The Business Viewpoint of Securing the Industrial Internet

Executive Overview

[IIC:WHT:IN:V1.0:PUB:20160908]

CONTENTS

1 INTRODUCTION

Increasingly, standard Internet technologies are finding their way into industrial control systems, displacing the purpose-built technologies historically used to build such systems. By enabling global access and applications such as advanced analytics, this trend is enabling industrial enterprises to improve business performance and production efficiencies by orders of magnitude.

An industrial control system is a collection of devices (sensors, actuators, and controllers) that work together to sense, monitor and control something in the physical world. These systems are ubiquitous in the modern world and control much of the critical infrastructure around us – dams, power plants, transportation systems, the electric grid, mining, chemical and manufacturing plants, commercial buildings, data centers and medical systems.

The continuing explosion of connected devices provides opportunities for unparalleled growth and performance gains in industrial systems. They present unprecedented risks of hostile attacks to plant personnel, to society and the environment at large, and to the businesses that operate industrial processes. Industrial networks originally designed to be isolated are now exposed to continuous attacks of increasing sophistication.

Recent events[1] have illustrated the risk of being attacked from unexpected sources both inside and outside the system, whether intended or accidental. There is a commanding need to protect against error, mischance and malicious intent. The Industrial Internet Consortium (IIC) believes that these industrial security risks represent a major threat to world safety and security. To that end, the IIC has developed a common security framework and an approach to assess cybersecurity in Industrial Internet of Things systems. The framework and approach will be published in September 2016 in the IIC's *Industrial Internet Security Framework Technical Report* (IISF).

The IISF is written for CTOs, CISOs and other technical experts. This white paper summarizes the IISF for CEOs and business managers to encourage them to allocate resources to their technical experts for education, to assess risks and to plan ahead. They can then implement the Industrial Internet security technologies available today to enhance the availability and reliability of their system and thus gain significant return on investment (ROI).

This executive overview of the IISF offers a window into the technical report's considerations and best practices. It highlights the need for every organization across every industry to secure their IIoT systems and to deploy best-practice security solutions immediately.

[1] http://www.bbc.com/news/technology-30575104

http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

1.1 DEFINING IIOT

The Industrial Internet concept has evolved over the last decade to encompass the many systems that combine hardware, software and networking capabilities to sense and control the physical world. These interconnected end-to-end systems are called *Industrial Internet of Things* (IIoT) systems. They enable significant increases in performance, scalability and efficiency that drive transformational business outcomes.

Designing and operating IIoT systems with security and privacy is essential to meet regulatory and compliance requirements and to ensure safe and reliable operation of the systems themselves. Proper system security isolates failures and problems to prevent their spread, enhancing system resiliency and reliability in the face of error or attack. Managing security and privacy risks also reduces the financial and reputational costs of any breach or safety issue, as evidenced by the costs of well-known breaches[2] to small and large businesses and government organizations.

1.2 THE EVOLUTION OF IIOT SYSTEMS

Historically, security in critical industrial control systems relied on physical and network isolation of vulnerable components and on access rules. Security was, and still is, enforced through physical locks, alarm systems and, in some cases, armed guards. The potential for human error or misuse was primarily through direct access, with that risk mitigated by good design, review, testing and training. It rarely occurred to designers that these systems might one day be exposed (directly or indirectly) to a global network, and be remotely accessible by not only by legitimate users but also rogue actors or nation-states.

Over the past few decades, increasing computing power, ubiquitous connectivity and data analytics techniques have led to a convergence of control systems and Operational Technology (OT) with Information Technology (IT) and the Internet. This integration can increase productivity, efficiency and performance of the existing operational processes. Some examples: Operations data can be mined for performance metrics to enable failures to be predicted; optimizations can be performed across fleets and software upgraded remotely.

However, with these gains come risks. Systems that were originally designed to be isolated are now exposed to attacks of ever-increasing sophistication. Connecting control systems to IT systems and the Internet presents an inviting target for attacks and collecting large amounts of data ("Big Data") raises privacy concerns.

