Key Safety Challenges for the Industrial Internet of Things

IIC Whitepaper Executive Summary

Authors:

Dr. Qinqing Zhang
Johns Hopkins University[1]
qinqing@ieee.org

Dr. Andrew King
University of Pennsylvania[2]

Frederick Hirsch
Standards Manager
Fujitsu
frederick.hirsch@us.fujitsu.com

Semen Kort
Senior System Analyst, KL ICS CERT, Critical Infrastructure Defense
Kaspersky Lab
semen.kort@kaspersky.com

[1] This work was done when Dr. Qinqing Zhang was with Johns Hopkins University, Applied Physics Laboratory. She was an assistant group supervisor, and had a joint appointment of research associate professor in the computer science department at JHU.

[2] This work was done when Dr. Andrew King was with the Computer Science Department at University of Pennsylvania

KEY SAFETY CHALLENGES FOR THE INDUSTRIAL INTERNET OF THINGS - EXECUTIVE SUMMARY OF IIC WHITE PAPER[3]

Industrial Internet of Things (IIoT) systems connect industrial control systems to form larger end-to-end systems, connect them with people and integrate them with enterprise systems. The *trustworthiness* of an IIoT ecosystem is defined as "the degree of confidence one has that the system performs as expected with characteristics including *safety*, *security*, *privacy*, *reliability* and *resilience* in the face of environmental disruptions, human errors, system faults and attacks." [4] This paper focuses on safety challenges related to the IIoT.

Safety is a critical aspect of trustworthiness and a major concern in many IIoT systems. Safety is defined as "the condition of the system operating without causing unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment." An increasing number of devices and systems combine hardware, software and connectivity to sense and control the physical world in public spaces, factories, offices and homes. Many of these systems could cause harm to humans, animals or the environment if they did not have designed-in safety mechanisms that mitigate potential risks to a tolerable level. Harm in modern connected systems can result not only from unintentional system defects and random failures, but also from intentional manipulation of the system by a malicious adversary.

While different industrial sectors have long-established approaches to safety, those approaches and corresponding standards are still evolving to address new and unique safety challenges that IIoT brings. This white paper articulates four key challenges unique to the IIoT that affect safety characteristics and recommendations to address these challenges:

- increased security risks due to an increased attack surface,
- convergence of IT and OT,
- pervasive autonomy and
- inadequate regulatory framework and evolving standards.

CHALLENGE 1: Increased Security Risks Due to Increased Attack Surface

Security risks related to an increased attack surface expand the safety challenge in IIoT systems. The increase in connectivity at every level of the system leads to a much larger attack surface that adversaries could potentially exploit to remotely cause unsafe system behavior. Moreover, IIoT systems are becoming more dynamic than traditional

[3] "Key Safety Challenges for the IIoT" Qinqing Zhang, Andrew King, Frederick Hirsch, Semen Kort. 27 November 2017. IIC Whitepaper, IIC:WHT:IN6:V1.0:PB:20171127 https://www.iiconsortium.org/pdf/Key_Safety_Challenges_for_the_IIoT.pdf

[4] The Industrial Internet of Things Volume G8: Vocabulary, IIC:PUB:G8:V2.1:PB:20180822, Version 2.1, August 2018, IIC. https://www.iiconsortium.org/pdf/IIC_Vocab_Technical_Report_2.1.pdf

safety-critical systems, with participation of many organizations in the management of systems, with access rights assigned across organizations and changing over time. The blurring of traditional IT boundaries between internal and external systems increases risks.

The increase of the networked integration of systems and the increasing ability of adversaries to conduct attacks over the internet requires a new view of security in safety-critical systems designed to meet stringent safety requirements. IIoT stakeholders must be prepared to implement comprehensive security solutions at each level, from the system of systems down to the individual sensor or actuator. The Industrial Internet Consortium's (IIC) *Industrial Internet Security Framework*[5] provides plenty on this topic.

CHALLENGE 2: IT/OT CONVERGENCE

IIoT is driving tighter integration between Information Technology (IT) and Operational Technology (OT). IT assets include the enterprise network/information bus, database services, analytics engines and web services. OT assets include the technology of real-time networks (e.g., industrial Ethernet), programmable logic controllers (PLCs) sensors and actuators.

Integration between IT and OT implies not only physical convergence but also convergence of expectations and mentalities. Organizations must be prepared to address the security challenges due to IT/OT convergence that affect safety.

1. Organizations undergoing IT/OT convergence should attempt, wherever possible, to enforce the non-interference of IT and OT elements that share computing and communications platforms.
2. Manufacturers of safety-critical system components should investigate (and be prepared to implement) the types of IT-like capabilities users will come to expect, such as firmware updates via the network of their OT systems, while still ensuring safety.
3. Vendors of equipment and software with an IT legacy who want to participate in the IIoT community should familiarize themselves with how safety-critical software and hardware is developed, from requirements through validation and verification.
4. An organization should define areas of responsibility and ways of interaction between OT and IT specialists. For example, a computer security incident response team in an IIoT system should include OT and IT specialists.

