Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 16 (2018) 193–207

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

7th International Conference on Through-life Engineering Services

Through-life cyber resilience in future smart manufacturing environments. A research programme.

Paul Theron, PhD

Cranfield University, Professor, Atkins-Cranfield Chair of Cyber-secure engineering systems and processes, Head of the Manufacturing Informatics Centre; email: p.theron@cranfield.ac.uk

Abstract

Smart manufacturing has recently become the industry's buzzword, with the promise of improved performance and greater agility. Also named Industry 4.0 (I4), this concept relies upon a system of systems made of myriads of Industrial Internet of Things (IIoT) components. Along with the expected enhancements come new cyber-threats as the attack surface and pathways will increase. This conference paper argues that I4's cyber resilience demands an ad hoc research programme. Firstly, we briefly compare Operations Technology (OT) with classic Information Technology (IT) and IoT technology to highlight their differences and the latters' impact on cyber resilience. Secondly, we depict the concept of operation of future I4 systems and point out the specific challenges they raise. Next, we review the concept of through-life cyber resilience assurance and complement the list of future I4 environments' challenges. Fourthly, we present Cranfield University's Manufacturing Informatics Centre's (MIC) research & education strategy and show how it relates to the identified challenges. In our conclusion, we suggest ways to foster collaboration between the Industry, the Government and the MIC to address these challenges and to allow the United Kingdom to approach I4's challenges with increased confidence.

Keywords: Type your keywords here, separated by semicolons ;

10.1016/j.promfg.2018.10.157

IT, OT, IoT: differences and impacts on cyber resilience

Information technology (IT) provides our society with the means to process the data feeding management systems of all kinds, from online commerce to human resource handling, from production scheduling to quality control, from banking and insurance to local government administration, etc. In terms of security, their designers seek to assure the confidentiality of data, their integrity and their availability. The recent introduction of the European GDPR act has placed the focus on privacy.

Operations Technology (OT) systems are those systems mixing hardware and software components that detect or cause changes in physical processes and devices in order to deliver intended functions in the physical world. Their designers seek to confer them constant availability and reliability. Those goals are reached if OT systems' availability, integrity and confidentiality characteristics are engineered into systems and preserved along systems' full lifecycle.

Examples of OT systems include:
- Industrial production;
- Home and building automation;
- Ground transportation networks;
- Power generation;
- Security and surveillance systems;
- Weapon systems systems…

Their failure or a severe disturbance of their processes may result in dramatic consequences, ranging from halting industrial installations to the abortion of defence missions or creating collateral damage in combat situations.

Therefore, OT systems are designed to satisfy very high-performance requirements, including:
- Reliability
- Safety of people, the environment and installations
- Data & systems' classification in military contexts
- Rapidity of execution and quality of results
- Availability, and continuity in tough running conditions
- Autonomy in case of disconnection from energy sources or communication networks
- Robustness, long life span and low-cost maintenance.

Current industrial systems are usually made of:
- Robots, sensors and actuators, i.e. cyber-physical elements that deliver and help controlling production or transportation or building automation processes;
- Programmable Logic Controllers (PLC) that pilot those operational components;
- Remote Terminal Units (RTU) that pilot sets of PLCs;
- Engineering terminals that allow to diagnose and (re)configure RTUs and PLCs (note that PLCs themselves often have an embedded minimal man machine interface for the same purpose);
- A Supervisory Control & Data Acquisition (SCADA) system that supervises the entire (or a part of an) industrial network;
- Networks and communication protocols, like Modbus and many others [1], to connect the previous elements together.

Between different domains of application, there are differences in protocols and technologies.

In this context, we define *cybersecurity* as systems' ability to be immune (robust) to cyber-threats, and *cyber defence* as systems' ability to resist successfully cyber-incidents (attacks) and to improve out of lessons learnt [2]. *Cyber resilience* is understood as the "sum" of cybersecurity and cyber defence.
It aims at preserving the continuity, reliability and safety of our social, industrial, security and military activities in the face of ever increasing and evolving cyber threats.