One example is the IIC case study[3] at a large water and wastewater treatment plant where interconnection to the city's IT network increased operational efficiency but created risk that

[2] http://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/

[3] http://www.iiconsortium.org/case-studies/Belden_Wastewater_Systems_case_study_final.pdf

system operation could be attacked through the city-wide IT infrastructure. The city reviewed the end-to-end system design and added segmented security controls throughout the control network to retain the business value and enhance system reliability while closing the attack surfaces. Connection to the Internet, whether direct or indirect, consistent or intermittent creates new risks in operational processes to society and the environment.

A successful attack on an IIoT system has the potential to be as serious as the worst industrial accidents to date (e.g., Chernobyl and Bhopal), resulting in damage to the environment, injury or loss of human life. There is also risk of secondary damage such as: interruption or stoppage of operations, destruction of systems, leaking sensitive business and personal data resulting in loss of intellectual property, harm to the business reputation, loss of customers, material economic loss, damage to brand and reputation, damage to critical infrastructure handling electricity, water, oil, and gas, irreparable damage to the environment. Attacks on critical infrastructure and IIoT are growing and appropriate responses must be strategically planned.

The need for security exists throughout any industrial manufacturing facility and outwards to public infrastructure. Obscurity or small size is no protection in an interconnected world.[4] To this day, many systems remain vulnerable. Although there is awareness and concern for security, the ability to address these shortcomings adequately has not always been feasible. However, to succeed, this new Industrial Internet evolution requires a comparable evolution in security. The Industrial Internet requires a security framework that formalizes knowledge and best practices from both IT security and industrial control (operational) security and a rigorous approach to make trade-offs between their contrasting perspectives.

1.3 SAFEGUARDING THE BUSINESS INVESTMENT IN IIOT SYSTEMS

Given the risks, it is not surprising—even before the Industrial Internet—that governments have put in place wide-ranging regulations for critical systems and require their compliance. Regulatory and compliance rules mandate controlling access to financial systems, protecting credit card information, upholding privacy expectations and protecting critical infrastructure. Decisions on the implementation and operation of an IIoT system must account for these externally imposed business policies, including strict safety requirements. These are requirements the business must meet, no matter the cost.

Looking beyond compliance, maintaining business value requires safeguarding the business investment in IIoT systems and protecting their operations against the risk of damage brought about by security breaches, but this costs money. A balance must be achieved between the ROI of the security and its effectiveness, as gauged by the threats to that system.

Evaluating the ROI of an implementation of a secure system design must be grounded in a realistic assessment of current and future threats, the risks they pose and how they may prevent the system from fulfilling its intended business functions. Threats may be inadvertent (from

[4] http://www.cnn.com/2015/12/21/politics/iranian-hackers-new-york-dam/

hazards, device errors, or human error) or intentional (from attackers). From that, implementation choices can be made rationally to deliver an acceptable ROI.

Security can also enable new value-added features and capabilities. For example, intelligent metering[5] can support pay-per-use revenue models; rights management and private data enables useful sharing of data from devices[6]; and predictive maintenance[7] maximizes the ROI of industrial equipment. These kinds of value-added capabilities may require more robust and secure behavior extending beyond the core functions of the underlying devices, and they may drive requirements for additional security features.

Security should not be implemented for the sake of security; it should contribute to the reliability and availability of the system and the business decision-making process. IIoT security helps make available valuable information that was not previously available, for example, the trustworthiness of business data points. Applying this new information improves the accuracy of the business-critical decisions, justifying the ROI for the security investment.

1.4 THE CORE ELEMENTS OF TRUSTWORTHINESS IN IIOT

An IIoT system exhibits end-to-end characteristics that emerge as a result of the properties of its various components and the nature of their interactions. These characteristics include safety, resilience, reliability, security, scalability, usability, maintainability, portability, composability and a long list of other "-ility" terms. For an IIoT system, a main stakeholder goal is trustworthiness. *Trustworthiness* is the degree of confidence one has that the system performs as expected with respect to the key system characteristics in the face of environmental disruptions, human errors, system faults and attacks.

