IIoT-ARAS: IIoT/ICS Automated Risk Assessment System for Prediction and Prevention

Bassam Zahran
bzahran@towson.edu
Towson University
Towson, Maryland, USA

Adamu Hussaini
ahussa7@students.towson.edu
Towson University
Towson, Maryland, USA

Aisha Ali-Gombe
aaligombe@towson.edu
Towson University
Towson, Maryland, USA

ABSTRACT

As IT/OT convergence continues to evolve, the traditionally isolated ICS/OT systems are increasingly exposed to a myriad of online and offline threats. Although IIoT enhances the reachability in ICS, improved data analytics, ensuring ease of access and decision making, it unwittingly opens the ICS environment to attackers. The design of IIoT introduces multiple entry points to an isolated system, which is used to protect itself via air-gapping and risk avoidance strategies. This study explores a comprehensive mapping of threats and risks for IT/OT convergence. Additionally, we propose IIoT-ARAS - an automated risk assessment system based on OCTAVE Allegro and ISO/IEC 27030 methodologies. The design of IIoT-ARAS is aimed to be agentless, with minimum interruptions to the OT environment. Furthermore, the system performs automated regular asset inventory checks, threshold optimization, probability computation, risk evaluations, and contingency plan configuration.

ACM Reference Format:
Bassam Zahran, Adamu Hussaini, and Aisha Ali-Gombe. 2021. IIoT-ARAS: IIoT/ICS Automated Risk Assessment System for Prediction and Prevention . In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (CODASPY '21), April 26–28, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3422337.3450320

Keywords: Cybersecurity; Security; IIoT; ICS; IT/OT Convergence

1 INTRODUCTION

Industrial Control Systems (ICS) are systems that consist of software and hardware that monitors and control industrial operations. The Operational Technologies (OT) are the networking devices and protocols serving the ICS. The most common examples of OT used in ICS are the Supervisory Control and Data Acquisition (SCADA), Plant Distribution Control Systems (DCSs), and Programmable Logic Controllers (PLCs). IIoT are interconnected devices designed to improve the reachability, efficiency, and decision making in ICS systems. Industrial Internet of Things (IIoT) provides smart functionality such as energy consumption monitoring, control of environmental release, and the ICS network's overall safety and security. In recent years there is a big shift to fusing the evolving IT technologies with OT systems. This creates a convergence of IT/OT technologies that enhances connectivity, data analytic and real-time reporting which helps in decision making. Since security is considered a major concern with respect to IT/OT convergence, research must continue to find better ways to be up to the increasingly threatening challenges. In this study we are focusing on vulnerabilities and threats facing Industrial Internet of Things (IIoT) devices and how it will affect the functionality of Industrial Control Systems (ICS). In this paper, we present - 1) a mapping of threats and risks for IT/OT convergence, 2) a proposed automated risk assessment system for integrated ICS- IIoT systems called IIoT-ARAS. Our tool performs general information security assessment, vulnerability analysis, and penetration testing based on the Octave Allegro[1] and ISO/IEC 27030[2] (Draft, expected to be published in 2022) risk assessment methodologies. Existing risk assessment systems are mostly designed for OT or IoT systems only. To the best of our knowledge, this is the first automated risk assessment system designed specifically to deal with the potential threats associated with IT/OT convergence based on OCTAVE Allegro-ISO/IEC 27030 Frameworks.

CODASPY '21, April 26–28, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8143-7/21/04.
https://doi.org/10.1145/3422337.3450320

2 BACKGROUND

2.1 ICS - Existing Threats and Potential Impacts

The special nature of ICS systems makes it a challenging task to modify or propose enhancements to security. Most ICS setups are built to work for prolonged times with no interruptions. If anything went wrong, a fail-safe or a backup system would ensure processing continuity. The main business driver for ICS is to minimize processing overheads while maximizing productivity. This implies rejecting or at least resisting any attempt to propose changes. System stability and network isolation are important requirements in an ICS environment. Nevertheless, with the growing need to connect systems to the outside world, data collection, cloud computing, and emerging technologies, OT struggles to cope with these changes. It is a known fact that risks have a greater impact on ICS/OT than IoT/IT. Over the years, the ICS defensive mechanism depends mostly on being an isolated system by creating an air-gap to separate the OT system from the outside world. Nowadays, this risk avoidance technique is not sufficient. In fact, even the air-gap setup has become susceptible to attacks like AirHopper, BitWhisper, GSMem, OOB-CCs, Ramsay, and lately, the Stuxnet. Figure 1 (the blue section) maps existing challenges/Threats in ICS systems to Impact/Risk-based on the survey of related literature[4].

