based methods, such as SPINS (Perrig et al., 2001) and Kerberos (Steiner et al., 1988), rely heavily on the existence of a resource-rich KDC in the network to operate as a trusted entity for the key establishment. A security mechanism is essential for ensuring that only the legitimate parties are engaged in the exchange of information and protecting confidentiality of the data in order to safeguard user privacy and secure communication between them across an unprotected channel.

**Evaluation of Proposed Approach – Secureauthkey**

Only by launching a live assault against the CPS network can the effectiveness of the SecureAuthKey security mechanism be proven. If it protects against assaults, then the SecureAuthKey-based system is doing well; otherwise, it may be made better. If you want to make sure your system is safe under the secure mechanism you've implemented, you need to attack it. If you discover that the system is secure even after being attacked, then you may likely have some faith in the security mechanism you've put in place. Three distinct assaults will be used to evaluate the system in real time.

- Replay Attack

- Penetration Testing

- Man in the Middle Attack (MITM) The reason to choose these three attacks on SecureAuthKey based system is mentioned below

Penetration Test - The goal of penetration testing is to determine whether a system is vulnerable to attack and, if so, how those vulnerabilities manifest themselves. By simulating actual assaults, penetration testing reveals weak spots in the system.

Replay Attack- To breach the victim's network security, the attacker steals their login credentials and then sends the same data many times or delays it. It is also known as a playback assault.

Man in the Middle Attack (MITM) – In a man-in-the-middle (MITM) attack, the attacker poses as both the sender and the recipient of a normally encrypted conversation. By eavesdropping on a private conversation, an attacker may get enough information to pose as either participant in the conversation. An attacker may eavesdrop on a conversation between two people by physically accessing their encrypted communication channel. The session can only continue if the attacker can read and send communications between the two participants. Assessment of security is performed by assaulting the encrypted channel, stealing user credentials, and analysing the system for flaws. For this reason, we will only consider the aforementioned kinds of assaults.

**Parameter Evaluation of CPS based Resource Constraint Devices**

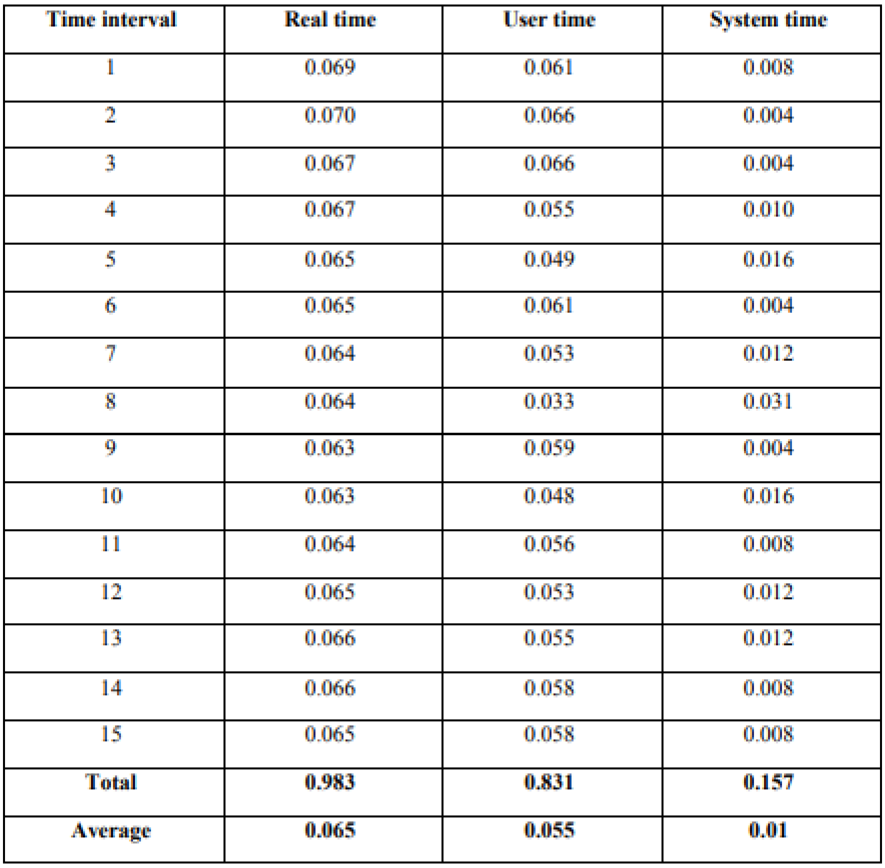
Due to limitations in processor power, storage space, network bandwidth, and battery life, the suggested technique requires the simultaneous execution of two programmes. The aim of execution using constraint-based devices will be achieved if programmes can be effectively performed with reduced computational, storage, and communication requirements.

- Programs must run in the central processing unit in the shortest amount of time possible (CPU). It means that if the execution time in the processor is negligible, it will easily work on constraint-based devices.

