PLATTFORM INDUSTRIE 4.0

Shaping a globally secure Industrie 4.0 Ecosystem

Enabling international interoperable security policies

Conference Volume

Imprint

Published by

Plattform Industrie 4.0 secretariat
Bülowstraße 78
10783 Berlin

Text and editing

Plattform Industrie 4.0 secretariat
Bülowstraße 78
10783 Berlin

Design

Plattform Industrie 4.0 secretariat

Status March 2021

Illustrations are contributed by the authors of the articles.

This publication as well as further publications can be obtained from: Plattform Industrie 4.0 secretariat. E-mail: geschaeftsstelle@plattform-i40.de.

Editorial

There is an opportunity in every challenge. And the pandemic brings many challenges. One of them is that we were not able to meet in person this year to discuss IT security in Industrie 4.0. Thus, I am very pleased that over 700 international guests saw this as an opportunity. They followed our invitation and participated virtually in the “Conference on Shaping a Globally Secure Industrie 4.0 Ecosystem”.

Elisabeth Winkelmeier-Becker,
Parliamentary State Secretary at the Federal Ministry for Economic Affairs and Energy, Germany

The pandemic also shows the challenges for IT security, as well as the opportunities that we can and must seize. Since the previous event two years ago in Berlin, many important decisions have been made in terms of IT security. At the same time, it is becoming clearer every day that cyber security and trust are a central basis in all areas of digitalization.

With Industrie 4.0, completely new, agile, and highly flexible value networks are emerging. Machines communicate with each other autonomously - both across companies and across countries. These machines have to conclude legally binding contracts. In the process, vast amounts of data are exchanged and analyzed - in real time. The increasing number of data-based platforms, also in the industrial context and in the B2B area, clearly shows where the journey is headed.

In order to increase the willingness to exchange data, one of the major challenges is securing data sovereignty. This is a fundamental issue for Europe. And this is what we are addressing with the GAIA-X project. GAIA-X prioritizes standards and rules such as interoperability, portability, or transparency. The aim is to build a flexible and federated data infrastructure in Europe and beyond. We are convinced that completely new and highly innovative data ecosystems can develop on the basis of GAIA-X. But there are also new challenges and requirements for IT security.

Solutions from the IT world as we know them, cannot be easily transferred to a flexible and networked production world. New approaches are therefore required. We are currently working on this in many places and in many countries. This conference has strengthened the international exchange of experiences. It contributed to establishing the most common understanding possible on the international cyber security issues of Industrie 4.0.

We invited to this conference together with Plattform Industrie 4.0. The platform develops concepts for IT security topics. The participants presented these concepts at the conference and put them up for discussion. We are already in bilateral cooperation with the USA, Japan, France, Italy and China on the subject of cyber security. Representatives from all these countries took part in the conference and presented their strategies.

The key questions at the conference were:

- How can we effectively secure international value networks?
- What are security concepts do other countries apply?
- Which regulatory requirements need to be addressed in a European and global context?

Against this background, standardization played a major role at the conference. Many states have not yet made final decisions on regulatory issues.
The participants exchanged views and concepts. And they started a process. This helps us all to work together on the guidelines for future interoperable solutions.

Enjoy the read of this conference report.

Editorial comment

To make your reading experience as comfortable as possible, the order of papers does not reflect the order of presentations at the conference. Instead, we arrange the contributions according to thematic clusters.

The conference volume starts with a broad overview regarding cyber security and standards, followed by four contributions dealing with trustworthiness. After that you will find the cluster “asset administration shell” (AAS) which consist of two contributions. The third cluster consists of three papers discussing different aspects of the broader topic “data sovereignty”. The conference volume is closed by a paper of a initiative to make secure Industrie 4.0 ecosystems a reality.

You can find the whole documentation following this link: https://www.plattform-i40.de/PI40/Redaktion/DE/Kurzmeldungen/2021/2021-02-05_documentation_IT-conference.html

Table of Contents

Building cyber resilience through agile regulation – standards as enablers

Author:

Dr Jed Horner, Jed.Horner@standards.org.au**,** Strategic Advocacy Manager, Standards Australia

Abstract

Cyber security is now a global imperative, and the transition to industry 4.0 requires strong cyber resilience. But embedding the right frameworks, controls and practices remains a challenge at national and international levels. This is particularly the case for multi-national supply chains. Different micro-regulation impacts not only businesses, but fractures what should be common baseline practices, potentially impacting the broader community. In this paper, I outline the opportunity to harmonise and streamline standards for cyber security, using globally recognised Standards such as ISO/IEC 27001. We will outline the work undertaken in Australia, include at State levels, to re-imagine what a more harmonised approach might look like for responsible countries and the companies that operate within, and across, their borders.

Global challenges to cyber security and the industry 4.0 transition

The challenges posed to cyber security, for individuals, companies and countries, by both state and non-state actors, are growing in both likelihood and magnitude.[1] Jaikaran has defined cyber security as encompassing "not just data, but the networks, hardware, software, services, and infrastructure that data relies upon."[2]

Sophisticated actors, including criminal gangs, and nation-state sponsored hackers, are engaging in cyber offensive activities that challenge cyber security, threatening intellectual property rights, personal privacy and safety and the functioning of core services and infrastructure. Little-Limbago argues that offensive cyber operations, which may be termed *attacks* in everyday parlance, can be classified according to "four distinct areas: insertion (for example, malware), blocking (distributed denial of service [DDoS]), removal (cyber espionage), and destruction (such as of critical information or infrastructure)."[3]

In the industrial context, the exfiltration of information, including that which is commercially sensitive, such as specifications for new products, services or technologies more broadly, is occurring at an arguably unprecedented rate. Very recently, it was disclosed that the European Medicines Agency (EMA) was targeted in a cyber-attack, with those who gained access reportedly able to view regulatory submissions concerning specific COVID-19 vaccines awaiting approval.[4] Historically, there are other examples, with the design of the newer generation Chinese fighter jets allegedly based on designs for the F-35 joint striker.[5] A study conducted within the European Union, which had specific regard to the industry 4.0 transition, also noted that the magnitude of specific threats such as the theft of trade secrets is increasing.[6] The report cited examples of phishing operations targeting sectors such as defence, aerospace and engineering, and audio

[1] Australian Cyber Security Centre (2020). *ACSC Annual Cyber Threat Report July 2019 to June 2020.* Canberra: Commonwealth of Australia. See also: Government Communications Security Bureau (2020). *2019 Annual Report*. Wellington: Government of New Zealand.

[2] Jaikaran, C. (2017). *Statement before the US Senate Committee on Banking, Housing, and Urban Affairs 'Consumer Data Security and the Credit Bureaus.'* Washington D.C.: Congressional Research Service.

[3] Little Limbago, A. (2015). 'One Size Does Not Fit All: The Multifaceted Nature of Cyber Statecraft,' *Joint Forces Quarterly,* 78(3): 84-90.

[4] BBC (2021). 'Pfizer/BioNTech vaccine docs hacked from European Medicines Agency', accessed 14/01/2021 from: https://www.bbc.com/news/ technology-55249353

[5] Pellegrino, M. (2015). 'The threat of state-sponsored industrial espionage,' accessed 14/01/2021 from: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_26_Industrial_espionage.pdf

[6] PwC (2018). *The scale and impact of industrial espionage and theft of trade secrets through cyber*. Brussels: European Union.

recording of conversations, based on network compromise.[7] This has implications, simultaneously, for national security, trade and commerce, industrial innovation and social wellbeing.

Some of this activity is driven not just by criminal actors, with financial motives, but as part of cycles of industrial espionage, some of which align with the aspirations of nation-states. The adoption of cyber tactics as part of economic statecraft is clearly part of the picture and is not limited to defensive operations. In short, these activities represent the pursuit of technological, and subsequently economic, dominance, through nefarious means. This is important, because without the *likelihood* and *magnitude* of, and *intent* behind, various forms of cyber-attacks being factored in, one cannot undertake adequate risk assessments or impose measures robust enough to mitigate these and, importantly, to recover quickly.

In the context of the industry 4.0 transition, which relies on rapid prototyping, innovative breakthroughs in manufacturing and personalisation, including in industrial settings, these threats are pronounced. Lee-Makiyama observes that, in a connected environment fostered by industry 4.0 "an entire connected business can be copy-pasted and stolen, including equipment settings, operational schedules and production details."[8] Indeed, these threats might be considered to pose a greater long-term impact, as they may seek to, or have the effect of, undermining the manufacturing sector that underpins the defence industrial base itself or other areas relevant to the effective functioning of societies. This might encompass healthcare and critical utilities, including power and water. When enacted with the tacit support of state actors such activities, whether targeted at medical advances or advanced manufacturing machinery or processes, can distort markets and undermine genuine competition.[9] They also, in many instances, can endanger national security, in the ways described above.

There are a range of factors that exacerbate the risk that an entity, whether a government agency, non-governmental organisation or private company, might be particularly adversely affected by a cyber-attack. For example, smaller companies within a supply chain might not implement adequate security controls, or undertake broad-based risk assessments, that lead to concrete risk mitigation measures – effectively becoming the weakest link in an important supply chain. Conversely, they might be best equipped, but be let down by the (in)actions of other supply chain partners. A report within the EU attributed some of this risk landscape, particularly in relation to the theft of trade secrets, to specific (and sometimes macro) factors, including:

---

[7] PwC (2018). The scale and impact of industrial espionage and theft of trade secrets through cyber. Brussels: European Union, p. 25.

[8] Lee-Makiyama, H. (2018). *Stealing thunder: Cloud, IoT and 5G will change the strategic paradigm for protecting European commercial interests. Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?,* ECIPE Occasional Paper, No. 2/18. Brussels: European Centre for International Political Economy (ECIPE).

[9] See, for instance: https://www.state.gov/united-states-charges-russian-military-intelligence-officers-for-cyber-crimes/

- *Lack of awareness and competences within businesses;*
- *Wider online exposure of companies, which are also moving to cloud platforms;*
- *Growing speed with which hackers create new malware and develop their skills in using advanced technological tools;*
- *Slow pace at which policy makers address the problem;*
- *Increase in globalisation of markets;*
- *Global changes in geopolitical strategies; and;*
- *The development of new technologies, such as artificial intelligence*[10]

Fortunately, there is growing global recognition of the importance of raising the baseline cyber security posture. This is important when we think about the centrality of connections between researchers and manufacturers, the interconnectedness of devices and the use of greater volumes of data – both on the factory floor and in earlier iteration and design phases, within industry 4.0.

Responding to these challenges: standards as a baseline for cyber resilience

But how might we respond to these threats to cyber security, in a way that leverages good practice and demonstrates results? After all, if we are working in the spirit of industry 4.0, scalability is critical, as is adaptability. And we need to move beyond the notion that security is merely about lines of code, firewalls and multi-factor authentication. It is equally about protective security measures, such as adequate and cyclical personnel screening, and physical security, ranging from sound access control to facilities, and appropriate surveillance.

The response to these cyber challenges is taking many forms. Companies themselves are making high level commitments, and implementing robust policies, procedures, and controls. The Siemens-initiated *Charter of Trust*, in partnership with others, is but one example.[11] There is also the continuing work to shape and strengthen common cyber security standards through the joint International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Sub Committee 27, within Joint Technical Committee 1. This Subcommittee have produced the following notable cyber security standards over recent decades and years:

- ISO/IEC 27001: *Information Security Management*[12]

---

[10] PwC (2018). *The scale and impact of industrial espionage and theft of trade secrets through cyber*. Brussels: European Union, p. 24.

[11] See: https://new.siemens.com/global/en/company/stories/research-technologies/cybersecurity/what-makes-the-charter-of-trust-such-successful-model.html

[12] https://www.iso.org/isoiec-27001-information-security.html

- ISO/IEC 27701: *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

Companies, ranging from Microsoft to Google and SAP, are adopting these standards at-scale, as part of Azure, Google Cloud, and SAP Cloud offerings, for example. This is significant because it represents, at a global level, the embedding of common cyber security baselines for cloud services. This is of course complemented by highly trained, and skilled, workforces and the elaboration of sophisticated new cyber security practices. Many commentators and some policy-makers conflate these complementary approaches. They are not mutually exclusive. And just because some techniques in cyber security are not reflected in standards, doesn't make the standards redundant. Baselines are meant to be just that – baselines. Otherwise, the maturity gap would be so broad that common practices would be codified nowhere.

National Governments are also implementing specific policies and practices to bolster cyber defences, some of which take a sectoral approach. Australia, for example, is proposing amendments to existing critical infrastructure legislation, through the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*. If passed, would not only expand, in real terms, the definition of what critical infrastructure is, and impose Positive Security Obligations (PSO) on entities operating in these defined sectors of the economy and deemed systems of national significance.[13] These amendments appear to go further than those embodied in earlier reforms in the United States, including through Executive Orders under the Clinton, Bush and Obama Administrations, specifically insofar as they impact the private sector.[14] These Australian measures would also see cloud computing captured, which is a true horizontal – underpinning microservices infrastructure in banking, retail, and other 'sectors.' Again, the question here is how impacted industry 4.0 is – the answer is that focusing on OT in isolation will become increasingly difficult as we truly platform services and manufacturing.

National measures, which might come in the form of legislative changes, regulations, procurement policy directives or rules, can be useful, but from a regulatory perspective it is always advisable to leverage the baseline provided by recognized international standards. There are at least three public policy reasons for doing so:

1. WTO obligations

A great many countries have obligations under the World Trade Organisation Technical Barriers to Trade Agreement to avoid creating Technical Barriers to Trade (TBT). As the WTO has noted:

[13] See: https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6657_ems_928e0092-fabb-4c31-a67b-b47ac1123e17/upload_pdf/JC000738.pdf;fileType=application%2Fpdf

[14] Tehan, R. (2018). 'Cybersecurity: Legislation, Hearings, and Executive Branch Documents,' accessed 13/01/2021, from: https://fas.org/sgp/crs/misc/R43317.pdf

Technical regulations and standards are important, but they vary from country to country. Having too many different standards makes life difficult for producers and exporters. If the standards are set arbitrarily, they could be used as an excuse for protectionism.

As a result, States are encouraged to use International Standards (developed by Standards Development Organisations such as the ISO and IEC), as a basis for any technical regulations or conformity assessment procedures they develop or adopt, or through the relevant identical or modified adoptions of those standards through their respective National Standards Bodies (NSB's).

2. Supply chain certainty

Leveraging recognized international standards can also have the added benefit of ensuring that operations across different sites, offshore, can be streamlined. Increasing granularity, through standards imposed by national governments (where there is no regard to existing baselines), might have the opposite effect in more complex supply chains, introducing a complex patchwork of requirements, some at the level of specific technical controls, that fracture the global landscape.

3. A stronger posture off an existing baseline – increasing protection and minimizing unnecessary cost(s)

Many companies either embed these practices, whether through a formal certification-based approach, or their own documented internal approaches and accountability mechanisms. As an example, Google Cloud and Workplace are ISO/IEC 27701 certified, and this can be leveraged by partners, managing risk, easing compliance and improving the baseline cyber security posture.[15] Effective scaling of cyber security practices can therefore be achieved by leveraging baselines created by international standards. This creates a delta that is relatively straight-forward to bridge (particularly for partners and new entrants), rather than variable requirements which impose new costs, but perhaps without added business benefits or broader societal on an international scale.

Returning to the core question: *how, then, might we implement more agile approaches that acknowledge good industry practice, as well as existing standards, for the promotion of industry 4.0?* Below, I outline just a few examples, with different levers in the hands of the state and indeed private companies, specifically insofar as supply chains and commercial contracts are concerned.

Lever	Example of application	Implementation options (standards)	Potential benefits

[15] See: https://cloud.google.com/security/compliance/iso-27701

Legislation	Set a broad requirement for specific entities to have a *documented risk management program in place*, with specific reporting requirements, in relation to cyber security and/or specific areas thereof (i.e. protective security, information security etc.).	**Provide a choice for industry to leverage recognized (i.e. ISO/IEC) standards** in doing so. For example, ISO/IEC 27001, ISO 28001, or ISO 22340, depending on the specific nature of the business/sector, or, alternately, demonstrate how they leverage standards such as ISO 31000 (Risk Management – Guidelines) to shape their own documented risk management program, in accordance with the requirements.	*Adaptability:* recognizes common international standards and acknowledges the efforts of companies to embed risk identification and management in a rigorous, and demonstrable way. If done correctly, this can reduce heavy costs associated with granular government regulation in areas where businesses already undertake significant preventive measures, including internationally.
Regulatory instrument	Specify, through lower level legislative instruments, a broad set of security principles that apply in specific sensitive or affected areas.	**List recognized standards** that might help entities to meet these requirements. This can be through a dual pathway: (1) documented use of standards – deemed compliant, (2) alternative mechanism - subject to documentation, reporting and approval requirements, prior to being deemed compliant.	*Regulatory clarity:* Creates in-market agreement over baselines, without endangering trade obligations or fracturing requirements, if done correctly and consultatively.
Supply chain incentive	Adopt specific broad, but binding, requirements for supply chain partners in commercial contracts or through procurement channels	**Specify** specific recognized international standards to be met, with an annex of additional requirements, or more technical controls (and only if required). **Weight proposals** that demonstrate they have adopted, adapted and considered recognized international standards, through the bid or tender process.	*Market entry and expansion:* Equips a supplier with a portable set of cyber security credentials they can leverage to broader their business base (if they invest in certification, for example) and assures a customer/partner of a cyber security baseline across their supply chain.

A case study in collaboration: The NSW Cyber Security Taskforce - Identifying, elevating and adopting good practice

In mid 2020, in collaboration with AustCyber (Australia's Cyber Security Growth Centre) and the NSW (State) Government, Standards Australia convened a joint Government-Industry Taskforce, to accelerate the adoption of harmonised standards for cyber security in Australia. The objective was to support the creation of a baseline defensive posture, overcome existing barriers, promote greater interoperability, and better support Australian cyber security companies to go global, through the use of standards. The Taskforce had representation at senior levels from a number of industry associations, government agencies and experts, and was opened by NSW Minister for Customer Service, the Hon. Victor Dominello MP.

From thereon in, industry representatives attended a series of roundtables to identify what *good practice* looks like, to map commonly used, or referenced, standards, and outline amendments that might need to be made. We also spent considerable time identifying commonly used standards outside of cyber security, but whose adoption, as part of business practice, is now significant, such as ISO 31000:2018 (*Risk Management – Guidelines*). We also spent time talking through a critical priority – the interface between standards, regulation, procurement practice(s) and the broader goal of a heightened defensive posture for cyber security. Here, as I argued above, we identified the need to leverage existing standards, and clarify understanding, rather than create too many new normative documents.

In late January 2021, the final report from the Taskforce will be launched, along with a web resource, which maps, at a high level, the outcomes of this Taskforce.[16] The report focuses on priority actions to be taken across a number of sectors, including:

- Cloud
- Defence
- Education
- Energy
- Financial services
- Health
- Telecommunications & IoT

[16] Standards Australia & AustCyber (2021, forthcoming). *Recommendations Report: NSW Cyber Security Standards Harmonisation Taskforce*. Sydney: Standards Australia.

The web resource will provide a broad overview of standards that might be useful for different purposes. It is the intention of this Report, and subsequent conversations, to inform policy, regulatory and other work that may take place within government to shape an improved cyber security posture for Australia, which makes it highly relevant to industry 4.0.

Conclusion

The transition to industry 4.0 will be enabled by robust cyber security, given the likelihood and magnitude of the threats and the intent of different actors. Both industry good practice, and standards, when it comes to cyber security, will be central to this transition. However, given the globalized nature of the industry 4.0, leveraging recognized international standards will be key to any measures adopted in-market and at a national level. There are three key public policy motivations for this. Nascent government-industry-academic collaborations, including those in Europe, and undertaken in Australia, engaging both State and Federal Governments, provide some initial examples of collaboration to underpin these new approaches. Ultimately, the extent to which the architects of national approaches to cyber security, including responsible governments, are willing to adopt and adapt recognized international standards will determine whether we have an interoperable, secure baseline for industry 4.0.

The Role of Trustworthiness in secure supply chain for connected industries

Robot Revolution & Industrial IoT Initiative

Authors:

Ayaji Furukawa, Toshiba Corporation

Hirozumi Eki, JTEKT Corporation

Junya Fujita, Hitachi Ltd.

Atsuhi Kitamura, Robot Revolution & Industrial IoT Initiative

Masue Shiba, Toshiba Corporation

Prof. Tsutomu Matsumoto, Yokohama National University

Nobuaki Suzuki, Toshiba Corporation

Tsutomu Yamada, Hitachi Ltd.

Dr. Takeshi Yoneda, Mitsubishi Electric Corporation

Abstract

Under the “Connected Industries[1]”, our supply chain is highly automated international and global collaboration.

At the same time, due to the risk increases, global value networks require comprehensive trustworthiness architectures covering all entities, regardless of their geographical location. Therefore, we have to form secure global supply chain, where parties involved have an adequate maturity level for trustworthiness.

RRI (Robot Revolution & Industrial IoT Initiative)[1] has proposed a "Security questionnaires for suppliers” and answer form as a key tool to form secure global supply chain. It is shown that how the security questionnaires have developed based on METI[1] CPSF[1], and IEC62443[1] series to cover various kinds of manufacturing sectors.

Background

Robot Revolution Initiative (RRI) and Connected industries

RRI is a private-led organization platform to promote “Robot Revolution” based on Japanese government’s strategy. Around 500 companies (mainly manufacturing industry) are members of RRI.RRI promotes “Connected-Industries” in the field of manufacturing.[1]

Connected-Industries is an initiative which Ministry of Economy, Trade and Industry announced in 2017.The Connected Industries initiative aims to create new added value not only by increasing efficiency and optimizing the manufacturing process, but also by connecting the strengths of Japan’s manufacturing industry with each other. Connecting a variety of industries, companies, people, machines, data, and other social elements, contribute to create new added value and products/services.[2]

[1] https://www.jmfrri.gr.jp/english/

[2] https://www.meti.go.jp/english/policy/mono_info_service/connected_industries/index.html

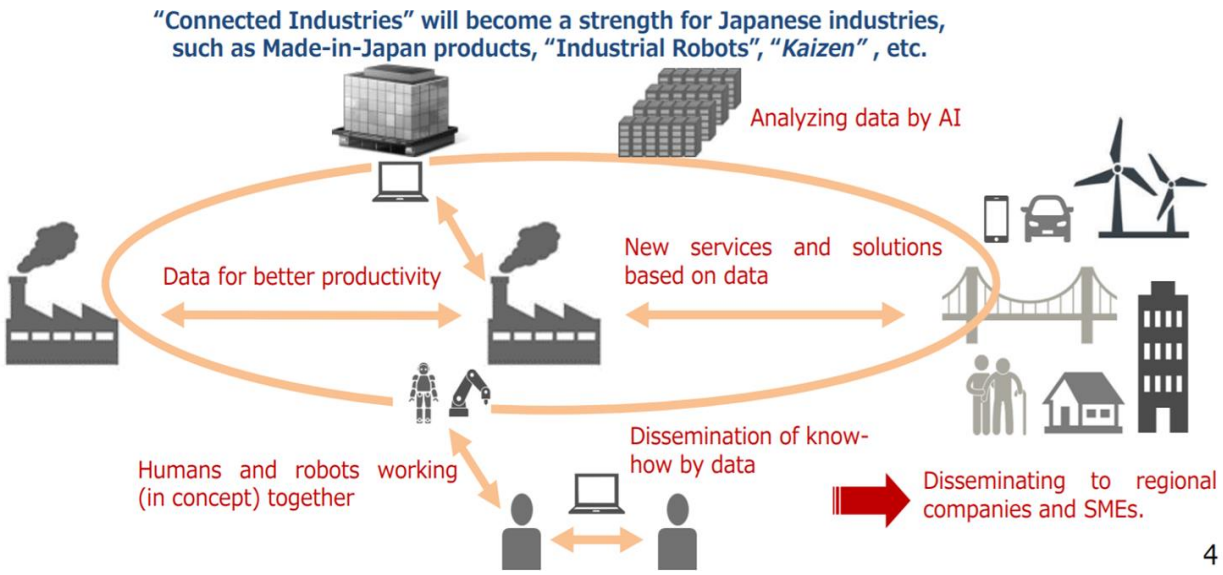


Figure1: Connected Industries

RRI and Plattform Industrie 4.0 (PI4) agreement

RRI, Japan and PI4, Germany, concluded an agreement on enhancement of collaboration（2016.4）[3] Digitization and the linking of production processes along the entire global value chain via the Internet of Things (IoT)/Industrie 4.0 hold great potential to revolutionize manufacturing.

Industrial cyber security is one of the areas which both parties create synergy by exchanging information on efforts concerning common challenges and support and promote cooperation among companies and research institutes of both countries.

[3] https://www.jmfrri.gr.jp/content/files/Open/2016/20160428_Joint_Statement_PFI40/Joint_Statement_E.pdf

Common position paper and whitepaper between RRI and PI4.0 for industrial cybersecurity

Based on the agreement, RRI and PI4.0 have collaborated and discussed past four years. In the past, RRI and PI4.0 announced three common position papers, “Facilitating International Cooperation for Secure Industrial Internet of Things/Industrie 4.0” (16th March 2017, 16th May 2018, 3rd April, 2019)[4]

We have examined and identified what is required to realize secure supply chains, and ensure trustworthiness in a connected supply chain.

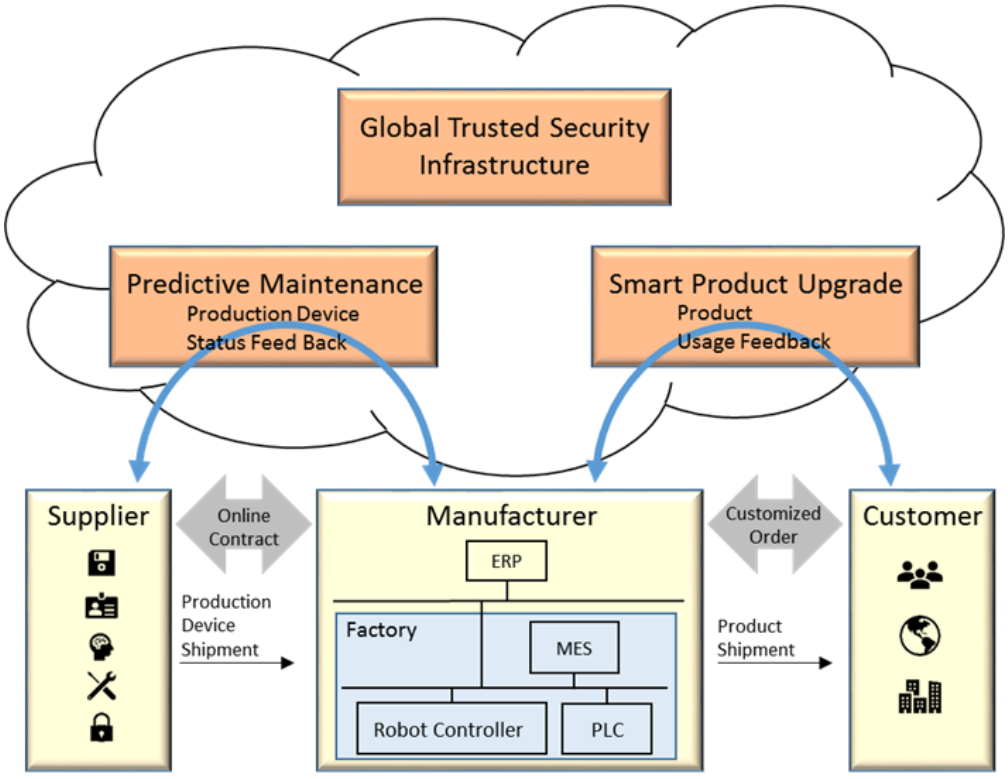


Figure2: Supply chain in Connected industries

[4] Common position paper RRI and PI4.0: https://www.jmfrri.gr.jp/english/document/library/1107.html.

Through our past activity our goal is

- To identify new security requirements in future manufacturing system in Industrie 4.0 and Connected Industries.
- To foster trustworthiness in increasing digital and interconnected economies.
- To have common understanding that Trustworthiness is an important qualitative decision-making criterion for the entire secure value chain.

In the latest white paper "IIOT Value Chain Security –The role of Trustworthiness" 2020[5], RRI and PI4.0 had discussed the role of trustworthiness intensively.

- In the context of our project, the definition of the term 'trustworthiness' proposed by the ISO/IEC JTC1/WG13 has been adapted as:

"For supply/ value chain security and risk management, the term 'Trustworthiness' corresponds to the supplier's ability to meet the expectations of the potential contract partner in a verifiable way".

Based on this white paper's discussion, RRI set our next activity is to create security questionnaires for suppliers.

The way to verify Trustworthiness capability

Risks in Connected Industries

Under "Connected Industries", a variety of industries, companies, people, machine and data exchange with cross companies and cross countries. It means that expected and unexpected risks are increasing, and value chain is expanding all over the world.

Global value networks require comprehensive trustworthiness architectures covering all entities, regardless of their geographical location.

1) Manufacturer needs to develop products that satisfy rapidly changing customer needs.

[5] White paper "IIOT Value Chain Security –The role of Trustworthiness" 2020: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.pdf?__blob=publicationFile&v=5

2) Manufacturer needs to collaborate with suppliers whose products (components) are required to develop their products.

3) Manufacturer needs to find appropriate suppliers from all over the world timely through the Internet.

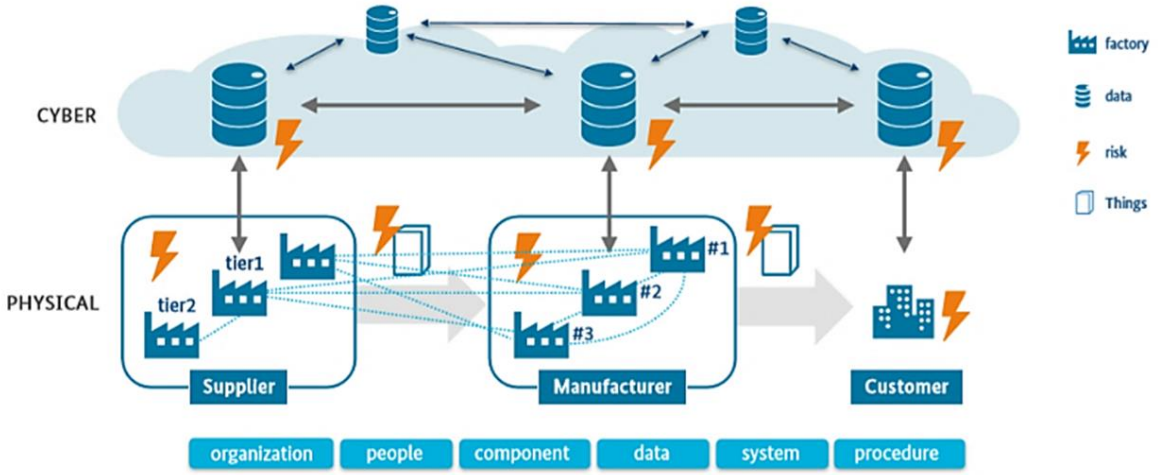


Figure3: Supply chain in Connected industries

Especially last these years, because of natural disasters or Covid-19, the manufactures were unable to procure the necessary parts or products from suppliers which they used to do business with. In that cases, the manufactures promptly must find suitable suppliers which meet manufacture's expected trusted maturity level.

In order to select suitable suppliers, RRI has developed security questionnaires to verify maturity level of suppliers' trustworthiness, which is an important qualitative decision-making criterion for the manufactures. The answer of questionnaires would be useful to visualize the gap between manufacturer's expected capability and supplier's capability.

Security questionnaires for suppliers

1) Overview and use case

Our security questionnaires for suppliers aim to be a template for security requirements and security maturity check in the supply chain to select trusted supplier before contract, being applied across sectors of manufacturing industry.

In Japan, most of manufacturing sectors, except for critical infrastructures such as electricity, defense, and automobile, don't have any specific guidelines and rules for cyber security. RRI's questionnaires target is

these areas at first. We recommend this security questionnaires requirements are for the minimum requirements that should be included to select suitable suppliers. Our questionnaires are flexible to modify for elimination or addition of item of questions. Manufacturers can choose how to fulfill these requirements and set the priorities in each requirement based on their needs. We assume the answer is generally self-declaration at first.

In addition, we focus on organization security and industrial control system security from the view point of product lifecycle, we eliminate technical requirements which depend on each sector specific requirements.

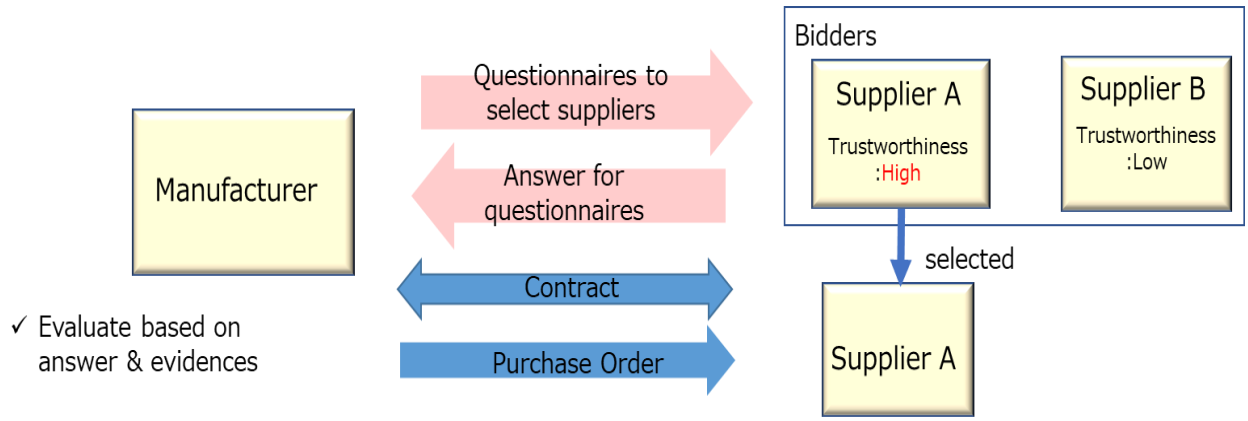


Figure 4: Security questionnaires to select suitable supplier

The procurement department for manufacturer could be a questioner, and bidder for development department could be an answerer for the questionnaires.

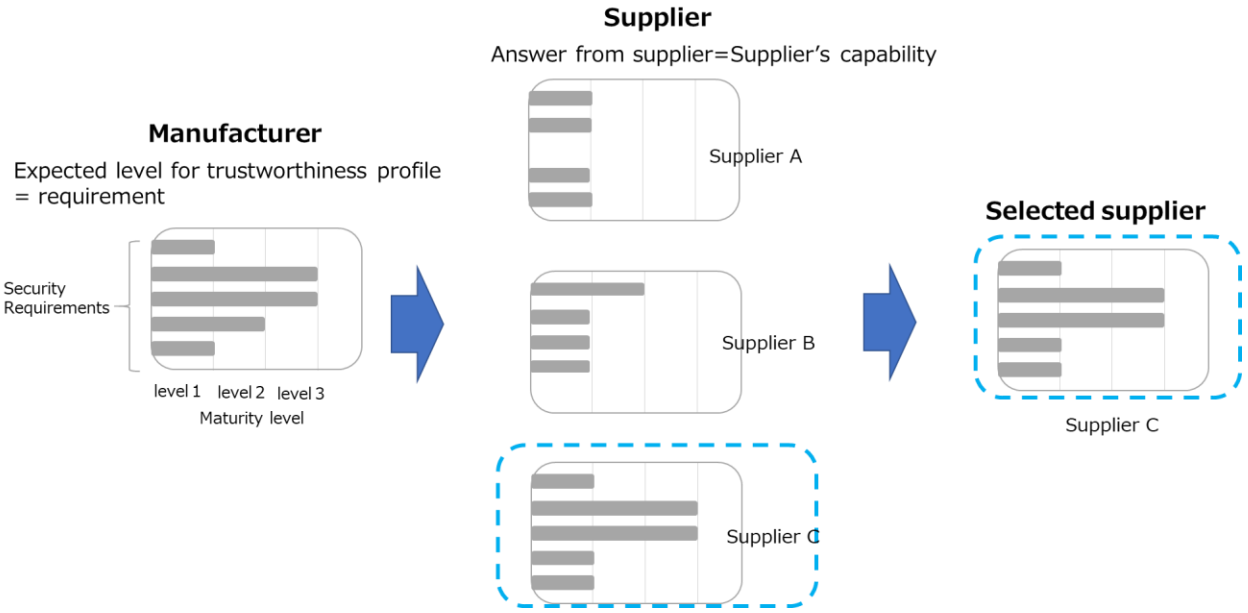


Figure 5: the process to select trusted supplier using questionnaires

The expected maturity level by manufacturer is requirements to be selected supplier. The answer for the questionnaire would be useful for the manufacturer to determine "the supplier's trustworthiness" and "how supplies in the value chain have the same trustworthiness maturity level", and visualize the gap between expected level and supplier's capability.