2.2 IIoT - Existing Threats and Potential Impacts

The IIoT inherits most of the vulnerabilities associated with IoT deployment. In fact, IIoT adds some more threats and risks due to

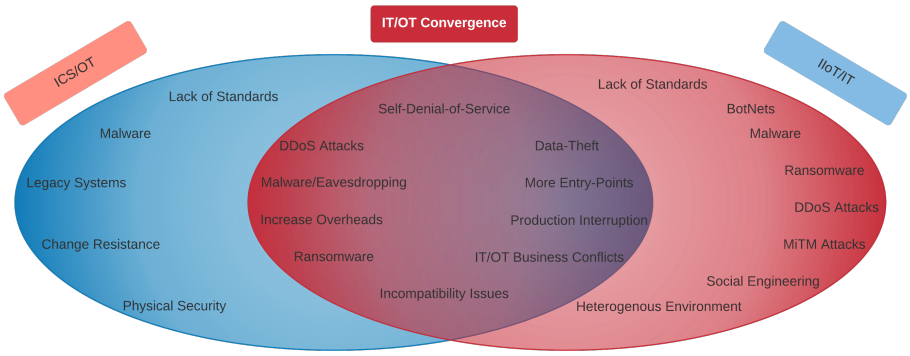

Figure 1: Potential Risks in IT/OT Convergence.

integration with Industrial Control Systems (ICS). While protecting the CIA triad is the ultimate security goal when bringing devices online, this is not easily achievable when it comes to IIoT.

IIoT devices suffer from many limitations and restrictions that make reaching the CIA difficult and complex task. This is especially true because the IIoT networks can spread in a large geographical area and be either indoor or outdoor. IIoT security is applied by the careful consideration of the confidentiality of data, information accuracy, availability, authentication of all objects in the network, lightweight security protocols, and ability to connect to objects and devices from different vendors and specifications.

Each of the IIoT layers suffers from several threats. The threats or attacks can be from within the network or from outside. In addition to common and emerging threats to many of these devices, there is also the possibility of infection through cross-platform malware that might cause to spread the attack to neighboring networks on the Internet[3].

Efficient countermeasures and mitigation of potential malware infections and other threats could only be achieved after a thorough understanding, assessment, and evaluation of the security risk in the IIoT environment. Figure 1 (the red section) lists the most common threats and potential risks in the IIoT network.

3 IT/OT CONVERGENCE

As technology continues to evolve, the convergence of IT/OT is increasingly becoming a crucial need in ICS networks. The industrial sector continues to face stiff competition in the globalized economy. The IT/OT opens a new opportunity for enhanced operational control and monitoring systems in the ICS networks. Additionally, it guarantees better reachability, performance, and efficiency, thus helping to speed up decision-making and fulfill market demands. New techniques in data science and analytics are now essential tools for market research and competitive analysis. The huge amount of data extracted from ICS systems needs to be modeled and processed promptly and accurately to support business growth and continuity. Through smart monitoring, the IT/OT convergence also enables factories and plants to save energy. In addition, one of the most powerful features of this convergence is the extension of visibility through real-time data and more reliable incident reporting.

3.1 Potential Threats and Risks in IT/OT Convergence

The conception of security in Industrial Control Systems is based on a risk avoidance strategy, where critical systems are secluded from other networks. As a defense mechanism, the OT in ICS is created as an isolated system that is air-gaped to guarantee safe and uninterruptible operations. This technique was sufficient and served the need for traditional ICS for prolonged operations without the risk of compromise or security breach unless it was a physical attack on equipment. The main focus of ICSs is to enhance productivity while reducing processing overheads. Unfortunately, security is often considered an overhead in the OT environment. The introduction of IIoT in the industrial field and the merger between IT and OT has led to a change in industrial models. The fusion of IIoT connectivity and data-oriented techniques into ICS's process-oriented isolated system has introduced newer threats into a highly productive ICS network, creating multiple entry points to the supposedly closed system. In addition, the ICS/OT and IIoT/IT have divergent business objectivity. Devices in the ICS environment are designed to operate for an extended period of time and have a whole domain of legacy systems still in active use. Devices in the ICS network often do not support basic protection methods enforced in the implementation of the IIoT systems. For instance, authentication and cryptography methodologies are not supported in much older, hard to replace legacy devices and software. Since most ICS devices are special-purpose machines and not general-purpose, it is challenging to add customization and implement efficient security measures. Installing or updating a security patch to a running ICS system is considered a challenging task and would not be accepted or at least welcomed in such an environment. Above all, the current security specifications are more like business practices rather than regulating policies. Thus, this special nature of IT/OT convergence requires a different and tactical approach to general security and risk assessment.

