Cybersecurity for Manufacturing Environments

Report from the Workshop on
Cybersecurity for Manufacturing Environments

held on 17th October 2018, BluePoint Centre, Brussels, Belgium

Organised by the European Commission, DG CONNECT
Unit "Technologies and Systems for Digitising Industry",
the European Factories of the Future Research Association (EFFRA), and the
European Cybersecurity Organisation (ECSO)

https://bit.ly/DigindEU – https://www.effra.eu – https://www.ecs-org.eu

Rapporteur: Ulrich Seldeslachts, Anakyn bvba

Disclaimer: The views expressed here are those of the workshop participants and do not necessarily represent the official view of the European Commission on the subject.

Executive Summary

A public workshop on cybersecurity for resilient manufacturing environments was held in Brussels, on October 17th 2018, organized by DG CONNECT, ECSO and EFFRA. Its objectives were: a) drawing attention to cybersecurity challenges in manufacturing and identifying potential gaps, b) bringing relevant stakeholders together, and c) to raise awareness on existing solutions, activities and research agendas. Cybersecurity challenges brought by all participants were mainly related to existing infrastructures (legacy systems, connectivity and applications), smart manufacturing developments (Industry 4.0, massive amounts of data, increasing automation, IoT, autonomous systems, integrated and autonomous manufacturing, digital platforms), the ecosystems (integrating supply & demand) and the human factor (involving operators, cybersecurity experts and the IT – OT discrepancies). Existing challenges are complex, involve multiple stakeholders with particular impact on the manufacturing operations, involve processes, people, procedures and technologies, with potential impact reaching far beyond the boundaries of the manufacturing environment. While many existing cybersecurity solutions exist, the workshop aimed to identify some specific approaches related to the manufacturing cybersecurity and resilience challenges.

The current role of governments is in setting out policies and strategies supporting the digitalisation of the market, regulating the market by setting out legislation (CIP, NIS, GDPR, …) and influencing sector regulations, by issuing operating schemes and providing licences, and by financing research and development and stimulating innovations.

A selection of nine European and regional research and innovation projects, from cybersecurity, advanced manufacturing and critical infrastructure protection, three companies specializing in the domain with dedicated solutions to manufacturing and industry, and a series of clusters presented their experiences in current development of cybersecurity in manufacturing environments. Project activities are oriented in influencing cybersecurity in different aspects of the challenges: identity and access, network, transmission and communication security, the use of encryption, considering personal data protection and privacy, situational awareness and decision support intelligence applications and systems, providing mechanisms increasing trust in components, integrations and operations, building frameworks for applications, systems and developments, integrating cyber and physical, focusing on risk processes and looking both to legacy and preparing for future directions. Most of the developments aim towards applied cybersecurity solutions, resulting in higher TRLs. There is a general tendency towards building open source applications and towards existing standards.

Only a fraction of the numerous cyber security solutions available in the market are represented. They present solutions specifically targeting the industrial control system environments (ICS), targeting industrial automation systems and industrial legacy environments in the first place. Attention is drawn to the importance of innovative European companies that have been developed with the support of European research funding. It is noted companies choose not to focus into some industrial sectors or environments such as critical infrastructures, because of restrictions, specifications and subsequent liabilities from a regulatory perspective limiting their commercial interest. Many technologies being applied are not new (authentication, zoning, DMZ, SIEM), but by combining them for an industrial environment, focusing on operations, they become very practical and are likely to cover quickly 80% of the basic requirements. A wide range of managed expert services is also available. Automation technology and application providers are making additional efforts to provide cybersecure systems, on the basis of self-assessments and joint self-regulation.

During the session a number of topics were identified as relevant and specific in relation to security and resilience for manufacturing environments for further follow-up, and for specific research attention: Operator Resistance, Devices, IT vs OT, Real Time, Fast & Stateful, Lower level

Communication Protocols, Legacy, Impact, Automation & Agility, Safety & Security, Systems of Systems, Ecosystem, Collaborative manufacturing and Legal.

ECSO's work on its strategic research and innovation agenda (SRIA) is organized around ecosystems, vertical application domains, trustworthy transversal infrastructures and technical priority area and includes a specific chapter dedicated to the developments of Industry 4.0. An earlier exercise by *ConnectedFactories* together with EFFRA on the basis of the 2017 SRIA had already identified emerging technologies as relevant for cybersecurity for Manufacturing and other Industrial demand. It will continue to develop and maintain a structured glossary and mapping framework comprising a specific component on cybersecurity for digital platforms amongst business cases, scenarios and technologies.

The closing break-out discussions and conclusions with all participants identified some residual threats: manipulation of signals, a false sense of security, operators awareness and ignorance and behavioural change. A call to further differentiate and isolate types of data, systems and cybersecurity capabilities and measuring all processes continuously whilst also including physical processes in the information analysis, was noticed. In view of the changing dynamics in supply chains, cybersecurity and security measures should consider broader ecosystems more and use good practices from other vertical domains.

Table of Contents

1. Introduction

On October 17th 2018, the European Commission's Unit "Technologies & Systems for Digitising Industry", the European Factories of the Future Research Association (EFFRA), and the European Cyber Security Organisation (ECSO) jointly organized a workshop Cybersecurity for manufacturing environments. The workshop[1] was set in the context of the European Commission Research & Innovation action ICT-08-2019 on "Security and resilience for collaborative manufacturing environments"[2].

2. Background

EFFRA and ECSO had already shared their visions and met a number of times to align their visions in the past year. As already indicated by EFFRA in 2016 in the "Factories 4.0 and Beyond" document[3], the idea is to develop a more focused H2020 call topic in the domain, meanwhile the cPPP (contractual Public Private Partnerships) on cyber security was established, with the creation of ECSO (European Cyber Security Organization). In the meantime, ECSO developed its own Strategic Research Innovation Agenda, where Industry 4.0 is one of the most relevant verticals deserving attention.

The concept of the workshop was developed together with DG CONNECT to bring projects, people and expertise together from both domains (manufacturing developments with a perspective on cyber security and cyber security research, also related to manufacturing).

3. Objective

The main objective of the workshop was to draw attention to the fundamental importance of cybersecurity challenges in manufacturing environments. The second objective was to bring the relevant stakeholders around the same table: end-users from manufacturing and cybersecurity solution providers to understand the needs and requirements and match them with the current cybersecurity solutions available on the market and best practices to identify potential gaps and future research directions to address the needs of the sector. The third objective was to raise awareness of the cybersecurity issues and priorities already identified and highlighted in the ECSO Strategic Research and Innovation Agenda (SRIA)[4].