2) Maturity level

Our security questionnaires introduce the idea of "Maturity level" to identify the supplier's trustworthiness maturity level. To determine the level, we use the NIST Cybersecurity Framework (CSF)6 approach, which uses Framework Implementation Tiers ("Tiers") to provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.

NIST defines four Tiers, Tier1 Partial, Tier2 Risk Informed, Tier3 Repeatable and Tier4 Adaptive.

In our target sectors, security rules or guidelines by government or industry group are not imposed and few suppliers is expected to lie in Tier4. We focused on Tier1, 2 and 3 in NIST.

Besides, we defined two layers to examine the maturity level for suppliers. "Management – layer process" and the other is "Operation-layer process".

Management-layer process Processes: security policies and procedures at the management layer, which governs organizational-wide operation.

Operation-layer process: Policies and procedures at enterprise or manufacturing sites. Sometimes, the processes are in place locally, not being integrated with management-layer process.

[6] https://www.ipa.go.jp/files/000071204.pdf

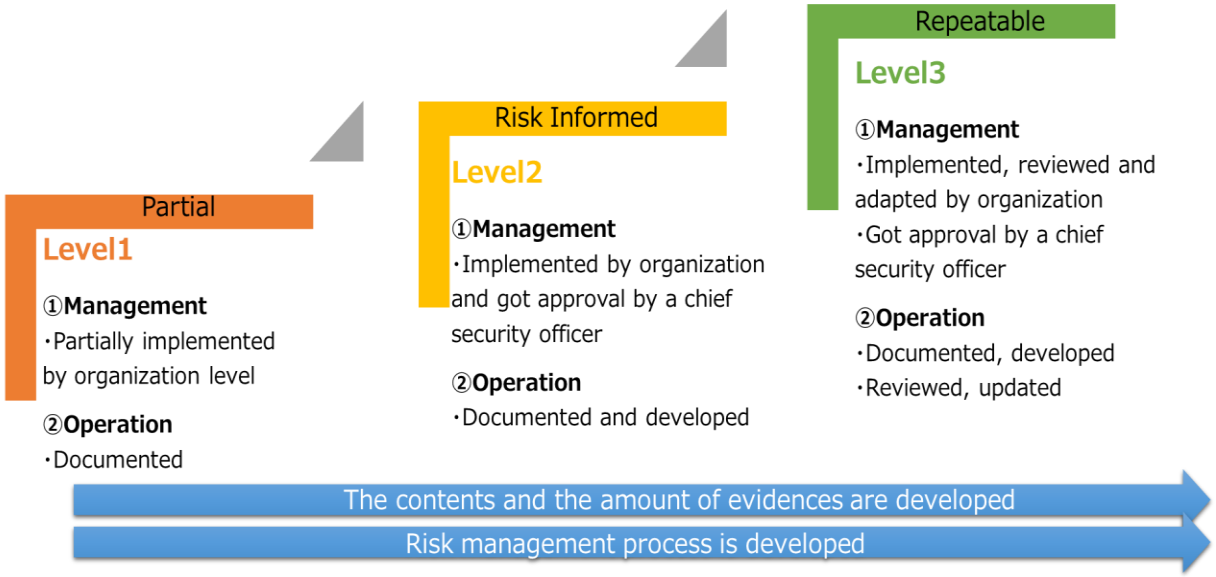


Figure 6: The idea of maturity level for RRI questionnaires

3) Selected requirements from CPSF

In selecting the requirements for RRI questionnaires, we use METI CPSF (Cyber Physical Security Framework) as base line.[7] CPSF is the framework which a well-organized an overview of security measures that industries are required to take in Connected Industries. CPSF provides cybersecurity requirements focused on communications between companies and/or organizations categorized as three levels, The 1st layer, The 2nd layer, The 3rd layer and six elements (organization, people, component, data, procedure, and system).

In addition, CPSF provides informative references of other standards (e.g., NIST CSF[8], ISMS and IEC 62443) on each requirement and this information supports our tasks.

CPSF is enterprise-wide security framework and security requirements are described for each entity in a company.

Based on CPSF, RRI selected 17 items using following criteria.

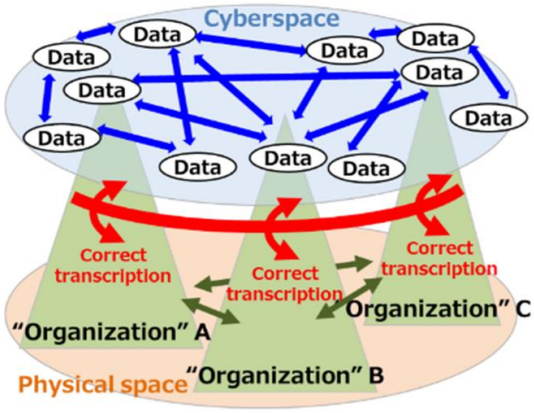
① Security requirements that we have already achieved in our companies.

[7] https://www.meti.go.jp/english/press/2019/pdf/0418_001a.pdf
[8] NIST Cybersecurity Framework https://www.ipa.go.jp/files/000071204.pdf.

② Security requirements that we require for product/system suppliers at least.

③ Security controls in operation, management processes and organization.

④ High (Policy)-level security requirements in the security risk management process.



- The 1st layer (Connections between organizations in physical space)
- The 2nd layer (Mutual connections between cyberspace and physical space)
- The 3rd layer (Connections in cyberspace)

Figure7: CPSF

See the annex we selected requirements.

NIST/CSF	METI/CPSF	
Identity	CPS.AM	ID.AM (Asset Management)
	CPS.BE	ID.BE (Business Environment)
	CPS.GV	ID.GV (Governance)
	CPS.RA	ID.RA (Risk Assessment)
	CPS.RM	ID.RM (Risk Management Strategy)
	CPS.SC	ID.SC (Supply Chain Risk Management)
Protect	CPS.AC	PR.AC (Identity Management and Access Control)
	CPS.AT	PR.AT (Awareness and Training)
	CPS.DS	PR.DS (Data Security)
	CPS.IP	PR.IP (Information Protection Processes and Procedures)
	CPS.MA	PR.MA (Maintenance)
	CPS.PT	PR.PT (Protective Technology)
Detect	CPS.AE	DE.AE (Anomalies and Events)
	CPS.CM	DE.CM (Security Continuous Monitoring)
	CPS.DP	DE.DP (Detection Processes)
Respond/ Recovery	CPS.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)
	CPS.CO	RS.CO (Communications) RC.CO (Communications)
	CPS.AN	RS.AN (Analysis)
	CPS.MI	RS.MI (Mitigation)
	CPS.IM	RS.IM (Improvements) RC.IM (Improvements)

4 domain
17 items

Figure 8: Mapping NIST/CSF and METI/CPSF

If a supplier has the ISO 27001 certificate, it can answer the questionnaire by refer ring ISO 27001 SOA (Statement of Applicability) showing implemented ISO27001 controls. Although in ISO27001, maturity levels are not clearly defined, if an organization have ISO27001 certificate though a 3rd trusted party, “the maturity level” is beyond “Partial”. So “Level2” can be assigned.

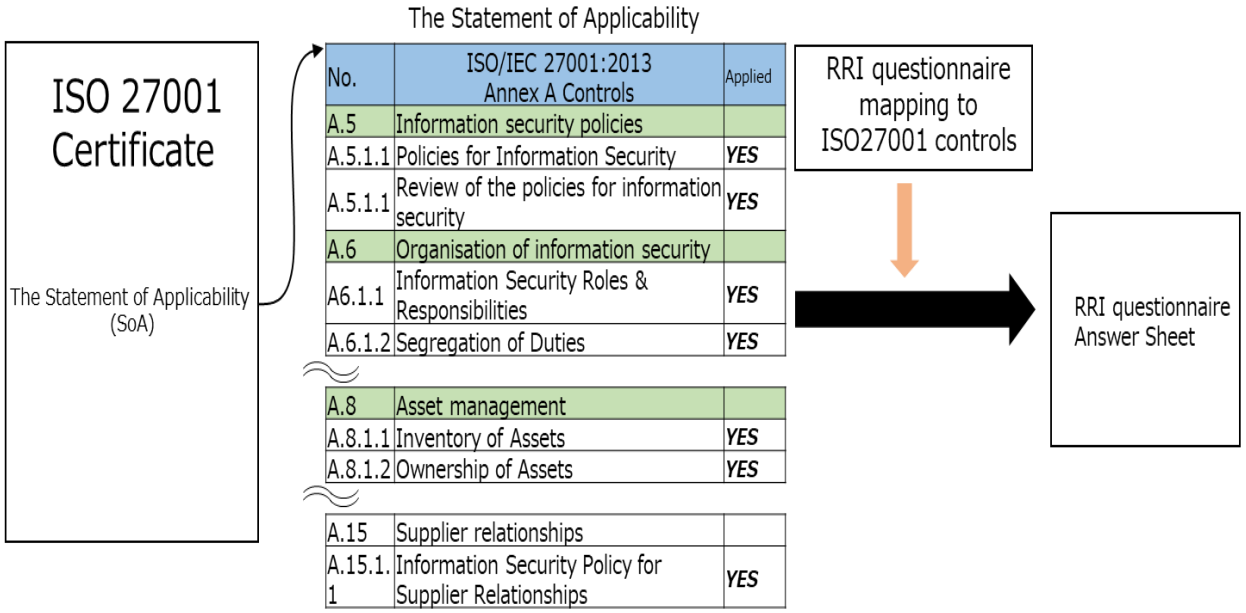


Figure 9: Mapping RRI questionnaire and ISO 27001

4) Selected requirement from the view of product cycle.

We selected 17 requirements from CPSF, but these requirements are not enough from the view point of “product life cycle”. Our questionnaires should be included these points taking into consideration supply chain. We added following aspects and selected the requirements from IEC 62443 2-1,2-4 and 4-1.

- Development
- Development environment
- Procurement
- Operation & maintenance (O&M)
- Product equipment

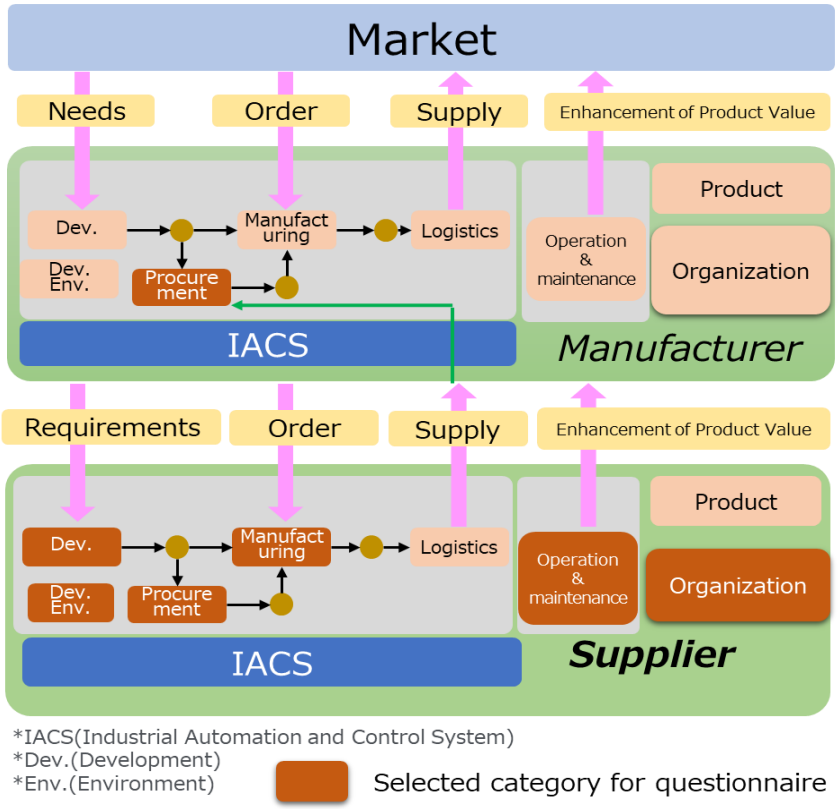


Figure 10: Additional requirements from the view of product life cycle

Figure 10 shows relationships among the market, manufactures and suppliers. It also shows the process relevant to product life cycle. Security requirements can be categorized by the processes. and we can prioritize security requirements by using the processes.

As well as the process of selection from CPSF, we selected additional requirements based on following ideas,

① Security requirements that we have already achieved in our companies.

② Security requirements that we require for product/system suppliers at least.

③ Security controls in operation, management processes and organization not technical

④ Security requirements are not too specific but moderately general

As an expectation, we included the requirements of “Product equipment”. This requirement would become important because product equipment is connected to IT networks within the company in the Connected Industry. However, at the moment, in Japan, most of manufacturing industry haven’ prepared enough these security measures as reality.

See the annex.

5) How to answer the questions

In order to answer easily for suppliers, to examine the answer smoothly for manufacturers, we illustrated some evidences in each questionnaires to define the maturity levels.

To answer the question, simply check one of the three answers: not applicable, planned to be implemented, or Implemented, for the defined maturity level.

Our questionnaires are based on self -declaration, we expect depending on manufacturer's needs, they can ask for suppliers to submit evidences to prove the answer.

Category			Governance
Security requirement			Develop and announce security policies, define roles and responsibilities for security across the organization and other relevant parties (Suppliers) .
Example : Answer	evidence		History of security policy development and approval, and approval of revisions to the security policy. Describe the security roles and responsibilities of the organization and other relevant organizations (e.g., contractors), and any arrangements for security with contractors in the security policy.
	Maturity level	1	The security officer of the organization has developed (documented) a security policy.
			☐Implemented ☐Planned to be implemented ☐Not applicable
		2	The organization's Chief information security officer has approved and implemented the security policy. The organization manages and implements the approved documents.
			☐Implemented ☐Planned to be implemented ☐Not applicable
		3	The organization's security officers and Chief information security officer regularly review, update, and maintain security policies.
			☐Implemented ☐Planned to be implemented ☐Not applicable

Figure 11: Format for answer

Next step

Collaboration activities between RRI and PI4.0

In the future, collaboration activities between RRI and PI4.0 plan to realize the TWP (trustworthiness profile) in a demonstrator, which would provide a standardized basis for establishing digitalized trustworthy relationships between buyers and suppliers.

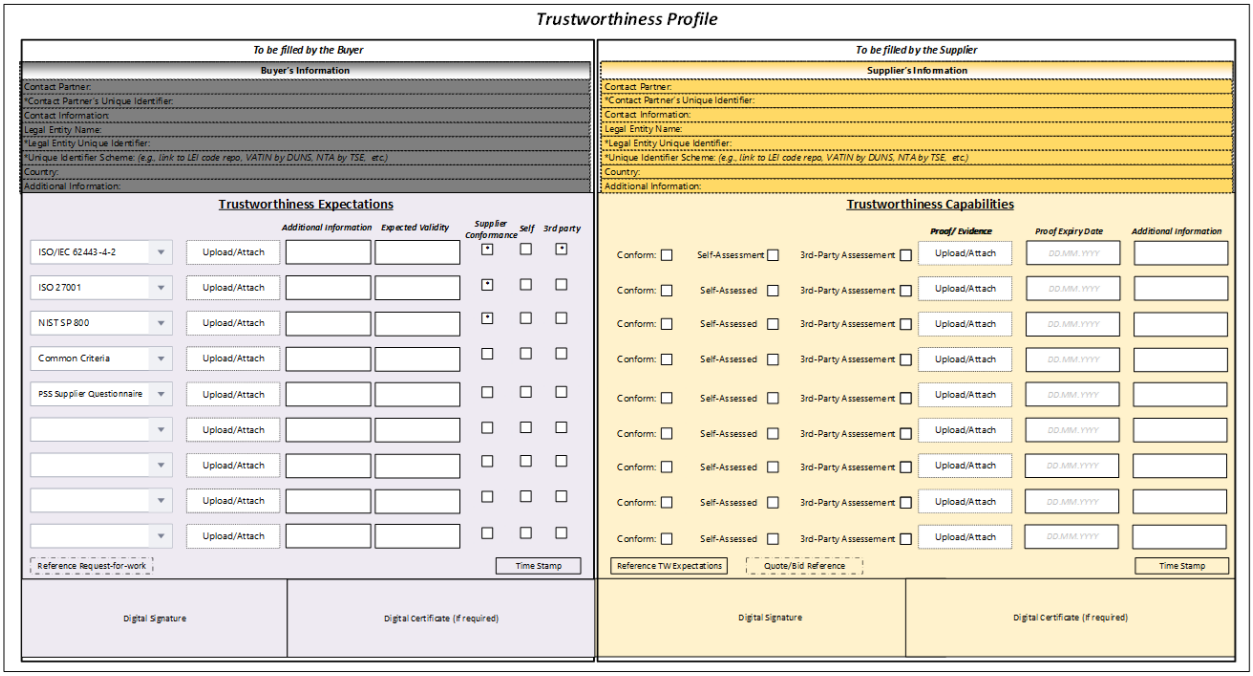


Figure 12: Trustworthiness Profile

RRI's Next step

RRI would like to conduct evaluations of RRI questionnaires locally in Japan and globally with PI4.0.

(1) Evaluation by procurement divisions in RRI member companies.

Aside from quality, cost and delivery, procurement divisions in the manufacturing sector may have a priority for safety and environmental issues rather than for cyber security. So, we first have to share the idea that cyber security is one aspect of quality by introducing recent supplier related security incidents such as vulnerable suppliers' products with Rippl20 and software updates infecting malwares. After that the priorities of the requirements in RRI questionnaires are discussed and identified from their view points.

(2) Evaluation though PI4.0 demonstrator.

The concept of trustworthiness expectations and capabilities exchange protocol and its demonstrator by PI4.0 would be introduced to global security and manufacturing communities. RRI would like to get feedback and make the RRI questionnaires practical by taking advantage of the opportunities.

Annex

RRI security requirements

Identify	CPS.AM-1 (Asset Management)	Document and manage appropriately the list of hardware and software, and management information (e.g. name of asset, version, network address, name of asset manager, license information) of components in the system in the organization.
	CPS.GV-1 (Governance)	Develop and announce security policies, define roles and responsibilities for security across the organization and other relevant parties (Suppliers) .
	CPS.RA-1 (Risk Assessment)	Analyze the vulnerability of the organization's assets and document the result.
	CPS.RM-1 (Risk Management Strategy)	Establish and manage the cyber security risk management process by appropriate relevant parties within the organization.
	CPS.SC-1 (Supply Chan Risk Management)	Establish and manage the supply chain risk management process by appropriate relevant parties within the organization.

Protect	CPS.AC-1 (Identify Management & Access Control)	Issue, manage, validate, revoke, and audit Identification (ID) and authentication information (credential) for authorized devices, people, and processes executed.
	CPS.AT-1 (Awareness &Training)	Provide appropriate training and education to all individuals in the organization so that they can understand assigned roles and responsibilities to prevent from or respond to security incidents.
	CPS.DS-1 (Data Security)	Agree in advance on security requirements for protection of information, if the organization exchanges protected information with other organizations.
	CPS.IP-1 (Information Protection Process & Procedures)	Initial configuration of assets and configuration changes to assets are managed based on security principles.
	CPS.IP-9 (Information Protection Process & Procedures)	Include items concerning security in personnel processes such as recruitment and transfer of personnel. Manage the access rights of personnel.
	CPS.MA-1 (Maintenance)	Maintain system components with approved tools and record the history.
	CPS.MA- 2 (Maintenance)	Maintain system components of the delivered system with approved tools and record the history.

Detect	CPS.AE-1 (Anomalies & Events)	Identify the routine network operation and the flow of information between people and systems during the operation.
	CPS.AE-2 (Anomalies & Events)	Establish a organization to detect, analyze, and respond to security events.
	CPS.CM-1 (Security Continuous Monitoring)	Monitor internal network and external network connection point.
	CPS.DP-1 (Detection Process)	Define the roles and responsibilities of security event detection.
Respond / Recover	CPS.RP-1 (Response Planning) (Recovery Planning)	Implement the response to detected incidents according to the established response procedure.

ECM development process	IEC 62443-4-1 SM	Include security management requirements in the product development process.
Development environment	IEC 62443-4-1 SM	Manage product development environment according to security requirements.
	IEC 62443-4-1 SM	Confirm that the source code and data contents of the product are maintained correctly.
Procurement	IEC 62443-2-4 SP.02	Present documentation that ensure the security level of the products and services provided.
O&M	IEC 62443-4-1 SG	Provide manuals to securely set up and make the equipment robust.
	IEC 62443-4-1 SG	Provide manuals for secure use and disposal of equipment.
Production equipment	IEC 62443-2-4 SP.01.01, SP.01.02	Manage construction of production equipment according to security requirements.
	IEC 62443-2-1	Manage operation of production equipment according to security requirements.

AUTHORS:

Ayaji Furukawa, Toshiba Corporation;Hirozumi Eki, JTEKT Corporation; Junya Fujita, Hitachi Ltd.; Atsuhi Kitamura, Robot Revolution & Industrial IoT Initiative; Masue Shiba, Toshiba Corporation; Prof. Tsutomu Matsumoto, Yokohama National University; Nobuaki Suzuki, Toshiba Corporation; Tsutomu Yamada, Hitachi Ltd.; Dr. Takeshi Yoneda, Mitsubishi Electric Corporation

Approaching industrial IoT trustworthiness in international standards and guidelines

Author:

Ekaterina Rudina, Ekaterina.Rudina@kaspersky.com, Kaspersky ICS CERT

Why IoT require trustworthiness, not only security

Hardly anyone can be surprised to say that there is no absolute security and safety. This means that at a certain moment one has to rely on some assumptions and expectations regarding them. This fully applies to the security and safety of the Internet of Things, industrial systems and critical infrastructure. The moment we realize the limitations of any security and safety guarantees, we start talking about trust.

In this case, trust is understood in a broad sense. But when it comes to the constraints on the safe behavior of the specific systems, especially physical ones, we expect that they are very concrete and straightforward.

For example, a traffic light at an intersection should not be able to give a permission signal for all road users. To make this impossible, a hardware module (malfunction management unit) is used as part of the traffic control system at the intersection. A smart traffic light, due to some reason - a failure, or even a remote attack - can switch to the default mode (flashing yellow or flashing red). Moreover, from a safety point of view, this behavior is trustworthy.

The situation is complicated by considering the behavior of multiple traffic lights in a traffic management system. The task of such a system is to regulate traffic in the city in accordance with the situation. For example, in an emergency mode, there is a need to slow down traffic. Law enforcement agencies can rely on this capability, which means they rely not only on the fact that traffic lights at intersections are safe, but also on the fact that they are reliable, operate consistently, respond to commands and provide feedback. In general, there are quite a few consumers of traffic management services in a smart city. Among them are road services and the traffic safety inspection. The latter may need to integrate a traffic management system, including processing data from video cameras, with a vehicle database. Automatically, this means applying the requirements for ensuring the security of personal data to the received service. And this automatically includes in the concept of trust in the system the trust on the part of the subjects of personal data and the regulator representing their interests in the sense of consent to the processing of this data.

However, all users do not unconditionally trust systems, services, and the entire infrastructure. They rely on this infrastructure, assuming that it implements the functions of protecting confidential information, ensures the correct operation of management teams, meets the requirements for reliability and resilience, and in itself does not pose a threat to human life, health and the environment. As systems evolve, the assumptions underlying trust, both explicit and implicit, change. Hence, the requirements for trustworthiness must evolve.

Why existing standards can’t cover trustworthiness

Reliable system operation is usually guaranteed by testing under specific conditions. Testing also provides the basis for the separate safety and security considerations of a system. However, it would be good to consider trustworthiness in a complex of aspects: how threats can affect the reliable behavior of the system, its availability, safety, and resilient execution.

Let us consider, using an example, why it is impossible to use the accepted characteristics of the vulnerability of a physical device to a cyber attack to assess the potential impact of this attack on the security of this device for a person.

The vulnerabilities CVE-2017-12712/12714/12716, discovered several years ago in Abbott Laboratories pacemakers, allow attackers to gain unauthorized access to these devices, issue commands to them, change settings, and maliciously disrupt their operation. The first vulnerability from the list relates to the authentication algorithm in the pacemaker: the authentication key and timestamp can be compromised or bypassed allowing a nearby attacker to issue unauthorized commands to the pacemaker via RF communications. The second relates to the absence of restrictions on the number of commands issued, which can reduce the battery life of the device. The third vulnerability is related to the lack of encryption during data transmission and storage. The discovery of vulnerabilities resulted in the recall of 465,000 pacemakers by the US Food and Drug Administration (FDA).

Another vulnerability CVE-2017-12701 in CPAP (continuous positive airway pressure, ventilation at constant pressure) devices manufactured by BMC Medical and 3B Medical allows attackers to achieve denial of service for the Wi-Fi module in the device. CPAP devices are designed to treat apnea syndrome. They maintain a constant air pressure so as to reduce the risks associated with insufficient air supply to the airways. This type of device usually operates continuously for several hours, mainly during sleep, and its sudden shutdown poses a risk to the patient.

However, denial of service in the considered case affects only the Wi-Fi module used for data transmission, but not control during operation, and therefore does not affect the performance of the main function of the device. For devices released after July 1, 2017, the vulnerability has been fixed, while previously released devices are proposed to be used without a fix, no hardware recall has occurred.

Formal analysis (according to CVSS v3, see Table 1) shows that none of the vulnerability description fields currently can be used to assess whether the exploitation of a vulnerability could have an impact on safety. This score (shown in the last column in the table above) obviously follows from the consequences of exploiting each vulnerability but does not follow from the formal description of the vector and CVSS rating.

Table 1

CVE id	CVSS v3 base score[1]	CVSS vector string[2]	Can affect safety if exploited
CVE-2017-12712	8.8	AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	Yes
CVE-2017-12714	6.5	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Yes
CVE-2017-12716	6.5	AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	No
CVE-2017-12701	6.5	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	No

The issue of the possibility of harm to the patient during attacks is a long-standing controversy and sometimes litigation.[3] The requirements of the international standard IEC 60601-1 General Requirements for Safety of Medical Electrical Equipment, which is the main required for the certification of medical devices and which is nationally adopted in the USA, European countries, Canada, Russia, indicate that in the risk management process for medical electrical products and systems not only the hazards use that are addressed in this standard, but also all other hazards, associated risks and risk control measures should be determined. The standard also specifies that in the event that the requirements of this standard relate to the prevention of unacceptable risk, the acceptability or unacceptability of this type of risk should be determined by the manufacturer in accordance with his accepted principles for determining the acceptable risk.

In other words, the manufacturer defines the principles for identifying and assessing safety risks associated with cyberattacks on medical equipment. This violates the fair application of separation of duties and does not facilitate the improvement of the whole situation with a possible impact of cyberattacks on safety. This approach can't provide enough level of assurance on a proper and safe system behavior.

Confidence that an IoT system, including industrial IoT, will operate in conformance with requirements results from assurance that several characteristics of the system are compliant with these requirements despite environmental disturbances, human errors, system faults and attacks. The complicated concepts must also address the dependencies and inconsistencies of the separate aspects (security, safety, reliability and others) of the system behavior.

These characteristics – security, safety, reliability, resilience and privacy – have been identified by the Industrial Internet Consortium (IIC) and some other organizations as defining trustworthiness of a system. These characteristics manifest themselves in operational, organizational, commercial, budgetary, architectural and security areas.

[1] NVD Database.
[2] NVD Database
[3] https://threatpost.com/st-jude-medical-patches-vulnerable-cardiac-devices/122955/

Approaching trustworthiness as a set of characteristics

The Cambridge Dictionary defines trustworthy as deserving of trust, or able to be trusted. 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. Trustworthiness, survivability, dependability and similar concepts characterizing industrial system behavior determine the varying sets of basic characteristics and requirements for the industrial IoT system. Probably, the first approach to this complex characteristic was a list of "dimensions" created in 1999 by the *Committee on Information Systems Trustworthiness* to describe the trustworthiness of *networked information systems* (NIS).[4]

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.

The Industrial Internet Reference Architecture (IIRA)[5] designated five key 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. IIC also specified four groups of factors 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]

That would be no interest in introducing trustworthiness as the new concept if the characteristics were just independent components of it. The complicated concepts like trustworthiness must also address the dependencies and inconsistencies of the separate aspects of IoT system behavior like conflicting security and safety properties, which are the "IoT incarnations" of the "fire safety in protective design" dilemma. Such dependencies and inconsistencies cause the additional constraints on the proper approach to IoT system design, its use, maintenance and support.

---

[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] Industrial Internet Consortium: Industrial Internet Reference Architecture (IIRA), V1.9, June 2019. https://www.iiconsortium.org/IIRA.htm

[6] Industrial Internet Consortium: Vocabulary, V2.3, October 2020, https://www.iiconsortium.org/vocab

In practice, the following factors and relationships between characteristics are the subject of concern:[7]

- The opposing goals of some characteristics. Security protects an industrial system and its components from malicious attacks, erroneous human behavior, or environmental disturbances. In direct contrast, safety protects humans (including the employees within the system) and the environment from any bad behavior of the system.
- The context dependencies. Reliability addresses the correct functionality of the system but only under specified conditions. In contrast, resilience addresses the functionality of the system under non-planned conditions. Both cannot be specified without these conditions are defined.
- Inner dependencies of some characteristics. Privacy protects the human-related data. Such data is part of the system, and if protection is necessary, security is responsible. That sometimes leads to the situation of mixing security and privacy whilst in reality their goals generally vary.

As a result, 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. Combined with the mentioned factors they contribute to better safety, better security, privacy, reliability and resiliency.

Trustworthiness standardization issues

While members of Trustworthiness Task Group in IIC already agreed on the set of characteristics comprising trustworthiness, the members ISO/IEC SC41 standardization committee are in process of discussions around that. The identified characteristics of trustworthiness are connected to so-called “-ilities”, the non-functional requirements which set up the criteria for the solution, system, product or environment according to the expectations about its functioning.

While these discussions are on their way, let’s focus on the main issues and tasks of standardization that should be addressed consistently in the following standards:

- ISO/IEC 30141:2020. This document provides a standardized IoT Reference Architecture using a common vocabulary, reusable designs, and industry best practices. It uses a top down approach, beginning with collecting the most important characteristics of IoT, abstracting those into a generic

[7] Marcellus Buchheit, Frederick Hirsch, Sven Schrecker. A Short Introduction into Trustworthiness. IIC Journal of Innovation, September 2018. https://www.iiconsortium.org/news/joi-articles/2018-Sept-JoI_A_Short_Introduction_into_Trustworthiness-TTG.pdf

IoT Conceptual Model, deriving a high level system based reference with subsequent dissection of that model into five architecture views from different perspectives.[8]

- ISO/IEC 30149:2021 Trustworthiness principles. This document provides principles for IoT trustworthiness based on ISO/IEC 30141 – IoT Reference Architecture[9]

We can say informally that an industrial IoT system is trustworthy if it meets the minimum requirements for security, safety, reliability, resilience, privacy and other characteristics, as defined by laws, regulations, standards and industry best practices. The following aspects of the requirements of all types may be considered:

- The role of objectives for each aspect of trustworthiness
- The role of assumptions for the assurance on each aspect
- The role and approaches to implementing the aspect “by design”
- The role of assurance (and control) for each element

Let’s consider these aspects and the issues that appear when it comes to the consideration of trustworthiness in terms of standard or guideline.

The role of objectives

There is no abstract security or safety, or resilience, etc. Each element for the concrete system, network or infrastructure is defined against the objectives valid for this system, network or infrastructure. These objectives may be informal or defined in a formal way. The stakeholders may approve the set of objectives, or they may be well known and generally accepted.

For maintaining assurance on the trustworthiness aspect, the set of valid objectives should be defined and approved.

Validity of the aspect objectives means their coherence, consistency, completeness and conformity with the informal aspect definition that has attained the broadest possible agreement of all subjects relevant to the use and general functioning of the system, network or infrastructure for which these objectives are set.

[8]https://iectest.iec.ch/dyn/www/f?p=103:38:0::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104064
[9]https://iectest.iec.ch/dyn/www/f?p=103:38:733215753278::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104432

The definition of the "universal" trustworthiness objectives, which would cover objectives for all trustworthiness aspects come up with the following issues:

- The way of defining the objectives vary per each trustworthiness aspect (security, safety etc.). Partially this is determined by the nature of the property underlying the aspect (safety vs.liveness), partially by the factors affecting the aspect. The ways for defining the objectives for each element have been established for a long time.

For example, the data security objectives may be referred as data confidentiality, integrity and availability. Interpretation of the system security as a characteristic inherited in some way from data security may be not invalid but very hard to validate. Safety objectives, for example, in aviation safety programs are managed through the specifically defined key performance indicators. System reliability is usually evaluated against using the Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR) measurements which set up the qualitative objectives. Privacy objectives usually represent the requirement of compliance of handling the information that may contain users personal data with legislative and regulating acts. Resilience probably is the most complicated thing; sometimes the objectives are set in a form of technical measures (e.g., applying backup), sometimes they are similar to reliability measurements, sometimes to safety KPIs.

- Objectives may be independent, or correlate, or make up the chain of conclusions, or go into conflict. Sometimes the relations of objectives may be not obvious and discovered in an unexpected way during system use.
- The objectives may be defined at different levels of architectural abstraction, for different system representations and components. Inconsistency of objectives may appear during system integration while for the separate components verification of separate trustworthiness aspects has been done already. Compositional complexity of the system leads to the increasing complexity of both validation of element objectives and verification of the system against these objectives.

It is not a simple task to describe for a general case how the objectives for security, safety, resilience, privacy and reliability can be aligned. Thus, the nature of trustworthiness objectives may be internally inconsistent leading to the inapplicability of standardized approaches.

The role of assumptions

The main difference between trustworthiness and trust is in assuming that some fact(s) we are relying on are true. The valid assumption gives a ground for reasoning about other facts. These facts then substantiate how <element> criteria are satisfied. The groundless assumptions lead to the <element> failure. That's why minimization of assumptions is important. However, it is not possible to make no assumptions.

The issue is that assumptions for the different elements may go into conflict. The example from a physical world is the assumption that for security reasons the access to the equipment is restricted for those who a

not authorized to work with it, and the personnel is checked before entering and exiting the room. The conflicting assumption for the fire safety is that the fire exits are available all the time. This conflict may be solved by introducing the additional technical measures, and similar approach should be applied for trustworthiness inspired conflicts.

The role of "by design" approach

Rational (method based) approach,[10] which we consider here under the name of "by design" approach, accumulates the experience in a form of useful patterns, principles and methods of constructing the system. This requires analysis and synthesis of well-defined representations that may partially base on theoretical conclusions but always are supported by real implementations and validated against the stakeholders' concerns.

As regard to trustworthiness, "by design" approaches for different aspects and the separate methods underlying these approaches should be analyzed. Then, the options of combining these approaches and making a good practice guide for applying them may be considered. This should not be oversimplified; the general methods and general conditions for their applying are preferable rather the concrete details and techniques that may be restricted by the industry, application area or technology. For example, "separation" method mentioning is preferable to "installing the firewall" or even "network segmentation"; "fault isolation" is preferable to "sandboxing" etc. The examples of implementation may be given but they must not restrict the understanding of the nature of every method.

The methods comprising the core of "trustworthiness aspects by design" are the subjects for further discussion. The main issue is that the definition of “by design” approach previously applied to the separate characteristics is usually understood in very different ways.

The role of assurance methods

Systems assurance is the process of building clear, comprehensive, and defensible arguments regarding the safety and security properties of systems. The vital element of that assurance is that it makes clear and well-defined claims about the safety and security of systems. Certain claims are supported through reasoning. The reasoning is expressed by explicit annotated links between claims, where one or more claims (called sub-claims) when combined provide inferential support to a larger claim. Certain associations (recorded as assertions) between claims and sub claims can require supporting arguments of their own (e.g.,

[10] According to Rechtin and Maier classification of system design approaches.

justification of an asserted inference). Claims are propositions which are expressed by statements in some natural language. The degree of precision in the formulation of the claims may contribute to the comprehensiveness of an assurance case.

System assurance methods and approaches are tightly coupled with an approach to system design. The appropriate design makes the assurance procedure(s) simpler and helps with decoupling these assurance goals for their efficient accomplishment.

Assurance goals definition strongly correlate with objectives of the trustworthiness aspect defined as discussed above. At the same time, assurance goals are set up in a more concrete way, e.g., through the defined indicators of their accomplishment. The recommended assurance procedure usually accompanies each defined goal (and the definition is given with a consideration of the appropriate assurance procedure).

For the systems requiring high assurance the assurance procedures, methods and even ways of defining the goals may be a subject of normative regulation, Thus, supporting architectural design of the system may also employ the recommended by normative acts practices, design techniques and approaches.

Assurance procedures and methods may go into conflict, including the conflicts at the level of established normative and industry regulations

For trustworthiness, one of the main problems is in interfering the aspects or in their possible conflict. Assurance procedures for one of the trustworthiness aspects that are normative and obligatory may lead to harm to other aspects. Thus, for trustworthiness assurance the priorities of aspects and introducing the changes into assurance procedures correlated with relationships of aspects are vital.

This is what is particularly important about trustworthiness assurance. The tricks that work, for example, for reliability or security level measurement may be inapplicable to trustworthiness.