[5] http://www.iiconsortium.org/case-studies/Cyberlightning_Fortum_Case_Study.pdf

[6] http://www.iiconsortium.org/case-studies/RTI_BK_Medical_case_study.pdf

[7] http://www.iiconsortium.org/case-studies/Blinded_Manufacturer_case_study.pdf

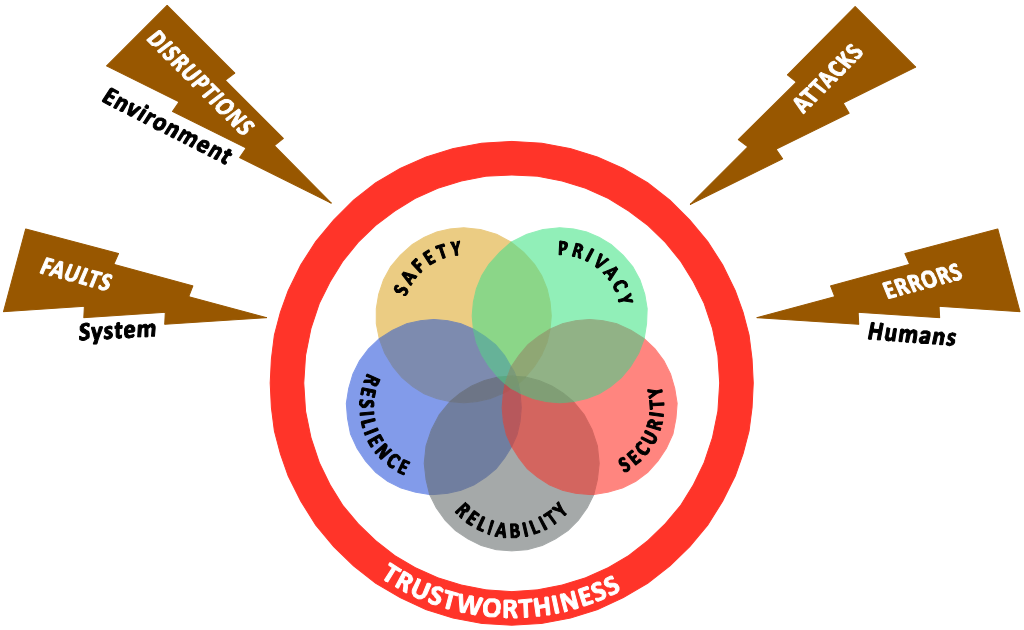

Figure 1.1: Trustworthiness of an IIoT System

Security cannot be considered in isolation. It interacts with other important characteristics of the IIoT system, and must be considered as a whole. The five characteristics that most affect the decisions about the trustworthiness of an IIoT system are security, safety, resilience, reliability and privacy. These are referred to as *key system characteristics.*

Key System Characteristic	Definition
Security	*Security* is the condition of the system being protected from unintended or unauthorized access, change or destruction.
Safety	*Safety* is the condition of the system operating without causing unacceptable risk of physical injury or damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.
Reliability	*Reliability* is the ability of a system or component to perform its required functions under stated conditions for a specified period of time.
Resilience	*Resilience* is the condition of the system being able to avoid, absorb and/or manage dynamic adversarial conditions while completing assigned mission(s), and to reconstitute operational capabilities after casualties.
Privacy	*Privacy* is the right of individuals to control or influence what information related to them may be collected and stored and by whom, and to whom that information may be disclosed.

Resilience, reliability and security relate to the functional characteristics, as they directly affect the system's ability to meet the stakeholders' functional expectations of the system. Safety and privacy relate to the system's ability to be compliant with their expectations about impacts on the environment.

The key system characteristics are under siege from four different types of impacts:

- faults of the system itself,
- disruptions from the environment, including weather conditions, loss of power, fire, physical force etc.,
- errors by humans, including operators, installers, owners, integrators and also the designers of the system, and
- attacks or deliberate efforts to reduce the trustworthiness of the system.

2 EVALUATING AN IIOT SYSTEM WITH KEY SYSTEM CHARACTERISTICS IN MIND

IIoT systems differ from conventional IT systems in many ways. This section describes some of these differences and their impact on IIoT security. Because of their strategic importance, IIoT systems are subject to many constraints, requiring security solutions to be designed or adapted to fit within the physical and regulatory environments in which they operate. Security solutions exist today. The lessons learned from testing and implementing them are captured in the IISF.

Key system characteristics such as resilience and safety take higher priority in the design, deployment and operation of IIoT systems than in conventional IT systems. IIoT systems also differ in the high value of the industrial assets involved and the potential economic impact of any disruption to the processes that they manage or control. Moreover, IIoT systems are often tailored towards specific business requirements and often perform these functions for decades, while general-purpose IT hardware may be replaced five to ten times during that lifespan. IIoT system security solutions need to account for these differences.

