Evaluating Security of Industrial IoT Testbeds

Authors:
Jesus Molina
Director of Business Development
Waterfall Security Solutions
jesus@waterfall-security.com

Suresh K Damodaran
Principal Cyber Security Architect
The MITRE Corporation
sdamodaran@mitre.org

Robert A. Martin
Senior Principal Engineer
The MITRE Corporation
ramartin@mitre.org

Vyacheslav Zolotnikov
Senior Technology Research Manager
Kaspersky Labs
Viacheslav.Zolotnikov@kaspersky.com

INTRODUCTION

The Industrial Internet Consortium (IIC) published the Industrial Internet Security Framework (IISF) [1] in 2016, to identify, explain, and incorporate security into the architectures, designs, and technologies of Industrial Internet of Things (IIoT) systems, as well as to add appropriate security procedures into the IIoT systems themselves. The IISF also introduced the concept of trustworthiness and trustworthy IIoT systems, adding system characteristics such as safety, reliability, resiliency, and privacy along with security into the evaluation. After the publication of the IISF, the IIC updated the security review procedures of its testbed program, which to date include 26 IIoT projects in verticals such as manufacturing, healthcare, farming, transportation, connected vehicles, energy, and retail.

The security review process is mandatory, done before testbed approval, and prior to its implementation. As a first step, the testbed creates a security profile using the IIC testbed security questionnaire. The security profile covers use cases, their security risks, threats analysis, and implementation goals for the security controls. The security profile is evaluated by the Testbed Security Contributing Group (TSCG), a volunteer group of security experts with relevant expertise and backgrounds from member companies of the IIC. This evaluation is complemented by an interview between the TSCG and the testbed team. The overall goal of the security review process is to provide candid feedback to the testbed proposers to improve the security posture of the testbed. This security review also provides an opportunity for continuous feedback based on subsequent revisions of the IISF.

This paper provides an introduction to the testbed program and uses two case studies to explain the parts of the security review process. It then describes the findings and challenges in evaluating security in testbeds, especially in the early stages of their planning and deployment.

TESTBED PROGRAM

The testbed program in the IIC is designed to support the IIC's goal of accelerating the adoption of the industrial internet and the transformation of the global economy. For this adoption and transformation to occur, guidance on interoperability, security, connectivity, business models, standards, architectures, and patterns must be firmly rooted in reality and practicality. The program provides realistic lessons and experience and is thus valuable to the IIC and its members.

The outcomes from testbeds form the essence of a feedback loop from concept to reality and back to guidance for further innovation to the IIC community. Therefore,

[1] Industrial Internet Consortium. "Industrial Internet of Things Volume G4: Security Framework," *Industrial Internet Consortium, IIC:PUB:G4:V1.0:PB:20160926,* (2016)

although member companies sponsor and own their testbeds, they also agree to share certain deliverables and progress reports with IIC members and the greater IIoT ecosystem.

Each IIC IIoT testbed is a technology platform that provides experience enabling IIC members to better understand innovations and to test new applications, processes, products, services, and business models to ascertain their usefulness and viability before taking them to market. In this way, IIC members can uncover the technologies, techniques, and opportunities essential to solving these and other important problems that benefit businesses and society.

Specifically, a testbed is a controlled experimentation platform that has the following properties:

- Implements specific use cases and scenarios;
- Produces testable outcomes to confirm that an implementation conforms to expected results;
- Explores untested or existing technologies working together (interoperability testing);
- Enables members to obtain insights to generate new (and potentially disruptive) products and services; and
- Generates requirements and priorities for standards organizations supporting the implementation of the industrial internet.

The Testbed Working Group is the centralized group that collects testbed ideas from member companies and provides systematic yet flexible guidance for creating new testbed proposals. These testbeds will often be funded by institutions (agencies, academia, and governments) in collaboration with industry.

The priorities and activities around testbeds continue to evolve but the IIC is committed to creating and developing testbeds that support the IIC's goals of innovation and interoperability.

IISF & SECURITY EVALUATION

The IISF provides guidance on performing security evaluations on IIoT systems, spanning across both Information Technologies (IT) and Operational Technologies (OT). The TSCG provides the testbed with a list of questions ("the questionnaire") to help them document and explain the security posture and decisions of the testbed. The format of the questionnaire evolved over a period of time from a free flow of information – the testbeds created documents and presentations – to a questionnaire that can be completed at any time through an online portal with some multiple-choice answers. The questionnaire is divided into two sections, mirroring the structure of IISF, specifically, Part II, the business viewpoint, and Part III, the functional and implementation viewpoints. The following is a summary of the information solicited in the questionnaire.

- *Architecture Diagram with Trust Boundaries*: Provide an architecture diagram of the testbed to show the information and control paths among the architectural elements, and to demarcate the trust boundaries. An architecture diagram may conform to the 3-tier IIoT System Architecture in the IIC's Industrial Internet Reference Architecture (IIRA),[2] as shown in Figure 1, but conformance is not mandatory. A trust boundary is defined by the TSCG team as the region enclosing systems and actors under the same security policy jurisdiction, supporting isolated execution within that trust boundary, and with interfaces through the trust boundary that support trusted path or communication among the architectural elements. The details of how various security mechanisms are used within each trust boundary and for which purposes (e.g. to protect privacy) should be documented. Mechanisms to provide confidential and authenticated communications across trust boundaries over trusted paths should also be documented.