In light of the ongoing digital transformation of industry and the Digitising European Industry (DEI) initiative[5], in a nutshell, the workshop aimed to provide:

a) an insight in needs and requirements for secure and resilient manufacturing environment,
b) a forum to understand the implications of the digitalisation of the industry and convergence of IT (Information Technology) and OT (Operational Technology),
c) the state of the art both from manufacturing research and cybersecurity research side, and a high-level insight of the state of the art of some of the commercial cybersecurity solutions available,
d) current and future key enabling technologies and cybersecurity approaches,

[1] https://www.effra.eu/news/challenges-explored-cybersecurity-workshop
[2] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/ict-08-2019.html
[3] https://www.effra.eu/sites/default/files/factories40_beyond_v31_public.pdf
[4] https://www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf
[5] https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry

e) how research and innovation projects and European or International Initiatives are already addressing cybersecurity in manufacturing,
f) future requirements and pathways towards secure-by-design manufacturing environments and better integration of cybersecurity in existing systems,
g) what specifically differentiates cybersecurity for manufacturing and how manufacturing can influence cybersecurity developments, and finally
h) what gaps can be identified and need specific attention from research, development and innovation.

4. Format

The public workshop was held in Brussels with participation from research projects from previous Factories of the Future calls, other European projects from both manufacturing and cybersecurity related domains, regional projects and initiatives, industrial cybersecurity services and solutions vendors, and associations and cluster organizations. Different organizations were asked to present their past and current experiences and future works, by means of highly focused presentations and short Q&As. Research projects presented their results and were asked to analyse on a high-level basis a mapping of their work to the ConnectedFactories[6] Security Framework for Digital Platforms. The day ended with an interactive workshop on few scenarios focusing on challenges and solutions for cybersecurity in the context of the factory floor and cybersecurity in the context of dynamic supply chains.

EFFRA and the EC outlined some of the challenges related to cybersecurity. Chris Decubber (EFFRA) opened the workshop, gave an outline of the day, and introduced cybersecurity as a barrier to digital adaption. Already indicated by EFFRA in 2016 in the "Factories 4.0 and Beyond" document, the idea developed to cooperate on cybersecurity with ECSO. The European Cyber Security Organisation (ECSO) is the industry-led contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). EFFRA and ECSO met a number of times to align, and the idea developed together with DG CONNECT to organize a dedicated workshop to bring together projects, people and expertise from both domains of expertise. By bringing projects and solutions / technologies together and challenging them on how they address security, the idea was to bring cybersecurity for manufacturing environments a step forward. With the research and other initiatives on cybersecurity Roberto Cascella (ECSO) also presented a quick overview of the ECSO association and main achievements in the different WGs addressing the industrial policy that were of interest to the participants.

EFFRA and ECSO had already been cooperating to support a more structured discussion among the manufacturing research and innovation community about security, in particular via the ConnectedFactories Coordination and Support Action activities[7].

On behalf of the European Commission, DG CONNECT, Unit Technologies & Systems for Digitising Industry, Cristina Sandoval and Arian Zwegers welcomed the participants. The EC supports interactions among the PPPs and would like to use the workshop to understand **what is specific about cybersecurity for manufacturing environments.** Mr Zwegers related the workshop also to the

[6] https://www.effra.eu/connectedfactories

[7] See the security session and presentations at the ConnectedFactories event on 5-6 February 2018 - https://www.effra.eu/events/5-6-february-2018-connectedfactories-dissemination-event and also section 11 of this report.

European Cybersecurity month of October[8], the annual EU's awareness campaign to raise awareness of cybersecurity threats, and which is linked to the global cybersecurity month awareness campaigns.

The day before the workshop, the European Commission opened the call for proposals for topic *"Security and resilience for collaborative manufacturing environments" (ICT-08-2019 in the LEIT-ICT work programme).* The topic seeks to develop tools and services guaranteeing an adequate level of data security for collaboration. It calls for practically usable solutions to be taken-up by industry to significantly increase cybersecurity levels in daily operations for manufacturing facilities and other actors in the value chains.

The workshop sought to further elaborate on the call by specifying the security and resilience issues for manufacturing, as a possible basis for excellent proposals.

5. Challenges for Cybersecurity in Manufacturing: click here to kill everyone

An overview of recent related developments was presented: the imaginary perspective of having someone at the other side of the world turning the lights on and off is an indicator of potential vulnerabilities for an industrial context. Examples of cases of industrial espionage, business disruption, ransom, forgery or plain theft of data up to the relation to cyberwarfare as a result of cyberattacks, physical intrusions, identity theft and impersonation, exploitation of vulnerabilities and DDOS, were given throughout the morning and day. Their potential impact ranges from a simple disruption of a device, through a machine up to a factory, its personnel and a whole ecosystem of an industry or even diplomatic incidents between countries. Presenters indicated the challenges related to the attribution of incidents (from simple misconfiguration and human errors to state attacks) and the challenges related to lack of timely responsiveness were touched upon. Reference was made to the *Cyber Security for Manufacturing report* by *EEF*[9]. According to this study, "almost all manufacturers have some technical protections in place", but "this isn't always comprehensive". The report indicates that "half of manufacturers have suffered from cyber-attack", and "only six in ten manufacturers include cyber-security on their risk register".

With experiences from the field for over a decade, *Stephen Smith* testifies from a very pragmatic point of view that **any device** and system **can be tricked**. He addresses the **prominent difference between IT** (Information Technology) **and OT** (Operational Technology – production & automation technology). Some impediments in addressing cybersecurity in manufacturing environments have to do with the typical challenges related to Automation Systems such as system lifetime, impact on production, modification of systems and technologies or programming instructions. Changes in the systems, i.e. due to software or operating system updates, could very well lead to **instability**. Anti-malware solutions, for instance, temper with the operating system and could cause harm to the operations. From a risk perspective, there are chances to **loss of integrity**, due to tempering with the systems and the data.

In many cases **threats originate from a human error**. Misconfiguration, software coding errors and connectivity are typical human errors, which sometimes could lead to security holes. Other threat sources such as hackers and terrorist threats could be avoided by reducing the impact of the human errors.

With the **ongoing trend of increasing automation** in mind, the current industrial attack footprint is therefore growing exponentially. The **number of cybersecurity experts and organisational solutions**

[8] https://cybersecuritymonth.eu/
[9] https://www.eef.org.uk/~/media/abea76a878164765af0c4b47f90fb3ec.pdf?la=en

such as integrating cybersecurity best practices in the industrial process **are scarce**. The gap to solutions for potential threats is growing.

Companies and project representatives jointly acknowledge that cybersecurity is very complex, that it requires a continuous effort and more structuring. Overall, cybersecurity in information technology (IT) is more advanced than in operations technologies (OT). Experiences from the field show that automation machines are being delivered with **viruses**, **airgaps** are being bridged, manufacturing **data is flowing beyond company borders,** and **remote access** to industrial machines is enabled.