2.1 THE CONVERGENCE OF OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY

In the past, there has been a strong separation between IT and OT. IT covers computer and communication systems that support corporate functions such as finance, human resources, supply chain, order management and sales. These functions tend to be common across industries. Software applications in IT are people-centric, involving human operators using computing devices, where software is developed and tested with regard to its reliability or ability to withstand unexpected input and keep performing its intended function at a degree that may not be adequate for industrial operations. Real-time behavior in IT usually is tailored to expectation of human interaction only—for example, how long an operator can wait until a website shows the requested information.

OT, on the other hand, is a combination of hardware (initially) and software (more recently) that collects information and causes changes in the physical world through the direct monitoring and control of physical devices in industrial contexts. OT covers systems that deal with the physical transformation of products and services. These tend to be task-specific, and are often highly customized for specific industries. Control of physical systems, unlike IT systems, is highly automated and requires less user interaction. As a result, the user-based access controls apply less in OT than they do in IT. On the other hand, real-time behavior can be essential for correctness: for example, a system not reacting quick enough after receiving alerts can create a disaster.

Converging IT and OT usually involves a complex merger of key system characteristics between the two. Though industrial systems have become a combination of both IT and OT, where devices are controlled by software, usually these systems have been isolated in OT clusters. Connecting or bringing systems together creates a security problem, as preserving information integrity and system reliability in OT systems now becomes a matter of safety: If the control information stored in an OT system is modified without authorization due to lack of correct security implementations, or parts of the process can be brought down, this may cause a safety hazard and reliability problems.

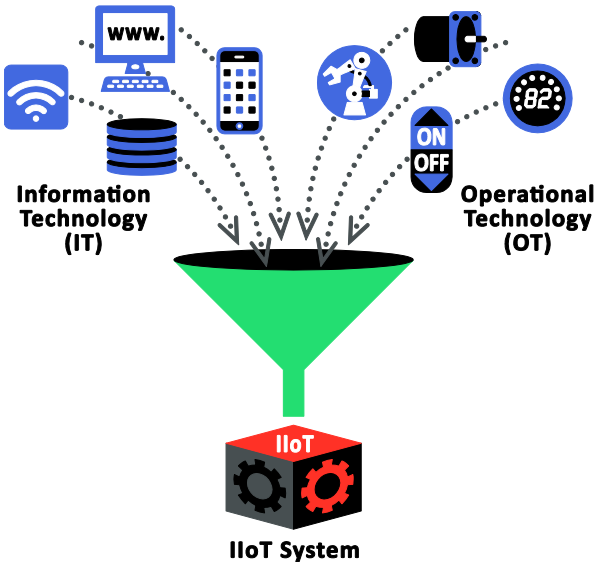

Figure 2.1: IT/OT Convergence

2.2 Data Management Aspects

A distinguishing characteristic of the Industrial Internet is that each vertical industry (e.g. Healthcare or Smart Cities) has unique needs. Within each vertical, use cases and applicable data boundaries are defined with key stakeholders, and then a data flow analysis must be performed, to make sure that data is protected at each stage – from sensor-generated data, to the handoff of data to other boundaries via trusted interfaces and the final path into the cloud.

It is difficult for one provider to deliver all of the services needed by a growing client base. That means that many closed systems will need to allow for trusted business partners or clients to access and manage equipment or system data. The ability to enable partner or client access and control over specific systems or data elements selectively is often a design requirement, even if that capability is not enabled or activated during the initial deployment of the system. The security implementation must consider this dynamic model in order to ensure continued protection when changes to control and management are enacted.

2.3 Data in the Cloud

Protecting information flows to and from the cloud and during processing and storage by cloud providers is vital for security and privacy. Protecting and securing information flows from the cloud back into control systems is also vital to protecting the safety and resilience of physical processes. The risks are large. For example, stolen credentials may allow attackers to control physical infrastructure remotely and stolen administrative credentials for cloud providers can facilitate attacks on many of the vendor's customers simultaneously.

