A Short Introduction into Trustworthiness

Authors:
Marcellus Buchheit
President and CEO
Wibu-Systems USA
mabu@wibu.com

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

Sven Schrecker
Vice President and Chief Architect, Cyber Security
LHP Engineering Solutions
sven.schrecker@lhpes.com

The Cambridge Dictionary defines *trustworthy* as *deserving of trust, or able to be trusted*.[1] In the context of an industrial system or a component used for an industrial system, *trustworthiness* means that a subject deserves trust or is able to be trusted. But what is trust? The dictionary says *trust* is *to have confidence in something, or to believe in someone*,[2] but this lacks technical guidelines, so the Industrial Internet Consortium (IIC) has refined the definition, as described here.

The Industrial Internet Reference Architecture (IIRA)[3] designated five Key System Characteristics to support a system's business purpose and to ensure that functions perform adequately without compromise. The five characteristics are: safety, security, reliability, resilience and privacy. A similar list of "dimensions" was created in 1999 by the *Committee on Information Systems Trustworthiness* to describe the trustworthiness of *networked information systems* (NIS).[4] In early 2016, IIC adapted the term to its own list of five characteristics, defining the core of trustworthiness. Contemporaneously, NIST also reintroduced the term based on the same characteristics.[5] In addition to the

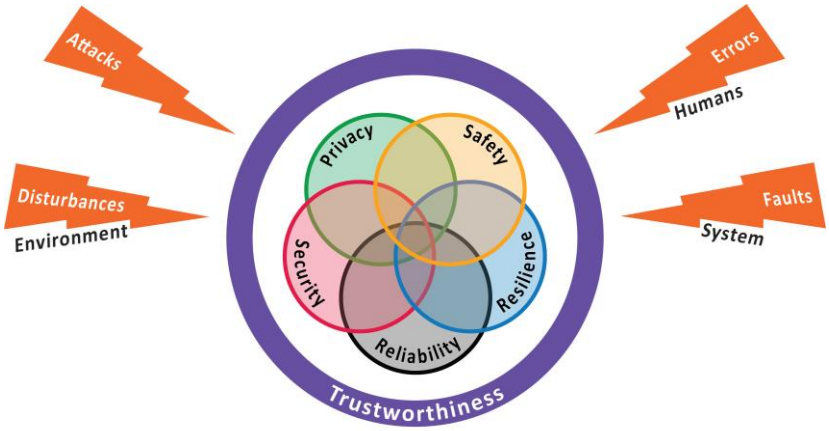

Figure 1: Trustworthiness Characteristics and Threats

[1] Cambridge Dictionary, Cambridge University Press, https://dictionary.cambridge.org/us/dictionary/english/trustworthy

[2] Cambridge Dictionary, Cambridge University Press, https://dictionary.cambridge.org/us/dictionary/english/trust

[3] Industrial Internet Consortium: Industrial Internet Reference Architecture (IIRA), V1.8, January 2017. https://www.iiconsortium.org/IIRA.htm

[4] Schneider, Fred B. (Editor), Committee on Information Systems: Trustworthiness: Trust in Cyberspace, National Academic Press, Washington D.C., 1999, retrieved 2016-09-26 *http://www.nap.edu/catalog/6161/trust-in-cyberspace*

[5] National Institute of Standards and Technology (NIST), Information Technology Laboratory, Glossary: Trustworthiness, https://csrc.nist.gov/Glossary/?term=2283 and https://csrc.nist.gov/Glossary/?term=2284

trustworthiness characteristics, IIC also specified four groups of threats that endanger a trustworthy system, which resulted in the following definition:

"Trustworthiness is the degree of confidence one has that the system performs as expected. Characteristics include safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks."[6]

The five characteristics are defined as *trustworthiness characteristics* and the group of threats as *trustworthiness threats,* as represented in Figure 1.

TRUSTWORTHINESS CHARACTERISTICS

A deeper view into the trustworthiness characteristics identifies the strengths of trustworthiness. All characteristics are defined in the IIC Vocabulary Technical Report[6]:

Safety ensures that a system operates without unacceptable risk of physical injury or damage to the health of people and indirectly on damage to property or to the environment. In general, nearly any damaging environmental event (e.g., pollution of soil, air or water) presents a risk to human health, in which case, safety implementations should minimize those risks. Safety does not protect the operation or the system itself, unless it involves human risk.

Security protects a system from unintended or unauthorized access, change or destruction. Information Technology (IT) security ensures availability, integrity and confidentiality (AIC model) of data at rest, in motion or in use. In industrial systems, the control data used to execute physical operations has a potential of physical damage and requires advanced protection. Systems also need "traditional" security that protects the system from theft or unauthorized access by installing fences, walls and locks or by employing security guards.

Reliability describes the ability of a system or component to perform its required functions under stated conditions for a specified period of time. This includes any considerations for physical abrasion, expired software versions, and well-known potential malfunctions that result in frequent maintenance, replacing end-of-life components or software updates. Reliability protects the operation of the system and the system itself, as it is essential for it to be a productive system.

