Mind the Trust Gap!

Strategies for Communicating Trustworthiness in Digital Twin Systems

2022-07-27

Authors:

Jon Geater
Jitsuin
jon.geater@jitsuin.com

Frederick Hirsch
Upham Security
hirsch@uphamsecurity.com

Detlev Richter
TÜV SÜD
detlev.richter@tuvsud.com

CONTENTS

FIGURES

1 OVERVIEW

Digital Twins (DT), virtual representations of real-world entities and processes synchronized at a specified frequency and fidelity in industrial settings, connect the virtual and physical worlds enabling new opportunities and efficiency through digital transformation. But as these DT systems become increasingly complex and various vendor platforms are involved, there is a growing need to communicate trustworthiness information between systems, where according to the Industry IoT Consortium (IIC)[1], trustworthiness consists of the security, safety, reliability, resilience and privacy characteristics considered holistically.

To be adopted at scale, Digital Twins need an interoperable and understandable model for maintaining security and safety assurance that satisfies all stakeholders (technical, business, and regulatory) and one which accounts for all the necessary dimensions of trustworthiness at the time.

This article outlines a strategy based on work from the Digital Twin Consortium (DTC)[2] and Industry IoT Consortium (IIC) to establish and communicate trustworthiness metrics enabling counterparties to rely upon and thus act on trustworthiness data in complex and dynamic systems.

This paper is an introduction to the topic which is expanded upon in more detail in a corresponding upcoming DTC whitepaper[3].

2 THE NEED FOR DYNAMIC AND PROACTIVE TRUST

Today's safety and security landscape is largely *static* and *avoidance-based*, by which we mean that the approach toward risk is typically a list of known things to not do as well as a list of certain controls to support. This is based on a concrete understanding of exactly how the system is composed, how it has operated in the past, and where it will operate. This presumes that the system is well defined and does not change and assumes that all hazards and threats are known and can thus be avoided through foresight.

This static approach provides a degree of safety, especially at the outset, but is also inflexible since it does not deal well with change or with opportunistic system interconnections. The price paid for relative certainty at the design stage is the inability to move to new operating models or adapt to new environmental conditions during the much longer operational stage. This means that the static approach is too inflexible to deal with the realities of today's software-laden

[1] *https://www.iiconsortium.org*

[2] *https://www.digitaltwinconsortium.org*

[3] "Assuring Trustworthiness in Dynamic Systems Using Digital Twins and Trust Vectors", Digital Twin Consortium whitepaper to be published.

connected systems where systems may be connected to achieve new functionality even when that connection was not anticipated at the time of the original design of the individual systems[4].

A similar stasis has historically applied to systems design and integration: in order to communicate devices needed explicit, design-time integration and often special code adaptations to speak each other's protocols, making combinations fairly static and favoring pre-existing relationships. If we can only certify things that we have seen before (A.K.A. "Proven in Use"), then how can we build anything new, especially when creating something new can consist of interconnecting existing systems in new ways? This problem has been noted in the desire to interconnect systems in a medical setting, for example, but until trustworthiness can be established dynamically, regulations will require each combination to go through a lengthy certification process[5].

But now with recent advances in standards and norms for Digital Twin operation, we are much better positioned to make new, even ad-hoc trustworthy connections between systems in a dynamic manner. This enables flexibility in system design and operation supporting business needs and extending the value of systems by allowing them to operate in a trustworthy manner in a changing world.

Adopting this approach also shifts from avoidance to pro-active trustworthiness. Having access to data from more sensors and being able to make sense of it using digital twin models means that this data can be used to support better safety decisions that are dynamic and based on the situation, going beyond attempting to avoid previously understood hazards. This new approach allows for a changing context, system and set of hazards while allowing safety measures to adapt. An example is the introduction of mobile robots to a factory floor and how use of a digital twin model can be used to adjust their use depending on the conditions, such as whether there has been a liquid spill leading to a slippery floor hazard, for example. Using data can be invaluable in making good safety decisions, especially in the face of dynamic and novel situations. This requires knowing how to use that information in context.

[4] In some sense this new dynamic captures the original vision of service oriented architectures.