2.4 GREENFIELD VS. BROWNFIELD DEPLOYMENTS

The term brownfield describes an environment where new solutions and components must co-exist and interoperate with existing legacy solutions already in place. The term is used in contrast to greenfield, where a new solution is unconstrained by what is already there. In general, OT environments are largely brownfield with legacy security controls that are often insufficient when deployed in an IIoT environment.

Many IIoT systems are designed and deployed in a brownfield environment with existing legacy equipment, protocols and practices. In general, it is not an option to rip out the existing legacy infrastructure to build a more secure system. Therefore, additional security capabilities must be retroactively added to an existing brownfield control systems to increase their overall security as they migrate to IIoT systems.

3 THE BUSINESS VIEWPOINT

Effective business decision-making is an important component of industrial security programs. Business decision-makers must understand the security risks and the costs and benefits of different defensive postures.

Investment in IIoT systems and their operations must be protected against the risk of damage. This damage may include interruption or stoppage of operations, destruction of equipment or systems, leaking of sensitive business and personal data resulting in loss of intellectual property or harm to the business reputation and loss of customers. On the other hand, heightened security may lead to additional investment and greater times to deploy. In some cases, it may affect user experience negatively. These additional costs must be justified to stakeholders in the context of the business risks they are addressing, sometimes in terms of costs saved by averting damages. Today much of this investment is made in terms of redundancies and safety systems: with IIoT, investment in security is required both to maintain reliability and safety as well as to protect against these threats.

Managing risk is an important goal of a security (and privacy) program. Security risk management requires an understanding of the system, important roles and their viewpoints and concerns, the process of managing risk, and an understanding of threats and choices of how they are handled.

Security risk is managed by evaluating risk, deciding what parts, if any, of a security program to invest in, and then deploying, operating and periodically re-evaluating risk, and the effectiveness of the program to address risk.

Security risk can be addressed in a variety of ways:

Risk Acceptance does not reduce the risk; it simply means one accepts it. This strategy is usually applied when the cost of the countermeasures exceeds the cost of the risk if it were to occur.

Risk Avoidance seeks to eliminate the risk entirely to avoid all exposure (diametrically opposed to risk acceptance). Common examples of risk avoidance include active countermeasures such as

patching vulnerable software and removal of vulnerable systems and software. When the vulnerability is gone, the risk is eliminated.

Risk Mitigation is implementing measures to reduce the impact of a vulnerability that cannot be avoided. A common example is the use of backup solutions when systems are compromised and data is lost or corrupted. This approach is one of the more common risk management strategies.

Risk Transferal removes the risk by handing it to a third-party that is willing to accept it. This is a common technique when the particular risks are not a core competency and are better addressed by another actor. Insurance and outsourcing are prime examples of risk transferal.

The success of any security management program and its resultant byproducts depends largely on the ability to define applicable metrics, use them to observe shortcomings and create and apply corrective actions in a timely and efficient manner.

3.1 METRICS AND KEY PERFORMANCE INDICATORS

Business decision-makers should monitor reports on the security of their IIoT systems from the moment the systems are conceived, through their design and creation, and throughout their operation. This should be at the same depth as they monitor other key characteristics like performance, throughput, cost and efficiency. Selecting the correct measures and metrics lets reports capture the right information about a system to inform decision makers, operators and other stakeholders.

To demonstrate the value of security to the operational process, it should be clearly and accurately represented by the security metrics and key performance identifiers (KPIs). If operational personnel can make improved business decisions based on security metrics and KPIs, then the value of the security can be quantified in terms of the costs saved by averting wrong decisions. Security then becomes a valuable part of the operational process.

On the other hand, security metrics set up a continuous feedback loop to identify areas of risk, increase accountability, improve security effectiveness, demonstrate compliance with laws and regulations and provide quantifiable inputs for effective decision-making. They help identify security problems early, and assist in quicker and more efficient management and governance.

3.2 RISK ASSESSMENTS

The core risk-assessment activity is the process of identifying and ranking risks as described by bad outcomes that could result from attacks identified as unacceptable. To mitigate risk, one may deploy actions, controls, processes or techniques that reduce the risk of vulnerabilities to or impact of an attack. These *countermeasures* function by eliminating or preventing the attack, minimizing the impact of a vulnerability or an attack, or exposing and reporting the existence of a vulnerability or an attack in order for mitigation to occur.