If, currently, security requirements are deemed to differ between IT and OT systems (see for instance [3]), demands for processing speed, availability and reliability do not really diverge between the two types of systems. So that it is not so important to argue about which security goals are a priority in one or the other domain. But OT specialists' engineering culture is specific [3] as they have an "*inherently change- and risk-averse culture on the shop floor*". And for the purpose of this paper this is very important as it constrains the way cybersecurity can be (retro)fitted and maintained in OT technologies and systems. It can only be slow as multiple tests and precautions are then requested.

IoT is a particular species of OT technology. It allows creating "systems that interact with the physical world using networked entities (e.g., sensors, actuators, information resources, people)" [3]. It is made of many-to-many interacting components some of which have sensors and actuators to interact with the physical world and an IoT component "has some combination of the following capabilities: actuating, data storing, human user interface (UI), networking, network interface, processing, sensing, and supporting" [3]. Those basic building blocks of IoT systems can themselves be sets of IoT components or even entire IT systems. Due to their cheap price, the varied ways they may be procured and their sometimes fuzzy origin, their sometimes basic technologies and computing and memory capacities, their variable energy requirements, or else latency issues, different integration middleware, variable orchestration choices, at times inexistent or succinct documentation, intellectual property rights, variable update policies, or IoT system builders' level of control over all these factors, IoT components are usually better seen today as simply black box constituents selected only for the delivery of a desired function and performance, based on a set of specified interfaces.

A variety of open source and proprietary IoT development platforms is available on the market, with their respective advantages and limitations [4].

In terms of system architecture, many configuration scenarios are possible for IoT-based digital supply chains, including point-to-point, star and mesh topologies [5]. Event-driven, resource-driven, auction-based (Liang & Hsu, 2014) and need-driven distributed operations, as well as unpredictable alterations and reconfigurations can shape and alter the IoT's set of components and their operating relations. In any-to-any infrastructures (CISCO, 2014), clusters of cooperating components vary in time and space (Mahmud, et al., 2018), at the speed of needs, of changes, of incidents and dynamic reconfigurations. Software defined networks will also cause IoT-based digital supply chains to vary in shape and set of active components through through continuously evolving logical topologies (Vicino, et al., 2014), the decoupling of function and location (Lopez, et al., 2016) and dynamic, automated SDN programs (Bista, et al., 2013). As those digital supply-chains will grow in complexity, solutions like autonomic computing (Ganek & Corbi, 2003) may be adopted with the consequence of also making IIoT networks' configuration highly changeable.

These factors make the cybersecurity of future smart manufacturing and other IoT systems far more uncertain than todays well-connected, centrally administered networks.

Besides, cybersecurity may be breached by unknown vulnerabilities in uncontrolled – unsafe – IoT components, while the latter may connect to open, equally uncontrolled public networks via the Internet, both exposing others to cyber-threats and making them a potential source of cyber-threats (NIST, 2018).

Unless designers or business decision makers manage to impose the generalization of cybersecurity certification, the choice of stable and well-controlled architectures and telcos' or cloud providers' commitment to a high level of connection quality of service and security for the entire Industry 4.0, securing and monitoring IIoT systems, responding to cyber-attacks and restoring their cybersecurity in the short times required by industrial production continuity imperatives – this is the ultimate business challenge – may reveal hard, if not impossible.

The concept of operation of future Industry 4.0 systems

Future smart manufacturing Industry 4.0 systems will be based on the Industrial Internet of Things (IIoT). Its architecture will be built along the following components and layers such as described in (NIST, 2018):

1. The device layer includes all the elements that compose manufacturing processes;
2. The communication layer allows the coordination and cooperation of manufacturing processes;
3. The cloud layer stands as the application-enabler layer and permits data consolidation and sharing, including Machine to Machine (M2M, and we could also use the acronym for Manufacture to Manufacture), the availability of APIs for connecting the manufacturing cloud with other applications (for instance, web-based commercial applications, supply chain and logistics management, and E2E – Enterprise to Enterprise – applications), and management applications;
4. The big data layer leverages the huge masses of data gathered in the manufacturing cloud to prepare and analyse data for later use at the next level of the architecture;
5. The supervision layer calls upon intelligent software technologies (visualisation, IA and especially machine learning) to monitor and optimize manufacturing processes in the lower layers.