Tasks covered by standards and guidelines

To address the issues related to the complex nature of trustworthiness and unique background behind each of characteristics comprising it, it is needed to decompose the tasks for their description in standards and guidelines. This decomposition starts from approaching the definition of required aspect and their priorities specific per an industry or a sector. The aspects and priorities may be used by a standardization committee or an industry (sector) regulating authority to further specify approach to addressing threats, hazards and risks, then – to recommend the approaches, measures and best practices applied in building trustworthy systems, and then – to describe the approaches to getting the assurance of systems and infrastructures trustworthiness.

The tasks related to each of these steps may be grouped as follows.

1. **Problem structuring.** Guidelines and standards approach the trustworthiness as a whole and try to decompose it to different aspects, address these aspects both separately and in their

relationships for the given industry or sector. The set of aspects may follow the characteristics proposed by IIC or be different depending on the specific requirements of the industry and authority issuing the recommendations.

2. **Hazard identification and structuring.** Tasks of this group are usually solved based on hierarchical (or even structured) representation of the factors which are considered as the direct issues for trustworthiness or related characteristics (safety, security, etc.). These issues may have different names (threats, hazards, etc.) Examples of the concrete recommended approaches are the attack trees, fault trees, HAZOP (a study representing a structured and systematic examination of an operation in order to identify and evaluate hazards to personnel or equipment), “bow-tie” risk evaluation method and so on.
3. **Risk evaluation.** Risk evaluating methods are mostly oriented on the likelihood and impact assessment, but other approaches exist as well. This assessment may be performed in a quantitative or (more often) qualitative way. It is important that there is no “trustworthiness risk”, risk evaluating models usually work at the level of the separate trustworthiness aspects (safety, security and so on) because the risks for these aspects usually have significantly different nature.
4. **System design, recommended approaches and best practices.** Trust and trustworthiness are determined by a plenty of factors and there is no way to cover all IoT or even IIoT cases with a single approach to enabling “trustworthiness through design”. However, some design methods may facilitate one or more trustworthiness characteristics for the most of systems, thus moving system developers closer to the system, tolerant to the hazardous conditions or reducing the conditions under which risks can materialize.

All approaches to making the system trustworthy in some aspect “by design” have the one thing they got in common. Such an approach usually increases the cost-effectiveness of enhancements to this aspect provided during integration activities and system usage, or even eliminates the necessity in such enhancements. The “by design” approach anticipates possible issues related to the trustworthiness aspects. The difference with other methods is in foreseeing the possible issue and making the decision at the design stage how to withstand this issue.

As Rechtin and Maier define it, systems designing builds on four methodologies:

(1) Rational (method based) such as systems analysis and engineering. This approach accumulates the experience in a form of useful patterns, principles and methods of constructing the system. This requires analysis and synthesis of well-defined representations that may partially base on theoretical conclusions but always are supported by real implementations and validated against the stakeholders' concerns. The ultimate form of the rational approach is the formal model. Normally the rules and methods are validated by experiments and testing.

The examples are

- Public key infrastructure model (the model of trust relationships)
- ACL-based discretionary access control (or any other model for access control)
- PERA (Purdue Enterprise Reference Architecture, the reference model)
- MILS approach implementing the system based on the predefined Policy Architecture

(2) Participative (stakeholder based), mostly represented by SDLC-based methodologies. The SDLC-based models assume that they may address (already identified) issues through applying the methods, best practices, tactics and techniques during the product lifecycle

- V-cycle adopted by ISO 26262 set of standards for automotive safety
- Microsoft Secure development lifecycle based on STRIDE
- Automotive EVITA project
- 30147 CD currently elaborated by WG3
- Concurrent Engineering (CE) is a systematic approach to integrated product development that emphasizes the response to customer expectations. It embodies team values of cooperation, trust and sharing in such a manner that decision making is by consensus, involving all perspectives in parallel, from the beginning of the product life cycle.

(3) Heuristic (lessons learned). The heuristics methodology is based on “common sense,” that is, on what is sensible in a given context. Contextual sense comes from collective experience stated in as simple and concise a manner as possible. The example of the method implementation is the set of security principles defined by Saltzer and Schroeder in 1975 which had not become obsolete. Over time, some proven heuristic methods become the normative ones or turn into rational (method based) approach.

(4) Normative (solution based) such as building codes and communication standards. The example is "prevention through design" approach. **Prevention through design** (safety) represents a shift in approach for on-the-job safety. It involves evaluating potential risks associated with processes, structures, equipment, and tools. It takes into consideration the construction, maintenance, decommissioning, and disposal or recycling of waste material. Thus, this approach tends to become a normative one.[11]

[11] https://en.wikipedia.org/wiki/Prevention_through_design

Each of the approaches rarely covers all concerns. They are applied together to address the issues identified and evaluated according to the results of hazard structuring and evaluating model kind.

5. **System assurance** on trustworthiness and its separate aspects. This may cover a variety of methods from simple testing to model checking approach and behavior verification and other run-time methods. Assurances approaches relate to the hazard identification and risk evaluation and may change depending on the methods of trustworthy system design.
6. **Maturity models** that are aiming to cover the gaps in processes of development, configuration and maintenance of (not only) IoT solutions thus indirectly contributing to the quality of code, in-time discovery of vulnerabilities and patching those of vulnerabilities that may have an impact on trustworthy solution functioning. Among the models addressing the task of maturity evaluation and enhancement in regard to trustworthiness may be mentioned the following:
   - OWASP Software Assurance Maturity Model (OWASP SAMM)
   - IIC IoT Security Maturity Model (IIC IoT SMM)
   - Capability Maturity Model Integration (CMMI)
   - Automotive SPICE
   - Lockheed Martin Cyber Resilience Level™ (CRL™)
   - Cyber Resilience Review methodology by the US Homeland Security

Trustworthiness principles

The last but not the least, to address the issues and cover the tasks dependently and avoid the situations like in the described case for medical devices certification, the following principles are proposed in implementation of standards into life.

Principles related to the system and context

1. **Trustworthy system should reflect the real-world (business or mission) trust relationships.** For example, hierarchical relationships in PKI infrastructure reflect the hierarchy of trust between the actors ant the dependence of some actors on others
2. **Trustworthy system should clearly set up the priorities for the trustworthiness aspects**, for example, for nuclear facility the safety is in highest priority so the depend on it and must facilitate it.
3. **Trustworthy system should implement the fail-safe design at least for the for the prioritized aspects.** This is more strong than just fail-safe defaults. That means that system's default behavior

must keep invariants defining the objectives for the prioritized aspect (e.g., safety objectives) even if new requirements are set for this system. It must be noted that this principle includes composability.

Principles related to the methods and methodologies

4. **Rational (method-based) approach** in design, implementation, configuration and maintenance of trustworthy system **has a preference over the heuristic (lessons learned) approach**
5. **Normative (solution-based) approach** in regulatory, design, implementation, configuration and maintenance **has a preference over the voluntary approach**

Principles related to the process

6. **Participative (stakeholder-based) approach** to attain trustworthiness **has a preference over the unilateral** (e.g., compliance-based only) **approach**
7. Trustworthiness assurance processes should enforce the **separation of duties principle** in implementation and assurance procedures for trustworthiness aspects
8. Established (standardized) protocols, procedures and methods to attain trustworthiness **have a preference over the ad-hoc approach**

Conclusion

Since 2016 when IIC first introduced trustworthiness in its current understanding, several groups of experts inside the IIC and ISO/IEC work on this issue. The goal the change of the focus from traditional considerations such as “safety first and nothing else matters”, “security has absolute priority” or “system should demonstrate resiliency” to “let’s design a system with a proper behavior, which is safe and secure by design, based on trustworthiness standards and guidelines that everyone can trust.”

This work is ongoing.

Trustworthiness as facilitator of Policy and Access Management in Supply Chains

Authors:

Jürgen Neises, juergen.neises@fujitsu.com

George Moldovan, george.moldovan@rbinternational.com

Thomas Walloschke, thomas.walloschke@secon-tc.eu

Cosmin Grigoras, cosmin.grigoras@siemens.com

Bianca Popovici, bianca.popovici@siemens.com

Abstract

Typical transactions in cross-company Industry 4.0 supply chains require a dynamically evaluable form of Trustworthiness. Therefore, specific requirements on the parties involved, down to the machine level, for automatically verifiable operations shall facilitate the realization of the economic advantages of future flexible process chains in production.

The core of the paper is a modular and extensible model for assessing Trustworthiness in industrial IoT. This model reflects trust as a continuous dynamic system of features with corresponding attributes and policies. Interactions of communicating entities then may depend on the degree of fulfilment of those.

A framework for the automated computation of Trustworthiness in a dynamic environment based on a trust metric is described and its utilization and integration into an ABAC based access control is outlined in an exemplary M2M scenario based on the results of the Horizon 2020 project SecureIoT. (GA #779899)

Introduction

The typical form of secure cross-company communication in Industrie 4.0 also concerns transactions in supply chains in particular. In general, supply chains that can be flexibly automated are increasingly in demand. In addition to the electronic form, this also affects the physical logistics part and the associated expectations of trustworthiness, "to receive that, and only that, which was ordered". These additional requirements, as well as all existing requirements, demand a much more dynamically evaluable expression of trustworthiness than is usually mapped in established supply chains of existing grown ecosystems. The generation of a system for **measurable trustworthiness** is explained in the following chapters.

The goal is primarily to keep possible security-related disruptions as low as possible.

To illustrate the urgency of taking appropriate measures to create transparency in the area of trustworthiness, Figure 1 shows how the development of Global Incident Growth of several orders of magnitude in the area of manufacturing in the period from 2012 to 2020 compared to the overall development in the same period.

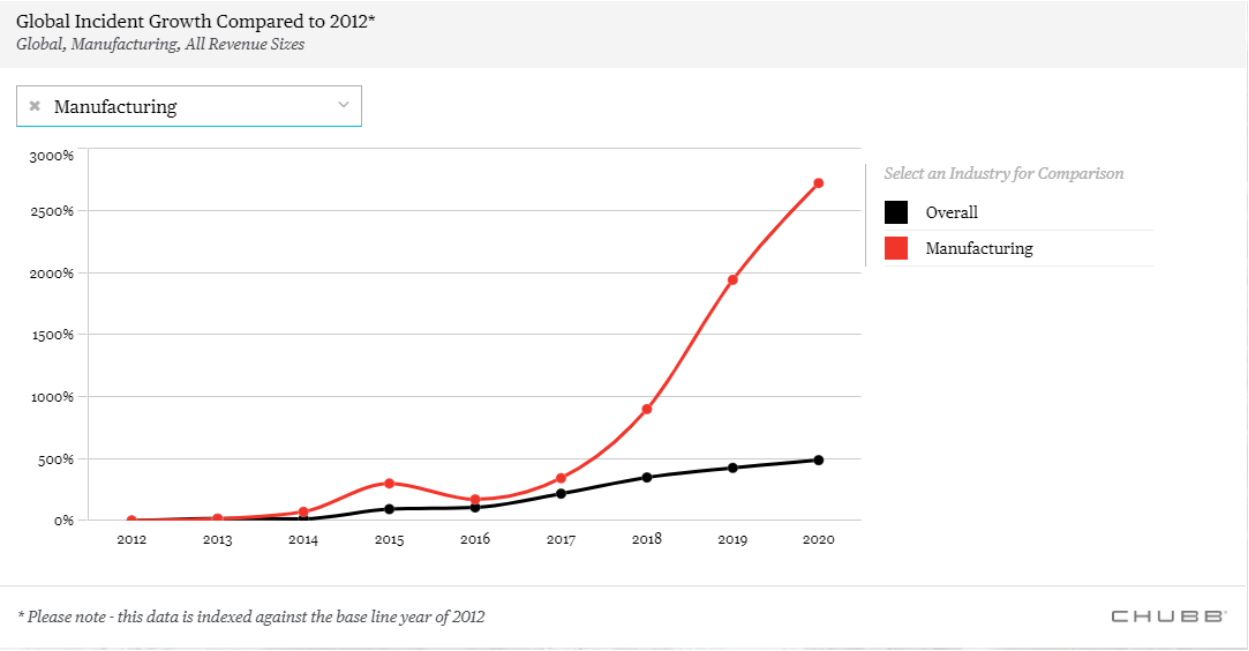


Figure 1: Global Incident Growth Compared to 2012 based on industries (Source: CHUBB[1])

[1] Chubb Cyber Index: Providing Data Driven Insight on Cyber Threat Trends, https://chubbcyberindex.com/#/incident-growth

As depicted in Figure 2, attacks on the manufacturing and technology sectors have reached the 2nd and 3rd place in the ranking of attacks in 2020, the absolute highest since 2007 after the professional services sector, which is number 1.

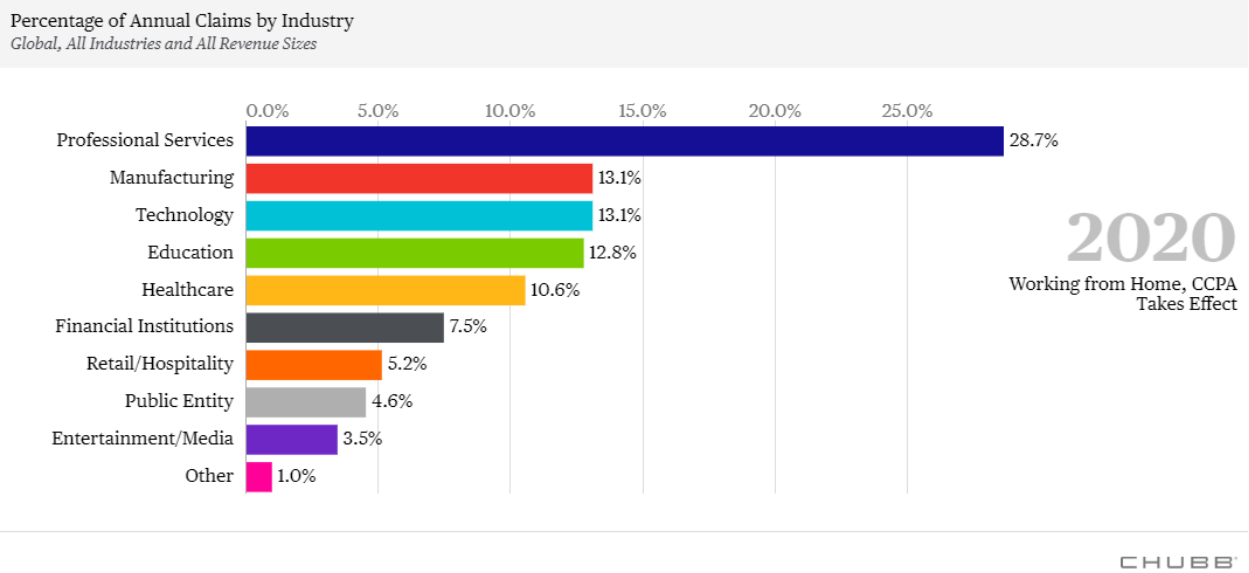


Figure 2: Percentage of Annual Claims by Industry (Source: CHUBB[1])

The development since 2007 clearly shows in Figure 3 how manufacturing has entered the focus of attackers in recent years, as perpetrators increasingly recognise the lucrativeness and sometimes clear low threshold for their attacks.

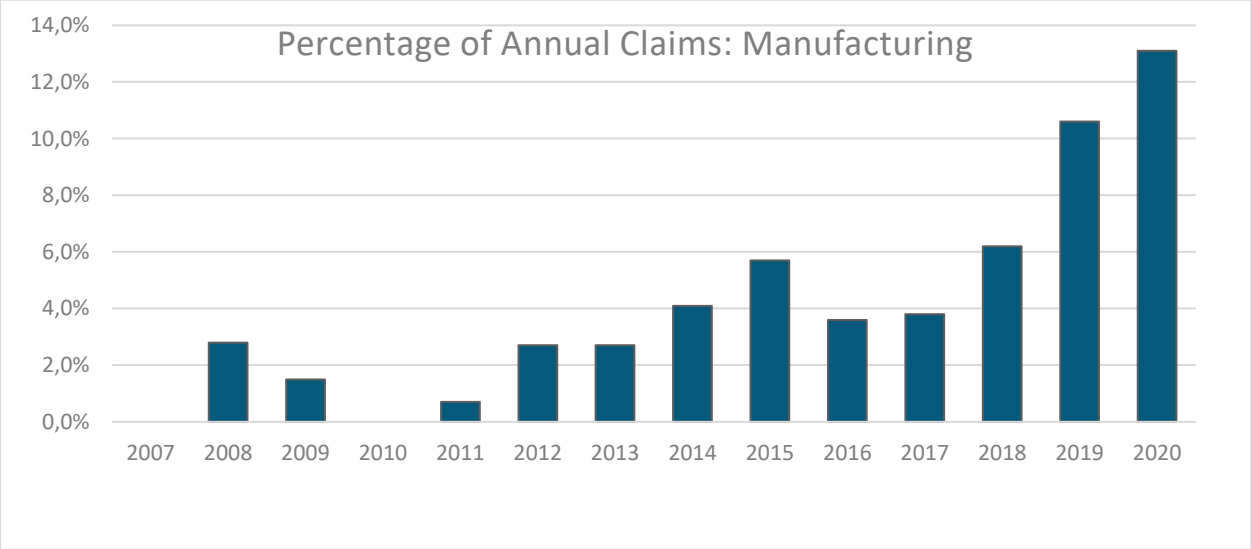


Figure 3: Percentage of Annual Claims of Manufacturing since 2007 (Source: CHUBB[1])

Finally, a further analysis in Figure 4 shows that the dramatic increase in cyber incidents from 2016 onwards primarily affected companies with an annual turnover of between €150 million and €500 million. This fate then also affected those companies in the traditional SME sector with an annual turnover of up to €25 million from 2018 onwards - and ultimately at the same incident level in 2020. These two company sizes are clearly in the focus of the attackers and are obviously most at risk. We are talking about total losses in the billions, which will not be examined more closely in this context. Some of the reasons for this situation are explained below.

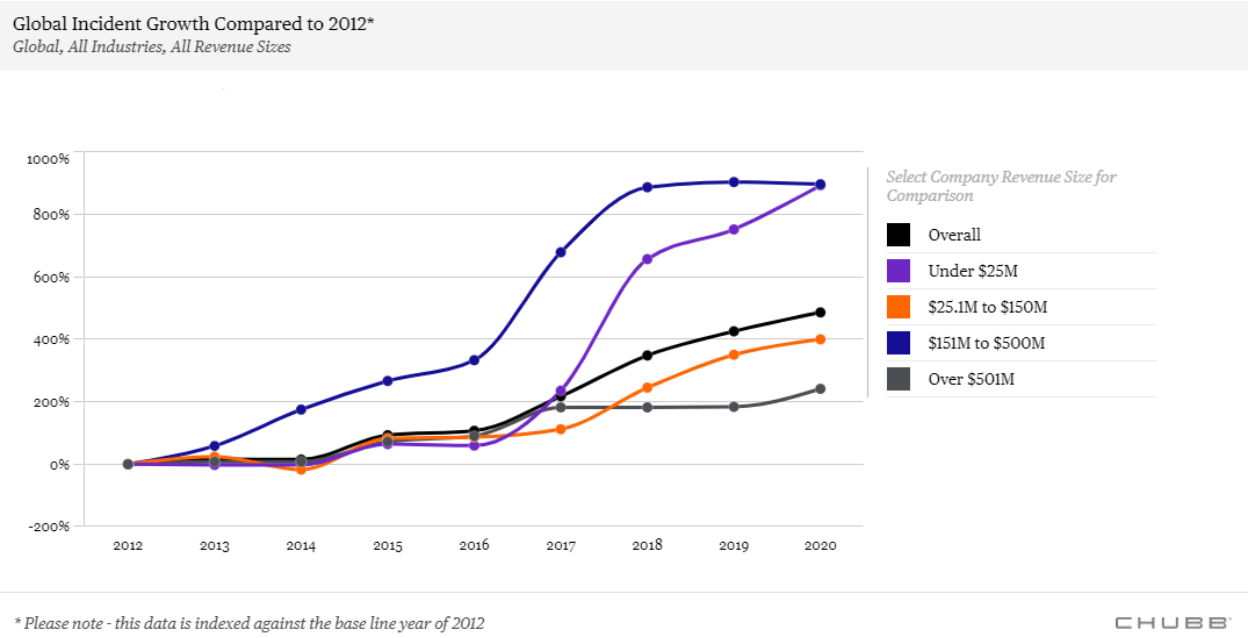


Figure 4: Global Incident Growth Compared to 2012 based on Revenue (Source: CHUBB[1])

From this, concrete steps must be taken to create modified trust models. In the future, all participants down to the machine level should be subject to automatically verifiable processes, especially in communication. In practice, these models require a flexible and at the same time globally understandable and internationally accepted procedure to enable the economic advantages of future flexible supply chains in production.

The current situation shows that these measures have not yet found their way into manufacturing and that the value contribution of security investments to the overall value creation is not sufficiently clearly recognised. In certain sensitive areas, however, such as critical infrastructures, government regulation will increasingly force the implementation of appropriate measures.

Some important underlying factors for this situation are:

- Fear of increased system complexity due to security measures that cannot be managed in the traditional established processes for development and operation.
- Lack of universally applicable and industry-compatible implementation standards for security with moderate certification efforts for trustworthy solutions.
- Lack of a global trust infrastructure that supports compatibility of security implementations in terms of trustworthiness.

To overcome these barriers, security standardisation, among other changes, must be supportive.

This document is specifically about:

- the modelling for assessing trustworthiness
- the creation of metrics for measuring and evaluating the usefulness calculation
- the use of access control technologies to build trust

and consideration of the important Industry 4.0 issues

- Access, role and authorisation mechanisms for Industry 4.0
- Security for agile systems
- Trustworthiness of the value network

In addition, security management processes are classified as a very important future goal of Industry 4.0.

In the following, the topic modelling for assessing trustworthiness will be discussed.

Modelling

While trustworthiness interpretations vary from one system to the other, some variations are regional-specific or industry-specific. Also, the importance of the different trustworthiness characteristics will vary according to industry vertical and regional interpretations.[2]**Fehler! Verweisquelle konnte nicht gefunden werden.** Hence, a wide range of approaches exist on Trustworthiness not only in the area of Industry 4.0 and beyond. For instance, the concept of Trustworthiness has been also adopted in the automotive industry.[3]**Fehler! Verweisquelle konnte nicht gefunden werden.** Ongoing work among various organisations like ISO (esp. ISO/IEC JTC1), NIST, VDI (cf. VDI2182) contribute to the progress.

In the context of supply chain resilience major topics of Trustworthiness are[4]

- protection of availability and robustness of the supply chain
- assurance of the integrity and proof of origin
- secure access to resources, e.g. machines
- agile automated evaluation of participants' Trustworthiness

[2] Walloschke, T.; Neises, J.; Soldatos, J.: „Multi-Level Policy Matching applied to Industrie 4.0"

[3] Putzer, H. J.; Wozniak, E.: "Trustworthy Autonomous/Cognitive Systems – A Structured Approach", fortiss Whitepaper (2020), https://www.fortiss.org/fileadmin/user_upload/Veroeffentlichungen/Informationsmaterialien/fortiss_whitepaper_trustworthy_ACS_web.pdf

[4] Wolfgang Klasen, „Shaping a globally secure Industrie 4.0 Ecosystem - Roadmap for Standardizing Industrial Security", Web Seminar (September 23rd, 2020), https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/Webinar_Trust_Pr%C3%A4sentation.pdf?__blob=publicationFile&v=2

Within the global work on the subject of Trustworthiness several views on Trustworthiness have been published by the German Plattform Industrie 4.0,[5] the Japanese Robot Revolution & Industrial IoT Initiative (RRI)[6] and the Industrial Internet Consortium (IIC).[7] These views have in common, that Trustworthiness shall ensure confidence in relationships between companies, people, systems and components meeting expectations among participants in the industrial value network as claimed in an adaptation of the proposition by the ISO/IEC JTC1/WG13.[8][9]

"For supply/value chain security and risk management, the term 'Trustworthiness' corresponds to the supplier's ability to meet the expectations of the potential contract partner in a verifiable way".

Thus, the expectations define a set of requirements, which shall be continuously monitored, measured and evaluated in time of interacting with a resource due to ever changing conditions and their timely verification. This set may include legal and economic information based on publicly available information, e.g. from the Global Legal Entity Identifier Foundation (GLEIF)[10] and may be adapted. Therefore, an approach for Trustworthiness evaluation needs to be modular and flexible thus enabling extension of requirements.

The model of the IIC may be taken as a first example point of view illustrating the approach of this paper. This model reflects trust as a continuous dynamic system of system characteristics with corresponding attributes (i.e. measurable features like height) and properties (i.e. a measured description of an attribute, e.g. 1800 mm for height).[11] These characteristics describe a resource, e.g. a system. Interactions of communicating entities then may depend on the degree of fulfilment of those.[12]

---

[5] Michael Jochem: "Trustworthiness and Integrity – Integrity a fundamental Protection Goal for Trustworthiness" (2018) https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation-gesamt/praesentation-5.pdf?__blob=publicationFile&v=1

[6] Plattform Industrie 4.0, Robot Revolution Initiative "Facilitating International Cooperation for Secure Industrial Internet of Things/Industrie 4.0" (2018) https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/secure-industrial-internet-of-things-update.html

[7] Industrial Internet Consortium (pub.): "Industrial Internet of Things Volume G4: Security Framework" (2016) https://hub.iiconsortium.org/iisf

[8] ISO/IEC JTC1/WG13: https://www.iso.org/committee/45020.html

[9] Kitamura Atsushi et al.: "IIOT Value Chain Security – The role of Trustworthiness." (2020), https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.pdf?__blob=publicationFile&v=5

[10] https://www.gleif.org/en/

[11] Birkhofer, H.; Waeldele, M.: "Properties and Characteristics and Attributes and – An Approach on Structuring the Description of Technical Systems", AEDS 2008 Workshop (2008)

[12] Neises, J.; Moldovan, G., Walloschke, T Popovici, B.: „Trustworthiness in Supply Chains - A modular extensible Approach applied to Industrial IoT", GIoTS 2020

Figure 5: IIC IoT Trustworthiness Radar

Within Figure 5 several levels of Trustworthiness are depicted. A minimum level sets the required lowest level of Trustworthiness. The current and the target levels show the state and the objective. Finally, the maximum level sets the maximum level of Trustworthiness, which can be obtained. This kind of Trustworthiness radar illustrates the policies and requirements in each entity.[12]

Based on the policies described by the set of characteristics, their attributes and properties, the calculation of Trustworthiness using this model may be considered as a weighted combination. Each characteristic is a weighted combination of properties showing the degree of fulfilment of the specified attributes in the range of [0,1]. Each weight will be assigned according to relevance of the attributes per system characteristics. The sum of weights shall be one with each weight in the range [0,1]. This calculation is illustrated schematically in Figure 6 and will be explained in more detail in the following section describing a specific metric. An overall Trustworthiness score can be obtained the same way, by aggregating weighted characteristics.

Additionally, The illustrated evaluation schema may be easily extended by mandatory criteria, which lead to zero values for a characteristic or the overall Trustworthiness score in case of not meeting a given threshold of fulfilment.

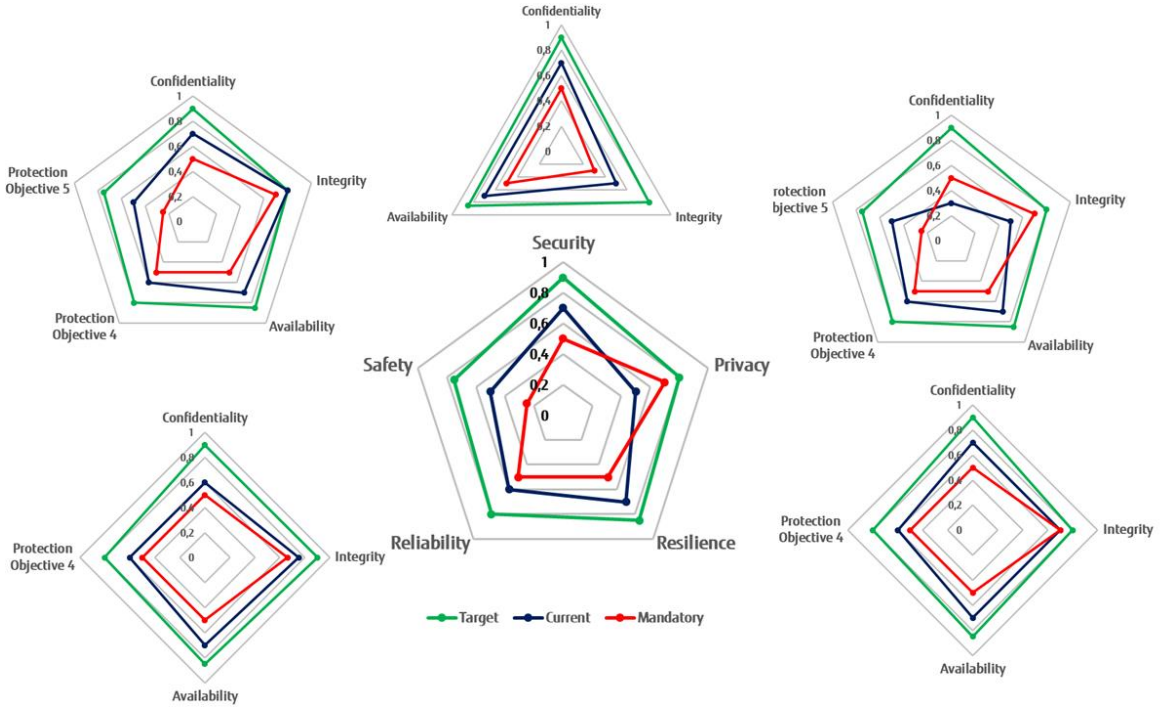


Figure 6: Staggered Evaluation Scheme

The vectors of weights and evaluated fulfilments characterize the IIoT resource and the related policies like a fingerprint. Hence, this is a kind of biometric characterisation of a resource and should be protected like biometric data and should be communicated with care. E.g. in communications the least necessary information should be transmitted.[12]

However, an appropriate Trustworthiness schema depends on the specific expectations and policies, participants' profile and related application in the value chain. The presented model is not yet a final tool. It provides a methodology for measuring and evaluating trustworthiness adaptable to concrete needs. However, human and domain specific knowledge is still required to populate the model with meaningful measurement points. Up to now the development of pragmatic schemas is subject of individual analysis and specifications. Therefore, future work should lead to catalogues of Trustworthiness metrics and schemas, which may extend common Information-Security Management-Systems. In the subsequent chapter constituents of such metrics and a framework for the automated computation of Trustworthiness in a dynamic environment based on a trust metric are presented.

Metrics and Utility Calculation

Passive Observable Metrics

The research and standardizing literature provide core observable software metrics which can be referenced or queried in order to evaluate specific required characteristics such as Security or Reliability.[13] and[14], as well as standards such as ISO/IEC TR 24028[15] or ISO/IEC 27001[16] provide a comprehensive overview of potentially relevant attributes.

Measuring specific attributes, however, can be challenging and usually requires full support and reporting capabilities of infrastructure elements or control over the entire build and development process – which are usually not supported or exposed to a system integrator such as a complex manufacturing line.

In addition, a trustworthiness evaluation relies mostly on external observations in order to avoid a reporter's bias or the ingestion of malicious reported information. In the context of trustworthiness evaluation, metrics represent numerical values associated to mainly external observable events and observable properties of entities (or devices) – meant to complement standard attributes and metrics as previously referenced. The exact state and duration of specific events varies depending on their (i) type and (ii) source: dynamic interactions such as message exchanging or transitions (physical or logical) are short-termed and dynamic – either a change in a physical location, or of software states, respectively. Other properties, such as model-specific features and their limitations or certifications are static in nature or rarely changing since these are model specific and usually reflecting hardware and manufacturing constraints.

The source of quantifiable metrics provides a second dimension alongside the previously mentioned type, which allows for a generic, unambiguous classification based on functional and organizational properties.

[13] A. Bicaku et al., "Towards trustworthy end-to-end communication in industry 4.0," 2017 IEEE 15th International Conference on Industrial Informatics (INDIN), Emden, 2017, pp. 889-896, doi: 10.1109/INDIN.2017.8104889.
[14] Mohammadi, Nazila & Paulus, Sachar & Bishr, Mohamed & Metzger, Andreas & Könnecke, Holger & Hartenstein, Sandro & Weyer, Thorsten & Pohl, Klaus. (2014). Trustworthiness Attributes and Metrics for Engineering Trusted Internet-Based Software Systems. Communications in Computer and Information Science. 453. 19-35. 10.1007/978-3-319-11561-0_2.
[15] ISO/IEC TR 24028:2020, "Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence", ISO/EIC, 2020.
[16] ISO/IEC 27001, "Information security management", ISO/IEC, 2017.

Semantic Grouping of Metrics

We then distinguish therefore between:

- Device (Entity) Metrics, which capture the state (either dynamic, or static) of a device. The states include both physical and logical properties, such as its physical location either in a manufacturing plant, logical responsibilities or position in a manufacturing workflow, its software stack, as well as manufacturing details (manufacturer, certifications, sensor accuracy) (see Table 2).

Table 2 Device Metrics

Metric	Description
Manufacturer	Reflects the reputation of the manufacturer, based on the level/confidence in the provided certificates, known reliability of the manufacturer within the domain, and typical quantifiable service agreements such as mean time between failures.
Firmware Version	Derives a confidence level based on the active firmware version and its release date. Older firmware version might not be as up to date with security features and have, especially for well-maintained devices, known list of vulnerabilities and defects.
Model Number	Model manufacturing numbers contain detailed descriptions of the specifications of any build-in sensors, actuators and their accuracy. Based on the known deviations with regard to sensing or actuating capabilities, optimal functional temperatures, data rates and performance, numerical metrics can be derived.
Power/Battery Levels	Battery driven devices have their batteries replaced regularly, which is usually a disrupting process requiring physical access. From a security or reliability aspect, this means that the device can be damaged, improperly mounted, tampered with or replaced with other models altogether – in addition to it being unavailable during the operation.
Exposure Level	Devices which are embedded into infrastructure or equipment cannot be easily accessed or tempered with. In contrast, devices which are either mobile by nature or transitive deployed, are more exposed. In addition, a mobile device can change either security domains, or expose itself to different environments with different security mechanisms and enforcement.
Mobility	Mobile devices – be it either as part of mobile infrastructure elements or equipment, have usually a higher chance of developing defects than those which are part of static installations, due to the higher risks of physical shocks or damage suffering during transitions – from vibrations, for example.

- Connection Metrics, which capture the state of the component's interconnectivity with other (observable) entities, and which quantities communication properties such as cryptographic parameters during required handshakes in establishing SSL or TLS connections (see Table 2).

Table 2 Connection Metrics

Metric	Description
Communication Protocol	Quantifying the nature of the communication protocols and their specific reliability and security – such as Profibus, Modbus, Ethernet, as well as their medium – Wired, Wireless, Low Power transmissions and similar.
Protocol Versions	Referring to the specific version and supported mechanisms as currently supported by the device.
Certificate Issuers	Trust in the Certification Issuer is critical – the issuer's level in a certification tree, its current availability, security and processes are subject to external reviews, classification and scoring.
Certificate Validity	Referring to the remaining validity of used certificates. The lower the remaining duration, the higher the chance that an update to the certificates can lead to unexpected communication issues due to the failure of updating an expired certificate.
Update capabilities	Denotes to the ability of a note to be updated periodically and reliable. A straightforward process allows for potential known vulnerabilities to be updated periodically and as dictated by safe security policies.

- Behaviour Metrics, which quantify an entity's behaviour in observable scenarios. Typical observations relate to its responsiveness (in tie), quality of service delivered (such as reliability, robustness and similar, typical SLA properties), but also its typical connection quality performance – such as the average packages loss, number of retries required to deliver a package, the average end-to-end delays, package collisions and similar (see Table 4).

Table 3 Behaviour Metrics

Metric	Description
Forwarding of Messages	Denoting whether the devices forwards events and message to the expected destination.
Forwarding Delay	Reflecting whether devices promptly communicate events within the expected timeframe, or with unexpected delays.
Packet Loss	Number of packages the devices fail to receive from a source – when the source reliable dispatches them.

Sensor Readings	Often, a device's readings can be aligned and compared to those of its peers or neighbours. Deviations outside the expected accuracy can denote developing hardware or software errors or security-relevant events. In addition, consecutive sensor readings can be compared and reviewed in a similar manner.
Activity Duration	Denoting whether entities are following their expected sleep-aware cycles. More specifically, whether the activity window matches the sensor's specification – thus, reflecting whether a device is active when there are not any known stimuli, for example.
Forwarding Delta	For those devices which can forward the messages of their peers, whether the forwarded message differs from that of the original source unexpectedly.
Message Destination	Evaluation of the target of messages dispatched by the devices, and whether this is conforming to the expected network, data and control structures.

- Context Metrics, which reflect mostly the operations of a node given a specific known observable contextual event or timeframe. Typical examples include the correct prioritization of tasks or routing messages by active entities, and the reliable execution of a specific required action as dictated by the observable context (see **Fehler! Verweisquelle konnte nicht gefunden werden.**).