[5] Key Safety Challenges for the IIoT, Qinqing Zhang (Johns Hopkins University), Andrew King (University of Pennsylvania), Frederick Hirsch (Fujitsu) and Semen Kort (Kaspersky Lab), Industry IoT Consortium, 2017, *https://www.iiconsortium.org/pdf/Key_Safety_Challenges_for_the_IIoT.pdf*

3 Four Simple (But Crucial) Steps Toward Achieving Dynamic Trust

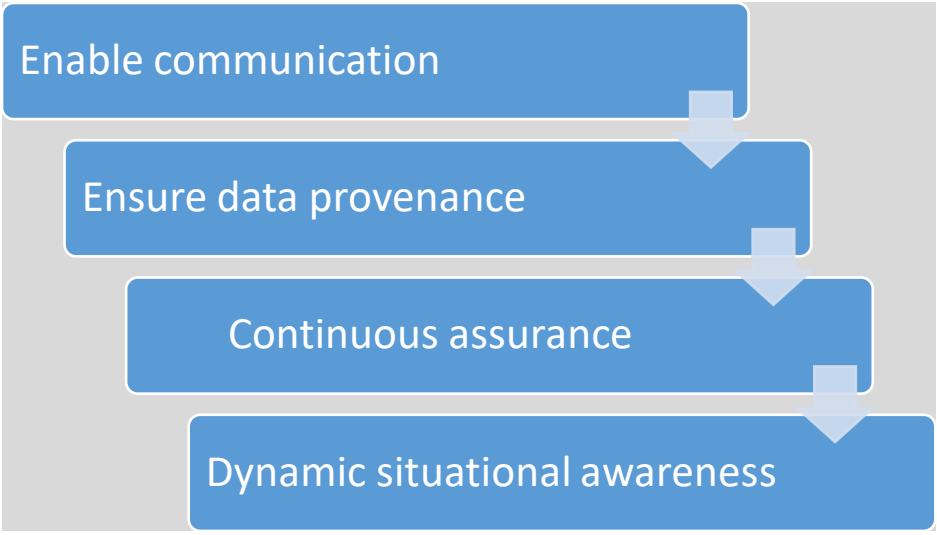

Figure 3-1. Steps for resilience.

Resilience in dynamic situations can only be achieved when the digital twin system has enough knowledge of its operating situation and the risk appetite of its stakeholders to make confident, automated choices about how to respond to alarm stimuli or unfamiliar situations. Better than simply stopping when uncertain, these systems need to be able to make accurate decisions about the minimum system degradation required to remain safe while maintaining maximum residual operation and business yield.

3.1 Step 1: Enable communication

The first step is to enable the flow of information between components and between Digital Twin systems so that they can share their operating and environmental data. This means designing systems with an expectation that they will be able to connect with the outside world and employing application and data storage architectures that are compatible with this. Enabling communications includes the following:

- Move away from the assumption of large-scale isolation based on network perimeter security and move toward zero trust architectures
- Use strong encapsulation, loose coupling, and service architectures.

3.2 Step 2: Ensure data provenance

Once data is flowing it is necessary to make sure it is actually fit for use. Focusing on provenance is important here, answering questions such as: “where did this data come from?”; “how was it produced?”; and “is it still valid?”. Enabling data provenance will require the following:

- Enable portable digital identity
- Enable data integrity at the application and processing layer, not just at the network edge

- Provide mechanisms to share information about the data (metadata).

3.3 Step 3: Continuous Assurance

Once data is flowing and its provenance is known, it is necessary to trust it before using it for decision making. By continuously collecting trustworthy data from all around the system and feeding it into the right engine at the right time it is possible to create and use assurance cases more quickly, more accurately, and with smaller windows of damage when an attack or exception occurs. This is the point at which connectivity turns to a true security advantage: rather than seeing it as increasing the attack surface it should be seen as increasing the knowledge surface.

Enabling trustworthiness is the subject of trust vectors discussed later in this paper.