The following diagram represents these five layers:

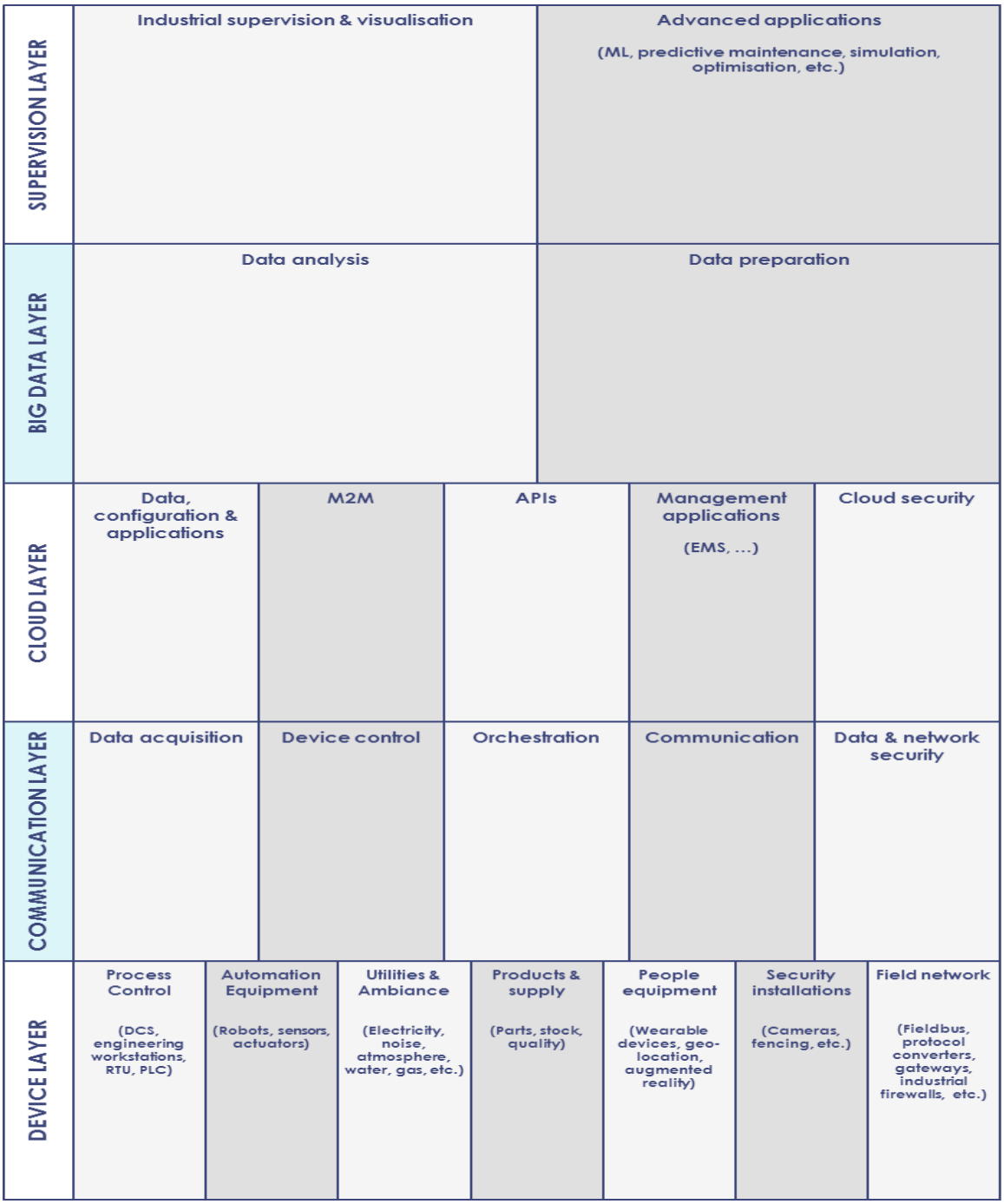

Fig 1. Industry 4.0's generic architecture.

One of the fundamental concepts of operation and motivations of Industry 4.0 smart manufacturing is agility. To illustrate what this means, Bosch explains (Ferber, 2012) that in the future Industry 4.0 make-to-order manufacturing, specifications will be embedded within each piece of work and the latter will itself give instructions and command to production robots within multi-product manufacturing lines.