Table 4 Context Metrics

Metric	Description
Forwarding of Critical Messages	In many scenarios, devices can prioritize tasks based on safety, security and manufacturing requirements. The metric denotes whether sensors are forwarding such critical messages with the correct priority and priority flags
Prioritizing of Critical Messages	Denotes whether the internal processing and execution queues process critical messages correctly and within the expected timeframe or time constraints.
Selection of correct routes	For those devices which can coordinate and maintain routing routes, whether they correctly select the expected secure routing routes when dispatching messages, based on the typical known requirements – for example reliability, security, performance and similar.

As demonstrated by the selection of possible observable metrics, there is one more core distinction and assumption being made – namely, that the observer can correctly reference both observable aggregated events in order to compute statistics and trends for dynamic metric types, as well as to refer on-hand knowledge sources which expand the amount of available information considerable – typically these include

known vulnerability databases, technical documents with specifications of the deployed devices, and typical process-specific requirements and configurations for the active manufacturing process.

Mapping Metrics to Characteristics

Next, each of the characteristic previously introduced shell be individually computed by aggregating the quantifiable metrics from the four main categories. The metric types thus represent building blocks which, properly tracked, weighted and accumulated, can be computed into near real-time weighted trust values.

To better explain how the metrics provide support in evaluating Trustworthiness relevant characteristics – such as the five introduced in the previous section, we provide a brief example for the Security and Privacy characteristics. A comprehensive one is not provided due to brevity reasons in this paper but can be reviewed at.[17].

Security metrics are used to quantify the property of a system of being able to withstand unauthorized access and changes.

Device Metrics Affecting Security

Due to its role of capturing, processing and communicating data, devices play a core role in the security process and the infrastructure they are part of. Typical Security concerns, such as confidentiality, integrity and authorization or access are governed at device level and rely on its correct functioning (see Table 5).

Table 5 Device Metrics Affecting Security

Metric
Manufacturer
Firmware Version
Model Number
Exposure Level
Mobility

Connection Metrics Affecting Security

Connection specific aspects, such as certificates used for credential generation and access control, employed transmission and agreed encryption protocols prevent malicious agents from eavesdropping or

[17] SecureIoT, https://secureiot.eu/

tampering with transmitted information, as well typical integrity check mechanisms to identify malformed and damaged messages (see Table 6).

Table 6 Connection Metrics Affecting Security

Metric
Protocol (App Layer) Specific
Certificate Issuers

Behaviour Metrics Affecting Security

Behaviour-based metrics rely on historical and known technical and operational requirements to determine the level of correct, expected functionality in processing timely data, reporting and transmitted it to the correct logical or workflow-required peers (see Table 7).

Table 7 Behaviour Metrics Affecting Security

Metrics
Network Presence
Activity Duration
Forwarding Delta
Message Destination

Privacy-relevant metrics, at their core, quantity the ability of a system to support data owner and data subject in retaining control of how their information is being processed, shared and stored.

Device Metrics Affecting Privacy

Using a similar argument as for the Security characteristics, the Device itself has direct access to any observed data, being able to expose process or expose it to unauthorized actors either by intent, accident or through an attack due to its nature – not just of processing data, but also of being able to partially store it as well (see Table 8).

Table 8 Device Metrics Affecting Privacy

Metrics
Manufacturer
Firmware Version
Model Number
Exposure Level
Mobility

Connection Metrics Affecting Privacy

The Connection-based Metrics in the context of Privacy denote the transmission medium which allows for data consumption through eavesdropping. At this level, transmission-relevant aspects with an expected impact on Privacy are the certificates used during security relevant operations, and on the protocol used for data transmission (see Table 9).

Table 9 Connection Metrics Affecting Privacy

Metrics
Certificate Issuers
Protocol (App Layer) Specific
Update capabilities

Behaviour-based Metrics affecting Privacy

Devices capturing data can transmit it to unauthorized sources consumes. The message destination thus provides an insight on the received, and on how often potential private information is communicated (see Table 10).

Table 10 Behaviour Metrics Affecting Privacy

Merics
Message Destination

Application in Access Management

Edge Deployment of Trustworthiness Services

As part of the Horizon 2020 funded project SecureIoT (GA #779899),[17] two trustworthiness-driven prototypes were developed, with the focus of developing prototypical, integrated Trustworthiness services: (i) as a centralized, cloud-based component for a fictious manufacturing line, and (ii) as a machine-to-machine specific, edge-based component in a modern supply chain.

The scope of the edge-specific implementation was to review and define a distinct, autonomous Trustworthiness service which can work within the constraints of a machine-to-machine requirement, namely less visibility and contextual information available than a centralized system.

In the following, we will briefly describe the system's architecture and the information exchanges.

System overview

The function of the supply chain system is to accept injection moulded part orders and satisfy them as a collaboration between two or more separate machines, regardless of any external influence on installation security (see Figure 7). Each moulding injection process is governed by specific attributes, namely quantity, quality, a bill of materials, and required physical states – mostly temperature of heating and injection elements, pressured at the injection nozzle, and similar.

Each machine installation runs a traditional industrial moulding machine (IMM) as the production process, which is monitored by its own standard sensor equipment and whose readings are correlated also with an additional sensing unit covering physical vibration and electrical current. This set of sensor data readings is analysed locally using a specialized component, running an Edge deployed Anomaly Detection algorithm which can perform typical machine learning operations on sensor-data, such as trend prediction and anomaly detection and, more specially, whose output of which is used to influence the trust score of the system, having mainly a process-related Behaviour driven metric reporting role.

Another component of the factory installation is a customized probe, called a SecureIT probe, which has as security-focused role and serves to relay system state information to the trustworthiness assessment service(s) deployed within the SecureIoT platform. The published data comprises of network connection, hardware and other OS runtime data and thus reporting Connection and Device-specific metrics, mainly.

The Trustworthiness evaluation service and the Policy Decision Point service – a service which consumes Trustworthiness ratings and can adjust system wide policies accordingly. More specifically, the latter allows to define semantically complex rules and execute them based on given context information, in our case based on whether anomalies were detected on the edge and whether the trust metrics are within the agreed thresholds – reside either as an Edge or a local Cloud component, having access and management roles.

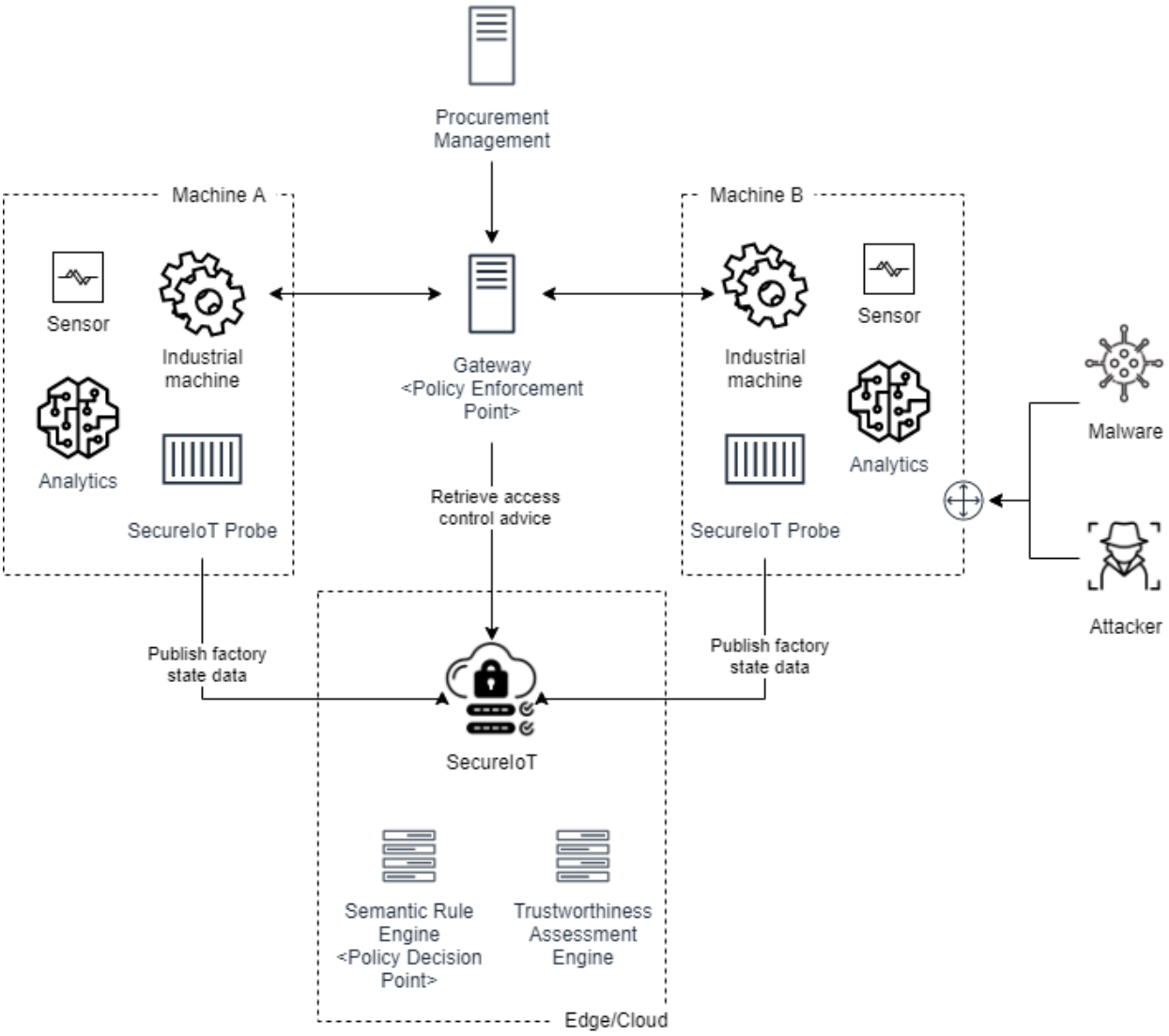


Figure 7: SecureIoT Trustworthiness Application Scenario

The attack scenario

The attack scenario used to demonstrate the viability of the specified integration is similar to the well-known Stuxnet[18] attack, as well as associated malware such as Duqu[19] and Conficker.[20] Stuxnet is one of the most publicized and specialized malicious computer worms, uncovered in 2010 that infected Microsoft Windows machines, remaining dormant and undetected for at least one year and seeking out specific political industrial targets, affecting their Supervisory Control and Data Acquisition (SCADA) and Programmable Logic Controller (PLC) systems. When connections to the required targets were established, the worm would malform the PLC output, destabilizing the machine by instructing it to exceed its safety limits, while reporting normal operation to the supervisory SCADA system. The specific of this kind of attack is that it is exceedingly difficult to detect using signature-based approaches, thus a concerted AI enabled approach is required.

In this defined scenario, thus, the attack would proceed in the following fashion: the attacker would infect one of the operator's machine with the malware. The operator would unwillingly infect the Machine B's SCADA reporting system that manages the IMM. The attack would normally remain undetected and all PLC sensors would report normal behaviour. There would be minimal communication of the malware to the external world since this would be easily detectable.

System response

At this point, the SecureIoT probe would report changes in the system state as a result of the intrusion, namely Behaviour inconsistencies triggered by (i) delays in the Machine's B expected delivery times, (ii) quality and quantity of processed material, as well as outputs, (iii) and finally external vibration and thermic sensors. The local analytics would also detect the changed running state of the production machine via the additional introduced vibrations and via different instantaneous power requirements. These two factors lead to a decrease in the Trustworthiness score for Machine B within the monitoring system. This fact would lead to disabling the connectivity of Machine B from both Machine A, its deregistration from the injection moulding queue system which initially was scheduling the customer relayed orders, as well as to notify operators of the decrease in overall Trustworthiness value or the threshold limit for a specific characteristic (such as Reliability).

An additional step that can be taken is to reschedule all work originally done by Machine B to other installations until the breach is circumvented. This idea fits well in the paradigm of self-managed smart factories.

---

[18] Symantec, "W32.Stuxnet Dossier", 2010, Symantec
[19] Symantec, "W32.Duqu The precursor to the next Stuxnet", 2011, Symantec
[20] Fitzgibbon, N.; Wood, M.: "Conficker.C – A Technical Analysis", Sophos Inc., 2009

At this point, the SecureIoT probe would report changes in the system state as a result of the intrusion, namely Behaviour inconsistencies triggered by (i) delays in the Machine's B expected delivery times, (ii) quality and quantity of processed material, as well as outputs, (iii) and finally external vibration and thermic sensors. The local analytics would also detect the changed running state of the production machine via the additional introduced vibrations and via different instantaneous power requirements. These two factors lead to a decrease in the Trustworthiness score for Machine B within the monitoring system. This fact would lead to disabling the connectivity of Machine B from both Machine A, its deregistration from the injection moulding queue system which initially was scheduling the customer relayed orders, as well as to notify operators of the decrease in overall Trustworthiness value or the threshold limit for a specific characteristic (such as Reliability).

Future Work

To overcome the barriers introducing a measurable Trustworthiness assessment, security standardisation shall play an important role. The development of generic sets or catalogues of characteristics shall allow comparison or mitigation of policies and Trustworthiness across different domains. Such an entity specific global trust ecosystem is still subject of research and standardization.

Such work should lead to catalogues of Trustworthiness metrics and schemas, which may extend common Information-Security Management-Systems facilitating a broad application of Trustworthiness in Industry 4.0 and beyond.

The approach described here relies on running anomaly detection and trust metric gathering on a potential exploited system, in order to circumvent this situation, all systems must be regarded as untrusted, monitoring code must be minimized on such systems and Trustworthiness computation must be done in a public place and be verifiable. Thus storing all data to a Distributed Ledger is sensible, as well as running all calculations in a manner that makes them transparent and verifiable to all partners.

The approach described can be extended in the future to include continuous evidence-based documentation of the production parameters. For example, the evaluation of trustworthiness during the production of a batch or even a single good can be documented in a secured distributed ledger alongside other product characteristics as proof of product quality.

Conclusions

To strengthen resilience in dynamic supply chains, a better trust model facilitating policy management is imperative.

A pragmatic model for automatic and measurable Trustworthiness is presented and the modelling as well as exemplary metrics and attributes for its evaluation are explained.

Based on an application in the Horizon 2020 project SecureIoT, it is presented how this model and the described metrics can be used to manage trustworthy access to resources in an industrial environment.

In further work, the development of generic metrics, the integration into an industrial ISMS and the application to distributed manufacturing are of particular importance.

Acknowledgement

This work has been carried out in the scope of the H2020 SecureIoT project[21], which is funded by the European Commission in the scope of its H2020 programme (contract number 779899).

Within SecureIoT, the dynamic evaluation of automatable trust models of industrial components was investigated with the goal of obtaining models in the area of Multi-Vendor-Industry (MVI) by calculating the trustworthiness of cross-enterprise integration and operation models and supply chains.

The authors Jürgen Neises, George Moldovan, Thomas Walloschke, Cosmin Grigoras and Bianca Popovici acknowledge valuable help and contributions from all partners of the project.

[21] SecureIoT, https://secureiot.eu/

Factory Belt:
Secure and Trusted Industry 4.0 Architectures

Authors:

Amjad Ullah (University of Westminster)

Hai-Van Dang (University of Westminster)

Antonis Michalas (University of Westminster / Tampere University)

Tamas Kiss (University of Westminster)

Christian Gehrmann (Lund University)

Abstract

Even though Industry 4.0 has been an agenda item in several public bodies for many years, the reality is that most industries have not been taking a strategic approach towards their further digital transformation. The low pace of Industry 4.0 adoption among enterprises (especially SMEs) is characterized as a common problem for the overall industrial development throughout Europe. While there is a number of reasons why companies do not adopt Industry 4.0 (e.g. investment, workforce, etc.), security is considered as one of the biggest obstacles. Considering the multifaceted nature of industrial environments and the fact that the attack surface area is increasing exponentially, we propose a forward-looking design of a layered-based architecture that can be used as a starting point for building secure and privacy-preserving smart factories. Our architecture departs from the traditional cryptographic and security mechanisms by incorporating modern and promising techniques for lightweight end-to-end secure communication as well as mechanisms for establishing trust relationships between two or more entities (attestation) and throughout the entire supply chain. The proposed architecture is based on the work defined in the CloudiFacturing and DIGITbrain H2020 projects.

Introduction

Information and Communication Technology (ICT) is essential for Industry4.0 and for the digitalization of the manufacturing sector. However, less than 25% of manufacturing companies in Europe profit from ICT-enabled solutions currently. In order to boost the competitiveness of European manufacturers (especially Small and Medium-sized Enterprises – SMEs), innovative solutions need to consider both technological and commercial scalability from the very early stages of the design process throughout the full implementation and utilisation of the solution. From this perspective, cloudification of services has become the ideal enabler in manufacturing digitalization.

CloudiFacturing (CFG) is an EU funded Innovation Action project[1] that brings and progresses advanced ICT in the field of Cloud-based modelling and simulation, data analytics for online factory data, and real-time support to European manufacturing SMEs, contributing to their competitiveness and resource efficiency via optimizing production processes and producibility. CloudiFacturing has developed a generic, workflow-oriented platform (Figure 1) that enables secure deployment and execution of workflow-based applications in cloud and high-performance computing (HPC) resources. These applications are deployed in a central workflow repository (EMGREPO) that accommodates for various heterogeneous workflow/application types

[1] CloudiFacturing Project, (accessed January 12, 2021). [Online]. Available: https://www.cloudifacturing.eu/

(e.g. Flowbster,[2] SemWES,[3] CloudBroker[4]). Additionally, a central data transfer and browsing component (EMGDATA) facilitates data sharing between the various workflow engines at execution time. Workflows and applications are executed via the workflow and application mediator (EMGWAM) component that enables the execution of pre-prepared workflows as black boxes and also facilitates their combination into higher level meta-workflow pipelines, In order to facilitate commercial utilization, the CloudiFacturing Platform provides a central billing system (EMGBC), and advanced security solutions for single sign-on and user authentication/authorization via the user management module (EMGUM), mutual authentication between platform components via the Public Key Infrastructure (PKI), and also secure storage for external resource credentials via the secret management module (EMGSMM). On top of the CloudiFacturing platform, the project also developed a Digital Marketplace (the emGORA – Engineering and Manufacturing Agora) for manufacturing companies, independent software vendors, and consultancy and training providers. The marketplace provides seamless access to the underlying services of the platform, enabling the publication, execution, billing and management of workflow-based applications for the manufacturing sector. Additionally, the marketplace also serves as a generic community hub where a wide range of activities, for example domain specific information exchange, value added services or training courses and material can be found.

CloudiFacturing demonstrated the technical and economic feasibility of its platform and marketplace by implementing 21 cross-national application experiments involving manufacturing companies, independent software vendors, technology consultants, digital innovation hubs and cloud/HPC resource providers. Typical application areas, among others, include improving quality control and maintenance at manufacturing SMEs using big data analytics and digital twins, optimizing efficiency of truck components manufacturing processes via discrete event simulation, numerical modelling and simulation of heat-treating processes in the aluminium industry, or optimizing design and production of electric drives.

As the development of the CloudiFacturing Platform and Marketplace is approaching completion, the results of the project are currently being commercialised and also further developed in a follow-up Innovation Action

[2] Peter Kacsuk, Jozsef Kovács, Zoltan Farkas: The Flowbster Cloud-Oriented Workflow System to Process Large Scientific Data Sets. J Grid Computing 16, 55–83 (2018). https://doi.org/10.1007/s10723-017-9420-4

[3] SemWES Platform: A Semantic Workflow Execution System, (accessed January 12, 2021). [Online]. Available: https://github.com/SemWES/

[4] Simon JE Taylor, Tamas Kiss, Anastasia Anagnostou, Gabor Terstyanszky, Peter Kacsuk, Joris Costes, Nicola Fantini: The CloudSME Simulation Platform and its Applications: A Generic Multi-cloud Platform for Developing and Executing Commercial Cloud-based Simulations, in Future Generation Computer Systems, Volume 88, November 2018, pp 524-539, https://doi.org/10.1016/j.future.2018.06.006

project, titled DIGITbrain.[5] The DIGITbrain project aims to extend the traditional digital twin concept towards the Digital Product Brain that steers the behaviour and performance of an industrial product (mechatronic system or manufacturing machine) by coalescing its physical and digital dimensions and by memorising the occurred (physical and digital) events throughout its entire lifecycle. The outcome of the project is the DIGITbrain Solution that incorporates a platform and an associated Digital Marketplace that manufacturing and technology companies and Digital Innovation Hubs (DIHs) can utilise to implement the smart business model of Manufacturing as a Service (MaaS). DIGITbrain utilizes the CloudiFacturing solution as starting point and extends and further develops it to fulfil its objectives.

The rest of this paper will focus on the security challenges and solutions that arise when implementing and operating the CloudiFacturing and DIGITbrain solutions. While CloudiFacturing applied a more conservative and traditional security approach, DIGITbrain will extend this significantly to realize the Industry 4.0 vision. Section 2 of this paper describes the security architecture of CloudiFacturing, while Section 3 explains the vision of DIGITbrain when extending the CloudiFacturing security solution. Finally, Section 4 concludes the paper also highlighting future work.

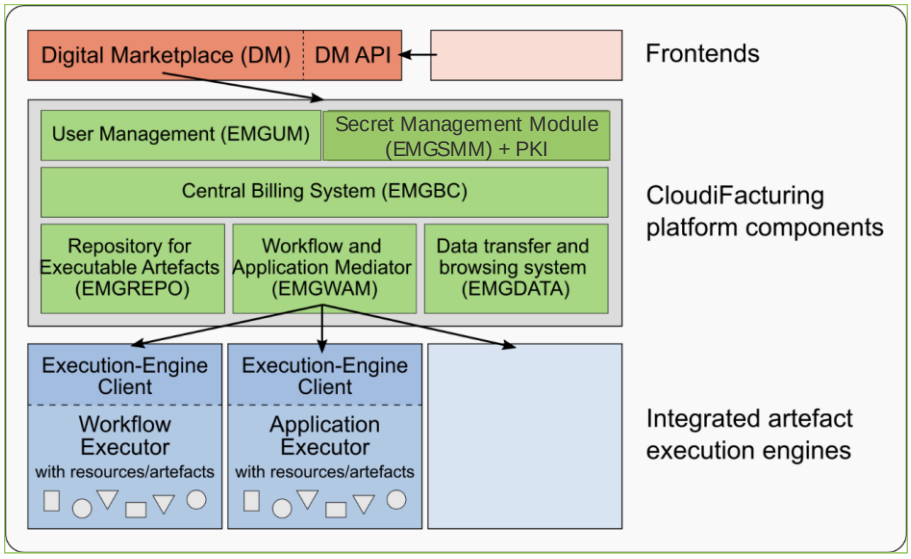


Figure 1: High-level architecture of the CloudiFacturing Solution

[5] Simon JE Taylor, Tamas Kiss, Anastasia Anagnostou, Gabor Terstyanszky, Peter Kacsuk, Joris Costes, Nicola Fantini: The CloudSME Simulation Platform and its Applications: A Generic Multi-cloud Platform for Developing and Executing Commercial Cloud-based Simulations, in Future Generation Com-puter Systems, Volume 88, November 2018, pp 524-539, https://doi.org/10.1016/j.future.2018.06.006

CloudiFacturing: A Traditional Security Architecture

The CloudiFacturing solution follows the architecture, where each component is implemented as a service that communicates with other services using REST APIs. Such a design brings a great deal of advantages such as individual level scalability, independence, higher level of flexibility and easy maintenance.[6] However, such isolation among the components means exposing wider attack interface area. In light of such an architecture, the security of individual components, their execution environments and the interaction amongst each other is up most importance.

In addition to these aspects, within the scope of CloudiFacturing project, the security requirements of the solution were formally gathered from each application experiment partner. The analysis of the gathered requirements indicates the following needs from the security point of view: (1) confidentiality and integrity of manufacturing process and simulation data, (2) single sign-on access to all services of CFG solution, (3) authenticated and secure connections between the manufacturing process or simulation data owner and the cloud provider, (4) authenticated and authorised access to services and processing of data, (5) secure transfer of input and production data to/from end-user to compute and storage resources, and lastly (6) secure storage and handling of external resources' credentials.

In light of the above-mentioned security requirements, the aim of the CloudiFacturing security architecture (Figure 2) is to achieve the following traditional security objectives: user authentication and authorisation, data confidentiality and integrity, and secure communication between the solution components. There are different approaches to realise these objectives. However, it is not straightforward, especially in a distributed framework.[7] There exist some challenges, such as (1) where to place the security mechanisms; (2) how to maintain an active session between the frontend (Digital Marketplace in this case) – where the user gets authenticated – and the rest of passive CFG components; (3) how to maintain a valid session to continue and/or provide data support for the execution (this is required as the execution of a workflow-based application may require longer time than the active session of a user); (4) how to authenticate components to

[6] Yarygina, Tetiana, and Anya Helene Bagge. "Overcoming security challenges in microservice architectures." 2018 IEEE Symposium on Service-Oriented System Engineering (SOSE). IEEE, 2018

[7] Loukidis-Andreou, F., Giannakopoulos, I., Doka, K., & Koziris, N. (2018, July). Docker-sec: a fully auto-mated container security enhancement mechanism. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (pp. 1561-1564). IEEE.

avoid unauthorised access and component impersonation; and (5) how to fulfil the needs to handle the secure storage of credentials to external resources.

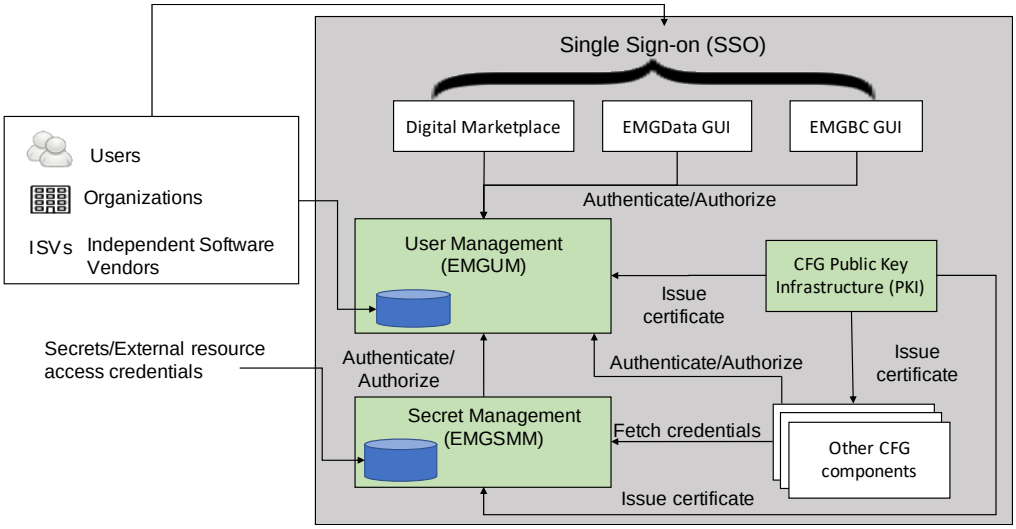


Figure 2: High-level centralised security architecture of CloudiFacturing solution

Figure 2 illustrates the high-level architecture of the CloudiFacturing solution from a security viewpoint. The depiction below highlights the key security components and their high-level interactions amongst each other, and with the rest of the CFG architecture. It can be seen from Figure 2 that the security challenges and requirements in CFG are handled through three key components, namely CFG PKI, EMGUM and EMGSMM. A brief description of each of these components and their key purposes are as follows:

- EMGUM – EMGUM is the central security component that is responsible for authentication, authorization and security policy management of the entire CloudiFacturing solution. EMGUM handles access control policies and issues access tokens to other CFG components. More specifically, it provides the following key functionalities to the CFG solution: (1) a single point for end user management by facilitating the central storage and management of users, credentials, roles and organisations, (2) a centralised authentication and access control mechanism that enables single sign-on and token-based authentication to the platform, (3) a platform level authentication mechanism to facilitate secure and authenticated inter-component interactions, and (4) a centralised authorisation mechanism for the facilitation of individual components of CFG to define and manage authorisation policies and decisions. The afore-mentioned functionalities of EMGUM are provided through the OpenID Connect (OIDC) standard[8] protocol and its implementation is based on a popular open source identity and access management

[8] OpenID Foundation, (accessed January 13, 2021). [Online]. Available: http://openid.net/specs/openid-connect-core-1_0.html

solution called Keycloak.[9] In the context of the OIDC standard, EMGUM is the OIDC Server and the rest of the CFG components, except the CFG PKI server, are the OIDC clients. All CFG components register with EMGUM as OIDC clients. Once registered, EMGUM is then responsible for handling the related authentication and authorisation decisions.

- CFG PKI – As discussed earlier, it is important that the components' interactions with each other remain secure. For this purpose, the public key infrastructure (PKI) based approach - that allows secure mutual authentication between certified components – is adopted to achieve secure inter-component interactions. The CFG PKI component issues internal certificates to all other components including the security components, i.e. EMGUM and EMGSMM. Once the certificates are obtained, the components can use their respective certificates to set up a secure and mutually authenticated TLS/SSL connection to issue API calls to other CFG components. The PKI is an important tool to make sure that only authorized components can interact with each other and that platform internal impersonation is prevented.
- EMGSMM – EMGSMM allows secure storage and retrieval of end-user credentials for platform external resources. The secret management module is needed in order to allow CloudiFacturing users to share credentials for external resources. For instance, this can be the case when executing workflows on the platform or there is a need for CFG components, such as EMGDATA to access external resources like storage and similar services. These external resources typically require the requesting party to present valid credentials, before access to the resource is allowed. Credentials of external resources are sensitive and should be handled with care. Therefore, from a security perspective, it is not a good design to share credentials with other functions within the system. Hence, the CFG solution includes a fully separated security hardened module (EMGSMM) to handle this task. The EMGSMM module is responsible for the long-term protection of credentials, being the main interface for the registration of credentials and also the module that grants or denies access to external resource credentials requests from other modules. The implementation of EMGSMM consists of a Redis database, where credentials are stored in a key-value pair. The confidentiality of the credential storage is achieved using the python crypto library. Lastly, it runs in a Dockerised environment, with an additional layer of Docker-specific security achieved by implementing Docker-sec[10] that generates a suitable AppArmor Docker configuration for the EMGSMM service.

The above-mentioned three security-specific components fulfil the security goals discussed at the beginning of this section (i.e. where the focus is mainly on the security of CloudiFacturing platform itself). However,

[9] Keycloak, (accessed January 13, 2021). [Online]. Available: https://www.keycloak.org/

[10] Loukidis-Andreou, F., Giannakopoulos, I., Doka, K., & Koziris, N. (2018, July). Docker-sec: a fully automated container security enhancement mechanism. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (pp. 1561-1564). IEEE.

this security architecture does not guarantee trust throughout the entire supply chain, which is one of the main aims in the DIGITbrain project. In addition to that the security of the communication between different entities is done by using only standard/traditional techniques – an approach that may not be suitable for constraint devices like the ones often used in smart factories (can affect the efficiency of a process). In the next section we will elaborate on how the DIGITbrain project will focus on solving those trust, security and efficiency issues.

DIGITbrain: Security Challenges of a Looking-Forward Architecture

The complexity of the technology underlying cloud computing and the Internet of Things introduces novel security risks and challenges.[11] While threats and mitigation techniques for these two fields have been under intensive scrutiny in recent years, there is only a little work done in the direction of modern infrastructures protecting facilities based on the use of both paradigms. This section presents the basic security-related concepts that will be utilized in DIGITbrain's architecture.

Secure Communication

Building networks that are heavily based on IoT devices, such as those found in smart factories, is not an easy task. As with any technology associated with data collection and transmission, there are many security and privacy threats that need to be considered during the deployment of such a network. Design and development of secure and privacy-preserving protocols for such environments is a topic that attracts extensive attention from both the academia and the industry.

Asymmetric key cryptography has become the standard for key exchange and mutual authentication when working on the Internet and is considered as a viable option for IoT devices. However, due to the resource constraints of these devices, it is often challenging to implement core public key cryptographic functions as these functions are computationally expensive. Currently, the majority of key management implementations on IoT devices are based on pre-shared symmetric keys. The security keys are pre-installed on the devices before deployment. However, this solution is not scalable for deployments that involve tens of millions of devices. For example, pre-installing 10,000 128-bit AES keys on a device requires certain memory resources and also poses significant lookup latency. Due to the vastly resource-constrained nature of the devices used in IoT, implementing secure and privacy-preserving services, using, for example, standard asymmetric cryptographic algorithms, has been a real challenge. The majority of IoT devices on the market

[11] Antonis Michalas and Ryan Murray. “Keep Pies Away from Kids: A Raspberry Pi Attacking Tool”. Proceedings of the 1st ACM CCS International Workshop on Internet of Things Security and Privacy (IoT S&P’17) in Conjunction with ACM CCS 2017, Dallas, USA, October 30 – November 03, 2017.

currently employ the use of various forms of symmetric cryptography such as key pre-distribution. Such implementations' overall efficiency correlates directly to the size of the IoT environment and the deployment method.

In DIGITbrain, we will implement a lightweight cryptographic library to secure communication protocols between multiple communicating nodes *without the need for external trusted entities or a server.* To do so, we will focus on analysing and further extending the current functionality of popular IoT operating systems such as Contiki-NG Operating System (OS).[12]

Remote Attestation and Trusted Supply Chain

In many industrial scenarios, most of the IoT devices are located in places where a large number of people can easily get physical access to the device. Hence, in case secret information (e.g. pre-shared symmetric keys) has already been stored on the device during the configuration phase, it makes it easy for adversaries to access this information and eventually compromise the entire network.

Another limitation with implementing traditional security solutions in such networks is with the decentralized ad-hoc nature of these environments. In a decentralized ad-hoc network setup, the individual nodes do not have fixed positions before deployment and do not possess neighbouring nodes' knowledge. By carefully considering and evaluating these special conditions, it is evident that *the practice of protecting these devices at the gateway or network boundaries is no longer an effective solution***.** Ensuring the end-to-end secure communication between two components and protecting private/sensitive data *is important, but it is insufficient on its own.* A well-rounded solution must also *provide guarantees about the trustworthiness and the integrity of the involved edge devices* incorporated in the underlying ecosystem and play a crucial role in the proper function of the underlying environment.

Verification of a device's trustworthiness is a problem that has been extensively studied during the last few years and is an area under intense scrutiny. However, most of the approaches target cloud-based environments and rely on the use of special hardware modules such as TPM and more recently isolated execution environments such as Intel SGX.[13] However, it remains a considerable, important, open and difficult-to-solve problem for constraint devices, especially those used in a smart factory. Hence, one of the core

[12] Eugene Frimpong and Antonis Michalas. “IoT-CryptoDiet: Implementing a Lightweight Cryptographic Library based on ECDH and ECDSA for the Development of Secure and PrivacyPreserving Protocols in Contiki-NG”. In Proceedings of the 5th International Conference on IoT, BigData and Security (IoTBDS’20). Prague, Czech Republic, May 7-9, 2020.
[13] Antonis Michalas. “The Lord of the Shares: Combining Attribute-Based Encryption and Searchable Encryption for Flexible Data Sharing”. In Proceedings of the 34th ACM/SIGAPP Symposium On Applied Computing (SAC’19). Limassol, Cyprus, April 08 – 12, 2019.

technologies to be enabled by DIGITbrain is local and remote attestation on constrained devices. Having identified the importance of building trust relations as well as recognizing this as a challenging open research problem, DIGITbrain will investigate approaches for device-agnostic software-based attestation mechanisms that will increase the trustworthiness of the entire network and the underlying services.

While remote attestation offers some great functionality that allows a user to verify the integrity of both the hardware and software of a device, most of the current approaches require the use of special secure hardware. This can be an obstacle when considering resource-constrained devices because, in many cases, these devices cannot have such a hardware component. Having this in mind the problem of verifying the integrity and therefore, the trustworthiness of an IoT device throughout the entire supply chain can be impossible. As a result, current supply chain practices start with trusting the source.

In DIGITbrain we plan to design and implement a protocol that will allow end-users and any third party to verify the trustworthiness of an IoT/edge device throughout its entire lifecycle. Our solution will not require any special secure hardware and will focus on managing the confidentiality, integrity, and access to platform data. By incorporating such a solution, DIGITbrain has the potential to enhance the interoperability of smart factories by allowing them to use devices of multiple vendors and software versions. Finally, such a mechanism will allow users to verify the integrity of the IoT devices that will be used in a smart factory – a process that will contribute to protecting the overall integrity of the infrastructure along with the underlying services.[14]

Conclusion

In this paper, we focused on the work that has been done in two large European projects looking on problems related to modern factories and industry 4.0. More precisely, our primary focal point was to highlight security, privacy and trust challenges that need to be considered and addressed to have a smooth and reliable transformation from traditional factories to smart factories. To this end, we presented the security architecture of the H2020 CloudiFacturing project, which, while it contains several security mechanisms, is still considered as a traditional approach. Then we moved on to the description of the DIGITbrain architecture - a more modern, promising but at the same time demanding architecture. We hope that this work will give several companies valuable insights and help them take a more strategic approach towards their further digital transformation. Finally, we believe this work can be an essential reference point for protecting smart factories and other similarly complicated environments.