CHALLENGE 3: PERVASIVE AUTONOMY

Autonomy is the ability of the system to make its own decisions with regards to external inputs and its changing environment and to be able to continue to operate even if disconnected from the

[5] Industrial Internet of Things Volume G4: Security Framework, IIC:PUB:G4:V1.0:PB:20160926 https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

network and remote analytics. Autonomy presents at least two safety challenges:

1. Autonomy changes how safety responsibility is divided between human operators and the system.
2. Sophisticated autonomy typically requires responding to dynamically changing circumstances and often involves the application of machine learning and artificial intelligence techniques that will themselves present verification challenges.

To meet the first challenge, the stakeholders of autonomous IIoT systems must engage with one another and come to a consensus on which safety judgments and tradeoffs are appropriate for the autonomous system to make on its own. To meet the second challenge, the IIoT community must invest in research and development for verification of autonomous systems.

CHALLENGE 4: INADEQUATE REGULATORY FRAMEWORKS AND EVOLVING STANDARDS

One important desired capability of IIoT system components is plug & play interoperability. The goal of plug & play interoperability is to enable systems operators to assemble and integrate a new system for use quickly. For example, a medical provider could combine a set of medical sensors, actuators and control algorithms on the cloud to automate the delivery of certain therapies. Although plug & play should be possible for certified safety-system components, scaling the certification process is a challenge because the certification process is not oriented toward plug & play. For example, the current US Food and Drug Administration (FDA) regulatory process for medical devices has provisions to approve devices designed to work with other specific devices via the so-called accessory rule. [6] Each time a manufacturer (or set of manufacturers) wants to market a pair of medical devices composed into a new system, they need to create a new regulatory submission. However, in IIoT systems, the number of possible device combinations explodes exponentially with respect to the number of devices in the ecosystem. In general, pair-wise regulation is hugely burdensome for both the manufacturers and the regulatory agency. Each regulatory submission usually takes significant resources to prepare and review.

To overcome existing regulatory burdens and help foster a large and vibrant IIoT ecosystem, industry and regulatory bodies should be prepared to move from system and pair-wise regulatory frameworks to approaches that scale with a larger number of interconnected components. An alternative is to have contract-based regulation, based on well-defined interfaces and behaviors of devices enabling the interfaces to be certified rather than the individual integrations.

[6] Medical Device Accessories – Describing Accessories and Classification Pathways - Guidance for Industry and Food and Drug Administration Staff, FDA-2015-D-0025, December 20, 2017, https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm429672.pdf

CONCLUSION

Achieving safety and security will require management and design efforts created to avoid faults and build-in safety and security in all phases of the system life cycle. Verification and validation, the use of safety compliant elements, adoption of security best practices and a review of the overall system and its components are all important practices to achieve a system that meets appropriate safety and security requirements. This all implies a safety and security in-depth strategy with a view toward the overall result.

The Industrial Internet of Things raises new concerns that go beyond such approaches. The number and broad distribution of devices significantly raises the security attack surface, especially when the potential difficulty of managing updates is considered. The increased security risks can impact safety due to the ability of attackers to misuse systems or cause denial of service attacks. This can be harmful to the individual health and life (e.g., in medical applications) or to the community (e.g., in manufacturing with potentially toxic or harmful materials).

The convergence of IT/OT has many implications due to the differing cultures and business requirements, including issues related to the difficulty to update software frequently while maintaining confidence in the safety of the system. This convergence may increase the impact of security vulnerabilities through increased time that they exist, increasing safety concerns. At the same time, frequent software updates can also introduce new security vulnerabilities and reduce the effectiveness of safety evaluations, also increasing the safety risks. This suggests that new approaches beyond reactive software patching may be required to produce safe software for IIoT.

If this were not enough, it is not exactly obvious how to ensure the safety of autonomous learning systems, especially if they have unintended side effects. The challenges of ensuring safety for autonomous learning systems in a dynamic and changing environment are not well understood.

Finally, the entire regulatory regime is oriented toward analyzing and approving the safety of pairs of devices for a specific purpose. This is at odds with the need for fast and dynamic business where new applications may be created by combining existing technologies in new and unexpected ways. This will require a new approach toward regulation based on new technical and procedural approaches.

The IIC white paper reviews these concerns in more detail and offers some possible approaches. Given the importance of safety to individuals and society it is essential that work be devoted toward solutions. The paper is a call-to-action and -cooperation to find and implement solutions to enable safety in the world of the Industrial Internet of Things.

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