- If only computer software needed a few hundred megabytes of RAM. Then it will function on devices based on constraints that are limited in storage..

- Communication overhead is reduced when programmes are run and data is shared between them across a network, which is especially beneficial for devices that run on batteries. We may infer that the suggested method will function with constraint-based devices in CPS if the aforementioned requirements are satisfied. The following details the outcomes of running the suggested algorithm and illustrating the use of Processing time, space, and energy..

Table.1 shows program execution at different time interval. 15 different time interval taken and execute programs.



| Time interval | Real time | User time | System time |
|---|---|---|---|
| 1 | 0.069 | 0.061 | 0.008 |
| 2 | 0.070 | 0.066 | 0.004 |
| 3 | 0.067 | 0.066 | 0.004 |
| 4 | 0.067 | 0.055 | 0.010 |
| 5 | 0.065 | 0.049 | 0.016 |
| 6 | 0.065 | 0.061 | 0.004 |
| 7 | 0.064 | 0.053 | 0.012 |
| 8 | 0.064 | 0.033 | 0.031 |
| 9 | 0.063 | 0.059 | 0.004 |
| 10 | 0.063 | 0.048 | 0.016 |
| 11 | 0.064 | 0.056 | 0.008 |
| 12 | 0.065 | 0.053 | 0.012 |
| 13 | 0.066 | 0.055 | 0.012 |
| 14 | 0.066 | 0.058 | 0.008 |
| 15 | 0.065 | 0.058 | 0.008 |
| **Total** | **0.983** | **0.831** | **0.157** |
| **Average** | **0.065** | **0.055** | **0.01** |

**Table 1 : Microcontroller execution at different time interval**

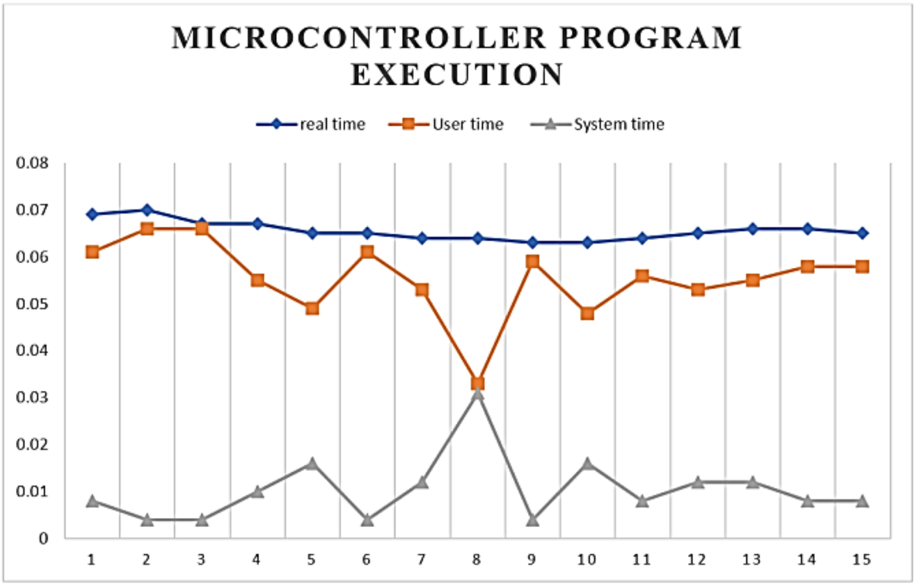


**Figure 3: Microcontroller program execution time**

Taking into account the data in table 1, the execution time graph for a microcontroller programme is shown in Figure 3. It demonstrates that 10 milliseconds, or 0.01 seconds, is the average time needed by the system to execute the programme. This demonstrates that running the programme on the CPU took hardly no time at all. There is a little impact on time. SecureAuthKey will be shown to be an efficient approach that places little strain on the computer's resources.

## Conclusion

For a cyber-physical system to be secure, it must adhere to certain requirements, the most important of which are processing speed, memory size, and battery life. Previous attempts have either relied on already existing, resource-intensive algorithms or security frameworks. The numerous researchers who have worked on CPS security difficulties and challenges and made relevant observations. On a CPS system with higher hardware support, the current security mechanism runs nicely. The algorithm-based software is assigned very little data storage capacity. Therefore, code based on the SecureAuthKey technique may be used to free up space in CPS-based constraint devices that are otherwise unable to run certain security-related programmes.