- *Use Cases and Security Objectives*: Document a collection of use cases, each providing the actors and security objectives.
- *Trustworthiness Constraints*: Summarize how the other non-security aspects of trustworthiness are relevant and considered in the testbed. These include safety, reliability, resilience, and privacy.
- *Threat Analysis*: Provide a threat analysis of the various system components using a threat modeling methodology such as STRIDE [3]. A ranking of the security threats as perceived by the testbed team is also documented.

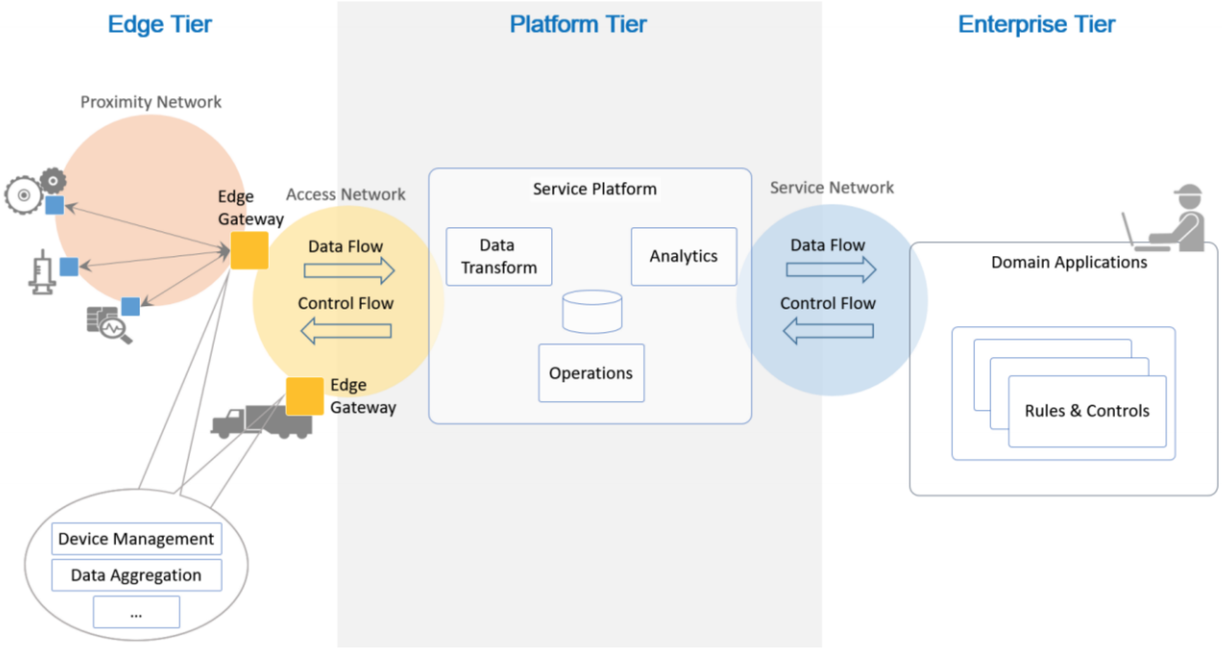


Figure 1: Three-Tier IIoT System Architecture

[2] Industrial Internet Consortium. "The Industrial Internet of Things Volume G1: Reference Architecture," *Industrial Internet Consortium (IIC), IIC:PUB:G1:V1.80:20170131,* (2015)

[3] Shostack, Adam. *Threat modeling: Designing for security*. John Wiley & Sons, (2014).

- *Standards and Compliance*: Document relevant security standards and compliance requirements.

The various pieces of information collected, as described in this section, are utilized in the security review process captured in the next section.

Objectives and Security Review Process

The primary objective of the security review process conducted by the TSCG is to ensure that a testbed considers security at the onset of its design and to provide feedback to the testbed team on whether the security objectives sought out by the testbed team appear to be met by the testbed design under review. The process followed by the TSCG for its evaluation is described in the figure bellow.

1. The Testbed team creates the Testbed presentation outlining the purpose and goals of the Testbed activity and receives related review comments from the Testbed Working Group. This presentation is shown as input to the first step in Figure 2.
2. The Testbed team creates and provides the security profile, with the help of the testbed security profile guidelines and the questionnaire.
3. The Testbed team schedules a review between the testbed team and the TSCG.
4. The TSCG team meet and discuss the security profile, fill in the gaps of the security profile for the testbed, and schedule a review with the testbed owners.
5. The TSCG team reviews the security profile, asks further questions and provides feedback.
6. The Testbed team updates the security profile according to the feedback provided by the TCSG team.
7. Additional iterations of review with the TSCG may be conducted, if desired by the Testbed team.