In operational environments where legacy ISA-95 automation has been in place, legacy security was based on shell security. When looking towards digital transformation like in the Productive 4.0 project[10] with Volvo Trucks, tons of holes were found in these systems. A focus is needed to a few functionalities, such as the new workstations migrating to IoT and Software as a Service. This requires a systematic risk approach.

Looking towards future challenges, the ECSO working group WG3 on vertical domains developed a "*Sector Report: Industry 4.0 and ICS"*[11]. Key learnings from this group do not focus on identifying research priorities, but more on security itself, challenges, sectorial needs and fostering productivity and protection against cyber-risks. The group identified the **digitization of the industry**, **datalakes across the whole supply chain, ensuring resilience** and **new data driven business models** as key challenges moving forward. *Adrien Becue* is Head of Research and Innovation for Airbus Defence & Space Cybersecurity and chairing the ECSO subworking group 3.1. Some trends towards Industry 4.0 include the use of edge & cloud computing, the use of Artificial Intelligence (AI), Augmented Reality and Virtual Reality (AR/VR), cobots & robots, additive materials (3D printing) and the vast use of sensors and wireless technologies. Cybersecurity requirements have been drawn from future scenarios for manufacturing environments on the basis of ongoing developments, similar to the ones developed by EFFRA. The hyper-automated plant, the customer-centric plant, the e-plant / mobile workshop and the learning factory present cybersecurity challenges beyond the ones already known today. As manufacturing companies are adapting their business models towards more **service and data driven** revenues and costs, such developments demand increased attention for six key areas of cybersecurity: 1) the safety – security convergence, 2) securing industrial IoT both from a device, system and platform perspective, 3) intrusion and anomaly detection in Industrial Control Systems (ICS), 4) managing cyber-physical threats as an organization, 5) managing organisational and behavioural changes, and 6) ensuring security throughout the value chain and throughout the production cycle and lifetime of the product. Manufacturing environments should have a cybersecurity vision, which entails a **roadmap for cybersecurity of safety-critical systems.**

6. Government Roles and Interventions

Governments can intervene by issuing regulations preventing things that could cause harm to citizens and protecting the public. Regulations can support protection in places where needed. These can take various forms, such as regulating manufacturers, integrators and operators, by issuing operating schemes and providing licences. Governments can also intervene by financing research and development, stimulating further innovations in the domain, or support self-regulation.

Government intervention should prevent manufacturers from losing data and money, potentially losing lives, from operational disruption, supporting interactions and innovations, detecting and

[10] A description on the project is in the State of the Art section of this document, under the list of projects.

[11] http://www.ecs-org.eu/documents/uploads/industry-40-and-ics-sector-report-032018.pdf http://www.ecs-org.eu/documents/uploads/industry-40-and-ics-sector-report-032018.pdf

preventing crime, while at the same time continuing to support the further growth and development of the European Digital Single Market.

Earlier initiatives related to the development of the Cyber Security contractual Public Private Partnership in 2016. These brought together the European Cybersecurity Industry, Member States' representatives, Regions and Research Community to drive the European Cybersecurity research agenda, support skills development, support industrial cybersecurity development, and align on certifications amongst many other topics. Today, ECSO brings together more than 241 organisations. In 2017 the European Commission launched the Cybersecurity Act[12], aiming towards continuing and enforcing ENISA as the European Cyber Security Agency and setting a certification mechanism for components, software, systems and services, which is currently being further debated. In 2018 both GDPR and the NIS Directive (Directive on security of network and information systems) were transposed into national law and came into effect throughout the Member States.

Recent initiatives from the European Commission were to support a strong cybersecurity in Europe, by developing a Network of National Coordination Centres, building on the development of National Competence Centres, the Competence Community and the European Centres of Excellence.[13] Ongoing are the development of the proposed Cybersecurity Act[14] on the ENISA agency *(today the European Union Agency for Network and Information Security)* as the EU Cybersecurity Agency and on Information and Communication Technology cybersecurity certification. While these policy proposals are at the end of 2018 being debated amongst industry, European Member States and within the European Commission, it can be expected that they will have a major impact on Cybersecurity in manufacturing and industrial environment all together.

These include ongoing works in the domain of certification and standardization, specifically in the domain of improvements on cybersecurity and on the roles from government. Through the participation of Member States' representatives, governments can play a significant role in international standardization bodies such as ISO, IEC, CEN/CENELEC, and ETSI.

Reference was also made to publications by *ENISA* as a reference architecture in the concept of Security by Design, by Default, Security through Life, and Verifiable Secure in the *Baseline Security Recommendations for IoT*[15] and – published after the workshop – the *Good Practices for Security of Internet of Things in the context of Smart Manufacturing*[16]. Other reports mentioned were the Gov.UK *Code of Practice for Consumer IoT Security*[17] and the Industrial Internet Consortium's *Internet of Things Security Framework*[18].

7. State of the Art of Cybersecurity in Manufacturing

A selection of nine projects, three companies and a series of clusters presented their experiences in cybersecurity in manufacturing environments. This selection is by no means aimed to be complete, but is meant to be a significant representation of the state of affairs and state of the art.

[12] https://ec.europa.eu/digital-single-market/en/cyber-security

[13] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf

[14] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3436811_en

[15] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

[16] https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

[17] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747413/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

[18] https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

As a first indication, FoF (Factories of the Future) projects focus primarily on their challenge as R&D projects related to factories of the future, rather than security. Existing factories already operate some forms of physical security and cyber security. The ISA-95 automation model drives an approach based upon additional shells to provide security, which is a traditional approach to legacy systems.

Some projects add additional layers such as **secure local clouds** requiring **authentication** (AAA-principle), **network access control,** and **encryption** on the network transport layer. Technologies such as role-based access control (RBAC) and next-generation firewall (NGF) that have already matured in ICT-environments and that are applied on the application layers have not been implemented yet into manufacturing production environments. The increased use of web applications and open source technologies allowing for web applications require additional layers of security and monitoring of the situation. The challenge is not only in applying these technologies into industrial context, but to deploy these in an environment that still allows for many other systematic vulnerabilities. The higher levels of cybersecurity for ICT-systems for applications can be evaded. Analogy can be made with a highly secured house with the latest and greatest lock system, but where the backdoor is constantly open with the keys under the porch.