Through increased connectedness, flexible supply chains and decentralized competing and responsive production capacities, customers will gain customized and innovative products at optimal prices and lead times from the most customer-oriented and best-cooperating manufacturers (Bechtold, et al., 2014), whatever their actual size. For this reason too, the underlying IT+OT manufacturing process will vary widely. A single business request may then materialize into numerous digital supply chains that will not anymore be placed under the control of major companies. Creative start-ups and niche players will enter these ad hoc cooperative supply chains (Bechtold, et al., 2014).

Such variety (and uncertainty as to who will take part in digital supply chains), even if communication and Production Performance Management standards emerge for the common good, will create differences in architecture and cybersecurity maturity. This will call for consistent improvements of market players' good practices for the development of their digital infrastructure and systems (Gates & Bremicker, 2017) as well as cybersecurity dispositions (NIST, 2018), (Sniderman, et al., 2016).

The fact that each piece of work contains its specific manufacturing and logistic data and instructions will also be a new vector for cyber-attacks.

As in all multi-stakeholder domains relying on shared infrastructures (like aviation, telecommunications, etc.), the need for norms and a collective governance of cyber resilience will grow in years to come (Gates & Bremicker, 2017).

The concept of through-life cyber resilience assurance

As said earlier, cyber resilience is the "sum" of cybersecurity and cyber defence. Building cyber resilience rather than simply cybersecurity into future smart manufacturing systems is a necessity caused by the now well-shared finding that the adversarial nature of cyber-attacks can defeat cybersecurity dispositions and take advantage in any relapse in measures aimed at preventing cyber-attacks.

Through-life cyber resilience is the activity that creates and maintains cyber resilience across all phases of a system's lifecycle, from the moment its concept is formulated, to the moment it is released for operation, and until it is decommissioned.

In through-life cyber resilience, three dimensions are at play:

- Cyber resilience governance;
- Systems' development processes;
- Cyber resilience mechanisms.

Cyber resilience governance

In domains, like smart manufacturing, the telecommunications, aviation or future global mobility, each one supported by vital infrastructures, there is a need for a collective governance of cyber resilience across the entire value chain and countless stakeholders.

For instance, the former European Public Private Partnership for Resilience (EP3R)* and now its replacement, the Network and Information Security (NIS) platform†, have been European Commission's attempts to organize some form of collaborative governance of cybersecurity in the telecommunications sector.

In the aviation sector, the European Agency for Safety in Aviation (EASA), under the STORM workstream (Shared

* https://www.enisa.europa.eu/publications/ep3r-2009-2013

† https://resilience.enisa.europa.eu/nis-platform

Trans-Organisational Risk Management), is currently trying to establish a similar mechanism to bring operators to the same table in order to reflect on transverse cyber-risks and to set-up collective mechanism to handle them. Similarly, various national aviation authorities and stakeholders aim at organising the collective governance of cyber risks across their national aviation chain.

In such a context, the collective governance of cyber resilience implies a multilevel, multi-stakeholder, cross-domain and even cross-border process (Lie, et al., 2009), (UN-DESA, 2011), (European Commission, 2017), just like the governance of telecommunication infrastructures' resilience (European Commission - DG JLS, 2011). A global governance framework is described, for instance, in (Theron, 2016). It summarises the findings from various studies and organises governance into a set of interdependent processes:

- A domain / cross-domain / international / national multi-stakeholder process that usually establishes sectorial regulations or legislation and the means to enforce them;
- A four-level corporate process that includes: top management steering, stakeholders engagement through continuous improvement loops, cyber resilience building, and cyber resilience preservation in operation.

In the automotive sector, the future ISO-SAE 21434 standard on *Road vehicles cybersecurity engineering* is likely to take these levels into account and to express ad hoc requirements for car manufacturers and their suppliers. However, challenges are manifold (Trimintzios, et al., 2017): sovereignty issues, differences and inconsistencies between legislative frameworks, lack of data, fierce competition (European Commission - DG JLS, 2011), difficulties in information sharing, differences in maturity, insufficient levels of investment and spending, ever-changing threats, technological developments, etc.