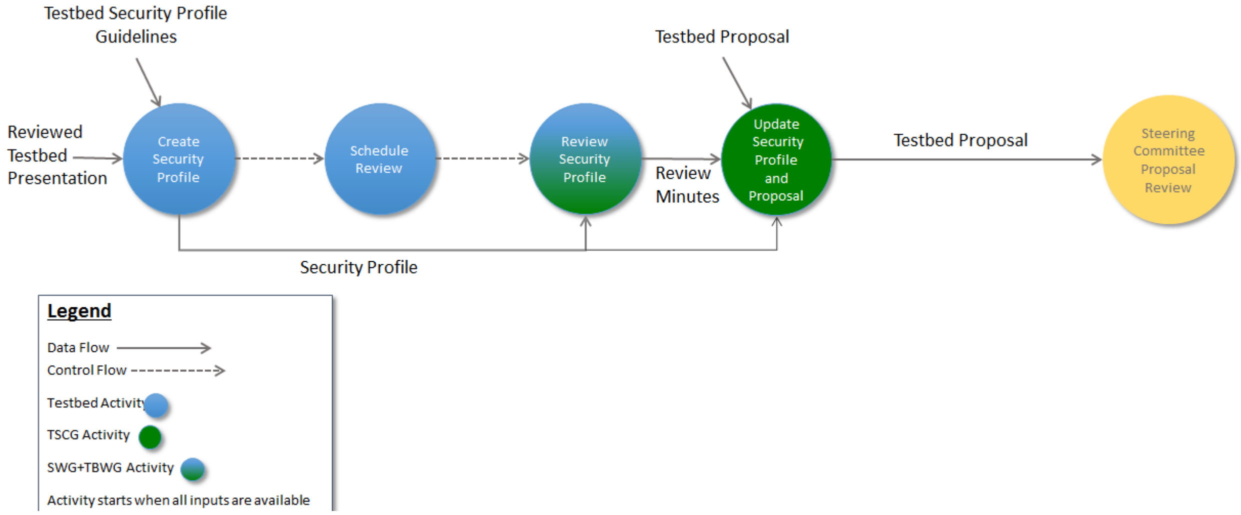


Figure 2: The security review process

8. The completed Testbed proposal will be brought to the IIC Steering Committee for approval.
9. Once approved, testbed starts operating.

Ideally, the TSCG team and Testbed teams will review the security profile periodically, as technology changes and experience with the Testbed is gained. This iteration in the review process has not been put into practice yet.

CASE STUDIES

The case studies described in this section provide concrete examples of the information collected as part of the testbed security review process. The first of these is the Retail Video Analytics case study that demonstrates the use of an architecture diagram to show trust boundaries, as well as a ranking of security threats. This case study shows a thread model generated using the STRIDE methodology.[4] The STRIDE methodology identifies the following types of threats: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. The second case study is the Smart Factory Machine Learning case study also shows a threat model generated using the STRIDE methodology.

Retail Video Analytics

The Retail Video Analytics Testbed personalizes the retail experience by using actionable insights in real time through the interconnection of video cameras, analytics, and machine learning algorithms. The companies' participating in the testbed are NEC Corporation®, Microsoft, Brierley+Partners® and a major retail enterprise.

Figure 3 describes the testbed architecture and trust boundaries as provided by the testbed team. The trust boundaries are delimited by dotted red lines. The

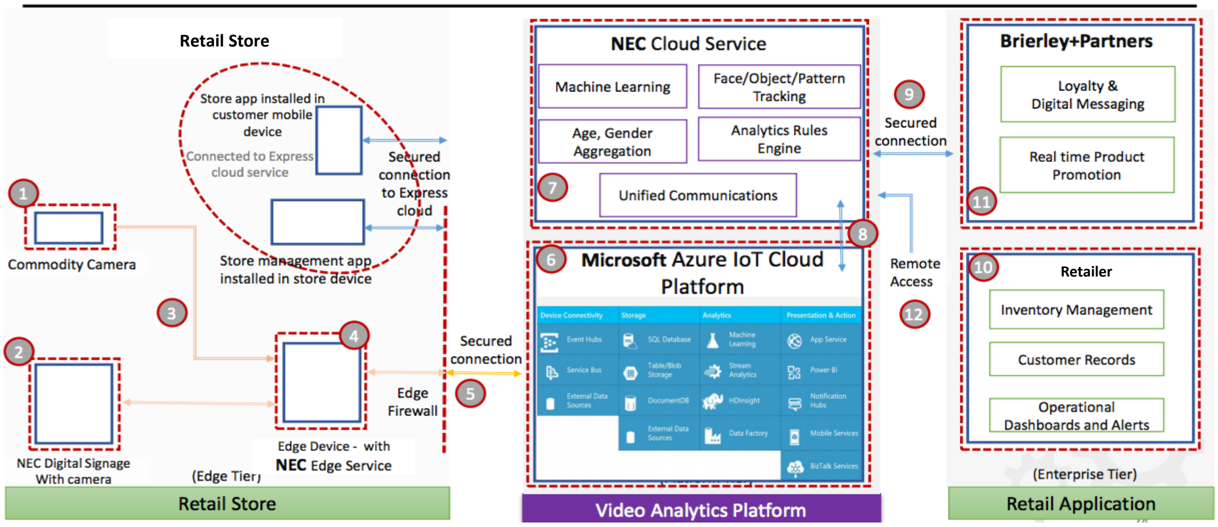


Figure 3: Retail Video Analytics architecture and trust boundaries

[4] Shostack, Adam. *Threat modeling: Designing for security*. John Wiley & Sons, (2014).