Most organisations have **multiple projects in the domain of advanced manufacturing** with **forward-looking scenarios**. Some of these projects include cybersecurity activities, and within the organisations, these cybersecurity activities are being re-utilized and further advanced in other projects. Some projects consider the challenges related to the changing business relationships across the value chain, amongst multiple suppliers and manufacturers. *IT'M Factory* has installed autonomous vehicles, cobots, digital twins, VR/AR, fixed & wireless communication technologies and indispensable software such as ERP for advanced controls. In ValueChain 4.0, a **framework** and a derived **event-driven middleware** allows for inter-enterprise coordination, by means of an *inter Enterprise Services Bus (iESB).* This bus includes cybersecurity measures for prevention of OT threats and attacks by means of continuous monitoring and remote attestation of IIoT. In *ANASTACIA* a framework for security development with distributed trust & security for **IoT** with **cyber-physical system** based environments is being developed. It tries to describe configuration and define **security policies** and **security properties** for the infrastructure. The higher level policies have been translated into medium level, in order to connect concrete nodes. Independent physical sensors – those connecting with other public networks LoraNet, Sigfox, …– remain a challenge for having them fully integrated.

Many cybersecurity technologies being developed **for factories of the future** get to **a higher than usual TRL** (technology readiness levels 5 – 6), due to the fact that they should be implemented and installed early on in the integration process. These security by design approaches are highly recommended. Experiences and validation have happened in multiple sectors and factory processes. This is also related to the fact that most technologies being developed under the projects consider open source components and technologies for their own platforms.

Challenging for research activities and innovative products and services overall, due to the challenges related to the requirements of certification of production systems, is the **design and development process** in itself. How software is being built (and the use of open source components), the costs and prices related to software development methodologies are less important than the functionality of a particular solution. This is a general challenge in current software development and security engineering, but especially challenging considering the high availability demand of production processes. In *eITUS* an analysis on safe robotic systems is investigated through *RobMoSys,* involving the industrial automation sector. In *DEFENDER*, specific requirements for **Critical Infrastructure Protection** are considered.

Most of the technologies in the presented projects have been developed with and in **Open Source**, allowing the reuse and further enhancement of components, platforms and other developments.

A specific *Arrowhead Framework* is **requiring systems and devices for vetting, onboarding and certifications**. In *ValueChain 4.0* remote attestation of IIoT is taking place to prevent OT attacks. *Productive 4.0* is trying to take into account monetary transactions next to instructions and data on the production and logistics of products. Organizations that have established supply chain agreements and track production progress consider including business transactions upon movements of goods. For inter- and intra-factory scenarios, *Composition* is using current available standards such as OAuth2.0, OpenID and SAML 2 & XACML 3.0 for authentication, a common authorization (EPICA) and attribute based access control. Reputation is therefore depending on digital signatures issued by project partners. Communication over **RabbitMQ** enables the authentication and authorization, for specific applications, over http. Efforts are being undertaken to securely configure the **MQTT** broker, with the use of agents. As **transmission layer security** communication protocol **TLS** is being applied, assumption is made for both higher level communication protocols stateless transmission up to near real-time. *ANASTACIA* utilizes **Openflow** for **SDN** and sets up distributed access control for a Broker server connecting wireless IoT sensors and actuators. Its components includes **Virtual Network Functions (VNF)** and **Network Functions Virtualization (NFV).** *IT'M Factory* considers continuous vulnerability assessments and points to existing exploitable Linux boxes and flaws in the Sigfox and Loranet transmission protocols.

Reference is made to the components available with FIWARE, where some of the projects already participate in and contribute open source components to.

The continuous assessment of compliance and security is an ongoing development on the basis of initial analysis and Measurable Security (& Safety) **Indicators** (MSI). While not everything can already be measured, *SEMI 4* considers taking into account available indicators and improving from there. This includes the capability of secure boot, capabilities of end to end secure communication. These indicators provide stronger evidence from insurance and **compliance** perspective. The use of **security agents** needs to be integrated in the process in order to be in line with updates of the system.

Certification schemes are being developed for Cyber Physical Systems in *AMASS.* Some projects already have to cope with existing regulations (e.g. *DEFENDER).* In these cases system-wide level security should also be applied, e.g. the inclusion of the **human factor**, by training people on different levels, and considering a **Cyber-Physical Social System (CPSS)**, also driven by users.

In these cases, attention should be paid to a **false sense of security**. When systems have been further secured, they still require continuous assessments, especially in an end to end security architecture.

Security Analytics for industrial platforms is being investigated on top of Industry 3.0 and 4.0 systems, on the basis of unified security analytics capabilities under the perspective of vulnerability assessments and ICT security. In *Cyberbasque*, the Unified Factory 4.0 Security Analytics Platform is developed. Its purpose is the monitoring of the factory on different aspects in a harmonized way from embedded security. This mainly focuses on Industry 4.0 technologies and is challenged on dealing with Industry 3.0 technologies. These include for instance the assessment and control of different assets and continuously assess cybersecurity. The actual tool is monitoring. The *analyticsOT* network of *ValueChain 4.0* considers the inter-Enterprise view. *Composition* develops the integration of cybersecurity data with physical world simulation and planning data, in order to achieve a single Information Security Management System (ISMS). Multiple companies involved are sharing their data, following a specifically developed cybersecurity framework, in an inter- and intra-factory scenario. The *XL-SIEM* agents collect security intelligence from different locations, from a business perspective. In *DEFENDER* multiple data sources and logs are being considered – as many as possible from what already is available – in order to process an integrated cyber-physical view as tool for incident management. Indicators include **access control event detection**, **unauthorized SCADA access**, **abnormal data flows** and **SCADA network events**. A ***Fusion centre*** will correlate events, utilizing

machine learning to provider further intelligence. To this, it adds the physical part and the humans in the loop as additional sensors. Attention is paid to how much of the specific SCADA instructions and subsequent security events can be generalized. In *ANASTACIA* an **orchestration pane** includes real components, existing Common Vulnerabilities and Exposures (CVEs), security properties, firewalls, databases and their respective deployment situations and configurations as part of the process. That also includes **enforcing** next to monitoring. It considers the **lifecycle of cybersecurity threats**, monitoring also changes (which could be both relevant for denial of service (cyber threats) and building entrance (physical risk)). An idea for a final goal is to evolve from Situational Awareness to a **Decision Support** system, by bringing things together.

The **security frameworks considered** follow a traditional information security perspective of CIA (Confidentiality, Integrity, Availability). In some cases also ISO 27k, NIST 800-171 or 800-53 and IEC 62443 have been considered, including the parts on control on removable media. Many projects report their lack of practical guidance: “how to link to operations in a manufacturing environment”.

The concept of **End to End** cybersecurity for Factory 4.0 manufacturing processes in line with different manufacturing scenarios (plug & produce / modular assembly cells, autonomous / transportation & logistics, safe human-robot collaboration, digital twin / real factory) is being considered in *Semi 4.0*. The project considers all components in the chain, such as industrial devices, communication infrastructure and assured data paths. In this case, **agents** check whether the Measurable Security Indicators are being met. Real-time analysis is performed in *REDEC.* Results from SEMI 4.0 are reported against overall compliance levels and information being aggregated. **Scenarios** are emulated testing the security of the overall architecture. The *CEI laboratory emulator* from *DEFENDER* is used for cyber & physical security testing.