3.4 Step 4: Dynamic Situational Awareness

Once trustworthy data with known provenance is available it is possible to determine how to make decisions. Once the components of the digital twin system are able to communicate and make high quality decisions based on up-to-the-minute information it is possible to make the final transformative change: dynamic assurance cases. This entails changing the expression of an assurance case from a static rule ("the light must turn green before the robot can proceed") into an outcome-based intent ("no worker should ever be hit by an autonomous mobile robot (AMR)"). By enabling all components of the digital twin to use all the rich situational data from the whole system, even unforeseen threats and pathological situations can be successfully dealt with.

4 Obstacles to Adoption

These steps are relatively simple, but there are a couple of practical problems to adoption: they demand cross-border sharing of data between supply chain partners which might have jurisdictional implications and using that data in critical (preferably automated) decision-making.

4.1 Obstacle: The Trust Gap

Moving data between organizations has long been a challenge in digital systems. Most of the historic effort in cyber security has gone into keeping data inside organizational walls and outside users and systems out. This is contrary to modern business where data has to flow across organizational boundaries and much of the perceived benefit of connection and digital transformation relies on the ability to use 'external' data in automated systems.

Unfortunately the vast majority of relevant compliance standards today focus on processes and operations and assume that all compliance of consequence is within the single organization. They do not take into account the need for cross-organization data sharing and communication to the degree needed. Thus compliance requirements are not easily transferrable across corporate boundaries, especially due to managing training, escalation procedures, and exception handling

across organizations. This makes it very hard for businesses to use data that comes from the outside in any serious process since it essentially requires blind faith that the sender of that data followed an adequate process when creating and handling it. Such blind faith is understandably rare, and this is one place where trust gaps are found in supply chains.

Traditional security products and techniques rooted in Internet and IT don't really help since they too are very silo-oriented, protecting one organization's data inside that one organization's network. Advanced or 'unbreakable' cryptography will not solve the problem since this technology does not address the business problems. For example, no matter how strong a digital signature may be, there can always be doubts over the quality of the input, the processes behind the creation of the signature (e.g. the authorization to sign in a given role) or the management and administration of the private keys behind the curtain.

This can be stated in short as: "your security is not my security". This can be overcome with paper agreements and audits, but this approach is typically slow, expensive and static which means information tends to flow far less widely or quickly than is needed to achieve business objectives.

4.2 Obstacle: The need for a holistic strategy

Many security and trust standards and best practices exist, but invariably they only focus on one of the key dimensions of trustworthiness: *security, safety, privacy, reliability, resilience*. These characteristics need to be considered holistically but often are siloed. Tradeoffs are always required based on business goals and considerations, but it is too easy to go deep into one dimension while ignoring the others. This is apparent in standards that are only very narrowly applicable or impractical to deploy at scale.

In cyber physical systems such as digital twins where virtual actions can lead to real-world consequences it is necessary to consider all of the dimensions of trustworthiness holistically. It is vitally important for system operators to be able to make tradeoffs appropriate to their needs, and for the system stakeholders to know what choices were made when they decide how much trust to put in the digital twin. It is not just making the tradeoffs that matters, but also communicating them to a relying party so that party can decide whether the decision is appropriate to their needs. The trust vector approach provides a uniform approach for handling the trustworthiness characteristics in a holistic manner.

5 Enabling Dynamic Trustworthiness

5.1 Bridging the Trust Gap with Continuous Assurance and Zero Trust

Manual assurance and audit processes tend to follow the model of "trust but verify". This is not only slow and expensive but also leaves long windows of potential vulnerability. Security audits go stale within days, site visits offer only a snapshot of operating capability, and yield numbers tend to be released too late to be useful. This means risk decisions are made on the basis of

information that is sparsely detailed and potentially months out of date. Taking a digital *zero trust* approach can address all of these problems by enabling businesses to *continuously verify evidence first*, *then trust*, and do this for *every decision* taken.

When it comes to building systems the number one core principle of zero trust is to "assume breach". This means accepting the reality that nothing is 100% secure and sooner or later an attack will get through. Nothing is 100% reliable and sooner or later it will break down and need maintenance to return to reliable operation.