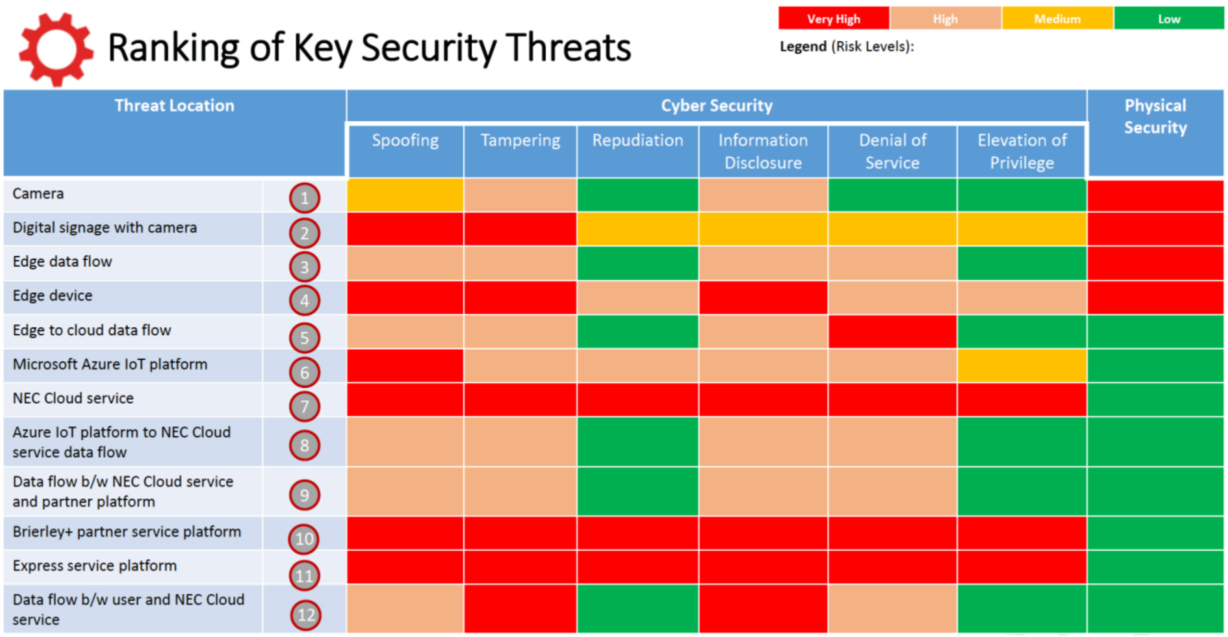
architecture follows the 3-tier architecture diagram: the edge corresponds to the retail store; the platform tier hosts the video analytics platform; and the retail applications by the retailer and Brierley+Partners correspond to the business tier. The edge tier includes three trust boundaries, representing the off-the-shelf cameras, the NEC digital signage, and the edge gateway device, which will require different security policies, and have different ownerships.

This security profile of the testbed included a description of the threats by using STRIDE. The results of the STRIDE analysis used to rank the security threats are shown in Figure 4. This figure classifies the threats by using four levels (Very High, High, Medium and Low) for each trust boundary. The last column in Figure 4 contains the risk of physical attacks against the endpoints. These classifications include the judgements of the Testbed team.

The TCSG team worked with this testbed team to refine the security evaluation, and to create a threat model. This early understanding of risk helped the team to better understand the implementation requirements. In this testbed, privacy of the costumer was critical and confidentiality measures will be implemented along with the security measures.

Smart Factory Machine Learning

The goal of the Smart Factory Machine Learning testbed is to increase energy efficiency, availability, and lifespan of high volume CNC (Computer Numerical Control) manufacturing production systems. This testbed, led, by Aingura IIoT® (formerly Plethora IIoT) and Xilinx®, provides the basis for development and evaluation of machine learning techniques for time critical predictive maintenance.



Ranking of Key Security Threats

Legend (Risk Levels): 🟥 Very High 🟧 High 🟨 Medium 🟩 Low

Threat Location		Cyber Security						Physical Security
		Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege	
Camera	1	🟨	🟧	🟩	🟧	🟩	🟩	🟥
Digital signage with camera	2	🟥	🟥	🟨	🟨	🟨	🟨	🟥
Edge data flow	3	🟧	🟧	🟩	🟧	🟧	🟩	🟥
Edge device	4	🟥	🟥	🟧	🟥	🟧	🟧	🟥
Edge to cloud data flow	5	🟧	🟧	🟩	🟧	🟥	🟩	🟩
Microsoft Azure IoT platform	6	🟥	🟧	🟧	🟧	🟧	🟨	🟩
NEC Cloud service	7	🟥	🟥	🟥	🟥	🟥	🟥	🟩
Azure IoT platform to NEC Cloud service data flow	8	🟧	🟧	🟩	🟧	🟧	🟩	🟩
Data flow b/w NEC Cloud service and partner platform	9	🟧	🟧	🟩	🟧	🟧	🟩	🟩
Brierley+ partner service platform	10	🟥	🟥	🟥	🟥	🟥	🟥	🟩
Express service platform	11	🟥	🟥	🟥	🟥	🟥	🟥	🟩
Data flow b/w user and NEC Cloud service	12	🟧	🟥	🟩	🟥	🟧	🟩	🟩