4 IIOT-ARAS AUTOMATED RISK ASSESSMENT SYSTEM

Given the aforementioned, and with respect to IT/OT convergence, a need arises for a tailored methodology to assess threats, risks, and possible consequences. Thus, this research's second contribution

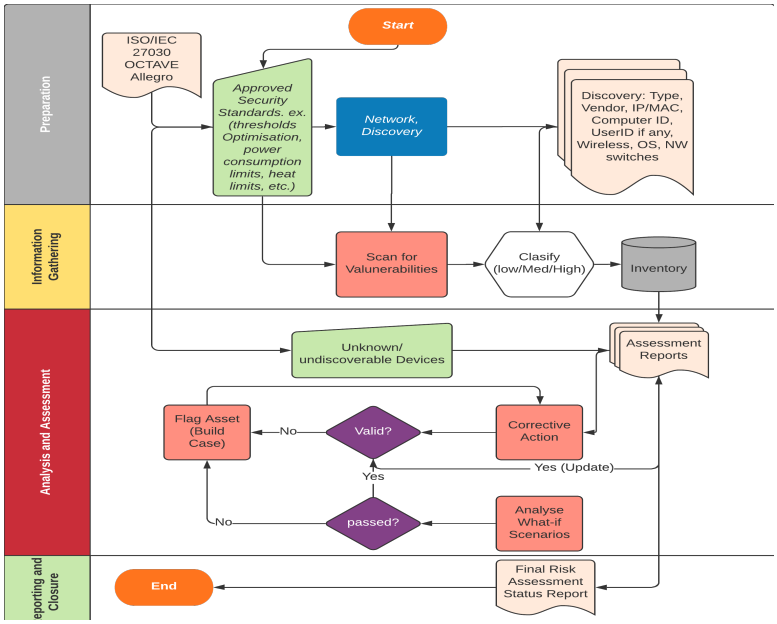

Figure 2: IIoT-ARAS System Overview.

builds a risk assessment solution titled IIoT-ARAS that fuses and automates the best practices recommended in the OCTAVE Allegro and ISO/IEC 27030. The OCTAVE is a framework for building an inventory of assets and associated risk factors in an IT environment[1]. Octave Allegro is a special version of the OCTAVE family designed to support information risk assessment in large enterprises and the industrial sector. This methodology uses worksheets to capture assets and assign priority in addition to recording vulnerabilities and potential threats/risks. Octave Allegro works based on a systematic approach consisting of phases and steps. Although this framework tends to minimize the work required to perform risk assessment, it is still considered an interruption to the OT environment[4]. On the other hand, The ISO/IEC 27030 is a special version of the ISO 27K series aimed at IoT Information Security and Privacy[2]. Specifically, this standard deals with internal processes and building trustworthiness in IoT systems. While the standard is still in the draft phase and expected to be officially published in 2022, its main function is to ensure that the CIA security model is adhered to while providing recommendations on contingency plans for data restoration and recovery. Existing frameworks designed for OT security, such as the Industrial Internet Consortium, ISACA, International Society of Automation, NIST, Technical Support Working Group, etc., all provide sufficient details on securing ICS/OT systems; however, they provide little or no consideration of IT/OT convergence. IIoT-ARAS, on the other hand, is an automated risk assessment system tailored specifically for IT/OT convergence. It is designed to perform automated regular asset inventory checks, threshold optimization, probability computation, risk evaluations, and contingency plan configuration. As shown in Figure 2, IIoT-ARAS has an agentless implementation, resulting in a minimal interruption to the OT environment while still utilizing the best security practices to collect data and optimize an acceptable threshold. In addition, the proposed system also performs periodic system check audits as part of preventive maintenance to ensure compliance with the CIA security model.

5 CONCLUSION AND FUTURE WORK

The IT/OT convergence is becoming an initial part of the industrial world. The benefits of this integration are endless but it comes with cost. ICS in the past, depended on obscurity and air-gapping as a defense mechanism. Introducing IIoT to the world of ICS created multiple entries to the used-to-be hidden system. In this study, we revealed many of the threats/risks resulted by the IT/OT convergence. Additionally, we introduced our proposal for IIoT-ARAS, an automated system for risk assessment and prevention based on customized version of OCTAVE Allegro and ISO/IEC 27030 Risk Assessment frameworks. The future work includes testing and evaluation of the proposed system in a simulation IIoT environment.

6 ACKNOWLEDGEMENT

This work is supported by the National Science Foundation (NSF) under Grant Number 1850054.

REFERENCES

[1] Caralli, Richard A., et al. Introducing octave allegro: Improving the information security risk assessment process. No. CMU/SEI-2007-TR-012. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2007.
[2] “Guidelines for Security and Privacy in Internet of Things” ISO/IEC 27030, https://www.iso27001security.com/html/27030.html
[3] Zahran, Bassam, Stacy Nicholson, and Aisha Ali-gombe. "Cross-Platform Malware: Study of the Forthcoming Hazard Adaptation and Behavior." Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2019.
[4] Conto, Ruggero, and Lawrence Orans. OT Security Best Practices, 14 Sept. 2018, www.gartner.com/doc/reprints?id=1-242JE25A