Next to manufacturing for **information technology** *(Semi 4.0), e*xperiences are being derived from **automotive** sectors *(FAR-EDGE),* and **electricity production** *(REDEC).* Specific protocols for specific devices are being considered in the latter, also taking into account standards and regulations. Together with systems manufacturers, new algorithms for cyber-attacks are being evaluated for energy sub stations. Attention is being paid to electricity production, not energy as a whole.

Industry 4.0 technologies and digital platforms are being developed **with a cloud architecture and app-concept** (including Appstore) in mind. These are taking into consideration some of the legacy back-end infrastructures, but generally lack the integration on the development and integration process, facing challenges with certifications.

Autoware particularly considers **safety** of manufacturing systems, also in relation to security. *ANASTACIA* tries to apply a holistic dynamic perspective on security & **privacy** *(DSPS).*

The concept of a **distributed ledger** and **blockchain technologies** are investigated as a solution for supply chains and product lifecycles, with interactions on multiple applications and for collaborative coordination. Certifying providers on the quality of raw materials or energy management are evaluated *(EuSkate)*. Other concepts include Trusted Data Sharing models. Agreements and achievements are being logged in the ledger to provide for a trusted stakeholder network of local clouds. Multiple interactions between the entities in the ecosystem utilise the public network to communicate, using authentication on the gatekeeper and gateway.

The following projects had a representation (alphabetical order):

3IF.be & 3IF Fieldlab:	Industry Digitalization program in Flanders and fieldlab on Condition Based Maintenance
Arrowhead Framework:	AAA and certification for applications

AMASS:	Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems
ANASTACIA:	Advanced Networked Agents for Security and Trust Assessment in CPS / IoT Architectures
Autoware:	Autonomous Automation
Boost 4.0:	Big Data for Connected Smart Factories
Composition:	Ecosystem for Collaborative Manufacturing Process – Intra- and Interfactory Integration and Automation
ConnectedFactories:	Cybersecurity framework for digital manufacturing platforms
Composition:	Ecosystem for Collaborative Manufacturing Processes – Intra- and Interfactory Integration and Automation
CyberBasque 4.0:	Connected IT/OT
eITUS:	Experimental Infrastructure Towards Ubiquitously Safe Robotic Systems using RobMoSys
EuSkate:	New blockchain based technologies for interoperability and collaborative coordination in Basque Country Industry
FAR-EDGE:	Edge automation security
IT'M Factory:	integration of digital technologies and new organizations
Productive4.0:	Supply chain and product life cycle security
REDEC:	Cybersecurity in Electric Networks
SEMI 4.0:	Power Semiconductor and Electronics Manufacturing 4.0
ValueChain 4.0:	Enabling platform of business processes and dynamic contracts through servitization of the value chain

8. Perspective From Industrial Cybersecurity Solutions for Cybersecurity in Industrial Systems

There are numerous cybersecurity solutions available covering many different aspects of cybersecurity from encryption and authentication to security management platforms and security incident analysis. Not all of these solutions are immediately applicable into an industrial environment. More specifically, constraints for deploying *general purpose cybersecurity solutions* are related to performance and impact on performance of the underlying systems and architectures, focus on confidentiality over availability, human machine interfaces (HMI), … and other specific industrial requirements (such as regulatory requirements). Industrial automation environments and industrial environments today sometimes have specific requirements that should be taken into account to prevent disruption or complete failure in the industrial operations.

Innovative solutions have been developed specifically targeting industrial control system environments (ICS), targeting industrial automation systems and industrial legacy environments in the first place. *LSEC* – 3IF presents an overview on the basis of a catalogue of the *Industrial Cybersecurity Center (CCI),* identifying mainly industrial solutions related to access control, traffic & systems monitoring, network, system & integrated protection. Innovative European solutions that have been identified in the domain of ICS & OT in international studies include *SecurityMatters* and *Sentryo.* Some of these, and up and coming innovative solutions, have been developed with the support of the European Commission through research funding. Other innovative cybersecurity solutions specifically targeting industrial production and manufacturing environments can be found in emerging cybersecurity for IoT, for Automotive and for Industrial IoT (IIoT) developments, in innovations related to IIoT Shields, next generation cloud security, cyber actuaries and security by design domains.

In some cases these *commercial* solutions and technologies, choose not to focus into some industrial sectors or environments, because of their restrictions and specifications from a regulatory perspective. **Critical Infrastructure**, for instance, is being considered as a too difficult, too small market by some.

Others tend not to focus on chemical, energy, healthcare, and other related domains because of potential legal **liabilities** derived from supplying in these domains. Developments towards **cybersecurity certifications for products and services** from the European Commission (empowering ENISA and the Member States into setting specific cybersecurity requirements) are expected to further impact Cybersecurity in Industrial settings.

Cybelius, MB ConnectLine and Stormshield via Airbus Cybersecurity present their appliances solutions. The *Stormshield UTM* is a next generation firewall, supporting going to cloud environments and with soft agents on machines protecting endpoints in OT. *Cybelius* focus on real-time detection and remote monitoring. It tries to further simplify the difficult and complex cybersecurity domain by integrating a number of security components and allowing joint responsibility between the more advanced cybersecurity teams of information technology in combination with industrial operators, bringing cybersecurity to the HMI's on the production floor. Many technologies being applied are not new (authentication, zoning, DMZ, SIEM), but by combining them for an industrial environment, they become very practical and are likely to cover quickly 80% of the basic requirements. *MB ConnectLine* testifies on the necessity for cybersecurity to better understand the challenges, needs and the requirements from the operations technology perspective, supporting the case for simplifying cybersecurity for OT, and bringing cybersecurity to automation engineers. It focuses on industrial remote access, firewalling OT machines and data restriction.

Airbus Cybersecurity proposes more advanced cybersecurity capabilities for industrial environments, amongst other derived from their Airbus Group manufacturing operations, which have to be adopted to requirements from defence, homeland security, and critical infrastructure. This implies more advanced use of cryptography in specific modules that can be embedded for aeronautics. Other technologies include **Penetration Testing** and **Vulnerability Assessments**, **Secure Remote Monitoring** and **Remote Maintenance**, a **Cyber Range**, for cybersecurity training purposes or a **Security Operations Center (SOC)**. Also *Siemens* addresses an *Industrial Security Service* protecting productivity and devices, and the importance of **backups**. Through a **Defense in Depth** strategy, beyond the implementation on **multiple layers**, there are also **security management** and **assessments**, **patches** and **training** being provided. An **app** with listings of equipment exists providing **security vulnerability information**. For remote access, Siemens offers **signed firmware updates**. For older systems, an approach towards **System Hardening** measures can be found.