Systems' development processes

Building secure systems and maintaining the latter's cyber resilience once in operation and until decommissioning requires that the process by which they are conceived, designed, developed, tested and approved for service prescribes the activities that permit to create:

- Cybersecurity measures that must be embedded into systems, their production chain, the tools to be used for servicing them and into any other processes that will operate systems (like owner changes, repair, decommissioning, etc.), in order to protect the latter from cyber-threats during their entire lifecycle;
- Cyber defence dispositions that must be embedded both into systems and in stakeholders' organisations to allow handling attacks targeting development and production platforms, systems of all kinds and marketed products, and support processes once systems are in operation until, and including, decommissioning;
- Measures that will help stakeholders, including tier-n market players, to continuously monitor cyber threats and evaluate cyber risks and to preserve and maintain systems' and products' cybersecurity once in operation.

For instance, again, the future ISO/SAE 21434 international standard on road vehicles cybersecurity engineering should make requirements in those directions.

But doing so is a major industrial challenge as investments cannot be extended as far as the cyber threat might demand. Tough choices must be made by business owners, based on their financial capacities and risk appetite.
In the automotive sector, cyber resilience investments should go in priority to components and systems that are deemed critical. Criticality should be defined a measure of the potential impact of a cyber-attack, on safety for instance. For example, a vehicle's breaking system is safety-critical. A cyber-attack that would target it could affect the vehicle's safety. Therefore, the breaking system is critical from a cybersecurity standpoint. Criticality levels are deemed stable across lifecycle stages and possibly across the automotive industry. It is then the designers' job to elaborate the car's architecture that will best assure cybersecurity. So that vehicles' development processes will be augmented of the required cyber resilience engineering tasks and dispositions.
This is nothing new. The Military progressively implement similar requirements in procurement programmes based

on their usual architecture frameworks such as NAF for NATO‡, DODAF for the USA§, MODAF for the UK**, etc. Creating the Industrial Internet of Things will obey similar considerations. An IoT architecture framework is being casted at the present moment by the IEEE Standards Association††.

Cyber resilience mechanisms

Several comparable frameworks exist today to help engineering infrastructures' cyber resilience:

- (Bodeau & Graubart, 2011) MITRE's Cyber Resiliency Engineering Framework, used as the basis of NIST's 2014 Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2014),
- The survivability framework (Sterbenz, et al., September 2002), (Sterbenz, et al., 2010),
- The P3R3 risk reduction model (Theron, 2013).

The review of these frameworks shows, as synthesised in the P3R3 model, that risk reduction is achieved through six mechanisms (the MITRE/NIST framework has 5 functions: Identify, Protect, Detect, Respond, Recover). The first three mechanisms correspond essentially to making an object robust (immune) to the cyber threat, the last three to making it resistant to cyber-attacks:

1. Prevision is the mechanism that seeks to identify in advance the hostile agents and the gross portfolio of threats to which a target object, such as an infrastructure, might be – or is – exposed. Cyber threat intelligence is a typical activity.
2. Prevention is the mechanism that reduces identified threats at their source, either by eliminating or distancing from hostile agents, or by deterring them from exercising their threats, for instance by making the exercise of threats over costly or over risky for hostile agents (Mikolic-Torreira, et al., 2016). Prevention leaves a portfolio of residual threats, i.e. a gross portfolio of risks.
3. Protection is the mechanism that seeks to reduce the likelihood that residual threats convert into incidents, and to reduce the impacts of incidents should they happen. Protection consists typically in fitting cybersecurity into systems and, when required, evaluating and certifying it (as per ISO 15408 Common Criteria for example). However, as the protection of complex systems cannot be complete, protection activities leave residual risks and therefore must also establish and train resistance mechanisms (the next three below).
4. Recognition is the mechanism that monitors an identified object, seeks to detect as early as possible the potential or actual occurrence of incidents affecting the object (despite the previous three "P" mechanisms), and raises alarms when incidents are confirmed.
5. Response is the mechanism that mobilises incident response forces and seeks to absorb / tolerate, contain, mitigate and stop incidents, to resist the destructive pressures of incidents, to safeguard the people and assets at risk and to mitigate damages, to maintain missions running even if only in an acceptable degraded mode, to restore nominal performances as soon as feasible, and to keep all pieces of evidence, traces and documents that may be useful later in insurance, litigation, judiciary or (military) retaliation procedures.
6. Rebound is the mechanism that seeks to give a damaged object (or set of objects if considering knock-on effects) a new course of life or status after an incident has been resolved by rebuilding lives and objects that most suffered, drawing and sharing the lessons of experience, analysing the adequacy of the object(s) to possibly new circumstances, and adapting the object(s) accordingly as and if appropriate. In that sense, the rebound mechanism processes residual damage.