[14] Nicolae Paladi, Christian Gehrmann and Antonis Michalas. “Providing End-User Security Guarantees in Public Infrastructure Clouds”. IEEE Transactions on Cloud Computing, a special issue on “Cloud Security Engineering”, IEEE, 2016.

Secure Asset Administration Shell exchange with Distributed Ledger Technology

Authors:

Andre Bröring, andre.broering@th-owl.de, Institut für industrielle Informationstechnik – inIT, Technische Hochschule Ostwestfalen-Lippe, Campusallee 6, 32657 Lemgo

Alexander Belyaev, alexander.belyaev@ovgu.de, Institut für Automatisierungstechnik, Otto-von-Guericke-Universität Magdeburg, Universitätsplatz 2, 39106 Magdeburg

Henning Trsek, henning.trsek@th-owl.de, Institut für industrielle Informationstechnik – inIT, Technische Hochschule Ostwestfalen-Lippe, Campusallee 6, 32657 Lemgo

Lukasz Wisniewski, lukasz.wisniewski@th-owl.de, Institut für industrielle Informationstechnik – inIT, Technische Hochschule Ostwestfalen-Lippe, Campusallee 6, 32657 Lemgo

Christian Diedrich, christian.diedrich@ifak.eu, ifak - Institut für Automation und Kommunikation e.V., Werner-Heisenberg-Straße 1, 39106 Magdeburg

Abstract

Advancing digitalization, increasing networking and horizontal integration in logistics, production and operation of machines and products are leading to the transformation of classic value chains into interconnected value networks in which partners can seamlessly find and exchange relevant information. Machines, products, and processes receive their digital twins, which represent all relevant aspects of the physical world in the information world. The Asset Administration Shell (AAS) is a standardized industrial interpretation of a digital twin proposed by the Plattform Industrie 4.0 and the Industrial Digital Twin Association. All life cycle data about an asset, means a physical or logical thing that holds a value for the owning organization, is stored in this digital twin. For a secure and trustworthy exchange of data contained in AASs among the cross-company value- and supply chain, Distributed Ledger Technology (DLT) as a common backbone containing data transactions between value network partners will be proposed in this work. In this context, DLT is considered as a trusted layer, i.e. a technology for implementing a trustworthy, decentralized communication infrastructure. From the authors' point of view, DLT provides the necessary characteristics to become a standard technology and basis for shaping open globally secure Industrie 4.0 ecosystems.

The paper provides an overview about the current state of research for the exchange of the content of AASs and an overview about the requirements for a common infrastructure to archive a wide adoption in the manufacturing industry and global supply chains and how those requirements can be fulfilled by the unique features provided by DLT.

Introduction

One of the key factors in Industrie 4.0 (I4.0) is the availability of trustworthy data and information about industrial machines, components, and products at all times over an asset's life cycle. Assets represent physical or logical *things* that hold a value for the owning organization. The Asset Administration Shell (AAS), as an industrial interpretation of a digital twin, is the data center for industrial assets. To exploit the full potential of data throughout the asset's life cycle, the linked AAS stores all relevant information about the asset and provides different APIs for the data access and communication to other assets and IT systems. The contained information can be e.g. construction data of a machine, process data from sensors, or a description of executed process steps.[1] Some of these information are crucial for the subsequent life cycle and require a high integrity and confidentiality to avoid fraud and manipulations on the asset. With a

[1] Plattform Industrie 4.0, “Structure of the Administration Shell: Continuation of the Development of the Reference Model for the Industrie 4.0 Component,” Working Paper, Berlin, Apr. 2016.

standardized and secure data exchange between different organizations, data can be made available for all value chain instances.[2]

Background and challenges

The following section describes fundamentals about the AAS, introduces the concepts and technologies for the exchange of the AAS's content that are currently discussed in the I4.0 community, and derives some challenges which, to the best of the authors' knowledge, have not yet been addressed in the relevant literature and discussions.

Asset Administration Shell – Fundamentals

The "Details of the Asset Administration Shell" document series[3][4] describes the basic concepts of the AAS as follows:

An asset together with its AAS forms an Industrie 4.0 component. If an asset type, described in an AAS type, is produced several times, several AAS instances with individual information for each asset instance are created. It is important to note that each asset instance can be operated by different partners in different phases of the life cycle. Accordingly, each asset instance can be represented by multiple operator specific AAS instances. In such a user- or operator-specific AAS, different organizations in the value chain can store different information, such as confidential engineering data held back by the manufacturer or confidential production data held back by the producer.

The information in an AAS is separated in several submodels. This allows different parties in the value chain to access or add submodels with data during the asset's life cycle. An AAS instance can be stored on the embedded storage of a corresponding asset or in an external repository and may support different communication capabilities. The AAS can be exchanged as a file (passive AAS), provide an API for information exchange (re-active AAS), or autonomously interact and communicate with other AASs (pro-active AAS)[5] as shown in Figure 1.

---

[2] P. Frey et al., "Blockchain for forming technology – tamper-proof exchange of production data," OP Conference Series: Materials Science and Engineering, Vol. 651, No. 1, 2019.
[3] Plattform Industrie 4.0, "Details of the Asset Administration Shell: Part 1 - The exchange of information between partners in the value chain of Industrie 4.0 (Version 3.0RC01)," Specification, Berlin, Nov. 2020.
[4] Plattform Industrie 4.0, "Details of the Asset Administration Shell: Part 2 - Interoperability at Runtime – Exchanging Information via Application Programming Interfaces (Version 1.0RC01)," Specification, Berlin, Nov. 2020.
[5] Plattform Industrie 4.0 and Industrial Internet Consortium, "Digital Twin and Asset Administration Shell Concepts and Application in the Industrial Internet and Industrie 4.0," 2020.

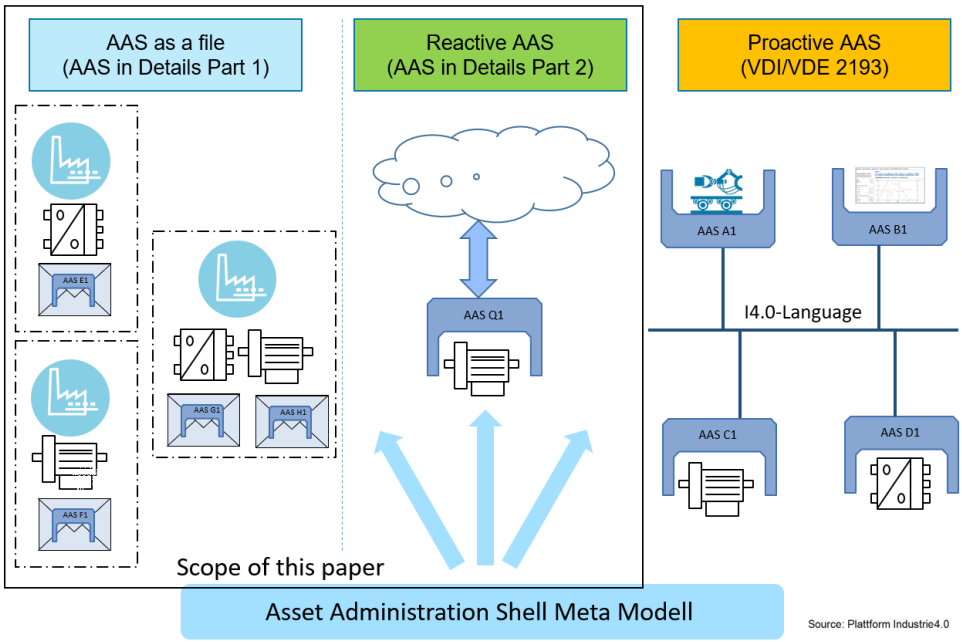


Figure 1: Forms of AASs[6]

The passive file-based AAS provides a standardized description structure of information associated with an asset in a form of XML, JSON or AASX files, as described in the refenced publication.[7] The re-active AAS basically provides the same information as the file based AAS through standardized interfaces using internet protocols. In a client-server relationship, such AAS acts as server and rather as an information provider for higher-level software systems. The pro-active AAS, which is out of scope of this paper, forms an intelligent autonomous service unit together with the asset.

Data exchange with passive AAS on file basis

A detailed description for an interoperable exchange of engineering data with AASs on a file basis is described in a discussion paper of the Plattform Industrie 4.0.[8] The described service is designed to be scalable to transfer big files like 3D models or software for simulations between asset supplier and asset integrator.

[6] Plattform Industrie 4.0, “Verwaltungsschale in der konkreten Praxis: Wie definiere ich Teilmodelle, beispielhafte Teilmodelle und Interaktion zwischen Verwaltungsschalen (Version 1.0),” Diskussionspapier, Berlin, Apr. 2019.
[7] Plattform Industrie 4.0 and Industrial Internet Consortium, “Digital Twin and Asset Administration Shell Concepts and Application in the Industrial Internet and Industrie 4.0,” 2020.
[8] Plattform Industrie 4.0, “Sicherer Downloadservice,” Diskussionspapier, Oct. 2020.

The Reference[9] proposes a combination of a git-based version control, a distributed file system to store the AASs on a file basis, and a blockchain to record the creation time and identity of the editor of each AAS version. The paper shows the life cycle of an asset and the parallel exchange of the respective AASs between developer, vendor, producer, and customer. In a git-based version control system, the data can be accessed by pulling the respective files from the distributed file system, and changed by commits and pull requests.[9]

Data exchange with re-active AAS via IP-based interfaces

Currently, the I4.0 community favors a CRUD-oriented (Create, Read, Update, Delete) approach for designing interactions with re-active AASs. Depending on the use case, OPC UA, HTTP/REST, or MQTT are suggested as communication technologies. From the authors' point of view, it is important to emphasize that the selection of the above-mentioned technologies is based on applications and use cases that imply a connection of the AAS to a higher-level software system or to a centralized platform that acts as an intermediary between the AAS and its multiple users.

However, through the advancing digitization, the classic value chains are turning more and more into interconnected value networks in which partners can seamlessly interact directly with each other and exchange information. Due to this fact, new digital ecosystems are emerging. The vision 2030 of the Platform Industrie 4.0[10] defines the general conditions and requirements for such future I4.0 ecosystems, these are: openness, decentralization, support of diversity and heterogeneity on the market and highlights the absence of central components with monopolistic position and superior rights.

As illustrated in Figure 2, the communication technologies mentioned above, like OPC UA and HTTP, are designed to enable client-server interactions. The direct interactions with the AAS in such envisioned flexible networks with ad-hoc emerging relationships and interactions based on these technologies can be associated with a large effort and an overhead of coordination and communication.[11] Furthermore, in a network based on OPC UA, HTTP or MQTT, centralized entities are required, which would take over the role of common registry or discovery as well as identity management.

---

[9] M. Redeker, S. Volgmann, F. Pethig, and J. Kalhoff, “Towards Data Sovereignty of Asset Admin-istration Shells across Value Added Chains,” in 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA): IEEE, 2020.

[10] Plattform Industrie 4.0, “2030 Vision for Industrie 4.0: Shaping Digital Ecosystems Globally,” Berlin, Oct. 2019.

[11] C. Diedrich, T. Werner, and S. Höme, “Abbildung von Industrie-4.0-Verwaltungsschalen-Kommunikation auf OPC UA,” Automation Kongress, Baden-Baden, Jul. 2019.

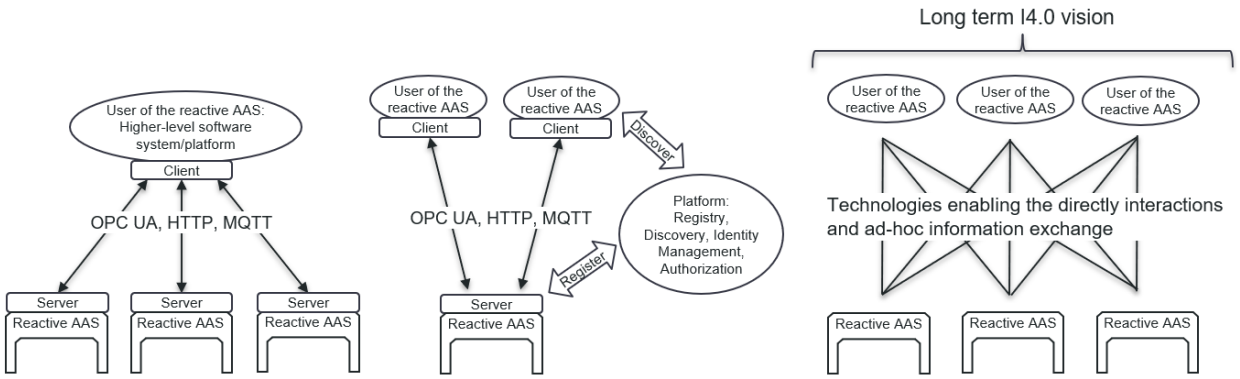


Figure 2: Possible communication technologies and their usage in different use-cases of the re-active AASs

The approach based on communication technologies such as OPC UA, HTTP, and MQTT is a first valid step towards the short-term realization of Industrie 4.0 applications, but from the authors' point of view it does not fully correspond to the long-term vision 2030 of the Plattform Industrie 4.0.[10] The applications should be extended by highly decentralized solutions for future cross-company digital ecosystems without components that can assume a central monopolistic position and whose unavailability would impair the secure operation of the overall system.

Challenges

During the life cycle, assets are processed and managed by different organizations in the value chain. Challenges are the infrastructure that stores and administrates the AASs and makes these available to other organizations in the value chain, and the creation of a digital twin as the single source of truth containing all relevant information from the physical world without conflicting information or the loss of information. Different asset owners and users should be able to access the information stored in the AAS or, depending on the life cycle phase, submit new asset describing information to the AAS.[12]

Challenge 1

The connection from the information systems and processes of the respective companies to the information stored remotely in the AASs should be as seamless and automated as possible. In practice, this means that today's centralized IT systems of companies hosting the AAS instances should enable ad-hoc connections to the systems of other companies and enable them to access and to edit the respective AAS. However, today's best practices in network segmentation are very restrictive in terms of allowing traffic from the

[12] S. Heißmeyer and J. Kalhoff, “Digitaler Zwilling komplett und sicher ausgehängt,” IT & Production, 7+8, 2020.

Enterprise IT to the production networks and vice versa. Furthermore, the exchange of information with external companies is also not desired, because it is always a potential vulnerability.[13]

Challenge 2

As it has already been noted above, it is possible that several digital representations of one and the same asset exist and may be operated at the same time, e.g., by the manufacturer, owner, and current operator of an asset.

In this context, some questions arise:

- How to ensure a consistent digital representation of assets through multiple AASs under the mentioned conditions?
- How can it be ensured that all relevant characteristics of the physical world are transformed into the corresponding information in the digital world and made available by each AAS?
- How can it be ensured that the AAS always provides the description of relevant aspects of an asset across the life cycle without loss of relevant information?

One of the possible approaches would be a central cross-company repository that provides the AAS API or operates a reference AAS instance for each asset instance. This would ensure the availability and actuality of AAS instances for all life cycle stages. However, a centralized approach carries certain risks that may not be acceptable for industrial companies. On the one hand, a central repository represents a single point of failure. The breakdown or misuse can affect the functionality of the whole I4.0 system. On the other hand, the operator of such a repository assumes a monopolistic position versus the users of AASs, who become partially dependent on the repository operator.

Analysis of Distributed Ledger Technology

To allow industrial enterprises and potential value chain partners to collaborate and exchange information directly in a secure and trustworthy way, a layer of trust is needed in a common infrastructure. The technology that makes this possible should meet security requirements like availability, integrity and confidentiality to be accepted in industries.[14][15]

[13] M. Ehrlich, H. Trsek, L. Wisniewski, and J. Jasperneite, “Survey of Security Standards for an auto-mated Industrie 4.0 compatible Manufacturing,” in IECON 2019: 45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal, 2019.
[14] Plattform Industrie 4.0, “Sicherer Bezug von CAE-Daten,” Diskussionspapier, Berlin, Nov. 2018.
[15] T. M. Fernandez-Carames and P. Fraga-Lamas, “A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories,” IEEE Access, vol. 7, pp. 45201–45218, 2019.

Distributed Ledger Technology - Fundamentals

With Distributed Ledger Technology (DLT) it is possible to create an open decentralized data base of performed transactions between different organizations. Behind DLT is the idea of a distributed system in which the participating parties are on an equal level and can interact directly with each other. Each network node holds the identical data base. The algorithms of the nodes ensure that newly added transactions are distributed throughout the entire network. The consensus mechanism ensures that the nodes agree on the current state of the data base.

To add a new data transaction, a node must validate previous transactions by a cryptographic function. Once a transaction is validated, it is not possible to alter this without also manipulate all validating transactions, which are also stored on the other nodes of the distributed ledger. Therefore, no central organization needs to be involved to guarantee the immutability of the transactions. Accordingly, DLT can provide an immutable transfer of the data between different organizations.[16]

Blockchain, as a more popular term, is a subcategory of DLTs. An often-mentioned challenge for blockchains is the scalability due to waiting time for validation of transactions. Also, the energy consumption due to the necessary computing power for the validation of new transactions can be high for a blockchain like Bitcoin. For creating blocks and storing transactions, a fee is often charged in public blockchains, which requires the purchase and handling of a Cryptocurrency.[17]

Some newer DLTs, like the IOTA Tangle[18] as an implementation of a Directed Acyclic Graph (DAG), aim to overcome the cost and scalability limitations of blockchains. The Tangle has not a single chain like a blockchain and thus can add several transactions parallel, which raises the number of possible transactions in a defined time. Instead of several miners trying to validate each block, in the IOTA network every node has to validate two previous transactions to add a new transaction to the ledger. Thus, there is no extra fee for the validation of new transactions required.[18][19]

Another challenge is the increasing demand on memory for the DLT because of the several synchronized local copies of the ledger. Nevertheless, the scalability, performance and memory consumption highly depends on the chosen DLT.[17]

---

[16] T. Locher, S. Obermeier, and Y. A. Pignolet, “When can a Distributed Ledger replace a Trusted Third Party?,” in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, Canada, 2018, pp. 1069–1077.
[17] W. Yang, S. Garg, A. Raza, D. Herbert, and B. Kang, “Blockchain: Trends and Future,” in Pacific Rim Knowledge Acquisition Workshop, 2018, pp. 201–210.
[18] S. Popov, “The Tangle,” Version 1.4.3, Apr. 2018.
[19] A. Belyaev, C. Diedrich, H. Köther, and A. Dogan, “Dezentraler IOTA-basierter Industrie-Marktplatz,” Industrie 4.0 Management, vol. 2020, no. 2, pp. 36–40, 2020.

Security Analysis of DLT

Availability, integrity and confidentially are the core objectives of information security. Additional objectives for industries are authenticity and non-reputability.[20] The following chapter analyzes whether DLT can achieve these objectives.

Availability

One of the most important objectives for manufacturing industries is to avoid down times of the production and guarantee a high availability. The availability of distributed ledger nodes is a crucial advantage of DLT, because the decentralized network replaces single server architectures that present a single point of failure. With the network of nodes storing the distributed data set, the probability that a node is available to receive or provide data increases with every node in the network. Also, in case of local data loss, there is always an identical copy of the distributed ledger on the other nodes in the network.[21]

Integrity

For data that is once added to the distributed ledger, a high effort for manipulations is necessary, as there are local copies of the ledger on the other network nodes, that would have to be changed as well. Additionally, each transaction is referring to previous transactions by adding a checksum of these to the current transaction. If one transaction is manipulated, all referring transactions also need to be edited, as the hash values would change.

A weak point for manipulations is the transition from real world values to the value in the distributed ledger. If already manipulated data is added to the distributed ledger, this cannot be detected by the DLT.[16]

Confidentiality and Authenticity

In contrast to the high availability and integrity, industrial organizations can see the distributed storage as a disadvantage in the view of confidentiality. The data can be protected through encryption before adding it to the distributed ledger.[22] [20]. However, for the encrypted data, there is the threat of deciphering. As a result, the companies do not have the control about the local copies on all the other nodes. To minimize the threat of deciphering, strong and quantum-proof encryption algorithms as well as a secure key management should be used.

---

[20] Plattform Industrie 4.0, “Sicherer Bezug von CAE-Daten,” Diskussionspapier, Berlin, Nov. 2018.
[21] P. Fraga-Lamas and T. M. Fernandez-Carames, “A Review on Blockchain Technologies for an Ad-vanced and Cyber-Resilient Automotive Industry,” IEEE Access, vol. 7, pp. 17578–17598, 2019.
[22] DIN SPEC 3103:2019-06: Blockchain und Distributed Ledger Technologien in Anwendungsszenarien für Industrie 4.0, DIN e. V., Berlin, Jun. 2019.

To guarantee the authenticity of the sender of a transaction, a signature of the sender can be added to each transaction. Therefore secure identities are needed.[23]

Solution proposal for a secure exchange of AAS content using DLT

The idea is to distinguish between two different categories of asset information contained in the AAS. The first category is the information that may be relevant to external partners in the value network and should be shared e.g. to comply with certain regulatory progresses. The second category is information that is relevant only to the user specific AAS instance and does not need to be shared with the other partners in the value network.

The concept is to store the information that needs to be shared with other partners as transactions in the distributed data set of the DLT network. Thus, a common set of submodels to be shared for a specific asset instance can be created. The AAS instances related to this asset can partially or completely duplicate or at least reference the information of this common set of submodels (Figure 3).

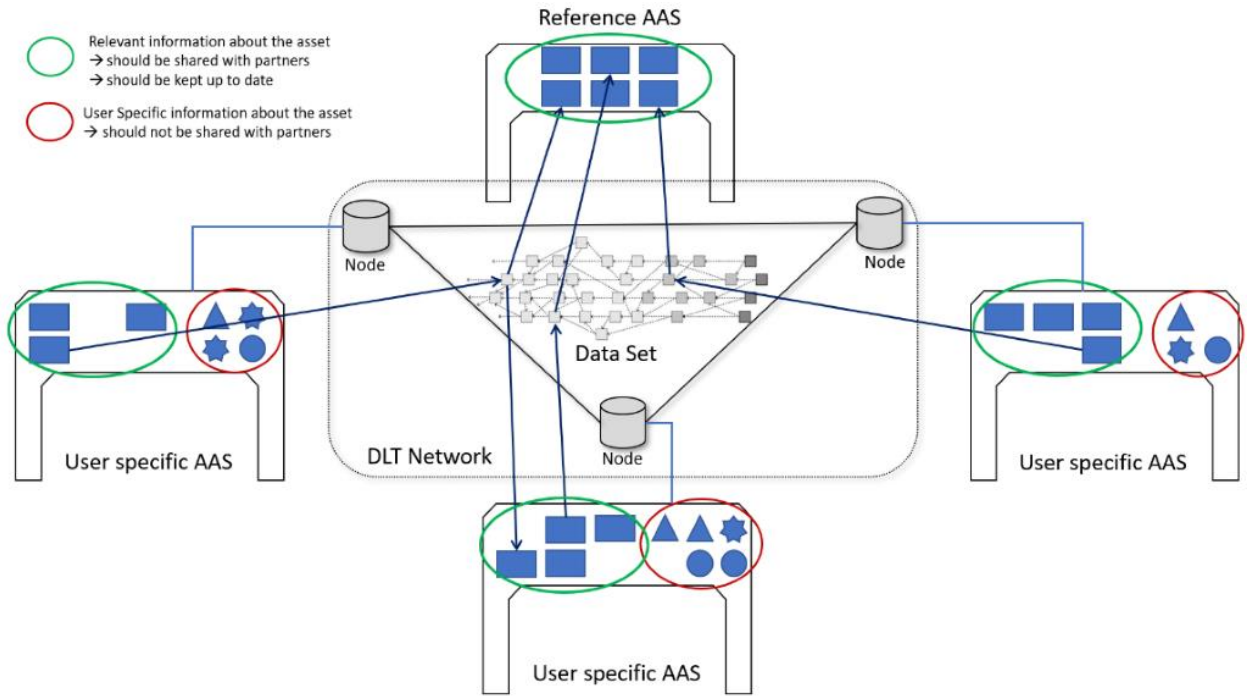


Figure 3: DLT as a backbone for the AAS

[23] Plattform Industrie 4.0, "IIoT Value Chain Security – The Role of Trustworthiness: International Paper," Apr. 2020.

The benefits in consideration of the above-mentioned challenges can be illustrated by the examples given below. If the partners are supposed to read or supplement information within the specific AAS instance, they do not have to connect to the IT system of a company operating this AAS to read or write this information. Consequently, they have no direct interaction with specific AAS instances and interact, i.e. read or write the information, only within the distributed data set stored on the nodes of the DLT network. Thus, the DLT network acts as a common backbone and as a layer of trust between interaction partners.

Any organization involved in the value network of an asset can transmit submodels with information to the distributed ledger and use this channel to add submodels to AASs and to make submodels available for other partners in the value network. This is leading to a new possibility to record all asset's life cycle steps especially during the instance phase. Single transactions in the distributed ledger are used to exchange single submodels containing small amounts of data in an asynchronous manner without establishing direct connections to AASs stored in remote repositories.

The core advantage is that the sender of the submodels do not have to handle the AAS instances in their own file systems. This makes it possible to use e.g. embedded IoT devices to transmit individual submodels with life cycle data about countless asset instances to the countless AAS instances without handling local copies of all these AASs. In addition, no direct connection via HTTP/REST or MQTT between the sender (e.g. supplier) and the repository on a remote file system (e.g. of the customer) containing the AAS instances is needed. The submodel transfer in the distributed ledger offers high integrity, the network for the transmission offers a high availability to process the data transfer, and the open source infrastructure is open for everyone and independent of any third party corresponding to the Open Source Software Strategy 2020 – 2023 of the European Commission[24] and the vision 2030 of the Plattform Industrie 4.0.[25]

Use case scenario: Tracking of product data

In a considered scenario, a company wants several instances of an asset type, like a standard power supply without communication capabilities, to be produced and keep track of all production steps. The producer can store the AAS type with all general information for the production in his file system. For each produced unit, an AAS instance is created to store individual information like fluctuating process data for each specific unit.

Now, further processes on the asset and the transportation of the asset need to be executed by other involved companies. All these companies can store the one AAS type locally in their file system, access this

[24] European Commission, Open-source software strategy 2020-2023. [Online]. Available: https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en (accessed: Dec. 21 2020).
[25] Plattform Industrie 4.0, “2030 Vision for Industrie 4.0: Shaping Digital Ecosystems Globally,” Berlin, Oct. 2019.

via the API, or use the download services proposed in the referenced papers.[26][27] In contrast, the countless AAS instances are stored in a remote repository to avoid lots of copies of all these instances.

Submodel transfer using the distributed ledger

For the submodel transfer via the distributed ledger, every AAS instance has an identity, for example an address, to receive data transactions in the distributed ledger. This identity can be stored in different ways, such as on RFID chip, NFC chip or printed as a QR-Code on the product itself.[28] By scanning the chip or code, every organization in the supply chain can send data to the AAS instance by sending a submodel to the identity in the distributed ledger (Figure 3).

Public submodels can be stored in the distributed ledger without encryption and are available for all actors in the value network.[28] To provide confidentiality for not public submodels, the submodel transactions can be encrypted with a public key, that can be also stored on the RFID chip, NFC chip or QR-Code. A signature can be added to each transaction to authenticate the sender.

Submodel access within the distributed ledger

At any point in time, the reference AAS instance and the user specific AASs can access the submodel in the distributed ledger and copy it (Figure 3). Before a submodel is copied from the distributed ledger to an AAS, the receiver can check the signature to verify the sender and, if needed, decrypted it with the private key which can be securely stored in the AAS in the repository. Also, the following partner in the value chain can access submodels from the distributed ledger.

The copies of the submodels in the repositories can be extended with a reference to the transaction in the distributed ledger, so that auditing organizations can validate the information in the AAS by checking the tamper-proof reference in the distributed ledger as a common shared data set. This information can be used for example for a proof-of-origin in complex global supply chains.

One of the ways to implement the proposed concept is to use the so-called second layer technologies to manage the data contained in the DLT data set and to manage the access to them, such as IOTA Streams.[29] In this second layer technology, related transactions in the distributed data set refer to each other creating a stream of transactions related to a common topic (Figure 4).

---

[26] Plattform Industrie 4.0, “Sicherer Downloadservice,” Diskussionspapier, Oct. 2020.
[27] M. Redeker, S. Volgmann, F. Pethig, and J. Kalhoff, “Towards Data Sovereignty of Asset Administra-tion Shells across Value Added Chains,” in 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA): IEEE, 2020.
[28] Abeyratne, A., Saveen and R. P. Monfared, “Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger,” International Journal of Research in Engineering and Technology, vol. 5, no. 9, pp. 1–10, 2016.
[29] IOTA Foundation, IOTA Streams. [Online]. Available: https://www.iota.org/solutions/streams (accessed: Dec. 21 2020).

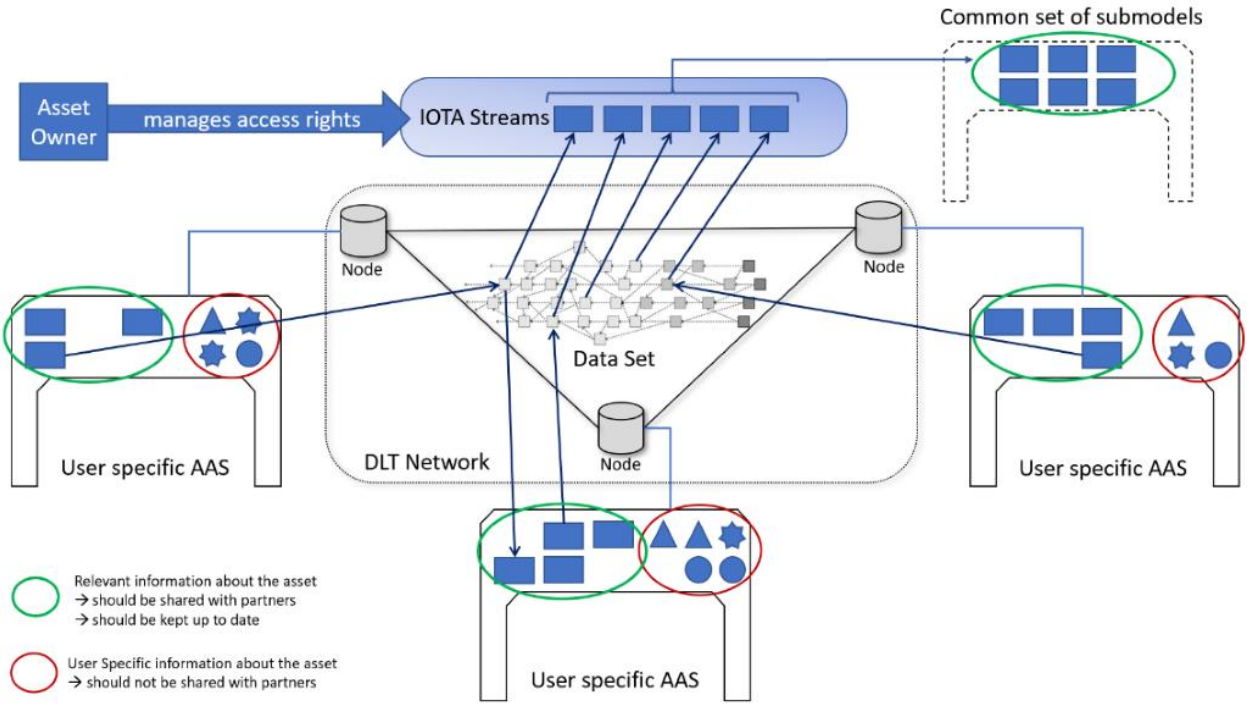


Figure 4: IOTA Streams[29] as a framework for implementing the stream of transactions related to a common topic

Evaluation

Besides the advantages in using the standardized AAS as a digital twin and storing submodel in a distributed ledger to provide a high integrity and availability, the proposed solution enables the target AAS instance to use the DLT as a buffer and accesses the submodel in an asynchronous manner at any point in time without the threat of manipulation in the meantime. The data supplier does not need any write access into the IT systems of companies hosting the AAS instances and the submodel receiver can do a security check for each submodel before adding it to the AAS. This enables a cross-company information exchange without the companies having to interact directly with each other and overcomes the challenge of the originally needed direct access to the IT systems of other companies.

Without establishing a direct connection to the AAS in the repository, the data supplier can always add submodels by sending these from embedded IoT devices to one of the nodes in the decentralized network running the distributed ledger. The other way around, other companies in the life cycle can always access the newest submodels from the distributed ledger even if the server with the AAS instances is not available and prevent production stops due to not available AAS instance data.

With this central, but decentralized exchange solution, data about production steps, directly coming from the supplier and other organizations processing the asset, can be tracked trustworthy. The tamper-proof storage in the distributed ledger provides an opportunity for more transparency in the future value networks. This data with the timestamps of the transactions can be used as a proof-of-existence and a proof-of-origin for each asset instance, as every life cycle step can be immutable recorded. This can help to minimize product counterfeiting, support the quality control, and retrace each part of a product. Customs and other logistics-related organizations can add and access data to and from the highly available distributed ledger. Thus, this technology can also be used for freight documentation in global supply chains.

Since a customer already can store the AAS instances on his server even before the products arrive in his organization, he can access all individual information about each product instance directly in his own file system. In any point in time, he can check the distributed ledger for new transactions containing submodels and thus monitor the production-, quality- and logistic-status of each asset. This might meet the challenge of the continuous and consequent representation of the asset in each of its multiple AASs across the owner, operator, and live cycle stages.

Conclusions

The proposed idea shows a new solution to improve the data exchange across different organizations in the value network of future Industrie 4.0 ecosystems. The DLT as a decentralized open-source data exchange platform enables every actor in the value network to send transactions with data about the asset's life cycle as submodels to the AAS instance. The exchanged submodels are buffered and stored tamper-proof in a distributed ledger and can be added to the AAS instances with a reference to the transaction in the distributed ledger to guarantee the integrity and to keep the AAS as the asset data centre and single source of truth for all asset information gathered in a complex value network.

However, the limited amount of data per transaction needs to be considered. At the same time, a solution to manage the high amount of data that is stored by all participating nodes in the network needs to be developed. Regarding the security goals of the stakeholders, especially audit-relevant data and data that requires a high integrity, like quality-, security-, and safety-relevant data, can be sent to the AAS by using the DLT. Consequently, not the whole life cycle data needs to be stored in the distributed ledger to limit the memory demands of the ledger.

With the distributed ledger, there is no dependency on third parties as central instances to trust for storing the data, and the companies with the AASs do not have to unblock their IT systems for many connections with write access for other partners. All organizations only send and receive transactions to and from the distributed ledger. All involved actors like supplier, customer, audit organizations, and product certification authorities share the same state and can trust the same database.

Sharing of Asset Administration Shells with the International Data Spaces

Author:

Friedrich Volz, friedrich.volz@iosb.fraunhofer.de, Researcher of Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, Karlsruhe (IOSB)

Abstract

Data exchange between industry partners is a challenging task, especially when critical production data from factories is involved. While the partner wants as much information as possible, the factory owner is hesitant and shares only minimal amount of data with his partners. After data sharing, control over the data is lost, making data sharing a question of trust. The IDSA strives to create a global secure network in which data owners can choose how their data is used and dis-tributed. The key concept in this architecture is the International Data Spaces (IDS) Connector, which provides access to the IDS and provides this functionality.

The Asset Administration Shell (AAS) is a new core concept in Industry 4.0 and is a further standardization attempt that includes many established protocols like OPC UA and several serialization formats.

Our contribution aims to connect different standards and organizations like the International Data Spaces Association (IDSA) and Plattform Industrie 4.0 (PI 4.0) in order to share AASs via the IDS. For this, a software service is generated based on AAS descriptions and deployed in an IDS Connector.

Introduction

Projects like the International Data Spaces (IDS) and GAIA-X[1] aim to provide innovative data networks and infrastructure for sharing data across the globe. The key advantages include "Data governance" and "Data security".[2] Security is improved by using standardized software architecture like the "Security Gateway" (DIN SPEC 27070)[3] and by certifications of the network governor for the implementations of the infrastructure. "Data governance" per definition of the IDSA enables data owners to decide how their data is used even when data was shared in the data network. The term "Data sovereignty" is also used synonymously in the IDSA context to describe "a natural person's or corporate entity's capability of being entirely self-determined with regard to its data".[2]

The Plattform Industrie 4.0 (PI 4.0) is meanwhile standardizing the data exchange between industry partners in form of Asset Administration Shells (AAS).[4] The AAS structures data with yet another meta-model while using the well-known and established communication protocols HTTPS, MQTT or OPC UA. The vision is to enable machines to understand and interact with each other without manual programming effort (smart machines). In order to achieve interoperability between machines, proprietary information models and communication protocols of hardware manufacturers are replaced or encapsulated by standards. Manual effort of machine and manufacturing configuration can also be reduced by those means.

Our work focused on bringing the AAS standard into our factory application scenario and sharing this AAS data with potential business partners over the IDS. Our demo scenarios are based on machines with OPC UA servers, which is a common set-up in today's production facilities.