The appropriate risk assessment approach takes into consideration the cost of consequences and the probability of a successful attack occurring. Both factors vary from situation to situation in the ability to be estimated accurately. Systematic approaches may be used to develop models of

possible consequences and possible attacks.

3.3 THREAT IDENTIFICATION

The term *threat* should be interpreted broadly to include any influence or incident that would interfere with the normal, intended use of the underlying system. A secure IIoT system must account for possible failures in the operating environment, such as human error, device failure, extreme environmental or weather conditions.

While it is not practical to anticipate every possible threat, a resilient security model that contemplates broad changes in the operating environment can mitigate the impact of many unplanned situations.

Risk comes from various sources, including risk to both the security and reliability aspects, as well as the ever-present safety considerations. All of these have to be carefully considered when designing the functional security model.

There are a number of considerations:

- What are the greatest sources of cybersecurity risk to the business?
- What IIoT systems are potentially involved?
- Where do threats originate?
- Who are the relevant threat actors?
- What is the impact of a successful attack or other security incidents?

IIoT system manufacturers, system integrators, owners and operators should establish and maintain a security program that provides governance, planning and sponsorship for the organization's security activities. These activities should align with the overall business objectives and risk strategy of the organization.

An evaluation framework enables organizations to evaluate security capabilities consistently, communicate the capability levels meaningfully and prioritize security investments. The IISF provides a comprehensive, trusted approach to evaluating security.

4 PERMEATION OF TRUST IN THE IIOT SYSTEM LIFECYCLE

A typical IIoT system is a complex assembly of system elements. The trustworthiness of the system depends on trust in all of the system elements, how these elements are integrated and how they interact with each other. *Permeation of trust* is the hierarchical flow of trust within a system from its overall usage to all its components.

Each IIoT system has a unique permeation of trust. Each element has designers, developers, manufacturers, operators, etc., (collectively referred to as *actors*) that execute the various roles in the creation, integration and usage of the hardware and software of an IIoT system. These roles cut across multiple organizations, each with its own interests that must be aligned.

Permeation of trust cuts across the complete system lifecycle, not just during operation. Everything from supply chain, to commissioning, provisioning, regular usage and finally end-of-

life decommissioning must be carefully monitored to ensure the initial trustworthiness is preserved through its lifecycle.

4.1 System Lifecycle

The trust may be based solely upon the reputation of the system vendor, without proper validation that the trust is warranted, but it needs to be explicitly described, verified, controlled and supervised.

Permeation of trust can be structured in terms of the role a specific actor has, in one of three different layers:

- *Component builders* represent hardware vendors, software publishers and service publishers that provide specific capabilities as a standardized hardware or software product or as a software service.
- *System builders* represent system integrators and solution providers that integrate or adapt the built components in usage-specific individual solutions or service capabilities.
- *Operational User* represents the *system owner/operator* that use the components, solutions or services for their intended purposes.