## References

1. Ashibani, Y. and Mahmoud, Qusay H (2017) ‘Cyber physical systems security : Analysis , challenges and solutions’, Computers & Security, 68, pp. 81–97. doi: 10.1016/j.cose.2017.04.005.
2. Ashibani, Y. and Mahmoud, Qusay H. (2017) ‘Cyber physical systems security: Analysis, challenges and solutions’, Computers and Security, 68, pp. 81–97. doi: 10.1016/j.cose.2017.04.005.
3. Brachmann, M. et al. (2012) ‘End-to-end transport security in the IP-based internet of things’, 2012 21st International Conference on Computer Communications and Networks, ICCCN 2012 - Proceedings. doi: 10.1109/ICCCN.2012.6289292.
4. Capossele, A. et al. (2015) ‘Security as a CoAP resource: An optimized DTLS implementation for the IoT’, IEEE International Conference on Communications, 2015-Septe, pp. 549–554. doi: 10.1109/ICC.2015.7248379
5. Chen, Y., Kar, S. and Moura, J. M. F. (2015) ‘Cyber-physical systems: Dynamic sensor attacks and strong observability’, ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings, 2015-Augus(1), pp. 1752–1756. doi: 10.1109/ICASSP.2015.7178271.
6. Chen, Y., Kar, S. and Moura, J. M. F. (2017) ‘Dynamic Attack Detection in Cyber-Physical Systems with Side Initial State Information’, IEEE Transactions on Automatic Control, 62(9), pp. 4618–4624. doi: 10.1109/TAC.2016.2626267.
7. Chen, C.-M., Hsiao, H.-W., Yang, P.-Y. and Ou, Y.-H. (2013). Defending malicious attacks in Cyber Physical Systems. [online] IEEE Xplore. Available at: https://ieeexplore.ieee.org/abstract/document/6614240/.
8. Friedberg, I. et al. (2017) ‘STPA-SafeSec: Safety and security analysis for cyber-physical systems’, Journal of Information Security and Applications, 34, pp. 183–196. doi: 10.1016/j.jisa.2016.05.008.
9. Granjal, J., Monteiro, E. and Silva, J. S. (2015) ‘Security for the Internet of Things : A Survey of Existing Protocols and Open Research Issues’, 17(3), pp. 1294–1312.
10. Jawadwala, Q. and Patil, K. (2016) ‘Design of a novel lightweight key establishment mechanism for smart home systems’, 11th International Conference on Industrial and Information Systems, ICIIS 2016 - Conference Proceedings, 2018-Janua, pp. 469–473. doi: 10.1109/ICIINFS.2016.8262986
11. Kim, K. D. and Kumar, P. R. (2013) ‘An overview and some challenges in cyber-physical systems’, Journal of the Indian Institute of Science, pp. 341–352.
12. Krimmling, J. and Peter, S. (2014) ‘Integration and evaluation of intrusion detection for CoAP in smart city applications’, 2014 IEEE Conference on Communications and Network Security, CNS 2014, pp. 73–78. doi: 10.1109/CNS.2014.6997468.

13. Lei, L. et al. (2013) 'A threat to mobile cyber-physical systems: Sensor-based privacy theft attacks on android smartphones', Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2013, pp. 126–133. doi: 10.1109/TrustCom.2013.20.
14. Lokesh, M. R. and N, Y. S. K. T. K. (2016) 'Challenges and Current Solutions of Cyber Physical Systems', 18(2), pp. 104–110. doi: 10.9790/0661-1821104110.
15. Moosavi, S. R. et al. (2015) 'SEA : A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways', Procedia - Procedia Computer Science, 52(Ant), pp. 452–459. doi: 10.1016/j.procs.2015.05.013
16. Nur, A. Y. and Tozal, M. E. (2016) 'Defending Cyber-Physical Systems against DoS Attacks', 2016 IEEE International Conference on Smart Computing, SMARTCOMP 2016, pp. 8–10. doi: 10.1109/SMARTCOMP.2016.7501685
17. Pietre-Cambacedes, L. and Chaudet, C. (2010) 'The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety"', International Journal of Critical Infrastructure Protection, 3(2), pp. 55–66. doi: 10.1016/j.ijcip.2010.06.003
18. Raza, S. et al. (2016) 'S3K : Scalable Security With Symmetric Keys — DTLS Key Establishment for the Internet of Things', 13(3), pp. 1270–1280.
19. Sabaliauskaite, G. and Mathur, A. P. (2014) 'Countermeasures to enhance cyber-physical system security and safety', Proceedings - IEEE 38th Annual International Computers, Software and Applications Conference Workshops, COMPSACW 2014, pp. 13–18. doi: 10.1109/COMPSACW.2014.6
20. Wei, J. and Mendis, G. J. (2016) 'A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids', IEEE Proceedings of the 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2016 - This Workshop is Part of the CPS Week 2016, pp. 1–6. doi: 10.1109/CPSRSG.2016.7684102
21. Yuan, Y. and Mo, Y. (2015) 'Security in cyber-physical systems: Controller design against Known-Plaintext Attack', Proceedings of the IEEE Conference on Decision and Control, 54rd IEEE(Cdc), pp. 5814–5819. doi: 10.1109/CDC.2015.7403133
22. Griffor, E. (2017). Handbook of system safety and security : cyber risk and risk management, cyber security, threat analysis, functional safety, software systems, and cyber physical systems. Cambridge, Ma [Und 11 Weitere] Elsevier Syngress