Resilience describes the ability of a system or component to maintain an acceptable level of service in the face of disruption. In contrast to reliability, resilience addresses unexpected and unplanned system statuses that can result, for example, from human errors in operation or an environmental event (loss of electric power, earthquake, etc.). The main purpose of resilience is to prevent or at least reduce any serious impact of a disruption to the system by damage or loss of operation.

[6]Industrial Internet Consortium: Vocabulary, V2.1, August 2018, https://www.iiconsortium.org/vocab

Privacy protects 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. Individuals comprise all types of people including customers, guests or employees.

There are several interesting relationships between these characteristics:

- Some characteristics' goals oppose each other. Security protects an industrial system and its components from the malicious attacks or erroneous behavior of humans (including the system designers and operators) and from environmental disturbances. In direct contrast, safety protects humans (including the employees within the system) and the environment from any bad behavior of the system.
- Some characteristics are context-dependent. Reliability addresses the correct functionality of the system under specified conditions. Ideally, reliability ensures that the operation of the system is not disrupted as long as it works under stated conditions. In direct contrast, resilience addresses the functionality of the system under non-planned conditions. In practicality, resilience cannot guarantee that the system operates completely as expected but can reduce the consequences to an acceptable minimum.
- Some characteristics are interdependent. Privacy protects only human-related data but does not address business- or operational-related data. Such data is part of the system, and if protection is necessary, security is responsible.
- The characteristics must be considered together, rather than in isolation. For example, safety is only involved in protecting people and indirectly the environment; security and reliability are responsible for the protection of the system itself when it works under stated conditions. Additionally, resilience is responsible as soon as the normal, reliability-controlled condition is lost.

Trustworthiness is still evolving. For example, safety addresses only human and environmental factors, as there is no "cyber safety" to protect data: If a sensor runs out of control and attempts to delete all data in a cloud database, no safety function will protect the database. But in that case, security around the cloud database should block the attack from the sensor.

The trustworthiness characteristics can enhance each other or limit each other. Reasonable system design has to control the impact of such challenges. Establishing trust in a system requires assurance that the system is trustworthy. Such assurance can be based on evidence that the trustworthiness characteristics have been met appropriately for a specific industrial IoT system. Different decisions and tradeoffs must be made depending on the nature of the system. Concerns in a factory are different from in a hospital operating room. This means that there is no simple course of action. Instead, one must develop an understanding of the many considerations

involved in defining the appropriate trustworthiness implementation.

For example, an oil pipeline may incorporate a comprehensive set of sensors that instantly report any leaks via a WAN network. Finding and closing even small leaks as quickly as possible will significantly increase safety efforts to protect humans and the environment. By keeping the functional downtime low during the repair of a leak, the reliability is also increased. But if a hacker attack shuts down the monitor center because the network security system failed, then safety would be compromised. Resilience in this case would initiate a permanent manual surveillance of the pipeline until the IoT sensor network is reestablished. Without such a backup plan to maintain pipeline safety after the IoT sensors were rendered unusable, a planned physical attack could create much larger damage to the pipeline, to the environment and to people.

TRUSTWORTHINESS AND IT/OT CONVERGENCE

Trustworthiness is essential to industrial IoT systems that combine informational technology (IT) with operational technology (OT) and can use data, sensors and actuators to impact people and the physical environment. The consequences of acting badly can lead to loss of human life, long-term impact on the environment, interruption of critical infrastructure, as well as other consequences including disclosure of sensitive data, destruction of equipment, economic loss and damage to reputation. Additional drivers include concerns over regulatory compliance as well as the fear of liability and litigation.

Designing an Industrial IoT system requires the interweaving of IT and OT principles,[7] frequently conflicting with IT and OT "traditions." Trustworthiness can help to describe such conflicts. As shown in Figure 2, security and privacy are part of the IT world

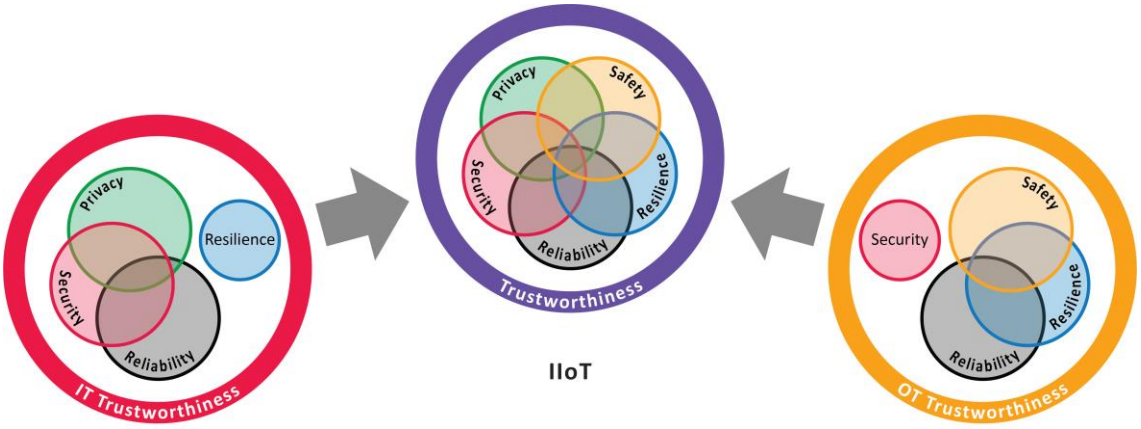

Figure 2: Bringing IT and OT Trustworthiness concerns together in the industrial IoT