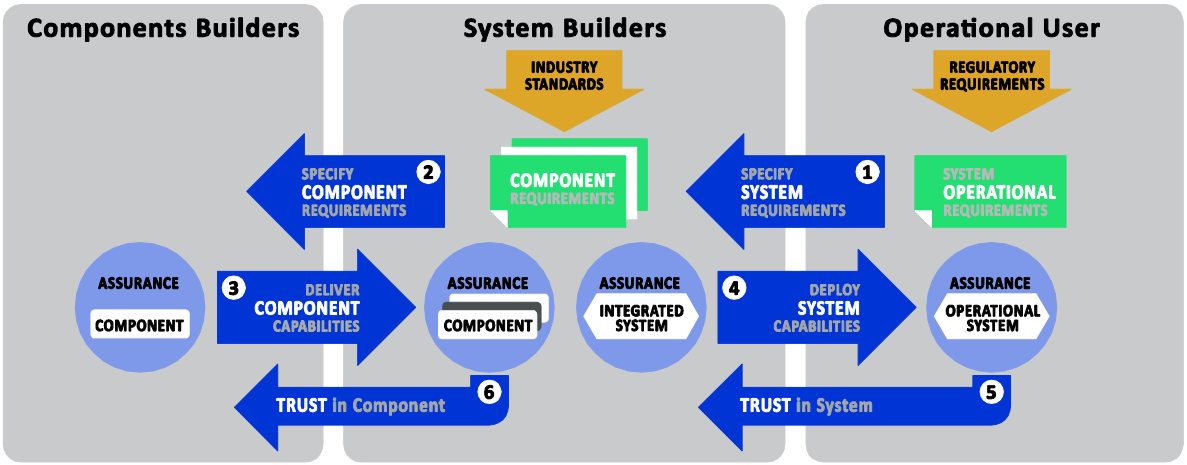

Figure 4.1: Permeation of Trust from an Industrial Operator Perspective

The trust lifecycle starts with the specification of trust requirements that result in the delivery of trust capabilities. The assurance that these capabilities meet the stated trust requirements becomes the basis of trust in the system.

- System owners and operators instigate the building of trust by (1) specifying trust-related requirements as part of the operational system requirements. These requirements are then issued to the system builders as part of the system specification.
- System builders in turn (2) break them down into specific trust requirements for each of the components of the system.

- Component builders respond to these requirements by (3) delivering components that meet the specified trust assurance requirements. Compliance of the delivered component capabilities to their specifications is a part of assurance performed by the vendors prior to delivery, and by system builders on receipt (and potentially independent third-party agencies).
- The delivered system capabilities are (4) verified and assured in the operational context by the owner/operator or an independent third party.
- Once operational assurance is achieved then (5) trust is initiated in the system and permeates down from the owner/operator to the component builders via the system builders.
- System builders are responsible for (6) integrating all the assured components and assuring that together, they meet the specified requirements for the integrated system.

Trust flows down from the owner/operator to all parts of the IIoT system, but trust must be built from the bottom up. Guidelines, capabilities, requirements and the roles involved in building trust throughout the IIoT system lifecycle are described in the IISF.

5 CONCLUSION

This white paper examines the basis of the Business Viewpoint for the IISF: key system characteristics, the notion of a trustworthy system and the need for managing the permeation of trust in IIoT systems. It is a brief summary of the IISF that benefits from the knowledge and experience gained by security experts in multiple IIoT system deployments. A true collaboration project in every sense of the word, the IISF reflects thousands of hours of security experts contributing their knowledge and experiences for the benefit of all IIoT system deployments. Sample case studies from some of these contributors, describing real world experiences of securing industrial Internet systems, are available on the Industrial Internet Consortium website.

Members of the IIC are developing many testbeds that implement functionality in different verticals. The Security Working Group provides security and privacy guidance to them for the implementation of more mature security solutions. Lessons learned in these testbeds are fed back to the IISF as the document continues to evolve with the Industrial Internet.

Besides the Business Viewpoint, the IISF covers the Implementation Viewpoint in depth. The Implementation Viewpoint guides organizations through the complex evaluation of and recommendations for securing IIoT systems. Topics covered in this section include: Endpoint Protection, Secure Communication and Connectivity, Security Monitoring and Analysis, Security Configuration Management, Endpoint Data Protection, Security Model, and Policy. The IISF is a living document reflecting collaboration of cross-industry expertise and the actual testing of these concepts, recommendations and practices.

For a full appreciation and understanding of the Industrial Internet Consortium's approach to securing IIoT systems, the IISF is the primary source.

6 ABOUT THE INDUSTRIAL INTERNET CONSORTIUM

The Industrial Internet Consortium® (IIC™) is a global, member supported, organization that promotes the accelerated growth of the Industrial Internet of Things by coordinating ecosystem initiatives to securely connect, control and integrate assets and systems of assets with people, processes and data using common architectures, interoperability and open standards to deliver transformational business and societal outcomes across industries and public infrastructure. The Industrial Internet Consortium is managed by the Object Management Group (OMG). For more information, visit www.iiconsortium.org.

7 ACKNOWLEDGEMENTS

This document is a work product of the Industrial Internet Consortium.

The Industrial Internet Consortium wishes to thank Daniela Previtali, Global Marketing Director at Wibu-Systems, Jeff Lund, Senior Director, Product Line Management, Industrial IT Division at Belden, Inc., Evan Birkhead, VP Marketing at Bayshore Networks, Stefania Boiocchi, Business Development Manager at Infineon Technologies and Steve Hanna, Senior Principal at Infineon Technologies for their leadership on this white paper.