Some vendors intend to indicate their responsibility efforts in the digital supply chain, by means of a minimum general standard for cybersecurity in keeping with the requirements of state-of-the-art technology. Siemens and Airbus amongst others have united under the *charter-of-trust.com* program, indicating their intentions on security for their products and technologies. No formal assessments are being done, but they are an indicator towards de-facto industry standards. Other technology providers and manufacturing industries have taken similar initiatives.

9. Specific security and resilience issues for manufacturing

The following considerations were identified during the session as specific in relation to security and resilience for manufacturing (in a collaborative environment):

- Operator Resistance
    - Not all operators have reasonable computer skills, able to identify cybersecurity challenges, or to differentiate cybersecurity incidents from other incidents.
    - Enable operations people and automation engineers to include cybersecurity into their systems and operations, by further simplifying HMIs and facilitating the process

between cybersecurity for operations technologies and more advanced cybersecurity processing.
    - Integrating cybersecurity best practices in industrial processes is a challenge in itself
    - Targeted attacks to individual operators through identity theft, social engineering or other actions
    - Specific requirements for industrial cybersecurity systems, improving the transferability of cybersecurity solutions, but also from HMI, performance, impact, footprint and other considerations
    - Industrial Cyber Range: specific training and assessment environments for operational environments
- Devices
    - Many devices in manufacturing operate autonomously, once the instruction of automation has been established. Many of these devices will remain unattended for long periods of time.
    - Fine grained access control & crypto – object-based encryption in industrial environments and related key (distributed) management
    - Devices are being tested and assessed for automation processes, but only to a limited extent on their cybersecurity capacities and capabilities.
    - Automation systems are expected to have a lifetime (5 – 20 years) far exceeding those of ICT-system (2 – 5 years)
    - There is an increasing significant trend in cloud computing, but a slow overall adoption rate from manufacturing organizations. Employees use Dropbox, Google and other cloud services for data and document sharing beyond the security perimeter (in enterprise cybersecurity known as Shadow-IT), but in these cases through unmanned systems and operations manufacturing data is being shared in the cloud.
- IT vs OT
    - Specificities of automation systems: expected lifetime, limited instruction set, impact of changes on the operational environment.
    - Defining the constraints of general-purpose cybersecurity systems for industrial environments. Considering these cybersecurity systems as evolutionary platforms.
    - Testing capabilities and assessment models for general-purpose cybersecurity solutions to be constrained to industrial environmental settings for industrial automation environment or Industry 4.0 environments.
    - Multifactor authentication is widely accepted in IT environments, but continues to be a challenging user requirement on a factory floor.
    - The organizational and supporting need for multi-disciplinary cybersecurity teams OT - IT
    - Changes in IT have a slower adoption rate in OT
    - The HMI (Human Machine Interaction) is completely different for an automation operator, as also the environments where they are active in.
    - Development process and development lifecycle. Today's technologies are being developed in an iterative way (agile), with multiple builds per day – continuously, to allow for continuous improvements. This is in strong contrast with existing automation development processes (design, build, test, (certify), run, maintain), even more than in any other industry vertical today.
    - Hardening cybersecurity of the available open source components widely used or specifically developed for manufacturing environments.
    - Security analytics are mainly covering Industry 4.0 types of applications, and do not fully integrate with Industry 3.0 solutions. Platforms are standalone and not integrated with other existing intelligence sharing platforms. Efforts are taken to integrate into one single Information Security Management System (ISMS) and with the physical world. This is work in progress.

    - Interdependency safety, security & cybersecurity: more particular in industrial and manufacturing environments, the impact of cybersecurity on the safety of production workers, in safety towards the environment and cyber-physical security developments
- Real Time, Fast & Stateful, Lower level Communication Protocols
    - Improving overall security and setting security architecture for Message Brokers, Messaging Protocols, and lower level communication protocols
    - Applying security on real-time communication and processing protocols.
    - Many industrial processes require stateful and fast communication (e.g. DDS, ZMQ, RTPS, UDP, …), with today only limited or restricted means for security mechanisms in the protocols themselves. Most of the security mechanics today are only available on physical lower levels or logical higher levels, allowing only for limited visibility and control for cybersecurity. Many of these protocols are susceptible to spoofing and Denial Of Service (DOS). They are frequently and increasingly being adopted in manufacturing situations.
    - Need for semi-automated solutions for crypto between level 0 and level 1, on signalling layers was addressed a couple of times, inspired by the requirement for critical infrastructure systems communication protection. Some of these solutions exist as industrial HSMs (Hardware Security Modules), but have not been addressed during the workshop.
- Legacy
    - Operational automation systems run for 30+ years. In IT, legacy systems not only still exist, but will be kept for economic reasons, rather than from operational / continuity perspectives.
    - Traditional PLC & SCADA-programming are slowing down, but to a lesser extent than RPG/COBOL in IT environments.
    - Use of X.509 certificates & managing machine identities and trust levels.
- Impact
    - On continuity of operations, on quality, on total production, resilience, safety or even environment. Impact could be much wider and immediate.
    - Changes in systems could cause major harm in production environment, even after stringent testing and requirements definition.
    - Due to the continuing trend of increased automation, the industrial attack footprint is expanding exponentially.
    - Minor changes in the programming and execution of the programming could cause a major effect on the quality of the product. This could cause not only economic impact on the producer (call backs, loss of image, …) , but equally on the safety (food, automotive, electronics, …) of products and their environments.
    - Some factory environments cannot cope with instant reaction due to cybersecurity, for process and safety reasons. Steel production, nuclear facilities and other environments need several days or hours to be able to shut down or restart. Not all of these environments are considered Critical Infrastructure or Essential Services. They might be regulated through sectorial competent authorities.
    - Requirement of novel security techniques for I4.0 scenarios in manufacturing, while many of the existing security techniques should be applied first. I4.0 scenarios should be especially focused on setting requirements for a series of basic security controls before being implemented. Guidelines should be developed on the basis of ongoing developments.
    - Responsible Disclosure: suppliers and operators should achieve a joint understanding in responsible disclosure, maximum time to repair and support of warranties.