We have extended the IDS Trusted Connector[5] for application in factories and secure sharing of AAS data including data governance. The PI 4.0 is working jointly with the IDSA on bringing "Usage Policies", descriptions of who can access the AAS data and their usage conditions, into the specification of the AAS. For technical enforcement of Usage policies, we have applied MYDATA Control in the Trusted Connector.[6]

---

[1] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

[2] B. Otto, S. Steinbuß, A. Teuscher, S. Lohmann, and et al. (2020) IDS ReferenceArchitectureModel3.0. [Online]. Available: https://www.internationaldataspaces.org/publications/reference-architecture-model-3-0/

[3] D. I. für Normung (DIN). (2020) DIN SPEC 27070: Requirements and reference architecture of a security gateway for the exchange of industry data and services.[Online]. Available: https://www.beuth.de/de/technische-regel/din-spec-27070/319111044

[4] Plattform Industrie4.0. (2020) Details of the Asset Administration Shell Part1 – The exchange of information between partners in the value chain of Industrie 4.0 (Version2.0.1).[Online].Available: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/Details-of-the-Asset-Administration-Shell-Part1.html

[5] Fraunhofer AISEC. (2020) Trusted Connector. [Online].Available: https://industrial-data-space.github.io/trusted-connector-documentation/docs/overview/

[6] Fraunhofer IESE. (2020) MYDATA Control Technologies. [Online]. Available: https://www.mydata-control.de/

Additionally, we have developed several software components for handling AAS in factories and integration with the IDS Connector. The components include the AAS Service Generator, AAS Services, AAS Registry and AAS Manager, which functions are described in the architecture section.

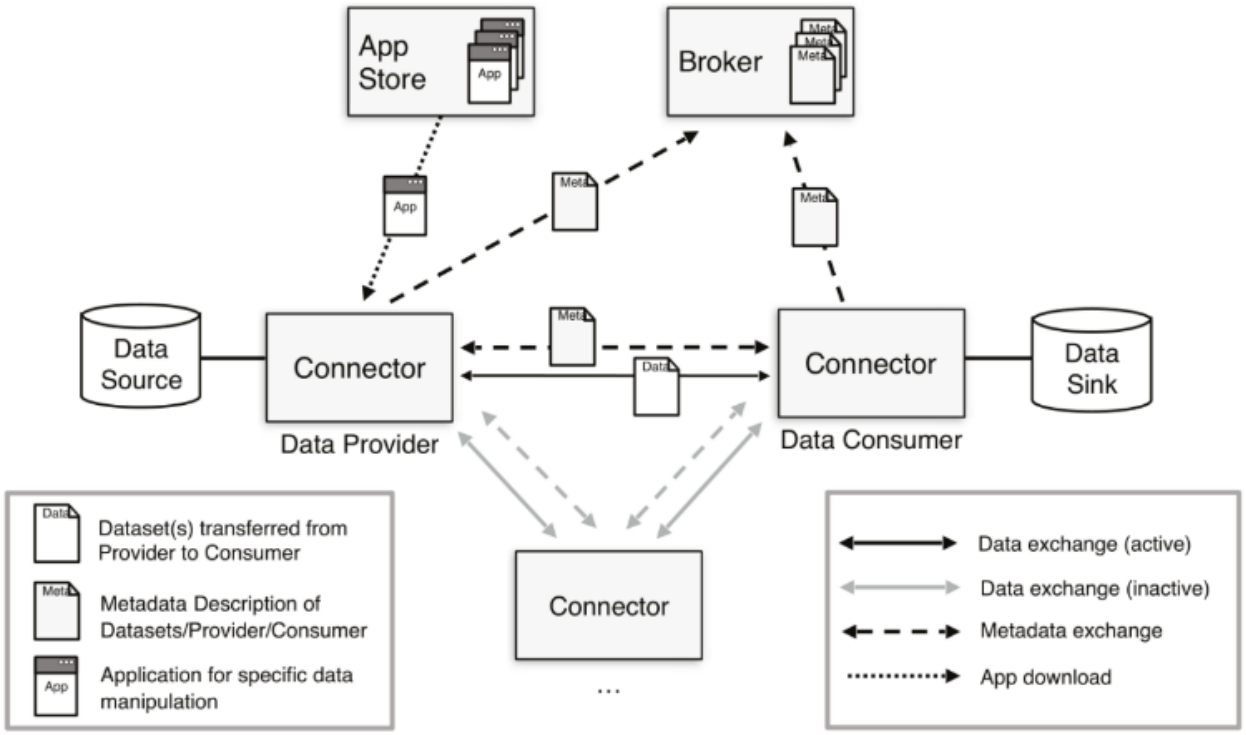
Concepts

International Data Spaces

The International Data Space (IDS) promises "data sovereignty", the ability of a data provider to determine who receives data, how it may be processed, and what purposes or conditions it should be bound to.[2] The IDS is a decentralized communication network in which data is protected by usage policies. Gateways (IDS connectors) are being developed to control, log and, if necessary, block the transmission of data. The connectors can register in the IDS Broker to advertise their capabilities and data. The key concepts are shown in Figure below.

The application scenarios are broad and to ensure realization in different industry branches, IDS Communities are created to focus on specific use-cases. One such community is the IDS-I Industrial Community which aims to connect the IDS to Industry 4.0 and vice versa.[7] There are two reference use cases namely collaborative condition monitoring (reference) and the Smart Factory Web (reference). Our work focuses on the use-case of exchanging data between a factory owner with sorting machines and his customers and has been demonstrated in the context of the Smart Factory Web.

[7] InternationalDataSpacesAssociation. (2020) IDS-IIndustrialCommunity. [Online]. Available: https://www.internationaldataspaces.org/ids-i-community-kick-off/



Architecture of the IDS

For the technical enforcement of usage conditions, usage control frameworks are in development. Based on the evaluation of the existing usage control frameworks and based on the requirements of the use cases we would like to support, we have decided to use MYDATA Control[6] in the IDS Trusted Connector. The Trusted Connector is a reference connector implementation in the IDS that focuses on security and trust.[5]

Asset Administration Shell

The Asset Administration Shell was specified by the Plattform Industrie 4.0 to promote standardized and interoperable data exchange in the factory. For this, a set of defined representations and protocols are used with a uniform information model.[4]

The AAS is a central component in the RAMI 4.0 (Reference Architecture Model)[8] of the Plattform Industrie 4.0. With the AAS, all kinds of devices and assets are described and modeled over the complete life cycle

[8] PlattformIndustrie4.0. (2020) ReferenceArchitectureModelIndustry4.0. [Online]. Available: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/rami40-an-introduction.pdf

of the assets. It tries to simplify the numerous APIs found in today's industry to a manageable subset and specifies interfaces for interoperable exchanges. An I4.0 system consists of several I4.0 components, which in turn consist of assets. These I4.0 components can interact with each other. The AAS models submodels, parameters, status, abilities and services of these assets.

According to different AAS documents,[4] there are three distinct types of Asset Administration Shells:

1. passive: content of AAS is static
    a) passive in file format, aasx.
    b) passive with IP/API-based access
2. dynamic with server interface: interface provides dynamic data
3. active: AAS is a client and interacts with other AAS

AASs can be serialized in different formats like AutomationML, AASX or JSON. These formats describe passive files with static content, but they can refer to live-data by a reference. For example, the AutomationML description of a machine could point to specific nodes in OPC UA servers. We can therefore describe that the temperature value of a machine can be found in a certain OPC UA server.

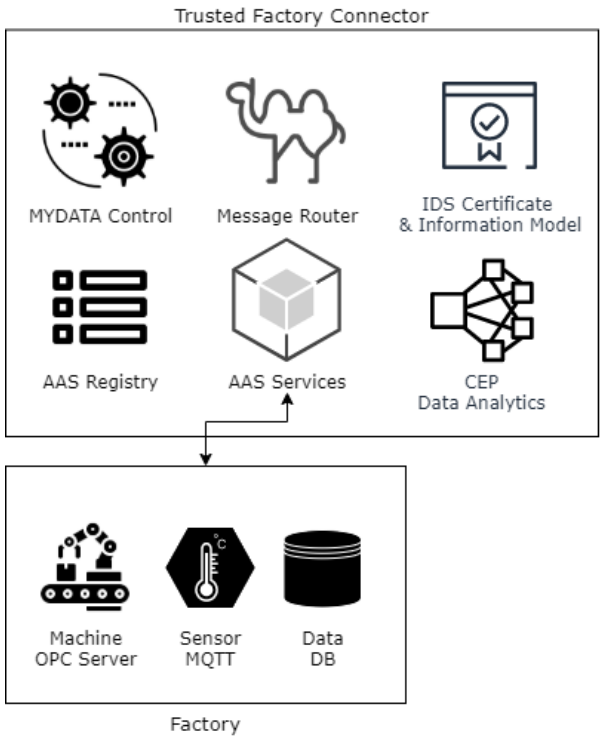
Use-Cases and Solution

Our goal is to access data described in an AAS and share this data with an IDS Connector. For this, we first tried to convert the OPC UA servers found in our factory to an AAS format. The I4AAS working group by ZVEI, VDMA and OPC UA Foundation is working on an OPC UA Companion Specification to describe AAS in OPC UA.[9] This Companion Specification includes an easy-to-follow guideline to structure the OPC UA server with AAS terminology. However, this involves some effort and knowledge about OPC UA modeling and I4AAS. We tried to minimize these requirements by only needing to model an AAS in an AASX, AutomationML or JSON file. The modeling of such files can be done with software tools like the AASX Package Explorer[10] for which tutorials in form of screencasts exist.[11]

Our solution therefore consists of the generation of a software component, the "AAS Service", that provides an AAS interface and connects to several data sources. The generation is done with a graphical interface

[9] OPC Foundation. (2020) I4AAS – Industrie 4.0AssetAdministrationShell. [Online]. Available: https://opcfoundation.org/markets-collaboration/i4aas/
[10] Github AASX Package Explorer [Online]. Available: https://github.com/admin-shell-io/aasx-package-explorer
[11] Home of Asset Administration Shell (AAS) [Online]. Available: http://www.admin-shell-io.com/

in the software tool “AAS Service Generator”. The asset connections could include proprietary protocols and so-called I4.0 languages. I4.0 languages provide additional vocabulary and interaction protocols so that machines can understand each other.[12]



Connecting to the factory with AAS & IDS

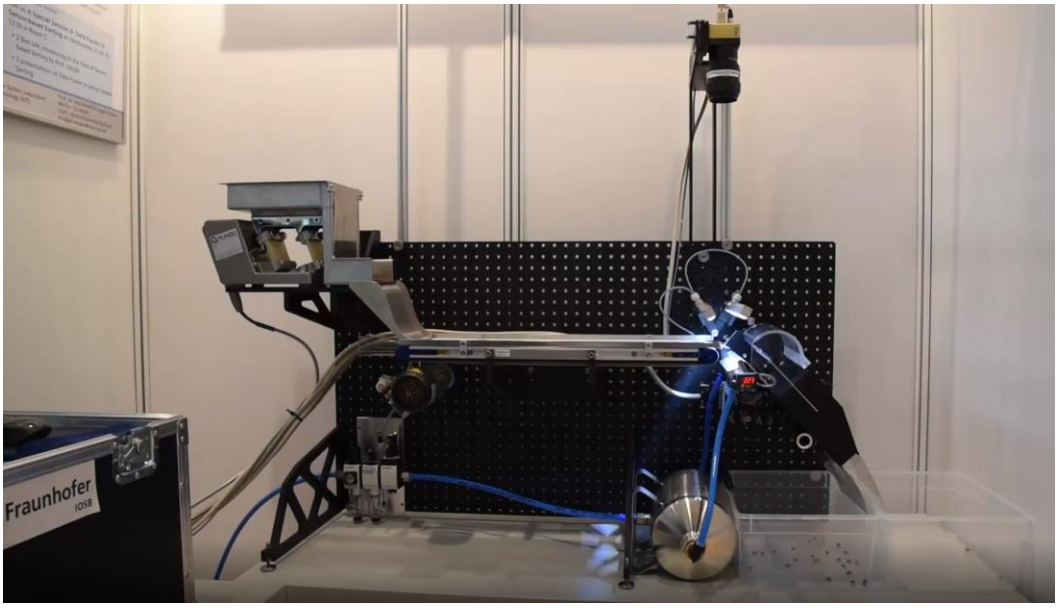
IDS Connectors like the Trusted Connector include the functionality of hosting any application as long as it can be wrapped in a container (e.g. Docker).[4] The above figure shows an implementation of our Connector, which includes message routing and an app for data analytics. Our idea is therefore the generation of AAS services from AAS files or AAS servers and hosting or sharing this service via the IDS. The additional benefit of the IDS is that shared AAS data can be monitored by data usage control, meaning the factory owner can maintain control and usage of data after access to the data was granted to partners.[6] Data Usage Policies could for example restrict which applications can use the AAS data or when data has to be deleted. A prerequisite for the functioning of Usage Control is that data stays in the data network (connectors or

[12] PlattformIndustrie4.0. (2018) I4.0Language. [Online].Available: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/hm-2018-sprache.html

applications). If the data can leave the network within an application without the IDS knowing, the restrictions on the data usage can no longer be guaranteed. This is why the successful application of the IDS for factories means, that every factory or business partner needs to adapt usage control to retrieve AAS data from the factory.

The AAS service is also highly useful for Industry 4.0 use-cases within the factory, which is why this service should also be deployable without the IDS Connector. For example, other machines in the factory could access a machine by the standardized interface in the AAS service of the machine. The connector is however important for data sharing between business partners in the data network. The integration with the IDS connector is necessary to protect the AAS with Usage policies. If Usage Control is needed for AAS data, it is necessary to establish a connection between the IDS and AAS Service in some form. We treat the AAS as a whole unit, so policies grant access and usage of the whole AAS. A working group from the PI 4.0 is working on fine-granular access control specifications for the AAS, so that only a part of the AAS can be shared. In future, the specification could include usage control, which basically is an extension of access control.

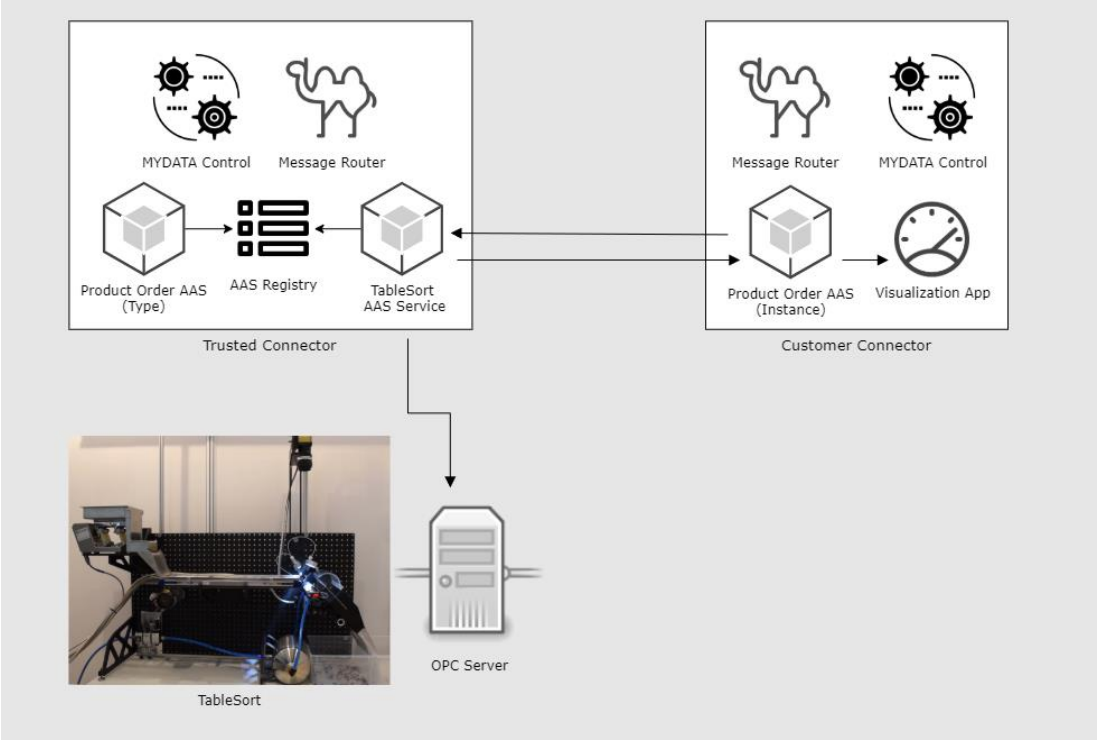
We evaluate our solution based on a demo factory called TableSort.[13] TableSort is a small sorting machine, that can sort different materials according to specific parameters.



TableSort machine

[13] Fraunhofer IOSB – TableSort [Online]. Available: https://www.iosb.fraunhofer.de/de/projekte-produkte/tablesort.html

In our use-case, customers can order sorted coffee-beans according to color, size from different origin countries. The factory owner is also sharing data with service providers, for example valve producers, which are necessary for the sorting machine. The service providers monitor the critical production data to recognize broken valves or conduct predictive maintenance. Customers are interested in the progress and quality aspects of the sorting, which is why they receive performance indicators. One example would be the amount of beans sorted out, so he can adapt his order parameters, because sorting out many beans would lead to a higher price. All this data should be protected with usage control, so the factory owner can restrict the usage. Our policies for example include restrictions on the customer, so that the data can only be visualized in certain visualization dashboard and that this data cannot be shared further.



TableSort Use-Case with IDS Connectors

Furthermore, we provide an AAS for the product orders. The type of this shell is provided by the factory owner connector and the instance of the shell is run inside of the customer connector. The visualization app is also part of the customer connector and connects to the product order AAS instance. This ensures that a policy can restrict data usage to the visualization app.

Architecture

In this chapter we take a look on the AAS services and their surrounding software tools including the IDS Trusted Connector, which we extended to realize our use-case.

The aim is to develop a framework for handling AAS data transfers with IDS infrastructure. The implementation is work in progress and will be available open-source under the name “FAST for Digital Twins (Fraunhofer AAS Tools)”.

To enable the AAS functionality for our existing OPC UA Servers, we need an additional software component: the AAS Service Generator. Instead of converting all our OPC UA servers with I4AAS, we provide an AAS with a software service, which connects to the OPC server. This can minimize the effort to transform existing factories to an industry 4.0 environment (Brownfield).

AAS Generator & AAS Service

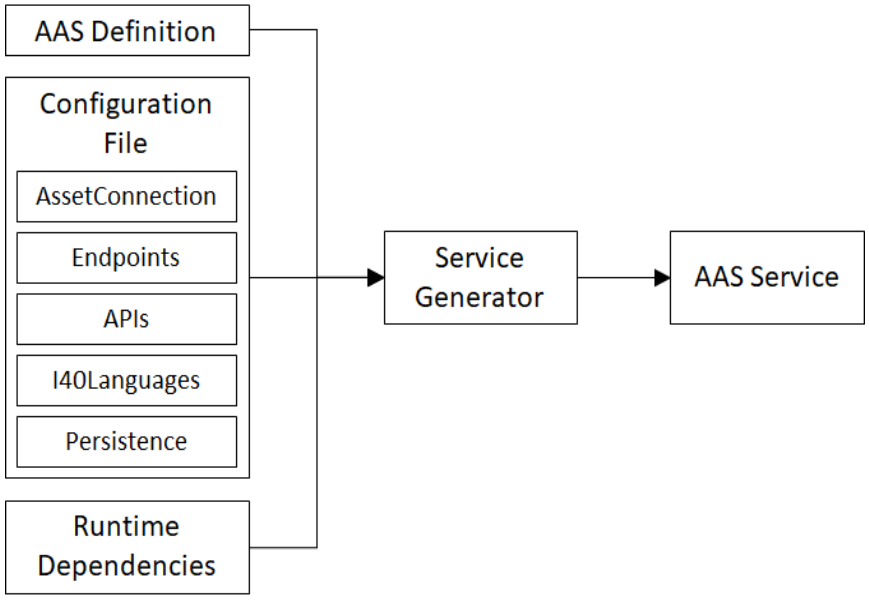
The Service Generator is a tool to create AAS services for assets. It can be used by people without programming knowledge because it has a graphical user interface. For example, it can generate a deployable AAS service that receives data requests over the standardized AAS API and connects to the asset. The AAS Service is similar to the AASX Server,[14] however it has some unique features that would not be possible for us to implement in the AASX Server.

One of these features is the integration with the IDS Connector, meaning that the IDS Connector can include several AAS services to share data with business partners.

In the case of our TableSort OPC UA use-case, all the live data will remain in the original OPC UA server. Requests to access this data will be handled by the AAS Service, meaning the service will connect to the asset and return the data, if the usage policies in the IDS allow it.

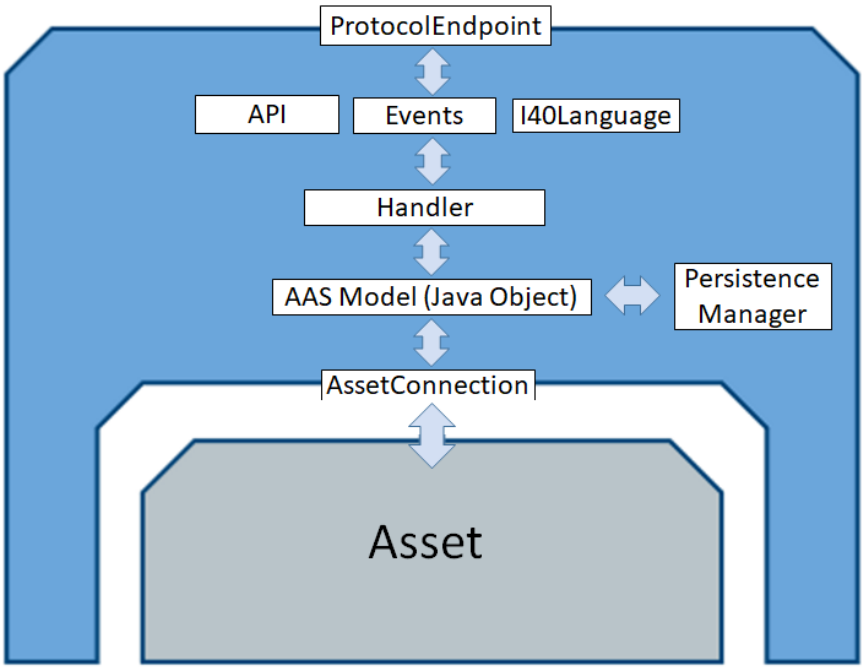
The user can provide different input files to the Service Generator which contains the AAS description (e.g. a file or server). With the Generator, users can generate a service for different file formats like AutomationML, JSON or OPC UA. In these files, the user describes the asset with AAS terms and defines where the live-data of the asset can be found. The Generator also verifies the specified AAS and will not work with AAS descriptions that do not conform with the standard.

[14] Github AASX Server [Online]. Available: https://github.com/admin-shell-io/aasx-server



AAS Service Generator input

In our TableSort use-case, an administrator could create an OPC nodeset describing the AAS or model it as an AutomationML file. This file could then be inserted into the generator and the output would be source code of an AAS Service. This service could then be deployed and connect to the existing TableSort OPC server. For this, the AAS Service can have additional libraries configured that allow it to access remote data. For example, when we need to access data from an OPC UA server, we need a library in the service that supports OPC UA. The following figure shows the architecture of the AAS Service. The AAS Model is represented by Java Objects, which are stored in different persistence solutions like databases or in-memory.



AAS Service architecture

When a new library is necessary, for example for proprietary protocols (e.g. Siemens S7), the library can be injected during the AAS Service Generator phase or added later in the AAS Service. We provide libraries for standardized connections like HTTPS and OPC UA.

AAS Registry

The AASs are usually registered in an AAS Registry to keep track of all shells and to enable users to find the AAS. It is suggested to put the AAS Registry into the AAS of a central system. Each AAS can be an AAS Registry, as long as is supports the full registry functionality. The AAS Registry, that tracks existing shells, can therefore be integrated into the IDS connector (option 1).

Alternatively, an interface to communicate with existing registries could be added to the IDS connector (option 2). In this case the connector does not include a registry, but communicates with existing ones in the factory.

Option 1 places the AAS registry in the connector, while option 2 has registries outside the connector. Option 1 is useful for factories that do not have AAS registries yet. Option 2 is useful for factories that already have existing AAS registries, so they do not need a registry in the IDS connector. Of course, some factories need several registries, which is why several instances can be created of our registry implementation. Our use-

case shows option 1 with the AAS registry inside of the IDS connector, but we are currently exploring other options in regard to the IDS Broker.

AAS Manager and Integration in the Trusted Factory Connector

The last component we are developing is the AAS Manager. It includes a simple GUI to check the current status of AAS services, manage them (update, configure) and delete them.

The AAS Manager and AAS Registry will be additional modules for the IDS Trusted Connector. The AAS services can be deployed directly in the Connector or connected via REST. The Trusted Factory Connector can forward AAS requests to the AAS Service and return answers to other IDS participants. This allows the factory owner to share AAS via IDS communication and restrict usage with a Usage Control Framework, in our case MYDATA Control.

Conclusion and Future Work

In this paper, AAS services and tools for the industrial use-case TableSort were introduced. We discussed the combination of AAS and IDS to secure communication of AAS data and allow usage control for an entire AAS by using the Trusted Connector. The IDS provides a secure data network for factory owners and their partners and reduces the need of trust in data sharing scenarios.

We also added support for AAS in different exchange formats and defined the concept of generating AAS services by providing descriptions to the Service Generator. These services are highly useful for providing access and functionality for machines, that do not currently support the AAS specification. The several AAS components allow to bring the benefits of AAS to factories and machines, that could not support it or would require high effort.

In the future, the specification of the AAS could include fine-granular usage control, so that parts of the AAS can be shared with different usage policies. The IDS community IDS-I (Industrial) is working on bringing the IDS and AAS further together.

Acknowledgment

This work was supported in part by the program "Fraunhofer Forschungszentrum Data Spaces" in the project "T37"

Cyber securing your factory floor

The technology for a tightly locked firewall with only OPC_UA access is there, but educate and train your OT-people.

Author:

Prof. Dr. Ir. Egbert-Jan Sol, Egbert-Jan.Sol@TNO.nl, TNO Industry, Netherlands, Program director Smart Industry NL (www.smartindustry.nl)

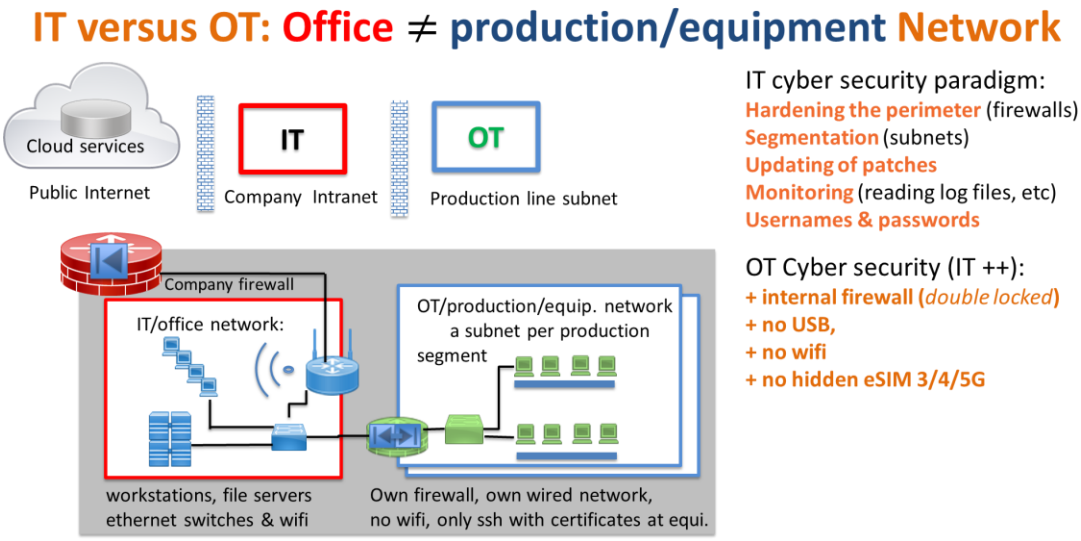
Abstract

We need to train OT (Operational Technology, i.e. non-IT/Information Technology) people to protect production equipment against cyber-attacks. With Industrie 4.0, or Smart Industry as we call it in the Netherlands, companies are rapidly connecting production lines and factory floor equipment to company IT-networks. To do so in a cyber secure way, one needs to use an OT-subnetwork with only OPC-UA (Open Platform Communication – Unified Architecture standard) messages between the OT-network with (open source) edge and classical PLC (Programmable Logic Controller) systems and the IT-network. With the OPC-UA messages one can update digital twin information (or AAS, the Asset Administration Shell) at the IT-side and from these digital twins own IT and external service provider applications can access the information they need using standard IT secure solutions as database, cloud or intercloud data exchanges such as sovereignty oriented IDS (Industrial/International Data Space) or Gaia-X.

This paper describes a workshop where the participants are continuously hacked until they get their PLC completely protected, i.e. own Ethernet/IP subnet, no Wi-Fi, no USB, changed username/passwords, and a double locked firewall with only the OPC-UA mouse-hole. In the end they demonstrate that they retrieve OPC-UA formatted equipment message from the OT-subnet at the company IT-network side of the firewall. The workshop is part of the Dutch Smart Industry program to improve digital skills of factory employees. All material is open source and searchable on internet for self-study in corona time on www.smartindustry.nl, Github and YouTube (smart industry talks).

Introduction

Let's be realistic. Big companies have their factories, plants, installations and equipment digitally connected in a cyber secure way. They are talking about Industrie 4.0 and consultants are already hyping on Artificial Intelligence. Such companies have the staff and purchasing power to do so. Say 90-95% of the companies have their production equipment not connected. If they have some equipment digitally connected, it is hardly in a cyber secure way. Those, often SME, companies are not to blame. Production equipment is rather closed, uses special fieldbus protocols if any and OT people (operation technology, read factor floor people) are no ICT specialists. But at the current rate of introducing Industrie 4.0 much equipment will be connected into networks with all kind of cyber security risks.



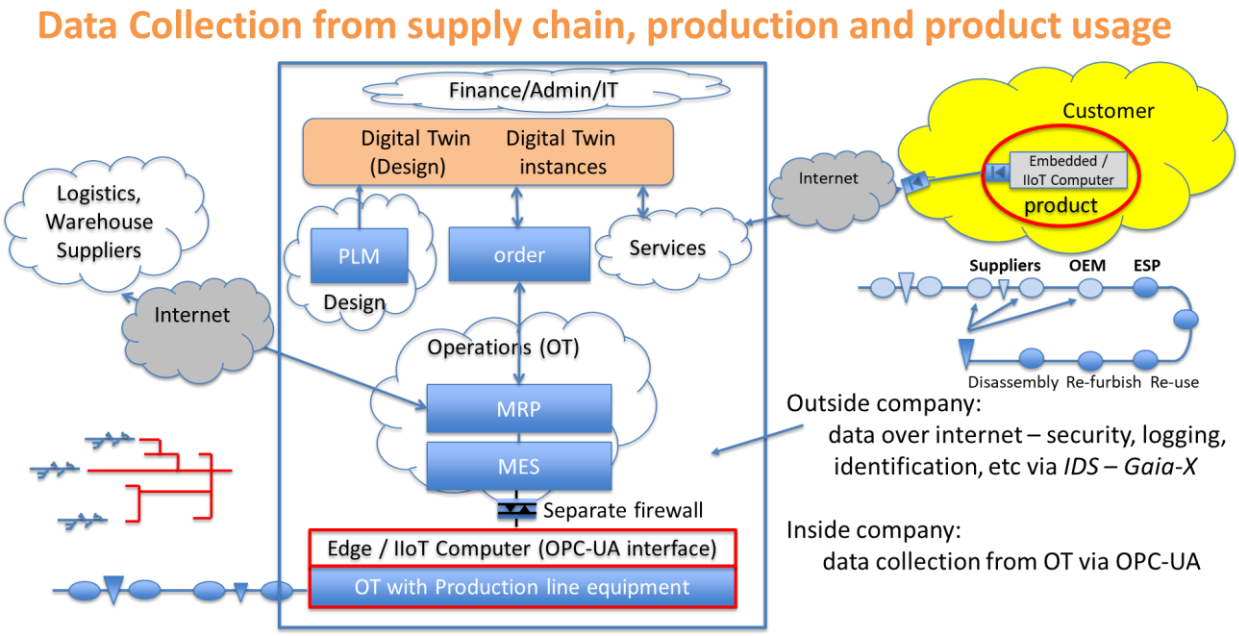
In cyber space, there is a vague war on going. Today you might think of a hacker trying to take hostage of your key bottleneck machine to squeeze out some bitcoins. But tomorrow all companies in a value chain, with the chain as strong as the weakest link, will need to protect their companies and in particular their production equipment against state-supported professional, semi-military hackers. The next war is not with guns and a clear declaration of war, but will be a vague cyber war where the infrastructure (traffic lights, power plants) and economy (factories, data networks) are attacked. Similar with the social media campaign and green men at the Crimea, you don't realize clearly at first what is happening, you think the rules of laws apply, but then the rule of power takes over. In a future case that is knowledge power on how to hack the enemy infra- and economic structures. And the best way to defense yourself is to learn how to protect your systems starting today.

At the same time while you lock your systems, customers are expecting that you have a customer portal where they can enter orders digitally over the internet. Next they want to trace the planning and production progress, just like consumers can follow their ordered packages. They ultimately want real-time digital information on the progress of their order, avoiding delays by human intervention (phone calls, emails). While those customers require more and more real-time information on all kind of traceability and quality data on their orders, you have to plug in your equipment on your company network. If you consider this farfetched, realize that your own ERP systems wants to have that same real-time overview of production progress too. Often companies have already a few automated work cells with a digital interface. Then they start using more and more paperless terminals on the factory floor and barcode readers to retrieve and report workorders. And finally, continuous real-time data collection from your factory floor is becoming crucial, not only for your own ERP planning and control, but also to service your customers. That's not all. Next to customers, some equipment vendors want digital access to service and maintain their equipment on your factory floor. So they want their equipment to sent information on their status over the Internet.

Whereas years ago you could shield your factory floor from all kind of interference from outside, these days with all kind of digital tools it looks as if everyone inhouse, at customer sites and vendor sites want to collect all kind of data from your factory floor. But so does a hacker, in particular a roque state tolerated ex-military hacker groups that want to extort bitcoins after taking your factory floor equipment hostage. Luckily the majority of factory floor equipment is not digital connected yet. But in this time of growing Internet-of-Things and Industrie 4.0 progress that is changing rapidly. Cyber securing your factory floor equipment becomes a must. To do so, you have to acquire your own digital knowledge and skills at OT level to safe guard your production equipment in a cyber secure way.

The challenge of Industrie 4.0 is not technology, all needed technology is there and 1% of the companies have it implemented. The challenge is training OT-people on digital skills. In particular you need to train 35+ year employees who 20 years ago, at the age of 15 year old, didn't got at school any Internet/digital skills taught. But even younger people need to catch-up on the recent developments as during the last 10 to 5 years where every webpage access takes your computer to multiple other website as e.g. Google and Facebook and leaving a trail of data on what they are looking at. Firewalls were good in blocking unwanted traffic from outside, but to block cookies, tracers etc. will lead to firewalls that not only block traffic from outside, but also block traffic from inside and only allow known traffic to pass the firewall. This is a new aspect, not uncommon by IT-firewall experts, that will become a standard way of working by Internet consumers and, in our case, OT /factory floor operations. With one advantage, in the industrial equipment the OPC-UA is becoming the standard and you have to open your firewall only allowed traffic can be OPC-UA messages you can control, using encryption and port numbers you select.

Factory floor data collection and its use



Deep Chain Realtime Planning and control

The introduction explained the trend to collect more and more on real-time production data from the factory floor, first for internal ERP use, but in the nearby future also to feed your customer portal. And in the long run OEM (the original equipment manufacturers) will demand their first tier suppliers and other subtiers suppliers to enable an all-digital chain deep real-time planning and control eco-system capable of planning simulations and rescheduling over their whole chain as well as error free propagation of design updates.

Digital Twins and AAS (Asset Admin Shell)

There exits other factory floor data collection needs too. One important recent development is the digital twin concept where a digital representation of the physical product, equipment, installation, even factory is maintained. It started with the CAD design, but today a Digital Twin (DT) contains all kind of status and historical information. In this context the AAS is a development to consider. In general these DT/AAS consist of an object tree with all kind of attributes and are stored in a data base/cloud in the IT-network. To update the data a digital connection to the product/equipment is needed and the OPC-UA standard with its XML object tree structure is well suited for this.

IT and OT network

Data storage is in general an IT (information technology) issue in the company or engineering IT-network. For security and safety reason you need to place factory floor equipment in separate so-called OT-network, an Ethernet/IP subnetwork without access from external and even the company network. But you need to send orders to this OT network and from this network you want to update ERP and DT/AAS information stored in the IT network. For this purpose you need to connect each OT-subnets with a firewall to your company IT network. Before continuing in detail, let's first describe the components in OT networks.