A zero trust approach does not mean that there is no trust. Instead, it aims to *increase* trust in the system by *driving down toward zero* all the assumptions, shortcuts, and blind spots that come with traditional network security approaches and manual verification. This is why it is so important to enable the flow of data between components and attach provenance information to all those data flows.

5.2 Achieving Interoperable Trustworthiness Assessment with Trust Vectors and Security Maturity Models

The zero trust approach enables decisions to be made with up-to-the-minute information and in novel situations: in other words, *contextual trustworthiness*. But in order to be make these decisions correctly it is important for all components to have a common understanding of what the data means. We need an interoperable language for trustworthiness information and the new trust vector concept from the Digital Twin Consortium offers this.

Trust Vectors are a standardized way of communicating trustworthiness needs and capabilities between systems within a digital twin system, including digital twins and assets. Trust vectors allow two entities to exchange and negotiate scores of each of the five dimensions of trustworthiness on a range between a score of 1 (least trustworthy) and a score of 5 (most trustworthy), along with an optional pointer to additional verification evidence to support the claims. The consumer sets out their needs ("privacy needs 5: I really care about privacy") while the provider puts out its capabilities ("safety is 5: this component has very high regard for safety"), and these can be updated and refreshed dynamically as the system and its operating context evolves.

The trust vector principle is a scalable way for system components to communicate and answer the question: *is this other component going to help me achieve my outcomes in a better, safer way, or do they represent an unreasonable risk? Confidence in the trust vector approach will require that trust vectors be handled in a trustworthy manner, using secure communication channels for example. More detail will be provided in an upcoming white paper on the trust vector approach.*

Determining the appropriate values requires understanding and a common approach, which can be achieved using a model like the IIC IoT Security Maturity Model (SMM)[6], for example. This model is designed for security, but the approach could be extended more broadly to trustworthiness[7]. The SMM organizes the complex security space into eighteen practices covering governance, security enablement and operations with guidance regarding four comprehensiveness levels for each, as well as a process for applying the model. Insights from this model may be used to understand practices that contribute to a security score. The SMM 62443 mapping for Asset Owners and Product Suppliers[8] further maps 62443 requirements to the security maturity comprehensiveness levels making it easier to understand an appropriate score. All of this can be taken into account (as well as related work such as the NIST Cybersecurity Framework) in assessing the general suitability for a supply chain partner, vendor, or other stakeholder as a trust vector counterparty.

It is certainly not necessary for every organization to have the maximum trust vector score for all (or any) trustworthiness characteristics – what is needed should be appropriate to the use case. It is vitally important, however, that how trust vector values are calculated and relate to maturity model scores be known to, and understood by, the partners who put their trust in them so that they can take control of their own risk.

6 PUTTING THIS INTO PRACTICE

Businesses have recognized the need for digital transformation, interconnection and faster operation. Managing risk and relationships needs to keep up with this change. Taking an approach of zero trust, using trust vectors and digital twins to manage risk can support the need to have dynamic trust in the emerging business world. If you have been struggling with unlocking the potential of digital transformation with connected systems due to issues with trustworthiness and feel that this article points to a way forward, then please read the detailed works of the IIC and DTC to find out more and join us in our efforts to improve the trustworthiness of our systems.

[6] IoT Security Maturity Model: Practitioner's Guide, Version 1.2, Carielli S, Eble M, Hirsch F, Rudina E, Zahavi R, 2020-05-05, *https://www.iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2020-05-05.pdf*

[7] Extending the IIC IoT Security Maturity Model to Trustworthiness, Hirsch F, Carielli S, Eble M, Rudina E, Zahavi R, IIC Journal of Innovation, 2018, *https://www.iiconsortium.org/news/joi-articles/2018-Sept-JoI-Extending-the-IIC-Security-Maturity-Model-to-Trustworthiness.pdf*

[8] IoT Security Maturity Model: 62443 Mappings for Asset Owners and Product Suppliers, Cosman E, Gilsinn J, Hirsch F, Kobes P, Rudina E, Zahavi R, 2022, Joint IIC and ISA white paper, *https://www.iiconsortium.org/pdf/SMM-Asset-Owner-and-Product-Supplier-Mapping-2022-05-05.pdf*

7 ACKNOWLEDGEMENTS

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