[7] See definition of IT/OT Convergence, Industrial Internet Consortium: Vocabulary, V2.1, August 2018, https://www.iiconsortium.org/vocab

but not well addressed in the OT space. On the other hand, safety and resilience are essential in the OT world but not widely understood in the IT world. Bringing these two worlds together in IoT requires deeper understanding, integration and tradeoffs. Trustworthiness is a helpful tool in this process.

the flow of trust within a system from its overall usage down to its smallest components and requires trustworthiness of all aspects of the system. Trustworthiness requires ongoing effort over time as systems and circumstances change.

Figure 3 shows the differing roles of

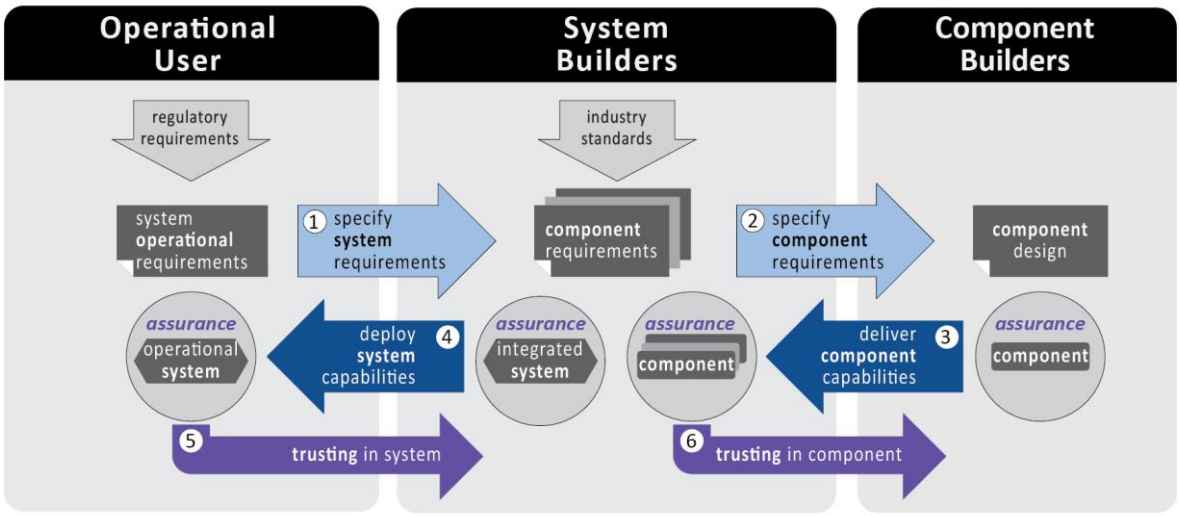

Figure 3: Permeation of Trust and System Roles

PERMEATION OF TRUST IN AN INDUSTRIAL IOT SYSTEM

Achieving trustworthiness in IoT systems requires recognition that a complex IoT system is a system of subsystems, built with components. The trustworthiness of the overall system depends on the trustworthiness of each of the subsystems and each of the components, how they are integrated, and how they interact with each other. Trustworthiness must be pervasive in IoT systems, which means there must be *trustworthiness by design* and a means to achieve assurance that the trustworthiness aspects have been addressed properly for the system of concern. Permeation of trust is

operational users, system builders and component builders that are helpful in modeling a system and making it more trustworthy. The operational user, for example an automotive manufacturing plant or a medical research lab, must define the trustworthiness requirements including tradeoffs, and must be able to verify, control and supervise that those trustworthiness requirements are met throughout all stages of the supply chain. System builders and component builders need to understand the requirements and provide assurance that they have been met. The operational users will require assurance of trustworthiness, demonstrated through evidence, so that they have confidence that the system will

adhere to the trustworthiness requirements based on the system-specific needs.

OUTLOOK

Since 2016, understanding of trustworthiness inside the IIC about the effect on design and operation of industrial system has been quite stable, though the trustworthiness model is frequently enhanced and refined. The IIC Trustworthiness Task Group, in close cooperation with the IIC Security Working Group, coordinates these efforts and is very open for input – from any source. The goal is a permanent change of thinking – moving from "traditional" considerations such as "I want to design a safe system," "security has absolute priority" or "reliability is most important" to "let's design a system with all these attributes, based on trustworthiness guidelines that everyone can trust."

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