PLC, edge and open systems

Around the sixties/seventies mechanical camshells were replaced by more flexible electronic programmable logic controllers. At that time, it were mostly 1-bit of 4-bit logic integrated circuits, but today it are 4-core, 64-bits microcomputers with next to logic control also all kind of data processing and communication capabilities. And such platforms are more and more running open source Linux based operating systems, although for special extreme cases of very fast, hard real-time logic control some additional hardware is still used.

Today, 50 years later, such systems processing the logic, the data, (graphic) user interfaces and the communication messages are called edge computers. Edge or Industrial IoT (Internet of Things) computers are practically all based upon open sources Linux operating systems. And remarkably they can be programmed in modern, highly capable Python suitable from logic control, user interfacing, data communication up to data processing including machine learning/artificial intelligence algorithms for which huge libraries of open source software modules are available. Yes, also logic programming beyond IEC-61131 can be programmed in Python.[1]

Classical 1000+ euro PLC's and costly software tools are not rapidly replaced by edge computers and open source software. This is meanly due to invested interest by incumbents and old-school bosses. However the future of reliable, industrial edge computers, running Linux OS and programmable in Python and using huge open source software library and tools, also for OPC-UA, is here today. And with one big advantage, a 40 Euro Raspberry with some 20 Euro digital 5-volt I/O are all the hard and software costs you need to invest into to train people, before they start using 200 Euro industrial edge computer with a few 24-VDC

[1] As Dutch member of the original standardization group led by Christiaansen of Allen-Badley that produced the IEC-1131 around 1990 the author was surprised 30 years later by the ease of using Python's new asyncio capabilities for logic control as they evolved in Python 3 from Python 3.4 to 3.7 to the level of asyncio routines now in Python 3.9.

digital/analog I/O in operational systems. You only need to plug the edge computer with its standard Ethernet/IP interface into your OT-subnet. In other words, coupling your equipment into the company network is becoming much cheaper than ever before resulting in the Internet-of-Things, or Industrial IoT where everything is connected. But do it in a cyber secure way.

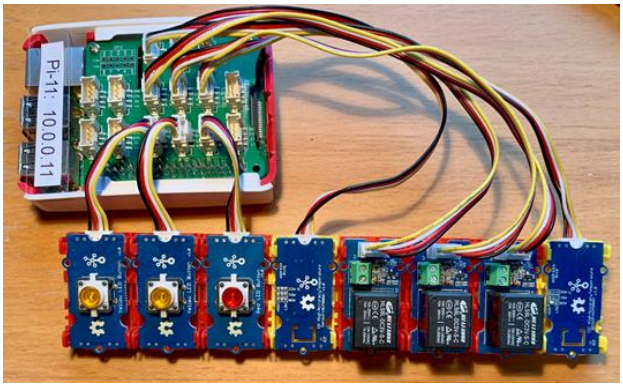


Photo 8 RaspberryPi with 5VDC I/0

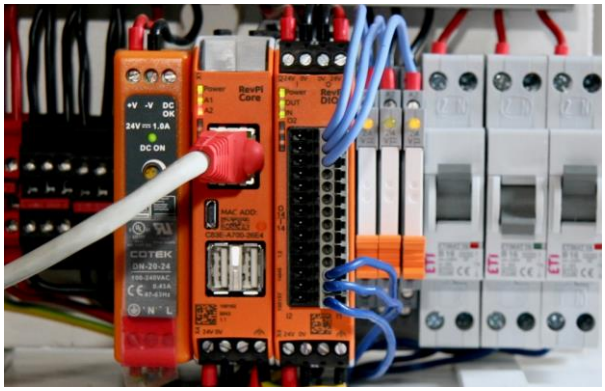
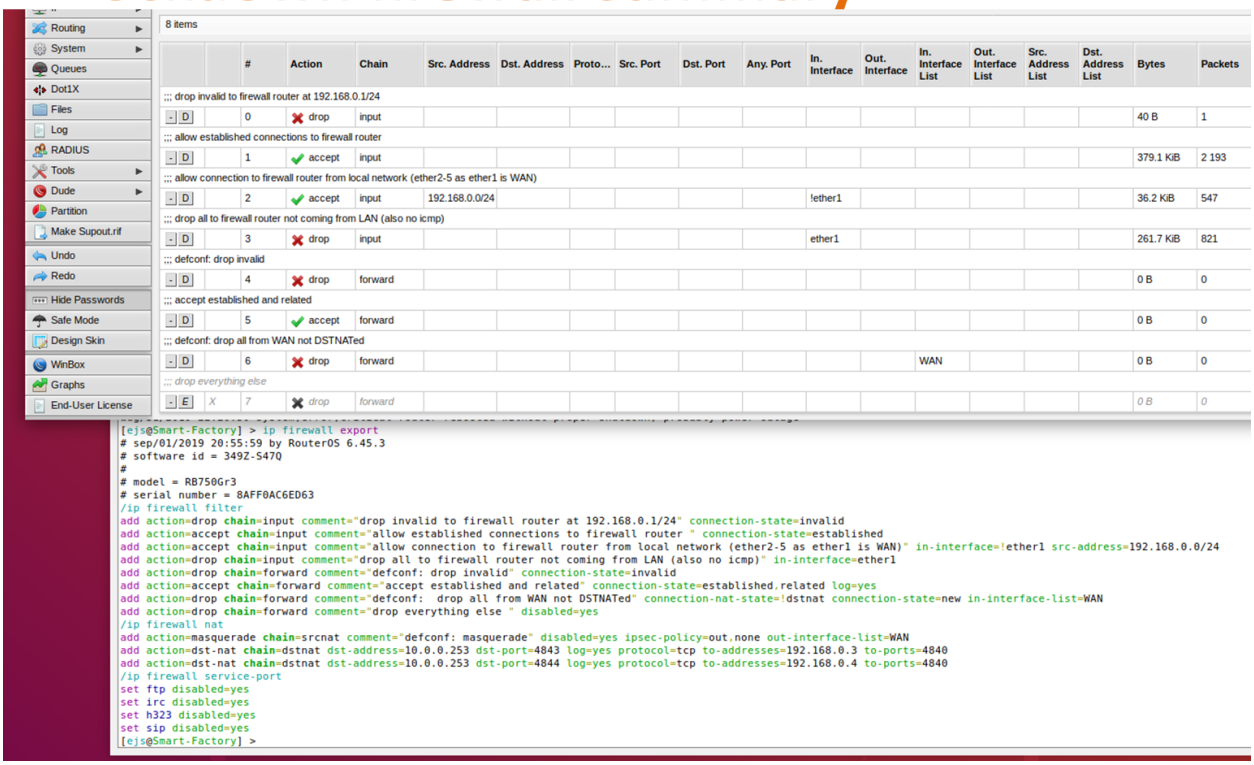


Photo 2 Kunbus Edge system with 24VDC I/O

Cyber securing your factory floor (OT) equipment

An OT subnet is an Ethernet network with its own OT-router/firewall. In Ethernet/IP terms, it is e.g. a 192.168.1.1/24 subnet with 254 IP nodes 192.168.1.2-254 and a router with firewall capabilities at e.g. node 192.168.1.1 with an external port towards your company network. Often the router has switched internal Ethernet ports for Ethernet connections (RS-45 wire or even optical fiber) to equipment. For security reasons one should not use (difficult or uncontrollable) wireless or mobile radio connections, only physical wired connections.

Lockdown firewall summary



The OT-network router must have firewall (IP message filtering) capabilities which you can program/configure with firewall rules. Such capabilities are not common or very restricted in the kind of consumer firewalls at home, but in the IT-world this is standard. Nevertheless firewall rules to safe guard a company or public IP provider networks can be extremely complex. For our OT-subnet we can keep the requirement and subsequent configuration rather simple. You want to block all incoming and all outgoing traffic except for messages that are formatted as OPC-UA messages and forwarded on the 4840 port and even better, your own selected port number. And one has to be able to turn the NAT feature on/off by hand to allow for controlled equipment triggered software update requests. The good news is that the regular, sometimes daily updates for Linux security reasons are not needed as the OT-subnet environment is now not coupled to the internet and hackers can't get in.

An OT-subnet should have no other access possibilities. So no Bluetooth, Wi-Fi or GSM mobile or other wireless access. It is in general a small network and if one needs wireless access to access company data or the internet, use the company Wi-Fi network. No open USB port, if not behind a locked cabinet, disable USB port by super-gluing them unusable. And first of all change standard user name en in particular passwords. It are a few layers of cyber hygiene measurements, but in the end you have a production network with equipment that will not receive any kind of updates or unknown and unwanted access, but that also

can’t change it behavior without you knowing it. In simple words, it is a tightly locked down subnetwork with only the OPC-UA message between the subnetwork and specified digital twin applications in the IT-network. And without any overnight software updates with error chances that might block or delay the startup of your production line the next day.

No 5G access from vendors to your equipment

Vendors and service providers would love to have direct access to your equipment to see its status, suggest repairs, etc. Nice extra features, but one big open door for hackers. Sometime, they even build-in a mobile data connection, e.g. with 3/4/5-G eSIM you can’t see. If you think that is not the case, have a look in your own car. Each modern car has a SIM hidden in it. The problem in industry is that **sensor data is not copyright protected** as it does not involve human labor/creativity nor data protected by privacy rules. So any data acquired by the external vendor is theirs too and you have no control over it. You have to forbid direct access in a legal contract and describe exactly which data they can get from you after you extracted it from the equipment, using as suggested OPC-UA message, and which you stored in your own digital twin/data cloud and then provide intercloud (think IDS/Gaia-X) access to the data part in your data storage you agreed the vendor can access and use under such and such conditions. But if you let them collect the data from the equipment directly themselves, e.g. using a build-in eSIM, they use it for AI-algorithm training, you can be sure that sometime latter you have to pay for additional smart services for which you made the costs of collection the data. This a one of the reasons why companies must collect equipment data themselves and used controlled, contractual data exchange.

Training workshop

The challenge of cyber securing your factory floor is not new technology. It is the fact that it requires a lot of OT people to be educated and trained. It is not very difficult. Only the firewall rules are somewhat more difficult to understand. But it is the need to capture more digital skills that is hindering implementation at a large scale. In particular learning to use Linux operation systems command, and for people dealing with data and who have to learn programming with Python, does require time and effort.

In a 1-day workshop one can only get some basic understanding on cyber securing a production line and setup up an own subnet with a simple firewall configurations. In a Smart Industry workshop participants get a Raspberry Pi with several I/O (100 Euro) for which a logic and an user interface program has been written in Python. In three exercise they have to debug the Python program, collect OPC-UA message and finally configure the Raspberry behind their firewall. During every exercise the participants are in an instruction network not connected to Internet and where each group get, next to their Raspberry Pi, their own router/firewall. In our case we used a 50 Euro Mikrotik device.

Once they start with the exercises, they are continuously hacked. To their own frustration each time in a more advanced way. First because they have not changed the standard password, then because there was a second login username called service which they didn't realize that a hacker could use. Then there is illegal software preinstalled and finally there were some ports open. Each time their Raspberry is hacked and the I/O (mechanical relays) makes a lot of noise so all other participants heard that one of the groups is hacked again. Finally, once every thing is configured right, they can't be hacked any more as the hacking instructor can't get into their own subnet any more.

Having experienced yourself how easy systems can be hacked multiple times in a row is an effective lesson. It gives the participants a solid motivation to protect their production equipment as good as possible and to be a partner to IT department employees who either want to construct something unworkable complex or want to keep systems open such that IT can control them and where OT finds their systems upgraded one morning such that they can not start production.

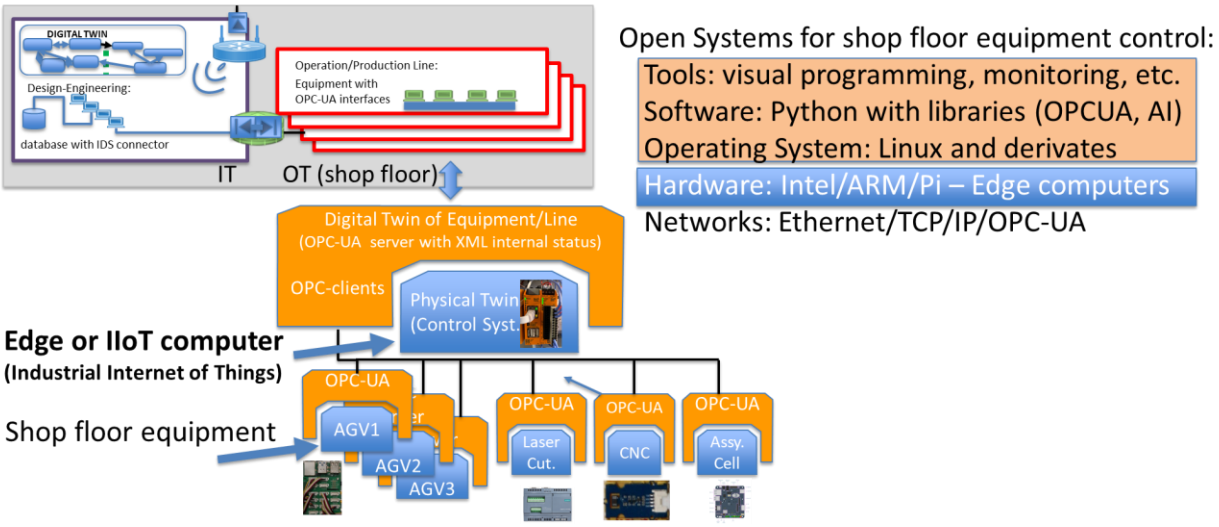
Coming back on learning cyber security, Linux and Python. Not every one on the factory floor will become fully digitally skilled, but all jobs will require the use of heavily digitalized equipment and tools and more and more jobs will have to deal with data and implicit data security. Learning how to use Linux is an investment well worth. The author learned it around 1987 and still can use the same command, albeit with e.g. Ubuntu's windows interface it is easier to use then in the old day with command prompts only. Regarding the use of Python, practically any AI program these days is programmed in Python, but one can use it for user interfacing, data communication and even logic programming. It is not needed for everyone, but those OT employees that are able to use it will be key employees as in the data driven industry of the future they are the ones that can get the most productivity out of their equipment and production lines. And on their journey to acquire more digital skills, they also get more and more skilled in cyber securing the factory floor.

Conclusion

Industrie 4.0, Smart Industry or Internet of Things (IoT) will lead to interconnecting all production equipment to ultimately the internet. This results in cyber security risks that need to be handled in the proper way. Inside production companies, the plant or factory floor equipment need to be extra secure not only for data security, but also for human safety reasons. For OT-employees this requires new ways of working and/or acquiring cyber security knowledge (and for IT-employees to understand the extra OT-requirements).

One need to be told and trained how to configure an Ethernet/IP subnet in an OT-environment in a secure way with proper usernames, passwords, firewall configuration, but also avoiding USB and wireless access. In particular for manufacturing and process equipment the OPC-UA is international data communication standard is to be used, together with new developments as digital twinning (DT/AAS) and secure inter-cloud/intercompany databases data exchanges (IDS, Gaia-X).

Towards open systems using standard interfaces as Ethernet/TCP/IP/OPC-UA



All the information is available as open source information. Part is in 10 YouTube lectures on open source systems, edge computing, Linux, Python using Raspberry Pi's and Kunbus Revolution Pi as well as configuring Mikrotik's routers and 4 on data management. Next to the Smart Industry Talk YouTube channel, you find the video's at www.smartindustry.nl/aan-de-slag/academy. Some YouTube video's are in Dutch, on purpose for medium level educated non-IT employees, some are in Engels, but all slides are in English. On Github all Python programs for logic, user interfacing and OPC-UA as well as the Mikrotik firewall rules can be found at https://github/ejsol/Smart-Industry-zelf-aan-de-slag.

The need is clear. The training material is available. Don't wait until it's too late.

TNO innovation for life this work for the Dutch Smart Industry program was made possible by TNO and a grant for the Dutch Ministry of Economic Affairs and Climate

International Data Spaces tailored to Industrie 4.0 – How to Address the Requirements for Data Sovereignty

Author:

Dr. Thomas Usländer, thomas.uslaender@iosb.fraunhofer.de, Fraunhofer IOSB

Abstract

This paper describes the working approach of the IDS-Industrial Community (IDS-I) for the analysis of requirements on data sovereignty. This activity is motivated by the vision 2030 of the Platform Industrie 4.0 that states autonomy, including data sovereignty, as one strategic field of action. The paper presents how IDS-I aims at systematically deriving data sovereignty aspects from the two reference use cases, Collaborative Condition Monitoring (CCM) and Smart Factory Web (SFW), in order to identify architectural and technological synergies and gaps between the International Data Spaces (IDS) and the specifications of the Platform Industrie 4.0.

Keywords

Data Sovereignty, Data Usage Control, International Data Spaces, Collaborative Condition Monitoring, Smart Factory Web, SERVUS

Motivation for the IDS-Industrial Community

Digitalization leads to the creation and usage of data. In the context of this social, economic and technical development, data has become an independent product, also in the domain of industrial production and smart manufacturing. As an economic good, they form the basis for new value-added processes and business models. In daily business practices data are used very often, however, exchanged rather rarely. Companies are still too worried about losing control over their data - and thus their valuable corporate knowledge. This is where International Data Spaces (IDS) come into play: with an architecture for virtual data spaces that guarantees the secure and sovereign exchange of their data.

The overriding objective of the IDS is to help companies and institutions to take advantage of the benefits of digitalization without increasing their risks. The means for this is a trustworthy architecture for data management with standards for sovereignty and secure data exchange.

The International Data Spaces Association (IDSA) represents the interests of more than 80 international companies and institutions. The IDSA bundles the requirements for all IDS application domains, organizes the exchange of knowledge between research and industry and develops guidelines for the certification, standardization and utilization of the results resulting from the various IDSA-related research projects at European and national level.

In its vision for 2030, published in August 2019, the Platform Industrie 4.0 formulated a holistic approach to the shaping of digital ecosystems and re-orientated the further development of Industrie 4.0 according to this vision.[1] At the heart of the design of digital ecosystems are the three strategic fields of action autonomy, interoperability and sustainability (see Figure 9).

[1] Platform Industrie 4.0 (Ed.): Position Paper 2030 Vision for Industrie 4.0. https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/Positionspapier%20Leitbild%20(EN).html.

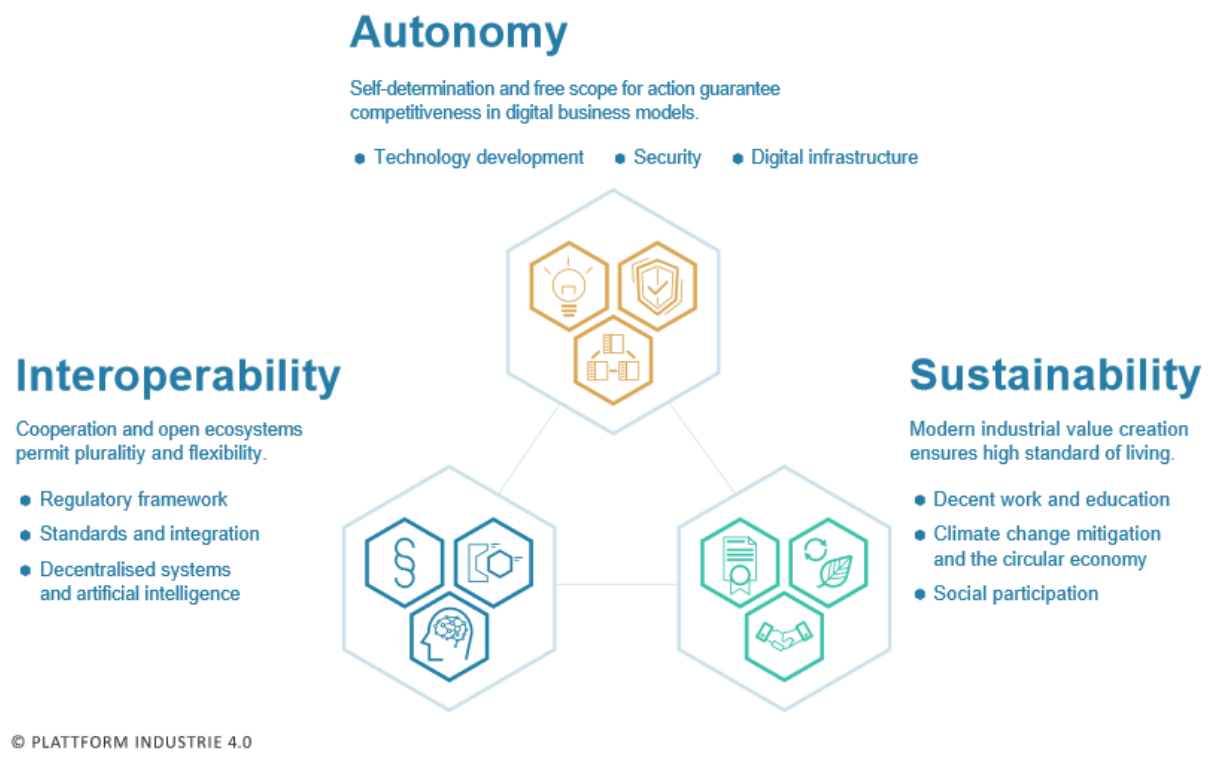


Figure 9: Strategic fields in the Vision 2030 of the Platform Industrie 4.0

For data sovereignty the strategic field of autonomy is highly relevant:

> *Autonomy is the freedom to take independent decisions and to interact in conditions of fair competition – from a chosen business model to an individual's decision to make a purchase. Autonomy requires an open digital infrastructure for everyone, data protection, IT and information security and technology-neutral research, development and innovation.*

The freedom to take independent decisions and the request for fair conditions are key characteristics of the demand for digital sovereignty – on the technological and infrastructural level as well as on the data level. The European initiative GAIA-X[2] focuses on the former level, and aims at creating a secure, federated

[2] GAIA-X: https://www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html.

infrastructure that meets the highest standards of digital sovereignty while promoting innovation. The data level, however, is the key concern of the IDS.

Within IDSA, the application domain of networked industrial production and smart manufacturing, hence Industrie 4.0, is gathered by a dedicated community entitled IDS-Industrial, abbreviated by IDS-I. This paper describes how IDS-I handles the problem of analyzing the requirements on data sovereignty for Industrie 4.0.

Requirements Analysis in the IIoT

The question of how to handle requirements on data sovereignty in joint Industrie 4.0 / IDS and GAIA-X service-oriented environments, falls into the general problem of Agile Service Engineering in the Industrial Internet of Things (IIoT).[3] As illustrated in Figure 10, an agile approach is recommended to reduce the conceptual and terminological gap between the views of the thematic expert (typically an industrial, mechanical and/or an electrical engineer) and the IT expert (typically, a computer scientist). Driven by the business strategy the thematic expert expresses his/her functional and non-functional requirements about the system's behavior and characteristics, whereby the IT expert "answers" in terms of (mostly technical) system capabilities and service registries. Usually, both descriptions cannot be matched without additional, tedious discussions and additional explanations.

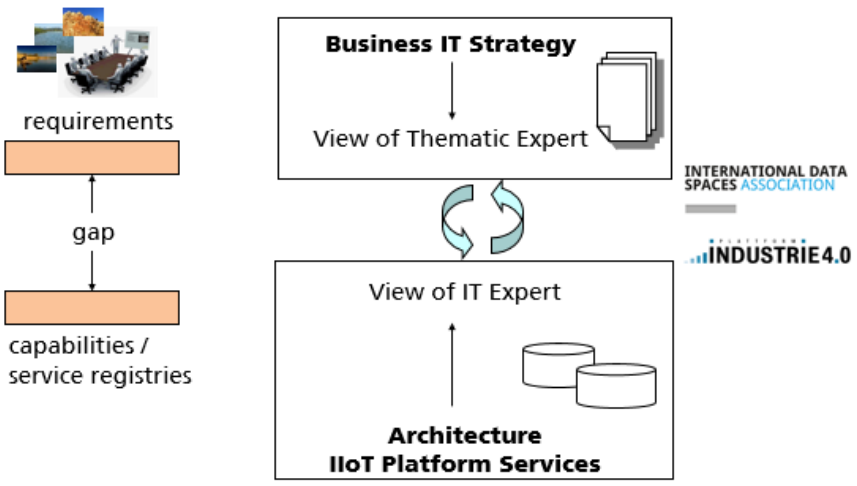


Figure 10: Mapping of Requirements in IIoT Platform Environments

[3] Usländer, T.; Batz, T. Agile Service Engineering in the Industrial Internet of Things. Future Internet 2018, 10, 100. https://doi.org/10.3390/fi10100100.

The idea of the SERVUS methodology[3] is to use semi-structured descriptions of use cases for this activity, following semi-structured use case templates,[4] see Figure 11. With SERVUS, this idea of a semi-structured description of analysis and design artefacts applies, too, when mapping the use cases step-by-step to other design artefacts such as requirements and when matching them with abstract, technology-independent capability descriptions of IIoT platforms. The terminological gap is approached by attaching semantic annotation labels to the basic terms used. The IIoT platforms of interest are those specified by the Platform Industrie 4.0, IDS and GAIA-X. In order to master this stepwise mapping process all the analysis and design artefacts are stored in an IIoT Platform Engineering Information System (IIoT-PEIS), which also provides documentation, information retrieval and visualization support.[3]

ID	<<will be defined later>>
Name	Name of the use case
Priority	[Low, medium, high]
Reference use case	[Smart Factory Web, Collaborative Condition Monitoring or other…]
Description	Textual description of the use case: • motivation • involved stakeholders • objective • constraints • …
Comment	Optional further comments
Preconditions	what is required before the use case may be started or deployed
Workflow	The following steps are required to perform the use case: 1. … 2. … 3. … … Note: may have loops and jumps (if … then go to step X)
Postconditions	Describe the situation after the use case was carried out
Sources	Literature or references
Authors	Name of the authors
Date	Date of last change

Figure 11: Use case Template as used in the IDS-Industrial Community

[4] Cockburn, A. Writing Effective Use Cases; Addison-Wesley: Boston, MA, USA, 2001.

IDS-I Reference Use Cases

The IDS-I community decided to describe use cases stemming from two so-called reference use case domains, also used by other initiatives:

- Collaborative Condition Monitoring (CCM), provided by the Platform Industrie 4.0 applied as GAIA-X use case, and
- Smart Factory Web (SFW), an accepted IIC Testbed of the Industrial Internet Consortium (IIC).

Collaborative Condition Monitoring (CCM)

The CCM reference use case deals with the collection and use of operating data to optimize the reliability and service life of machines and their components during operation.[5] In the real world, installed machines come from different machine suppliers that are equipped with different products from different component suppliers. In these multi-stakeholder environments, the exploitation of the data of components, machines and the factory plant to provide higher-level services such as predictive maintenance is still a challenge. This is due not only to the lack of interoperability, which may be solved by encapsulating the assets by the concept of the Asset Administration Shell (AAS), but also due to the uncertainty of how to control the access and usage of the datasets associated to and provided by the assets. IDS-Industrial aims at investigating the detailed requirements and concerns.

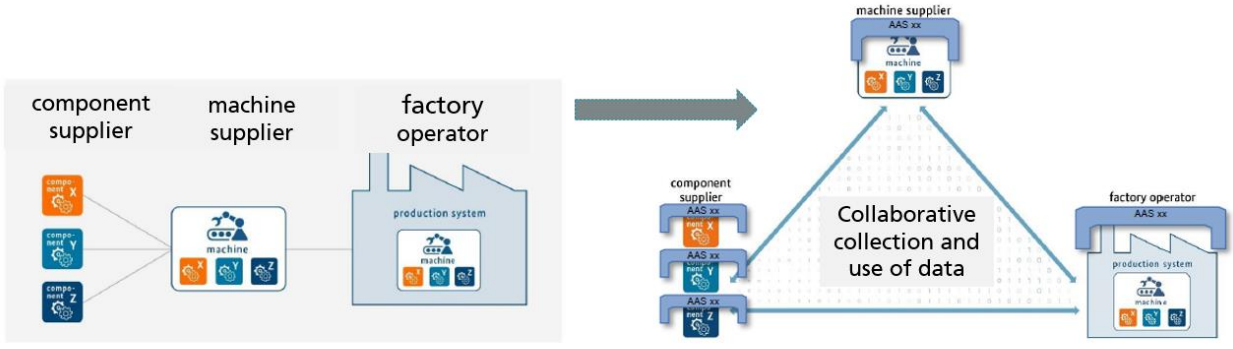


Figure 12: Problem Illustration of the Collaborative Condition Monitoring Use case[5]

[5] Plattform Industrie 4.0: CCM Webinar, 2020. https://www.plattform-i40.de/PI40/Redaktion/DE/Down-loads/Publikation/Webseminar-Collaborative-data-driven-business-models.pdf?__blob=publication-File&v=8.

Smart Factory Web (SFW)

The SFW reference use case provides a blueprint architecture for open sustainable and resilient production ecosystems.[6] One important SFW application is an industrial marketplace for industrial production following the platform-driven economy of other branches such as tourism or mobility. As illustrated in Figure 13 the demands of higher resilience, sustainable production, more flexibility, higher product variance, manufacturing on demand and smaller lot sizes do not only address the factory level, e.g. the shop floor environment, but also the supply chain level, the so-called “connected world” of the Reference Architecture Model Industrie 4.0 (RAMI4.0). A marketplace is highly needed that does not impose business dependency constraints upon the suppliers, but is designed on the principles of openness, fairness and transparency. It allows a user to quickly search for new and alternate suppliers in a supply chain network. More flexibility is demanded in case a given supply chain is at risk or about to fail due to broken transport lines, natural catastrophes, pandemics or material shortage. In order to enable searching for alternate suppliers and matchmaking by the marketplace, adequate data about the capabilities and assets of factories in the supply chain is required. IDS-Industrial aims at investigating the detailed requirements and concerns about sharing this type of data in a marketplace and within the supply chain network.

Figure 13: Problem Illustration of the Smart Factory Web use case

[6] Fraunhofer IOSB (Ed.): IIC Testbed Smart Factory Web, 2020. https://www.smartfactoryweb.eu.

Requirements Analysis for Data Sovereignty

When considering and analyzing the requirements for data sovereignty in case of scenarios spanned by these two reference use cases, it has to be distinguished between the classical aspects of access control (to data and operations) and data usage control.

Usage control is an extension to traditional access control.[7] After access to data and operations has been permitted, the question remains what happens to the data after the access and delivery of the data (as part of operation results). Hence, usage control is about the specification and enforcement of restrictions regulating what must (not) happen to data. Usage control is concerned with requirements that pertain to data processing (obligations), rather than data access (provisions) as illustrated in Figure 14. In general, usage control is relevant in the context of intellectual property protection, compliance with regulations, and digital rights management.

Figure 14: Usage Control as an extension to Access Control

As IDS-I aim to ensure data sovereignty in industrial value chains, requirements on data usage control are analyzed according to a common schema, following the list of obligations proposed by:[7]

- **Secrecy:** Classified data must not be forwarded to nodes which do not have the respective clearance.
- **Integrity:** Critical data must not be modified by untrusted nodes as otherwise their integrity cannot be guaranteed anymore.
- **Time to live**: A prerequisite for persisting data is that it must be deleted from storage after a given period of time.

[7] IDS Assocation: Usage Control in the International Data Spaces. Position Paper of the IDSA, Version 2.0, November 2019. Accessible at https://www.internationaldataspaces.org/wp-content/uploads/2019/11/Usage-Control-in-IDS-V2.0_final.pdf.

- **Anonymization by aggregation**: Personal data must only be used as aggregates by untrusted parties. A sufficient number of distinct records must be aggregated in order to prevent de-anonymization of individual records.
- **Anonymization by replacement**: Data which allows a personal identification must be replaced by an adequate substitute in order to guarantee that individuals cannot be de-anonymized from the data.
- **Separation of duty:** Two data sets from competitive entities (e.g., two automotive OEMs) must never be aggregated or processed by the same service.
- **Usage scope:** Data may only serve as input for data pipes within the connector, but must never leave the connector to an external endpoint.

The IDS-Industrial community has started a process to analyze the two reference use cases in more detail by means of use case descriptions that fall into these categories. For each of the use cases, requirements on access control (both role-based an attribute-based), usage control (according to the obligation categories described above) and data provenance tracking (where does the data come from) are gathered and analyzed.

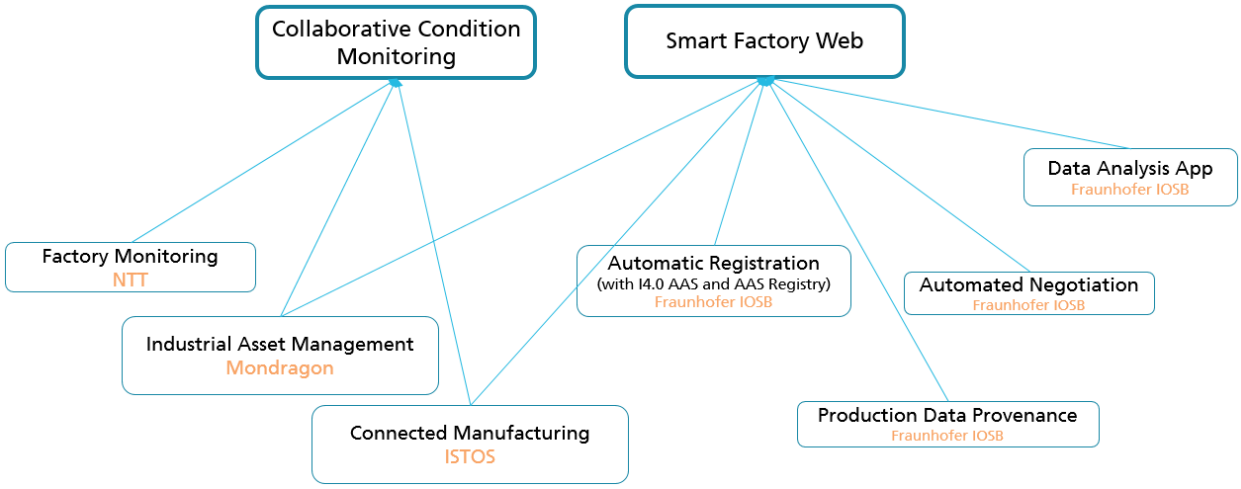


Figure 15: CCM and SFW use cases under investigation in IDS-I

Outlook

The mission of the IDS-Industrial (IDS-I) Community is to enable the design, set-up and operation of International Data Spaces tailored to the needs of the application domain of industrial production resp. smart manufacturing. IDS-I is an open community associated to the IDS Association, currently comprising 47 companies and research institutes around the world. Its overall mission is described below. After the

requirements analysis on data sovereignty, IDS-I will consider the architectural and technological consequences in a joint Industrie 4.0 / IDS and GAIA-X environment.

Mission of the IDS-Industrial Community

To gather requirements on data sovereignty incl. data sharing, data usage monitoring and control as well as data provenance tracking by means of reference use case specifications.

To map these requirements systematically to the standards, capabilities and recommended technologies of the International Data Spaces Association and the Platform Industrie 4.0.

To derive profiles of IDS/Industrie 4.0 specifications that support the requirements in industrial business eco-systems based upon standards and by means of common governance models.

To validate and demonstrate the applicability of these specifications by means of reference testbeds, e.g. Smart Factory Web and GAIA-X use cases.

To contribute to the outreach of the IDS architecture and specifications to the community of industrial production and smart manufacturing.

Implementing certificate based authentication on application level

Author:

Tianzhe Yu, Tianzhe.Yu@ifak.eu, Researcher at Institute for Automation and Communication (ifak).

Abstract

The typical use of cryptographic certificates for the authentication of clients in the Web context utilizes the capabilities built into the TLS protocol used for HTTPS. Since HTTPS connections are separated/relayed at filtering proxies, which act as application layer gateways, the mutual authentication capabilities designed into TLS cannot be used. Therefore, the client authentication with cryptographic certificates has to be performed on the application layer. The paper describes the technical details of the development and implementation of this concept and handshake with the JSON Web Token framework as used in the Discussion Paper “Secure Download Service” (Plattform Industrie 4.0).

Introduction

Certificate Based Authentication

The Transport Layer Protocol (TLS)[1] can be used to provide mutual authentication based on X.509 Certificate Chains which issued by trusted Certificate Authorities (CAs). This concept is mostly utilized by Hypertext Transfer Protocol Secure (HTTPS).[2] A Typical flow of such a procedure is shown in Figure 16 Client and server authenticate each other by verifying certificate chains and certificate verify messages which are digital signatures signed using their private keys bound to certificates.