Figure 4: Ranking of security threats

The architecture for this testbed contains four trust boundaries. Due to space restrictions the architecture diagram for this testbed could not fit in this article. The architecture diagram provided by the testbed contained, besides the system functional components, security implementation components, such as Next Generation Firewalls (NGFW) and DMZs (perimeter network or demilitarized zone, in computer security terminology). In this testbed, operators and users will access the testbed remotely to perform configuration and analysis using a client-side encrypted VPN network.

The enterprise tier is hosted in the Microsoft® Azure® Cloud, in which data processing and machine learning is performed for preventive maintenance, improvements in production and cost savings. The Azure platform supports needed security and crypto operations.

The edge tier is the Industrial Automation and Control System. This tier has three trust boundaries: The IIoT gateway, the Supervisory and Control Network, and the sensors and actuators. The IIoT gateway is the device intended to perform tasks of collecting relevant information about the state of the process and the production components, as well as data processing based on predictive algorithms. The Supervisory and Control Network includes process control equipment that receives inputs from sensors, then processes the incoming data using control algorithms and subsequently sends the output actuators for continuous, sequential, batch and discrete control. These devices run vendor-specific operating systems and are programmed and

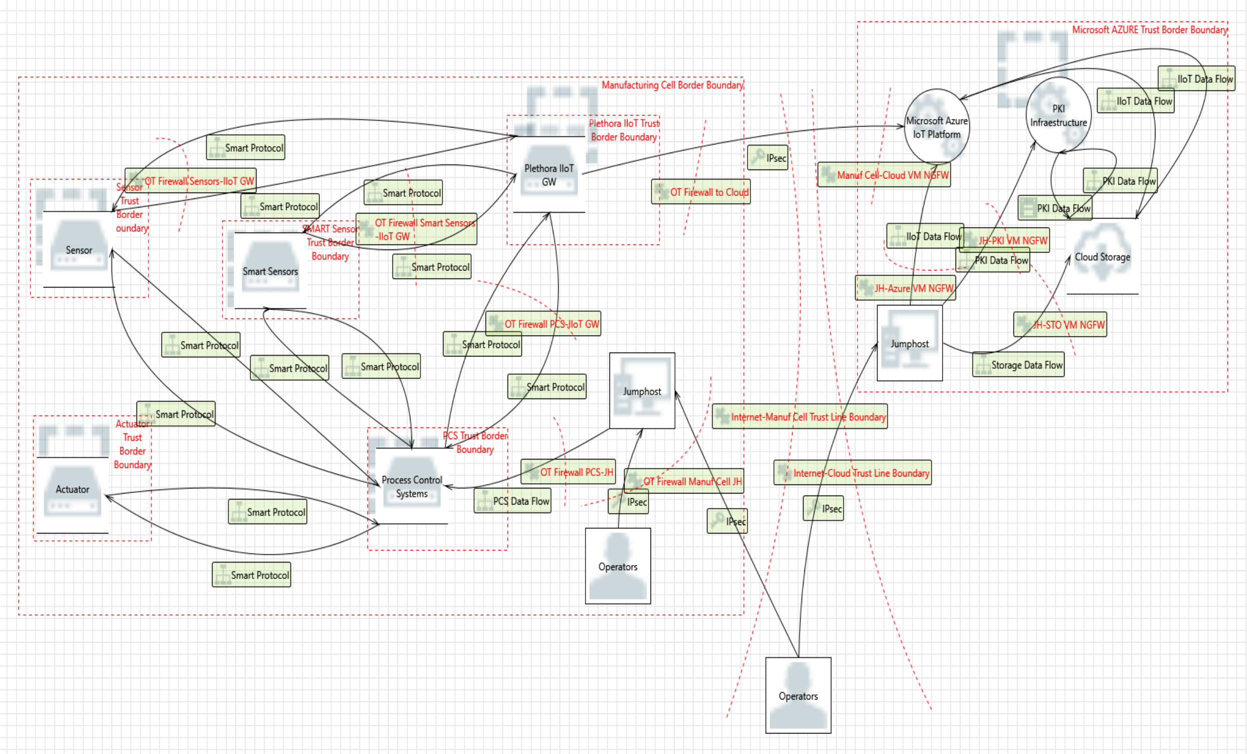

Manufacturing Cell Border Boundary
Plethora IIoT Trust Border Boundary
Plethora IIoT GW
Smart Protocol
OT Firewall Sensors-IIoT GW
Sensor Trust Border oundary
Sensor
SMART Sensor Trust Border Boundary
Smart Sensors
OT Firewall Smart Sensors -IIoT GW
OT Firewall PCS-IIoT GW
Actuator Trust Border Boundary
Actuator
PCS Trust Border Boundary
Process Control Systems
OT Firewall PCS-JH
PCS Data Flow
Jumphost
OT Firewall Manuf Cell JH
IPsec
Operators
OT Firewall to Cloud
Microsoft AZURE Trust Border Boundary
Microsoft Azure IoT Platform
PKI Infraestructure
IIoT Data Flow
Manuf Cell-Cloud VM NGFW
PKI Data Flow
JH-PKI VM NGFW
Cloud Storage
JH-Azure VM NGFW
JH-STO VM NGFW
Storage Data Flow
Internet-Manuf Cell Trust Line Boundary
Internet-Cloud Trust Line Boundary

Figure 5: STRIDE Model

configured from engineering workstations (Manufacturing Operation DMZ).