The examination of the frameworks previously cited also shows that a typical list of practical capabilities is needed within each of these six mechanisms:

---

‡ http://nafdocs.org

§ https://dodcio.defense.gov/Library/DoD-Architecture-Framework

** https://www.gov.uk/guidance/mod-architecture-framework

†† https://standards.ieee.org/develop/project/2413.html and http://grouper.ieee.org/groups/2413

P3R3 MECHANISMS	GENERIC P3R3 CYBER RESILIENCE CAPABILITIES
P1- Prevision (identifying threats)	P1.1- Threat intelligence (public or private sources & means, …)
	P1.2- Threat analysis (identification, capacities, targets, vectors, risks)
	P1.3- Threat evaluation & prioritisation and Resilience policy & strategy
P2- Prevention (of identified threats)	P2.1- Public-Private cooperation & legislative support
	P2.2- Reduction of threats at source or deterrence
P3- Protection (of systems against residual threats)	P3.1- Incident / attack avoidance and absorption dispositions engineering
	P3.2- Incident / attack coping dispositions engineering
	P3.3- Awareness raising, education, testing & training (preparation)
	P3.4- Management of systems' configuration, lifecycle and procurement
R1- Recognition (of an incident)	R1.1- Monitoring & analysis of events and detection of incidents
	R1.2- Confirmation of incidents
	R1.3- Alarm on incident
R2- Response (to incidents in order to defend missions & systems)	R2.1- Mobilisation process (response activation decision and activation)
	R2.2- Response
	R2.3- Evidence management & exploitation, forensics & inquiries
R3- Rebound (to new course of life / operation & status)	R3.1- Repair & reconstruction (Healing)
	R3.2- Lesson learning & sharing
	R3.3- Adaptation & improvement (Renewal)
	R3.4- Investigations, legal suits, insurance claims, retaliation

Fig 2. P3R3 cyber resilience capabilities.

Some of these capabilities are the fruit of governance choices, such as collaborating with national cybersecurity authorities or working to gain support from the legislator. Others must be implemented during the development of systems and products, such as the engineering of protective barriers. Some others stem from the culture built into organisations to address cybersecurity issues.

This review of through-life cyber resilience shows that it is a multi-facetted effort, not left to engineers alone nor to users or managers only. It is a collective elaboration.

Areas of research to invest in and Cranfield's Manufacturing Informatics Centre's directions

If we summarise the various challenges identified along this paper, we find:
- A governance challenge;
- A cyber resilience engineering challenge;
- A cultural challenge.

The governance challenge

This smart manufacturing challenge has several key aspects:
- The solitude of business managers in the face of upcoming huge system complexity, a long-known issue of business managers' information technology competencies (Bassellier, et al., 2001), and the challenge for them

to make enlightened decisions about investments on emerging technologies; this may affect the pace of adoption of smart manufacturing or change the balance of power between market players along the value chain;
- The challenge of multi-stakeholder collaboration in an individualistic, highly-competitive, heterogeneous (from the cybersecurity standpoint), large, multilevel-process, cross-border and cross-sector field at large; ill-managed, this may jeopardise the capacity of the industry at large to master the cybersecurity and cyber defence of the value chain;
- The {technology user - technology supplier - technology regulator} dialog in an offer-led market of both IIoT and cybersecurity, with legislation, standardisation and policy issues and challenges; this competition for power over markets will feed incomprehension and will further complicate technicians' tasks to ultimately delay progress towards cybersecure digital supply chains;
- Anticipating the implications of future technological breakthroughs and applications, with "more biology and less physics", with bio-electronics and bio-machine intelligence (Marsh, 2016), a different understanding of "value", friendly retail robots, scale logic changes (and downsizing / making local again product manufacturing), etc. (Evans, 2016); strictly from a cybersecurity standpoint, such breakthroughs will complicate system and security engineers' work at both the development and operation stages of the lifecycle;