- Automation & Agile
    - Increased machine learning and application of analytics, including artificial intelligence are leading to further automated decision in automated systems. Supervisory decision support making and controls will be needed to support this process.
    - Automation of security assessments
    - Agile factories rely on agile processes and require adapted security mechanics on each of the underlying processes that need to be integrated seamlessly again when components switch or change. Agile security development techniques should be investigated for their applicability in this evolving domain.
    - Security in digital twins in relation to the data exchanges, and the security of the virtual platform in relation to the physical platforms, ensuring the virtual twin is an integer representation of the physical platform
- Safety & Security
    - Risk assessments prioritize safety and security on a conceptual level above cybersecurity issues and incidents. These have not been properly implemented into policies and procedures, or into systems and digital platforms.
    - Situational awareness from traditional security & safety systems does not take into account specific requirements and opportunities derived from Industry 4.0 developments (sensors, cloud, …) and analytics in order to better support cybersecurity.
    - Models for insurances, their risk profiles and reasoning towards filtering or defining premiums, disclaimers and risk coverage.
- Systems of Systems
    - Orchestration of security measures is needed not only on the factory floor, on the security systems, but equally throughout the various systems being operated (MES, ERP, PLM, …) requiring various evolving mechanisms for security (at least authentication, access control, authorization, and monitoring). Such an orchestration is different from enterprise cybersecurity challenges due to the nature of the underlying equipment, networks, communication protocols and interaction with other entities (suppliers, customers, partners, …). Orchestration can allow policies to be developed, that can run over multiple companies and systems, and can be assessed at any time to provide levels of control and monitoring.
- Ecosystem
    - There is lack of coordination with and within the supply chain. Manufacturers are increasingly relying on their suppliers, trying to reduce the production cycles and reducing warehousing costs. Manufacturing involves physical products, and transition of goods, which have an impact on logistics, transport and environment overall.
    - New entrants into the manufacturing domain, both new manufacturers and existing manufacturers building new factories integrate new technologies without a transition phase, driving by a goal of hyper-efficiency through automation.
- Collaborative manufacturing
    - While not specifically addressed in the workshop, since most projects cover multiple factories, but not immediately from a collaborative perspective – some developments are taking place in the domain of the International Data Spaces Association (as was mentioned during the workshops on 15-16 October[19]).
    - Security solutions for sharing data between multiple manufacturing environments are investigated in the domain of blockchain.

[19] https://ec.europa.eu/digital-single-market/en/news/advanced-and-interoperable-digital-business-business-platforms

    - Data integrity challenges and multiparty encryption are identified challenges particularly to collaborative manufacturing, beyond the contractual and trusted relationships.
- Legal
    - Data ownership: project coordinators and participants indicated this not to be resolved. Industry operators did not (immediately) indicate this to be a problem, as this might usually be resolved under contract law, or as liabilities. As many products are designed, developed and operated by multiple partners, it is to some extent a more particular situation for research that might need further attention.
    - Data deluge: the spreading of industrial data amongst suppliers, operators, vendors, system integrators, users and multiple factories involved (in the case of different processes). Data will be distributed heavily, difficult to keep control over its spreading.
    - Privacy: while privacy has been regulated under for instance GDPR and ePrivacy, projects and industry indicated it to be of concern still today for manufacturing. The particularities are in the domain of handling personal data in manufacturing during the manufacturing and operations process that might require some specific technologies and / or considerations from a legal perspective.

10. Cybersecurity Strategic Research & Innovation Agenda

The European Cybersecurity Organization (ECSO) aims to support the continuous development of Europe as a global leader in cybersecurity. For the industrial sector at all levels (national, regional, …) a strategic research and innovation agenda (SRIA[20]) was developed by ECSO members, including industry (large and SMEs), academia, RTOs, associations and national public administrations in order to drive the focus of key research investment in the domain of cybersecurity both from public and private sector. Fabio Martinelli, co-chair of the ECSO WG6, presented the SRIA and specific thematic priority areas identified for WP2017-2020. The ECSO SRIA is organized around ecosystems, vertical application domains, trustworthy transversal infrastructures and technical priority areas. A specific chapter was dedicated to the developments of Industry 4.0. It includes subtopics on Industry 4.0 and Industrial Control Systems, on Trusted Supply Chains and hints to discussion topics such as interdependency safety, security & cybersecurity, security by design in industrial systems and towards product lifetimes, situational awareness and risk management, data deluge and insurance.

An earlier exercise by *ConnectedFactories* on the basis of the 2017 SRIA identified the following emerging technologies as relevant for cybersecurity for Manufacturing and other Industrial demand: trustworthy systems components for the different roles, security architecture components including convergence, distinguishing aspects of securing IoT, crypto and isolation techniques, OWASP attack vectors for Digital Manufacturing Platforms, protecting exchanged contents, forensic analysis mechanics, tamperproof communication protocols, software quality and overall protection of innovative ICT infrastructures.

11. ConnectedFactories Digital Platforms Cyber Security Control Framework

Part of the ConnectedFactories project[21] is to develop and maintain a structured glossary and mapping framework comprising a specific component on cybersecurity in addition to business cases, scenarios and technologies. With the view on aligning and coordinating the different projects in their security

[20] https://ecs-org.eu/documents/ecs-cppp-sria.pdf
[21] https://www.effra.eu/connectedfactories

developments and to provide guidance on the elementary security components, it is relevant for the digital platforms under development under the Factories of the Future PPP. The Cybersecurity Control Framework was developed as a guidance and assessment framework, allowing developing and existing platforms to indicate the components they take into account in their platform when indicating their level of cybersecurity developments. It allows the digital platforms to both widen and deepen their cybersecurity posture, as by including more components a hardening leading to a more cybersecure digital platform will be feasible.

The framework was sent to the participants in advance, in order to complete their own assessment of their digital platform (and other technologies) in view of the workshop. It is likely that not all technologies presented fit under the concept of "digital platform", as some are components and core technologies, or – as the case for some industrial solutions – are appliances. The combined result of the assessment by the participants, and upon review, provides a reasonable view on the level of security of the various platforms, but also their complementarity when it comes to security components. (The collection, sharing of information about security aspects will continue in the future, see www.connectedfactories.eu)

Where some projects representatives indicated to cover more on the user and access control component, others have been more focused on the risk analysis or the incident detection, situational awareness perspective. Many of the projects have also implemented varieties of encryption technologies (transmission mainly). While most individual security controls of the framework had been addressed, through the variety of projects, three controls remained unattended. The exercise did not diligently assess all of the self-assessed controls and it remains questionable whether the segregation, storage and data flows were properly addressed in the projects. More investigation will be required. Most components however, indicated to be available in **open source** format, and should be available for digital platforms and other manufacturing collaboration technologies to investigate their benefit or integration.