The sensors and actuators have instrumentation elements that directly connect to and control the manufacturing process. These devices are controlled by Process Control Systems in the Supervisory and Control Network.

Figure 5 describes the threat analysis conducted using STRIDE methodology. In this model, the testbed provides information about the endpoints, data stores, and how data is transferred across the trust boundaries.

The threat model in Figure 5 provides helpful automated information regarding threats. However, some details such as the existence of multiple owners and operators of the trust boundaries are not currently within the scope of STRIDE. Figure 6 provides a more detailed view of the OT aspects of the testbed.

In the detail for the OT side, Figure 6 displays the functionality of the IoT gateway as the main security component in OT, protecting the edge devices and procuring the connectivity to the cloud.

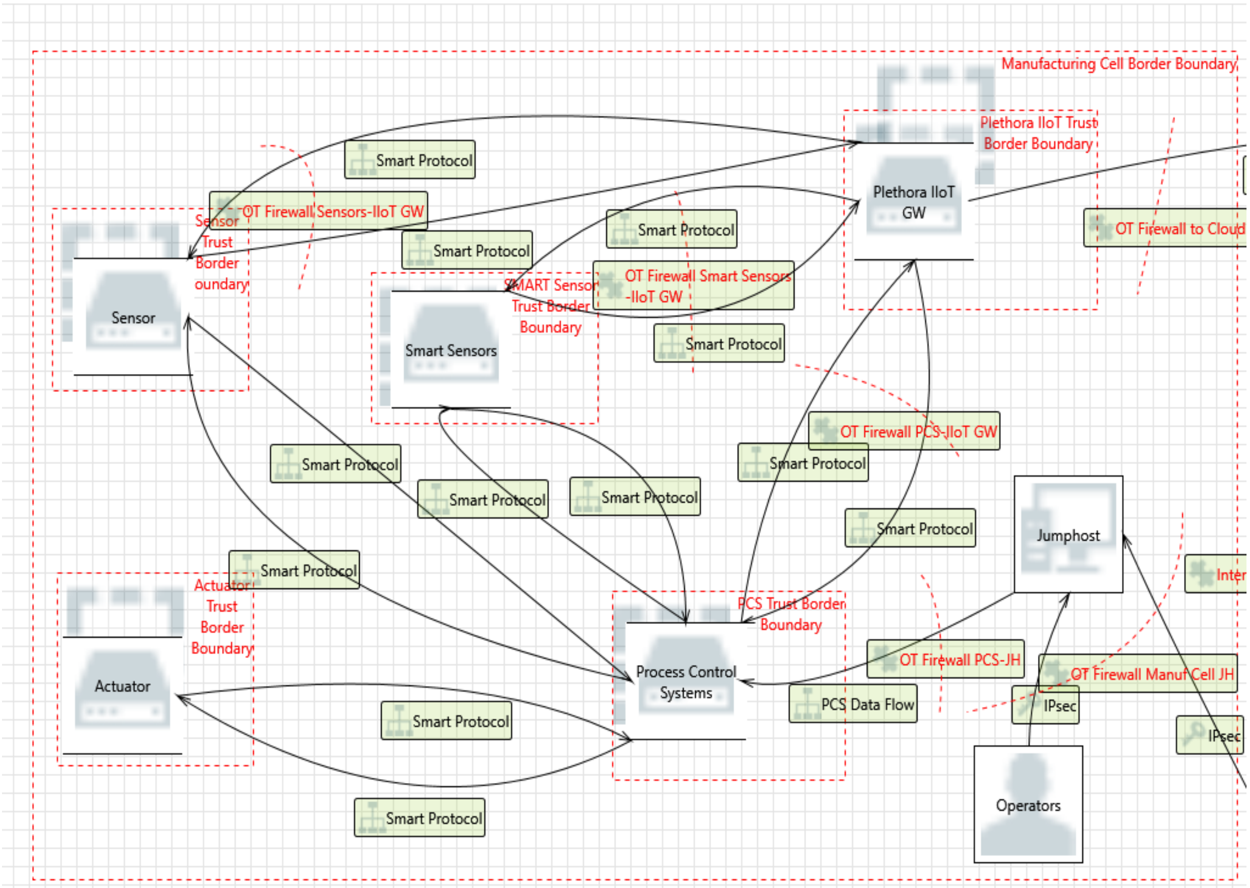


Figure 6: STRIDE model for OT

FINDINGS AND CHALLENGES

The process of security reviews and the practice of creating security profiles has proven beneficial to both the IIC Testbed program and the IIC Security Working Group. According to the feedback given by testbed teams, creating the initial representation of trust boundaries and corresponding threats helps testbeds to brainstorm on attacks, which leads to the early evaluation of possible vulnerabilities. While the risk analysis tools seem to have limitations, the initial assessment still provided testbeds with a good understanding of their risks. For example, the automated output from STRIDE helped one testbed to find a flaw in the design and motivated another to include additional security controls. The information collected from the questionnaire also helped start the evaluation of some of the best practices in the IISF, providing insights for its future revision.