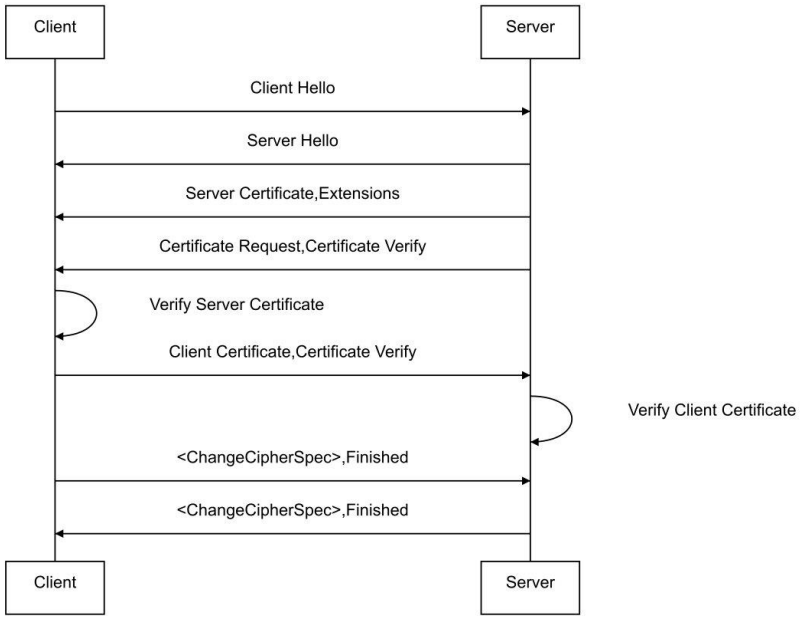


Figure 16:Message flow of a TLS connection

[1] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," Aug 2018. [Online]. Available: https://tools.ietf.org/html/rfc8446.

[2] E. Rescorla, "HTTP Over TLS," May 2000. [Online]. Available: https://tools.ietf.org/html/rfc2818.

Issues with TLS proxy

OAuth can also utilize this concept for Client Authentication.[3] However, it is not reliable or even unsafe if a TLS proxy is involved. As shown in Figure 2, TLS proxy acts as a Man-in-the-Middle and uses its own certificate to establish the communication channel with Sever,[4] which means Server can not verify Client's Certificate. Meanwhile, the Proxy can also intercept all the communication between Client and Server. Thus, in order to utilize the usability of certificate based client authentication, an implementation on application level is proposed in this paper.

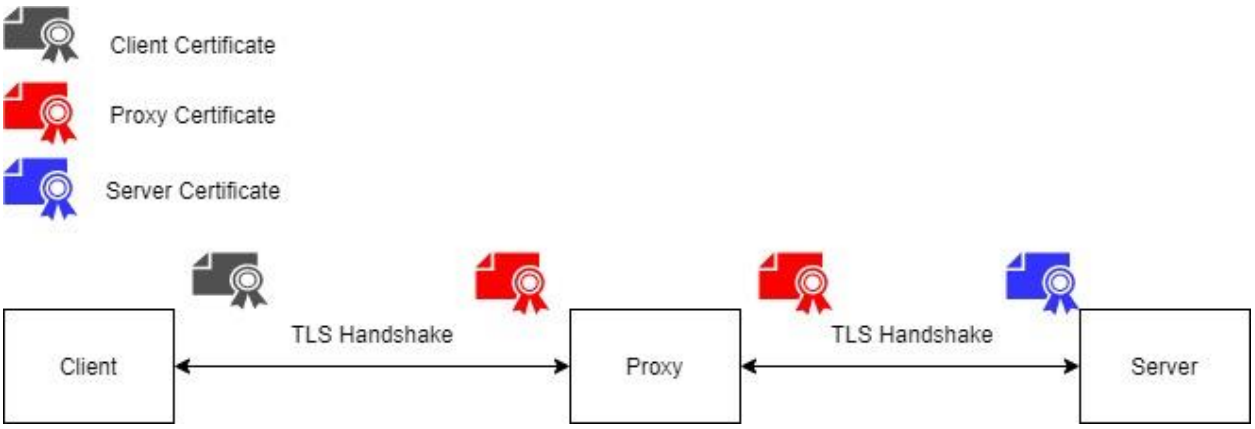


Figure 2: TLS Proxy Certificate Exchange

[3] B. Campbell, J. Bradley, N. Sakimura and T. Lodderstedt, "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound," Feb 2020. [Online]. Available: https://tools.ietf.org/html/rfc8705.

[4] M. O'Neill, S. Ruoti, K. Seamons and D. Zappala, "TLS proxies: Friend or foe?," in *Proceedings of the 2016 Internet Measurement Conference*, 2016.

Certificate Authentication on Application Level

Certificate with JWT

The proposed method uses JSON Web Token (JWT)[5] as data exchange format. It is a set of specific JSON objects and can be signed and represented as JSON Web Signature (JWS)[6] to ensure its integrity. A JSON Web Key (JWK)[7] is integrated to present the certificate chain. Such a JWT contains three parts:

- Header: Contains cryptographic info such as signature algorithm
- Payload: Info about Client and other data
- Signature: A digital signature of header and payload using the algorithm and key specified in header

The details of proposed JWT is shown in Table 11

Table 11 Structure of proposed JWT

Field	Description
Header	
alg	The algorithm used which is used to sign the JWT
typ	Type of token, in this case “JWT”
x5c	X.509 Certificate Chain. It should be an JSON array of certificate chain presented as base64 encoded strings from leaf certificate to root certificate
x5t	Base64url-encoded SHA-1 thumbprint of leaf certificate
Payload	
jti	A unique identifier of JWT
sub	Subject, should be client_id
iat	Issued at, the time stamp then the token is created
nbf	Not valid before
exp	Expiration time
iss	Issuer of the token
aud	Audience, normally the endpoint URL of authentication server
Signature	

[5] M. Jones, J. Bradley and N. Sakimura, "JSON Web Token (JWT)," May 2015. [Online]. Available: https://tools.ietf.org/html/rfc7515.
[6] M. Jones, J. Bradley and N. Sakimura, "JSON Web Signature (JWS)," May 2015q. [Online]. Available: https://tools.ietf.org/html/rfc7515.
[7] M. Jones, " JSON Web Key (JWK)," May 2015. [Online]. Available: https://tools.ietf.org/html/rfc7517.

Sign (base64UrlEncode(header) + "." + base64UrlEncode(payload), privateKey bond with end certificate in x5c , alg)

Full Process in Detail

The detail of a client authentication is shown in Figure 17:

1. Client or trusted root certificates need to be registered to Server e.g. through an out of band channel
2. When a client wants to get access to resource, it will be redirected to an authentication server
3. Client generates and signs a JWT when it is asked to present its identification
4. Authentication server verifies signature of JWT, certificate chain contains in the x5c, time stamp and client info
5. When verified, authentication server may issue an access token in JWT format, signed with authentication server's certificate
6. Client presents the access token to resource server
7. Resource server verifies the access token and grant client access.

Conclusion

In this paper, an authentication procedure is proposed to realize certificate based client authentication on application level. The proposed procedure utilizes x5c and JWS to ensure the security of the authentication process. The JWT based method can be used independently or easily integrated into existing authentication infrastructure e.g. OAuth.

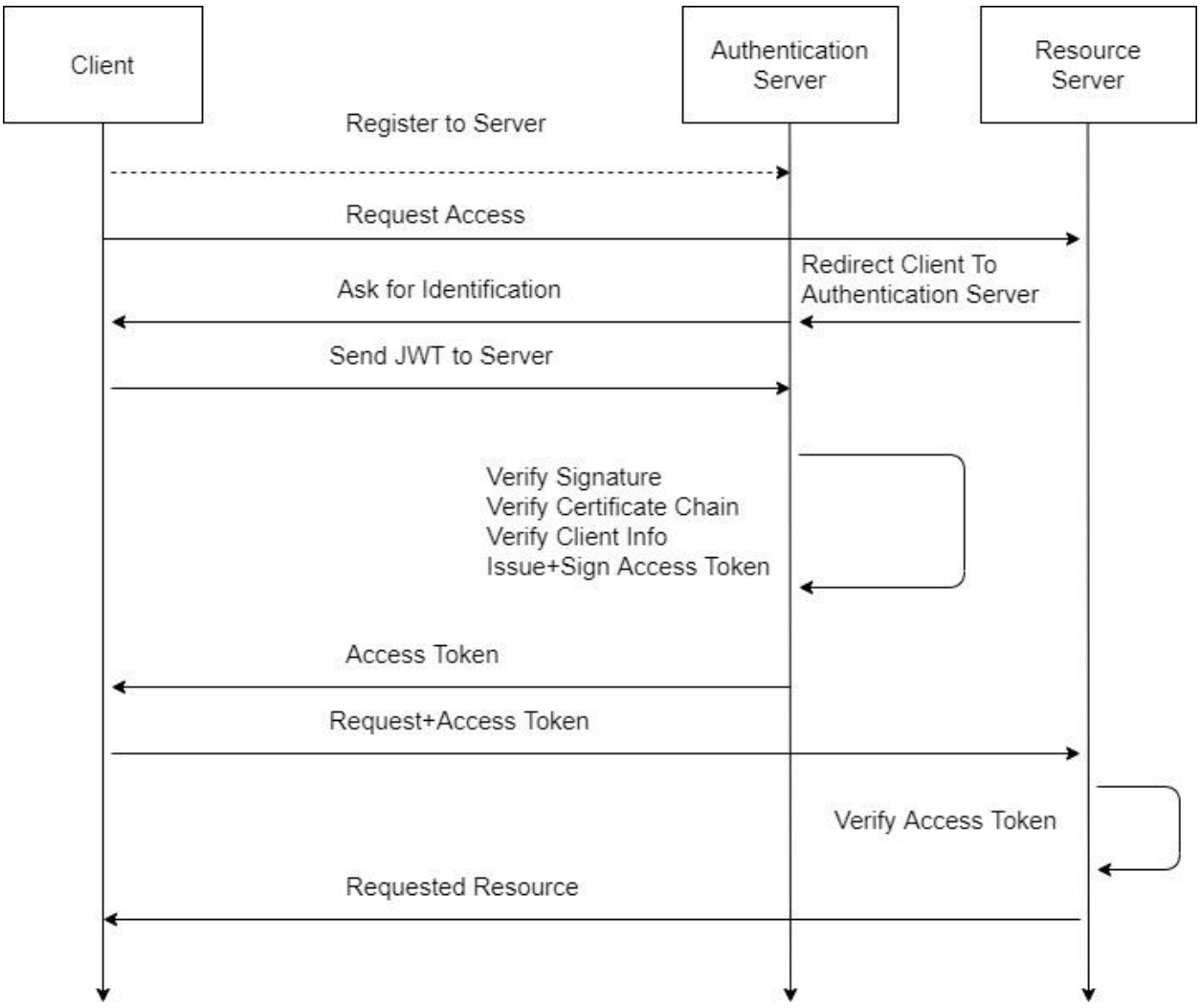


Figure 17: Sequence Diagram of Client Authentication

OPEN INDUSTRY 4.0 ALLIANCE – Bringing a secure Industry 4.0 ecosystem to life

Author:

Nils Herzberg, SAP / Open Industry 4.0 Alliance

The current paper is based on:

WHITEPAPER PRODUCT SECURITY – OPEN INDUSTRY 4.0 ALLIANCE

“Industrial Cyber Security Design Principle – Full Stack Design Reference for Integral End-to-End Cyber Security”

Contributors:

Thomas Greil Voith Group

Matthias Schmidt ifm solutions

Dr Stephan Theis Hensoldt Cyber

and

OPEN INDUSTRY 4.0 ALLIANCE GENERAL WHITE PAPER

Additional information can be found on the website: **https://openindustry4.com/**

1. Introduction to Open Industry 4.0 Alliance

The Open Industry 4.0 Alliance aims to congregate leading industry partners to drive the digitization of the factory, plant and warehouse domains and ultimately create an ecosystem by linking Information Technology with Operational Technology while bridging the divide between operators and manufacturers/OEMs.

The charter of the Open Industry 4.0 Alliance is to institute an alliance of innovative asset manufacturers (including asset digitization enablers) that adopts standards-based common semantic data models to enable the immediate instrumentation of smart assets in the end-to-end production life cycle of an operator while bringing together the required critical mass of industry players. With a vision to simplify the deployment and integration of intelligent assets into the operations of an operator to a near “plug-and-play” level and provide pre-integrated high-value solutions from the Alliance members that can operate with operator-desired architecture openness.

An architecture that is presented by the Open Industry 4.0 Alliance and implemented by its members appears advantageous and is sketched prototypically: an open, scalable ecosystem with the following layers:

- Edge Connectivity (to the world of physical things)
- Edge Computing
- Operator Cloud and
- Central repository for asset information and semantics.

Key principles are open interfaces, an open edge application layer and cloud application layer for the operator of a facility (either locally or in the cloud), data custodianship, role-based authorization for data access and private data and algorithms at every level for each provider and subscriber.

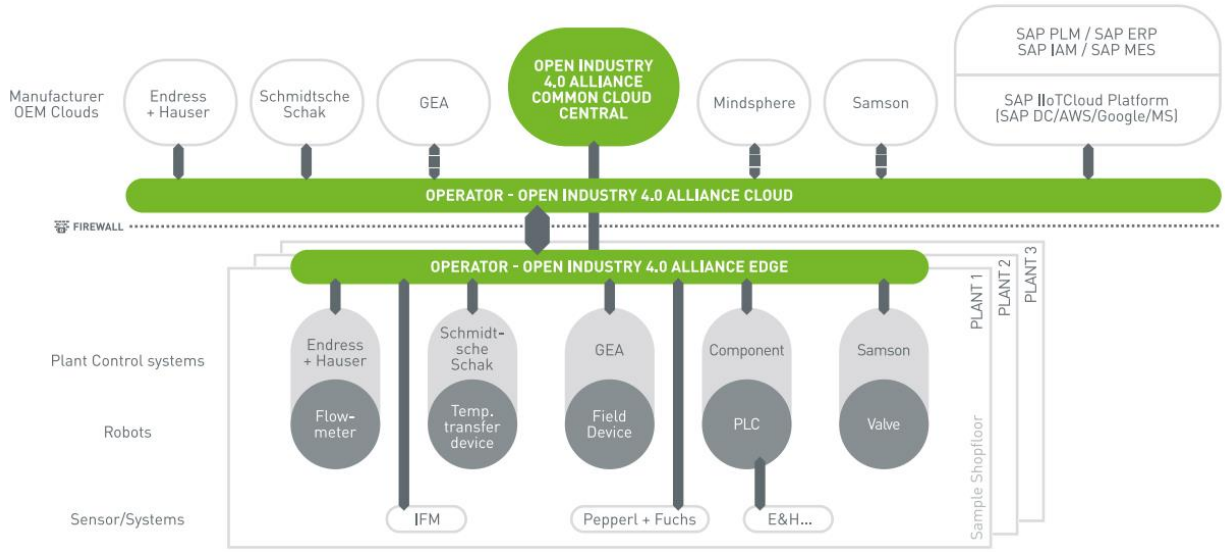


Figure 18: An open yet holistic approach to edge connectivity, cloud computing and asset management is required

The ecosystem of the Open Industry 4.0 Alliance has ONE focus – “Create Customer Value”. In order to achieve this, the ecosystem consists of all the essential roles for driving and enabling digitization of the processing plants, warehouses and factories of customers (operators). The contribution of the ecosystem is the Industry 4.0/IIoT relevant modular solution and professional service offerings. The major roles are summarized as:

- **Operators**: End customers who operate industrial assets in discrete and process industry as well as logistics
- **OEMs/ Manufacturers**: Makers of industrial equipment – production assets, lines, machinery, modules, and robotics
- **Technology Providers**: Those for software (IaaS, PaaS) and hardware (edge devices), IT and OT, automation technology providers (systems, components, sensors, actuators, controls, PLCs) who enable digitization
- **Application Providers**: Companies providing relevant software applications with their industry/domain-specific expertise
- **System Integrators**: Companies offering system integration services in OT (Operational Technology) and IT (Information Technology)
- **Service Providers**: Companies providing services throughout the life cycle of an industrial facility
- **Connectivity Providers**: Companies offering solutions & services for industrial connectivity

Compared with other initiatives on the market, the Open Industry 4.0 Alliance highlights the openness of the proposed approach. The Open Industry 4.0 Alliance design principles for approved solutions are aimed to deliver Industry 4.0/IIoT interoperability amongst solutions from members and enable faster adoption of customers’ digitization goals. The Alliance brings together actors from collaborating and even competing companies to align on common architectural concepts to integrate very differing Industry 4.0/IIoT solutions based on existing standards.

The market reality is that most industrial facilities consist of legacy assets. These assets could have different degrees of sophistication (e.g. analog with or without connectivity capability, digital with or without connectivity capability) to allow them to be connected to the Industry 4.0/IIoT hybrid solutions. The existing lack of interoperability for greenfield and brownfield assets amongst different vendors usually hinders the customer from deriving value out of seamlessly interoperating solutions and leaves the integration task to the customer. With the open, vendor lock-in free solutions integrating multiple standards, the Alliance offers a low-risk option for the operators. The Alliance aims to connect most of the assets in the brownfield to ease the grown complexity in the field and secure the existing investments.

The solutions offered are aimed to address enterprises of any size and support operators to start with a selective scope and grow the scope with time. The solutions and services can be sourced from the operators’ trusted and established business partners or suppliers who are members of this Alliance. Members

provide the semantics of their products through a common asset repository with the aim to offer standards-based high-quality master data to the operators along with it. For an operator to integrate solutions from different vendors, connectivity alone is not enough. Hence these semantics in a common asset repository can be leveraged in building interoperable solution components.

The solution architecture blueprint consists at the start of the collaboration effort of the Alliance of a central common asset repository and management system and semantic ontology, namely the Central Asset Repository in the common cloud central providing the built-in network for collaboration between business partners- operators, OEMs and service providers. The partners target to enhance access and interoperability of assets, applications and services including available ecosystem offerings in the market by leveraging the open, multi-protocol and multi-data semantic approach described above to grow the broadness, multi-ethnicity and collaboration capabilities of the approach.

Open Industry 4.0 Alliance aims at bringing several micro-ecosystems relevant for operators and leverage the individual and joint strengths in technical, commercial and subject matter expertise. Instrumenting industrial production processes demands high-security standards of the measured, processed and stored data. As such, the Alliance understands and supports the desire of customers and asset operators to determine the geography, location and legislation of Industry 4.0/IIoT data and indicators, either locally stored, on-premise, or in local or central cloud systems of their choice.

The Alliance acts as a data custodian: A critical hindering factor for broader success of Industry 4.0/IIoT solutions is the exposure of customers to the B2C business approach of “the customer is the product” established by hyper-scale cloud providers. What is evitable in the consumer markets cannot be the basis for implementation by businesses, as own know-how protection interest and liabilities towards clients’ IP assets build obligations for decision-makers in due diligence of their operations.

The only available solution for that problem is to establish services which guarantee single-sided and clear business models and strictly prohibit hidden agendas with customers and their data for back door exploitation. As a result, a non-negotiable principle of the Alliance is to demand by implementers and service providers to act in this regard as a trustworthy custodian for customer data and IP assets.

2. Introduction to Open Industry 4.0 Industrial Cyber Security (ICS)

2.1 Why is Open Industry 4.0 concerned with Industrial Cyber Security?

The objective of the Open Industry 4.0 Alliance is to establish an open and interoperable Industrial Internet of Things (IIoT) ecosystem involving all Open Industry 4.0 members. Therefore, cyber security is mission-critical for success as well as the acceptance within the industry and among applying customers. To guarantee openness and interoperability, a “security by design” approach is mandatory for robust setups,

systems and applications and reduces the risk for all end user business scenarios. All Open Industry 4.0 members are committed to contributing in their best manner possible to a joint, secure IIoT ecosystem that benefits the diverse customer use cases. Therefore, industrial cyber security is an integral part of the Alliance and stretches across the different layers of the reference architecture. It has the highest priority and is considered within all workgroups as well as the pilot projects of the Alliance in a meaningful and pragmatic way.

2.2 Background and Objective of Open Industry 4.0 Industrial Cyber Security

The number of cyber attacks towards manufacturing companies is increasing at a very high pace. Although a lot of companies still have not been a victim of these incidents, the unavoidable consequences on the business of the affected companies show a huge impact on productivity, availability and costs. This shows that many companies are not prepared for modern cyber risks on all levels of protection. Apart from the growing number of attacks, the amount of connected devices that more and more communicate with each other is also increasing exponentially due to the efforts of digitalization in general and industry 4.0 specifically. Therefore, the possible targets increase and make cyber attacks unfortunately a growing market in terms of economic “success”.

The reasons for this circumstance are manifold. Across industries, operators often have decades-old OT landscapes that lack the security mechanisms of modern systems. As more and more value adding IIoT solutions find their way into those long-established OT landscapes, the operators of those OT landscapes are creating a new attack vector for potential cyber-attacks. However, what’s the solution? Taking the risk into account? Or missing the benefits of value-adding solutions and technologies? What is the competitor doing? Am I losing my competitive advantage if I do not modernize my OT landscape? Surely, many questions come to mind when thinking about this topic. One of the answers lies in the need of a well thought cyber security concept across the underlying IT and OT landscapes. Part of this cyber security concept is a wise selection of OEMs, technology providers, asset suppliers, and service providers whenever an investment in modernization measures is foreseen by the operator. The associated purchase always needs to be aligned with the company’s cyber security strategy. A supplier that is not able to prove its product’s compliance with the operator’s cyber security needs is a security risk for the operator’s business. The Open Industry 4.0 Alliance asserts a clear and comprehensible security concept along the IIoT ecosystem that Open Industry 4.0 members are following. Every chosen technology in the Open Industry 4.0 ecosystem must meet the state-of-the-art requirements of security for encryption, authentication, data protection, and data privacy. Through these measures, the Alliance is seeking to ensure the claim for cyber security in industrial IoT applications and proactively help to protect the operators’ IT and OT landscapes.

2.3 How is Open Industry 4.0 dealing with Industrial Cyber Security?

Cyber security is an elementary and integral part of the basic system architecture for all products developed by the members of the Open Industry 4.0 Alliance. The integral approach towards cyber security is needed due to the layer structure of the reference architecture. All layers have to be included and security concepts need to be coordinated and aligned within the ecosystem.

Luckily, cyber security is nothing that just came into the Open Industry 4.0 mind. It is a task and objective that is already covered by various institutions, networks and associations. Therefore, all fundamentals are already covered by norms, regulations as well as best practices and whitepapers. Due to the deep integration of cyber security in the individual architecture layers, security-relevant functions are taken into account directly when developing solutions. All recommendations and guidelines are based on industry-known standards for similar applications.

The technical implementation is accompanied by an independent committee of experts. This committee, consisting of members of the Alliance, determines the necessary framework conditions and is available to advise all members of the Alliance. The aim of the Open Industry 4.0 Alliance is a comprehensive consideration of all relevant security aspects on all layers of the reference model based on existing norms and standards.

2.4 What are Open Industry 4.0´s deliverables in the context of Industrial Cyber Security?

Due to the current developments in attack scenarios and threats and the associated requirements for security measures, Open Industry 4.0 Alliance faces the challenge of providing secure development and operating concepts.

The solution approaches developed in Open Industry 4.0 Alliance contain basic security aspects according to the current state of the art. As a basis for reliable product development, the recommendations can be adapted to meet industry-specific requirements. Furthermore, measures are taken into account that enables the systems to be integrated into established product safety management systems.

The security functions used in the technical guidelines serve as recommendations for action for future product developments. The application of standardized requirements and the implementation of best practices on the part of the manufacturer result in a detailed platform for safe product operation.

The recommendations of the Open Industry 4.0 Alliance must be checked for the respective purpose when applied. The respective security measures are not absolutely sufficient in every area of application or may even be oversized. When applying the recommendations, it is mandatory to carry out your own risk analyzes and to define the respective safety requirements. In addition, the Open Industry 4.0 Alliance cannot assume

any responsibility for maintaining the respective security level over the desired product life cycle. The processes required for this must be implemented by each user himself.

3. Open Industry 4.0 Alliance Security Reference Architecture

3.1 Roles and Responsibilities in the Open Industry 4.0 Ecosystem

Securing an IIoT ecosystem requires a defense-in-depth strategy diligently followed by various members across the IIoT value chain. The defense-in-depth strategy should be developed and executed with the active participation of various alliance members involved with the manufacturing, development and deployment of IIoT applications, devices and infrastructure.

Amongst the member companies within the Open Industry 4.0 Alliance the following roles can be found:

- Application Provider
- Technology Provider
- Connectivity Provider
- System Integrator
- OEM/Manufacturer
- Operator
- Service Provider

Each role has an individual perspective on the subject as well as responsibility within a secure IIoT ecosystem.

Fehler! Verweisquelle konnte nicht gefunden werden. summarizes on a high level the responsibilities of various alliance members in achieving a holistic defense-in-depth strategy for IIoT.

Table 12: Roles and Responsibilities in the Open Industry 4.0 Ecosystem

Roles involved	Responsibilities
Application Providers: Members providing relevant software applications within their industry/domain-specific expertise	▸ Follow a secure software development lifecycle ▸ Carefully consider open source software components/tools and integrate only if needed ▸ Ensure vendor risk management when outsourcing development activities
Technology Providers: Software (IaaS, PaaS) and Hardware (Edge devices) technology providers who	Software (IaaS, PaaS) providers: ▸ Physically protect infrastructure

enable digitization and members offering solutions and services for industrial connectivity	▸ Ensure all systems are up-to-date with patch management best practices ▸ Monitor and protect against malicious activity ▸ Manage and protect cloud credentials ▸ Audit frequently Hardware providers: ▸ Design the hardware to meet minimum security requirements ▸ Ensure hardware is tamper proof ▸ Ensure secure software updates
System Integrators: Members offering system integration services in OT (Operational Technology) and IT (Information Technology)	▸ Deploy hardware securely, e.g., control access to the hardware with strong authentication and authorization ▸ Separate assets based on criticality using appropriate network security best practices ▸ Ensure a key management mechanism is present to keep authentication keys safe
OEMs/Manufacturers: Makers of industrial machinery, components, sensors, actuators, PLCs and robots	▸ Industrial automation and control system security
Operators: End customers who operate industrial assets in discrete and process industry	▸ Ensure proper supply chain risk management practices ▸ Ensure suppliers provide security assurance for their solutions and comply with internal security standards
Service Providers: Members providing services throughout the life cycle of an industrial facility	▸ Ensure proper life cycle risk management practices ▸ Ensure work methods and processes provide security assurance for customer solutions and comply with customer security standards

3.2 Full-Stack secure Solution Architecture

Based on the claim of the Open Industry 4.0 Alliance, security-relevant functions are implemented based on the following architecture stack. The Security-in-Depth method should enable the user to consider all necessary aspects and implement appropriate measures. In addition to the functional requirements, further non-functional requirements must be considered. These include, for example, product maintenance processes and the integration of security incidents into the corporate communication policy. An inadequate security consideration over the entire life cycle of the product can lead to complete cancellation of the desired protection goal. The security-in-depth approach minimizes the risk but does not eliminate it.

When considering security functionalities, the focus of the respective solution must be considered:

- A pure software application based on a container cannot contain security functionalities of the underlying layers;
- The provision of an operating system provides basic libraries and functions to the overlying layers, but application security is the responsibility of the respective vendor.

In addition, other basic principles relevant to safety should be taken into account in product development. An overview of the errors to be avoided was prepared by MITRE. The Common Weakness Enumerations (https://cwe.mitre.org/) are the most common development errors that can provide a weakness in the code.

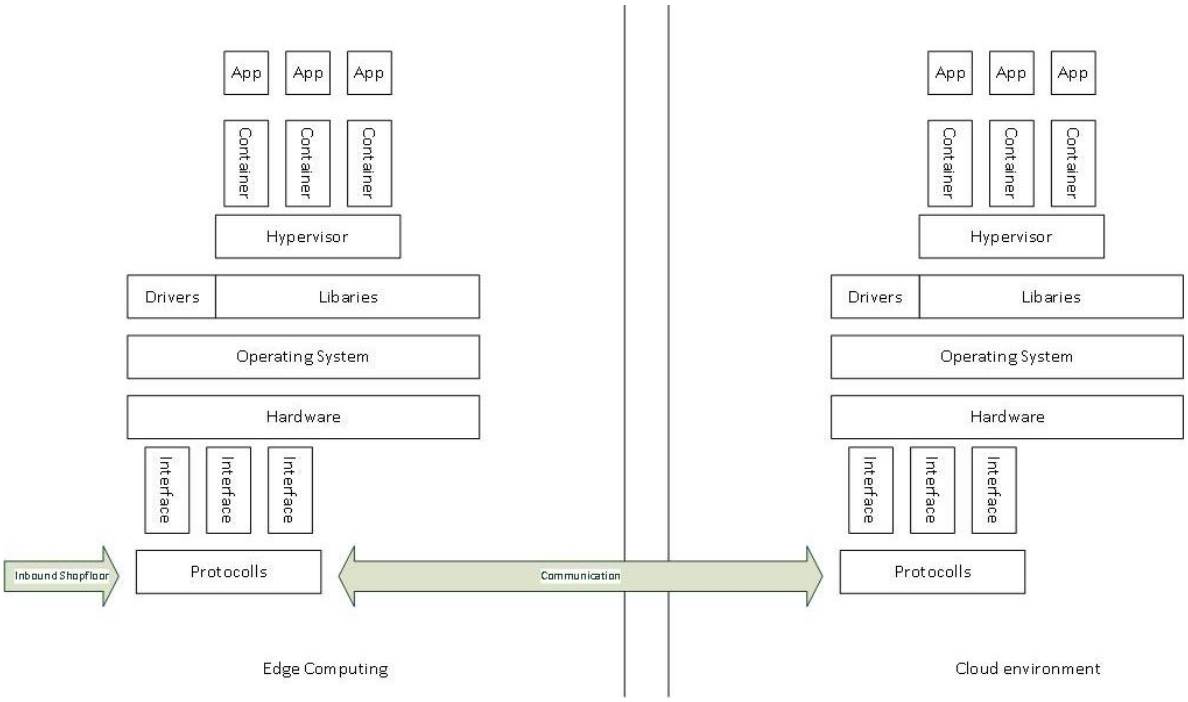


Figure 19: Overview architecture stack

4. Cyber Security Best-Practices, Regulations and Standards referred to by the Open Industry 4.0 Alliance

4.1 Security considerations on Layer 1 and 2

Due to the architecture of the Open Industry 4.0 Alliance, different security requirements are placed on the solutions. On levels 1 and 2, basic security functionalities are required to ensure individual protection goals.

According to IEC 62443-1-1, the following protection goals are defined in subsection 5.3

- Identification and authentication IAC
- Use control UC
- System integrity SI
- Data confidentiality DC
- Restricted data flow, RDF
- Timely response TRE
- Resource availability RA

These protection goals are assigned to a corresponding security level (SL):

- SL 1 accidental misuse
- SL 2 intentional experiments with simple means
- SL 3, like SL 2, but with knowledge and extended means
- SL 4, like SL 3, with complex means and with IACS expertise

Depending on the position in the life cycle to which the SL refers, a distinction is made between:

- SL-T (Security Level target), this SL to be achieved is a result of the threat/risk analysis
- SL-C (Security Level capable), SL, that a device or system can reach when properly deployed and configured
- SL-A (Security Level achieved), the SL achieved and measurable in the overall system

The user of the end device must determine the SL-T by means of a risk assessment. A manufacturer of a terminal device can only identify the SL-C. The manufacturer of the complete system indicates the SL-A achieved in the final. A system is correctly executed if SL-A corresponds to the SL-T.

According to the desired or required security level, functions must be implemented in accordance with IEC EN 62443-4-2.

The implementation of the required technical measures must be extended or supported by processes and measures based on IEC EN 62443-4-1 if product certification by a notified body is sought.

4.2 Considerations about Cloud security requirements (Layer 3 and 4)

In contrast to on-premises or security measures on hardware platforms, other aspects are of fundamental importance in the cloud area. In the various cloud models Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), different requirements are placed on the solution provider based on distributed responsibility. The challenge of distributed responsibility is to consider all factors necessary for the secure operation of the desired model. A misinterpretation or a function that is not considered can, if necessary, cause great damage. Taking into account the full stack, cloud architectures are based on the same model. The provided cloud models make demands on all underlying layers.

To provide technical security functionalities, it is necessary to validate the associated service contracts with the company's own compliance requirements. This includes, for example, the contractual requirements for service providers who perform activities on behalf of the provider. This includes, for example, the operation of the data center (IaaS) or the proper destruction of data carriers.

With regard to the operation of a global cloud solution, measures in the area of data protection regulations must be fundamentally validated. The possibility of storing data outside the desired jurisdiction can lead to massive penalties from the legislator and to claims for damages from customers.

The recommendations of the Cloud Security Alliance (https://cloudsecurityalliance.org/) can be used as a basis for necessary requirements.

If your company is already making efforts to obtain 270xx certification, ISO 27017 can also be taken into account to specify the necessary measures. The 27017 is the extension of ISO 27002 to include cloud-specific factors.

4.3 Requirements for Upstreaming connectivity

A fundamental goal of the Open Industry 4.0 Alliance is interoperability between the individual layers and participants. To achieve this goal, a unified schema for data sources and sinks is indispensable and decisive for the success of the architecture. For this purpose, communication between Layer 1 and the superordinate instances is based on the specification of International Data Spaces in the form of DIN Spec 27070.

4.4 Vulnerability Management System

The use of a vulnerability management system (SMS) is elementary for the security of products. In principle, an SMS can be divided into two components:

4.4.1 Product Security and Incident response team (PSIRT)

Across all levels of the Open Industry 4.0 Alliance reference architecture, it is essential to maintain the solutions throughout their entire life cycle. The challenges of this instance are:

- Detection of vulnerabilities
- The analysis and evaluation
- Removal of weak points
- Publication and communication of relevant information
- Training of managers and employees

During implementation, the frameworks of the "Forum of Incident Response and Security Teams" (www.first.org) have proven their worth in IT. For vulnerability management in industrial components, the framework for Product Security and Incident Response Teams can be used as a basis for implementation. This framework defines the necessary requirements and the corresponding results of the respective field of action.

4.4.2 Secure Software Development Lifecycle

Without a structured and standardized approach to the development of safe products, it cannot be tracked and guaranteed throughout the product's life cycle. In addition, weak points can be tested and eliminated in early development phases. This "Shift-Left" approach saves capacities since the elimination of weaknesses in later development phases is costly and therefore ties up capacities. The use of static application security testing solutions can automatically find weaknesses in builds and provide instructions for fixing them.

Furthermore, the consideration of security measures already in the product planning phase is necessary, since architectural requirements can be set in advance. This way, a subsequent adjustment can be avoided.

In recent years, various approaches have been established in the area of Secure Software Development Lifecycle. These include the SDL from Microsoft (https://www.microsoft.com/en-us/securityengineering/sdl) and the SAMM from OWASP (https://owasp.org/www-project-samm/).

Table 13: Relevance of Norms and Standards regarding Open Industry 4.0 Layer structure

Norm, Standard / Layer	Layer 1 - Devices	Layer 2 - OEC	Layer 3 - OOC	Layer 4 - CCC
IEC 62443-4-1 (organizational focus)	x	x		
IEC 62443-4-2 (device focus)	x	x		
OWASP		x		
SSDL - Secure Software Development		x		
DIN SPEC 27070		x		
PSIRT		x		x
IEC 27017			x	x
Cloud Ecosystem			x	x
CSA requirements			x	x

The norms and standards apply to the different layers of the Open Industry 4.0 setup. Nevertheless, a seamless interaction as well as interoperability is targeted with the combined approach along with the layers. The order of importance and suitability for Open Industry 4.0 compliant products follows the following listing:

- Officially available norms and standards from organizations, e.g. IEC, DIN
- Recommendations from vendors
- Well-Known Best Practices (can but must not be vendor-independent)

5. Open Industry 4.0 Alliance security compliance requirements

Due to the different requirements and purposes of the products, it is not possible to define the necessary security functions. The generalization of functions can lead to an oversizing of the scope or an underestimated requirement can lead to weak execution.

Basically, and decisive for the security requirements of products is the recognition of the necessity and the willingness to accept the effort and thus the costs for secure products. When developing safe components, the challenge lies in the above-mentioned safe development process and the maintenance of integrated solutions over the entire life cycle. The maintenance of the life cycle of a product also includes checking the implemented functions by regular penetration tests. The requirements of the Open Industry 4.0 Alliance include the following requirements.

5.1 Security requirements for edge computing devices (Open Edge Computing Platform)

As a component manufacturer in the field of edge computing, an SL-C 2 of the 62443-4-2 should be aimed for. The focus of the Open Industry 4.0 Alliance is on provisioning containerized applications and does not place any direct demands on the security of the underlying levels beneath these applications. However, general requirements about the environments will be made. It should be in the own interest of the component manufacturer to evaluate and integrate the necessary measures for the other levels in the product design and the development process.

5.2 Requirements for Cloud-based solutions (Open Operator Cloud and Common Cloud Central)

In the area of cloud-based solutions, the requirements for secure processes must be implemented at the highest level both during the development and operation of the solution. The attack vectors and the associated damage potential must be comprehensively considered by the provider of the solution and appropriate measures implemented in conjunction with the service provider. In addition to this, data protection relevant processes and measures must be developed.

At the time of writing this white paper, there are no legally defined requirements for security in industrial components. Due to this fact, the security requirements of the Open Industry 4.0 Alliance are based on self-declarations of the respective manufacturer.

PLATTFORM INDUSTRIE 4.0

Conference Volume