Digital Platform Environment Segregation	Operating System Privileged Account Control	Internal Data Flow Security	Security Updates	System Hardening	Physical Security	Password Policy
Far-Edge, Autoware	Autoware, *COMPOSITION*	Far-Edge, ITM'Factory, GRADIANT, *DEFENDER*	Far-Edge, Boost4.0, AMASS, ITM'Factory	AMASS, eITUS, REDEC, ITM'Factory	Far-Edge,CyberBasque4.0, AMASS, eITUS, ITM'Factory	*COMPOSITION*
Multi-factor Authentication	User Account Management	Token Management	Malware Protection	Software Integrity	Database Integrity	Cyber Incident Response Capability
Far-Edge, AMASS, *COMPOSITION*	Far-Edge,CyberBasque4.0, REDEC, *DEFENDER* , *COMPOSITION*	Far-Edge, EUSKATE, *COMPOSITION*	CyberBasque4.0, REDEC, GRADIANT	Far-Edge,CyberBasque4.0, AMASS, eITUS, ITM'Factory	Far-Edge, AMASS, EUSKATE	*DEFENDER, COMPOSITION*
Security Training and Awareness	Logging and Monitoring	Back Office Data Flow Security	Transmission Data Protection & Encryption	User /session- Hardware integrity	Vulnerability Scanning	Critical Activity Outsourcing
Far-Edge, REDEC	Far-Edge,CyberBasque4.0, Boost4.0, REDEC, *DEFENDER* , *COMPOSITION*		REDEC, EUSKATE, ITM'Factory, *COMPOSITION*	ITM'Factory	REDEC, GRADIANT	ITM'Factory
Transaction Business Controls	Personnel Vetting Process	Physical and Logical Password Storage - Key Management	Intrusion Detection	Penetration Testing	Scenario Risk Assessment	User Session
Far-Edge, Boost4.0, EUSKATE, *COMPOSITION*		EUSKATE	Far-Edge, Autoware, Boost4.0, REDEC, GRADIANT, *DEFENDER*	Far-Edge,CyberBasque4.0, AMASS, REDEC	Far-Edge,CyberBasque4.0, AMASS, eITUS, REDEC	
Resilience						
ITM'Factory						

Table 1: combined security controls matrix completed by projects self-assessment on the ConnectedFactories proposed Security Control Framework, after review and completion. Green boxes indicate basic security requirements. Orange boxes indicate variance with the original Security Control Framework proposed in the Structured Glossary of the ConnectedFactories project (FoF11-CSA).

12. Breakout Discussions and Conclusions

During the breakout sessions, *Cybersecurity in the context of the factory floor* and *Cybersecurity in the context of dynamic supply chains,* a well-balanced mix of industry professionals and research representatives contributed to lively discussions.

Beyond the cybersecurity issues already presented, residual threats were highlighted. There are several ways to manipulate signals, and cybersecurity threats will not get out of the market. A false sense of security should be avoided. This relates to, for instance, both active automation systems or IoT devices, but equally insider threats. Operators are not aware of cybersecurity issues, not even concerned. At the same time, plant operators are usually the best to know their processes, but resistant to hindering activities such as multifactor authentication. Improving operators' awareness and cybersecurity behaviour is one of the methods to improve security. Training and education on the job using simulation environments are needed, similar to training people that safety equipment and helmets are there to protect humans from harm. Machine and system builders should be empowered to build in more cyber-hygiene by enforcing cybersecurity from the outside and via simplification in HMI systems. This should not mean that things are simple, but should be made manageable. Alternative visions are to further reduce the possibilities from humans to interfere with processes, and inform them only on a need to know basis. Considering that people do not need to be aware, by further automating processes and systems preventing user interventions or further simplifying guidance and control of operators – using IT to further eliminate the human factor out of the loop.

Difference should be made between data for automation and data on production, production information and cybersecurity information. Cybersecurity should consider also the use of physical information, from a cyber-physical perspective. This includes integrating people and humans as cybersecurity sensors. By measuring dynamically ongoing physical processes such as the energy use, whereabouts, access control and surveillance systems, additional insight on cybersecurity can be gained. The engineering of manufacturing environments could be further improved towards specific minimal requirements and regulations. Reference is made to regulated engineering levels and resilience of safety products, connected cars and medical equipment.

In view of the changing dynamics in supply chains, cybersecurity and security measures have been organized from a rather traditional perspective and should consider ecosystems more. Data distribution is a work in progress, innovation being stifled by ownership aspects. Federated platforms, where inputs, access and controls have been distributed are still in their infancy. A need for meta-models is developing quickly, where digital twins and other virtual models could play a significant role. Ad hoc approaches have proven to be sometimes better than over-standardization efforts. When security is being dealt with on the shop floor, it should have been derived throughout the supply chain, using pathways and controls and incentivizing their respective managers. Systems developers should consider good practices from other vertical domains, such as healthcare and financial services.

13. Next Steps and Follow-up interactions

The following addition interactions have been proposed:

- 2018 December 4 – 6, Vienna: ICT 2018 – Imagine Digital:
  https://ec.europa.eu/digital-single-market/en/events/ict-2018-imagine-digital-connect-europe
  http://www.connectedfactories.eu/connectedfactories-cluster-news
  more specifically the Security topic session:
  https://ec.europa.eu/digital-single-market/events/cf/ict2018/item-display.cfm?id=22788
- 2019 February 27 – 28th, Brussels: 3IF.be annual conference
- 2019 February – March (tba), Brussels: webinar for proposers (of the ICT-08-2019 call)
- 2019 March 22-23, Bucharest: European Robotics Forum
- 2019 March 28, Brussels: deadline ICT-08-2019 call
- 2019 May 22, Brussels: ConnectedFactories closing conference

14. Contributors to the Workshop

The organizers want to thank the following contributors to the workshop:

Marcos Álvarez-Diaz, Gradiant (ValueChain 4.0)
Ana Ayerbe, Tecnalia (AMASS, eITUS, REDEC, Euskate)
Adrien Becue, Airbus / ECSO
Gert Boterweg, Siemens
Géraud Canet, CEA / ECSO
Chris Decubber, EFFRA (ConnectedFactories)
Roberto Cascella, ECSO
Jerker Delsing, Lulea University of Technology (Far-Edge, Productive4.0)
Ignacio Gonzalez, ATOS (Composition)
Philippe Jaillon, Institut Mines-Télécom (IT'M Factory)
Oscar Lazaro, Innovalia (Autoware, Boost 4.0)
Fabio Martinelli, CNR / ECSO
Cristina de la Maza, Eneo (Autoware)
Vito Morreale, Engineering (Defender)
Siegfried Müller, MB Connect Line
Frédéric Planchon, CYBELIUS
Cristina Sandoval, European Commission
Ulrich Seldeslachts, LSEC / ECSO (ConnectedFactories)
Antonio Skarmeta, Universidad de Murcia (Anastacia)
Stephen Smith, CCI
Markus Tauber, University of Applied Science Burgenland (SEMI4.0)
Mikel Uriarte, Nextel (Autoware)
Arian Zwegers, European Commission