There were several challenges that needed to be addressed within tight time constraints and resources to implement this security evaluation process. To adequately address these challenges, additional research and support from the larger IIoT security community is required. This paper attempts to outline those challenges as a call-to-action to all security practitioners.

Precisely Defining a Trust Boundary is Difficult

The IIC's Industrial Internet Vocabulary Technical Report[5] defines a trust boundary as a separation of different application or system domains in which different levels of trust are required. Since defining trust boundaries is a cornerstone of the IIoT testbed threat evaluation process, it is necessary to precisely define a methodology to determine a trust boundary in an IIoT testbed. From our experience, testbeds require more guidance to correctly create trust boundaries.

For example, edge devices can be diverse within the same testbed, including several classes of PLCs (programmable logic controllers) or other machinery. These devices may be within the same trust boundary or multiple trust boundaries. In the extreme case, there can be one trust boundary for each device. If the edge devices are exposed to anyone walking by or are sitting directly on the Internet, this extreme approach makes sense. If the edge devices are in a limited access environment, a single trust boundary may be sufficient for all the devices. Multiple trust boundaries also add to the complexity of the threat modeling effort. Hence a further refined definition of a trust boundary that addresses the nuances expressed in this section is essential.

[5] Industrial Internet Consortium. "The Industrial Internet of Things Volume G8: Vocabulary," *Industrial Internet Consortium, IIC:PUB:G8:V2.00:PB:20170719,* (2017)

The ISA/IEC 62443 defines the concept of trust zones and conduits,[6] which have been adopted by most testbeds to create the trust boundaries. A trust boundary may be enclosed within another trust boundary if the outer trust boundary has security policies that may override the trust boundaries it encloses.

In computing platforms, the vocabulary used by practitioners to describe a similar concept to a trust boundary are Secure Enclave, Security Zone, and Trusted Security Zone. In hardware security, an isolated execution environment with secure storage, remote attestation, trusted path, and secure provisioning has been termed Trusted Execution Environment (TEE).[7] However, a clear definition of a trust boundary, analogous to TEE, does not exist in the distributed hardware and software deployment environment of IIoT testbeds.

Multiple Owners May Obscure Trust Boundary Properties

The IIC testbeds typically follow the three-tier architecture for IoT systems illustrated by the IIRA as previously shown in Figure 2. However, the implementation of this basic architecture approach in the testbed systems has sometimes manifested as multiple and separate systems owned by different entities that interoperated within a single tier. For example, the Retail Video Analytics testbed included two cloud systems, owned by NEC and Microsoft, respectively, within the testbed platform tier. This section discusses the security evaluation challenges presented by the implementations of use cases that span multiple trust boundaries, often owned by different owners.

If a testbed use case spans multiple trust boundaries, it is under the jurisdiction of separate security policies. The trust boundaries that are part of a use case may be owned or operated by independent entities that do not share the same security policies or even the same rigor in enforcing their security policies.

One possible side effect of having multiple organizations with different security policies is that the security assumptions and guarantees within a trust boundary may not be documented by a testbed team or not shared well across trust boundaries. A simple example may involve the consistency of encryption strength. Messages exiting a trust boundary A and entering a trust boundary B may have a stronger encryption strength than the same messages exiting trust boundary B to another trust boundary.

A more complicated example may be based on different objectives of different organizations owning the trust boundaries. For example, a cloud platform owner may be more focused on the infrastructure up-time and efficiency than on making sure the

[6] International Society of Automation (ISA). ISA-62443-3-3-2013, “Security for industrial automation and control systems: System Security Requirements and Security Levels,” (2013)

[7] Sabt, Mohamed, Mohammed Achemlal, and Abdelmadjid Bouabdallah. "Trusted execution environment: What it is, and what it is not," *Trustcom/BigDataSE/ISPA, 2015 IEEE*. Vol. 1. IEEE, (2015)

privacy requirement of a particular use case is met. Since privacy requirements may not be stated in an easily sharable way for communication across trust boundaries, this can cause challenges to even a capable trust boundary owner. If the need for addressing privacy is not expressed clearly, then other organizations can not plan to implement the privacy requirements of a particular use case, nor can they provide sufficient evidence about how these privacy requirements they did not know about are met by their implementation. These challenges need to be addressed with more specific requirements about interoperability of security information across trust boundaries.

Limitations of Current IIoT Risk Analysis Tools

The IISF does not prescribe any one tool or approach for threat modeling, though it refers to OWASP Top 10[8] for threats, and STRIDE[9] for threat modeling. While STRIDE is a useful approach for threat modeling across pairs of trust boundaries, and the STRIDE methodology works well in web-based systems, the STRIDE methodology is not intuitively useful and sometime not applicable for the multi-trust boundary use cases often found in the IIoT testbeds. Specifically, STRIDE does not address the complexities described earlier related to multi-owner, multi-operator scenarios of trust boundaries, and threat modeling of end-to-end use cases in such environments. It also does not address interaction of security with safety, reliability, and other system characteristics. IIoT system security assessments will continue to be challenged in capturing threats and modeling them until additional tools and methods appropriate for capturing and analyzing IIoT challenges are readily available. The testbed teams, are still better served by using tools like STRIDE until better tools are available for testbeds.

Reconciling the IIoT Edge Gateway Focus with End-to-End Security Practices

While most IT security evaluations are based on deploying mitigation controls, the IIC focus is on “security by design,” an end-to-end security design. The IISF documents practices for securing the endpoint such as secure identities on top of a root of trust, which enables secure point-to-point communications, secure firmware updates and other necessary features. However, we observed that none of the evaluated testbeds featured strong end-to-end protections for all of their edge devices. Instead, most testbed’s security design relied on the edge gateway for its security, or on intrusion detection features existing in the Platform Tier. Unlike IoT security for consumer electronics, which usually feature point-to-point connectivity from each device to the cloud, industrial IoT assumes physical protections in the form of a strong perimeter and the existence of an edge gateway with security capabilities. The reliance on a gateway to protect the edge requires a

[8] OWASP IoT Top 10 https://www.owasp.org/index.php/Top_IoT_Vulnerabilities, (2014)

[9] Shostack, Adam. *Threat modeling: Designing for security*. John Wiley & Sons, (2014).

method to evaluate the security features of these type of devices with rigor, repeatability, and a consistent way of communicating the findings. In our evaluations, edge gateways included features such as next generation firewalls, intrusion detection, and point-to-point authentication, resolving most of the threats encountered in the risk analysis. However, the practical implementations of these capabilities in the testbeds were not well specified and are generally difficult to track as the testbed progresses.

Evaluating Trustworthiness

In the IISF and in the NIST Framework,[10] trustworthiness is described as the composition of security, safety, privacy, reliability, and resiliency. As part of the questionnaire, the TSCG tasked testbeds to provide qualitative information on their concerns related to these characteristics. Every testbed provided relevant information, as exemplified by the Retail Video Analytic Testbed which listed privacy as an issue, or the Smart Factory Machine Learning Testbed which noted that safety, reliability and resilience are important. However, the testbeds were not able to quantify the relationship between these characteristics or if they should be evaluated separately or together. The negative or positive effects of security controls on other characteristics, such as the safety at the edge or the reliability of a components, is still an evolving research problem.

Distinguishing the Testbed from the Eventual Production Deployment

A specific challenge faced by IIoT testbeds is answering the question whether they are evaluating the security of the current testbed or of the eventual production deployment of the testbed. While some of the evaluated testbeds did have a collaborating partner with security expertise, others did not. Even then, the testbeds tried hard to make their testbeds more secure, though omitting security requirements in the early stages of the testbed conceptualization and design makes it challenging for those implementing security on the testbed and those evaluating security.

CONCLUSIONS

In this article, we used two case studies to describe the current state of the art of security evaluation of IIoT testbeds within the IIC. To address the challenges documented, we are evolving the IIC Security Working Group's TSCG's evaluation methods to focus on particular security targets for the testbeds. The current work in the IIC developing Industrial IoT security maturity models for testbeds – similar to the Office of Electricity Delivery & Energy Reliability: Cybersecurity Capability Maturity

[10] National Institute of Standards and Technology (NIST): CPS PWG Cyber-Physical Systems (CPS) Framework Release 1.0, (2016)

Model[11] – will help create better profiles for different security levels.

The security evaluation process aligns with the IISF and, as the IISF and its related documents and methodologies evolve, the security evaluation process is expected to evolve as well. We described the challenges faced by testbeds in effective threat modeling. Adequately addressing some of these challenges will require considerable effort within the security community. We hope tools such as STRIDE will evolve to address these challenges.

This description of the security evaluation process and its challenges is intended to help testbed participants understand the process and for all to contribute to the further evolution of the security evaluation process and a stronger and easier basis for communicating about and making judgements on the security of IIoT systems, enhancing the trustworthiness of these systems. We hope the next version of IISF will consider these challenges and outline ways to address them.

ACKNOWLEDGEMENTS

We would like to thank the Testbed Working Group, and its chair, Joseph Fontaine, for the help in creating the security evaluation process. We also would like to thank the respective security leads of the testbeds showcased in this article, Aravind Parandhaman (NEC) and Borja Lanseros (Titanium Industrial Security), and the respective testbed technical teams for their expertise and collaboration during the evaluation process.

➢ Return to IIC Journal of Innovation landing page for more articles and past editions.

[11] Office of Electricity Delivery & Energy Reliability: Cybersecurity Capability Maturity Model (C2M2), retrieved 2018-02-01 http://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf from http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program/cybersecurity, (2014).

The views expressed in the *IIC Journal of Innovation* are the contributing authors' views and do not necessarily represent the views of their respective employers nor those of the Industrial Internet Consortium.