The cyber resilience engineering challenge

This smart manufacturing challenge has several key aspects:
- The challenge of making sure that industrial challenges of speed, productivity, continuity, reliability and safety will keep being met in the Industry 4.0 context; to that end, OT/IACS engineers will ask for guarantees that inspection, verification, validation and qualification activities be performed in ways that meet the challenge, meaning far more resource and spending and a potentially huge rise in the cost of industrial systems and products; alternatively, security-minoring trade-offs will endanger the entire value chain and create issues of trust between clients and manufacturers;
- The poor design of things, devices and systems, also a long-known issue (Fairbanks & Caplan, 2004), currently a mixture of technical complication for users and administrators and of a lack of widely shared HMI standards in a technical jungle of idiosyncratic product offerings, will keep both engineers and users struggling to install, interface, operate and maintain the IIoT; the same applies to cybersecurity; should this point be left unresolved, it might lead managers and engineers to make easy and quick, but potentially adverse, choices; this in turn would reinforce cyber vulnerabilities in devices, connections and operator terminals; this engineering challenge calls for a drastic simplification of systems and components' interfaces and procedures;
- The challenge of understanding how complex massively interconnected, shape-varying, ill-delimited systems will behave in a society itself massively connected but unaware of the dependencies and vulnerabilities that this creates for everyone; what is at stake here is the capacity of centralised security operations centres (SOC) to monitor IIoT systems, to detect cyber-attacks in real time, and to resolve the latter at the speed of events and systems, not at the pace of human operators; artificial intelligence deployed in such centralised contexts of operation will resolve nothing if IIoT systems are not built on today's centralised hierarchical models; this engineering challenge requires to research now how to create an autonomous, intelligent and seamless cyber defence technology that will fight malware for us humans; the idea has already been explored (Blakely & Theron, 2018), (Kott, et al., 2018), (LeBlanc, et al., 2017), (Theron, et al., 2019), but it raises ethical and technological concerns about the risks of technological entities' autonomy;
- The complexity of the co-engineering of systems and cybersecurity and of the visualisation of the impacts of architectural choices; today's model-based system engineering platforms (like Polarsys' Capella engineering suite‡‡, IBM's Rational Rhapsody§§, UNICOM's System Architect who acquired IBM's Rational System

‡‡ https://www.polarsys.org/

§§ https://www.ibm.com/developerworks/downloads/r/rhapsodydeveloper/index.html

Architect*** or standards like ISO/IEC 13719-2:1998 on Portable Common Tool Environment (PCTE)†††, etc.) are being progressively interfaced with model-based cyber-risk analysis software in an attempt to add the cybersecurity engineering dimension to traditional system engineering; if this seems to head into the right direction, recent projects such as MODESEC ‡‡‡ or the Model-based Security Toolkit (SecKit) and methodology§§§ attempt to tackle the difficulty inherent to the exercise: a modification of the system's architecture, for instance, impacts on its cybersecurity while a change in cybersecurity measures impacts on the system's performance at large; besides systems of the size and complexity of future smart manufacturing will imply numbers of design classes of objects and their relations measured in millions, far beyond any human's cognitive ability; this co-engineering challenge requires therefore research in two areas

- The issue of cybersecurity certification in a low-cost huge-volume market of things; this engineering challenge is linked to the idea that only cybersecurity-certified objects should be integrated in future systems to provide a baseline level of cybersecurity; this is the sense, for instance, of European projects on IACS cybersecurity certification conducted under the govern of the Commission's Joint Research Centre (Theron, 2016), (Theron & Lazari, 2018) and legislative moves (JOIN(2017) 450 final, 2017), (COM(2017) 477 final, 2017) ; however, reality defies practicality: the number of objects to certify will be so huge, while the effort for the certification of a single item is itself so big that the challenge is practically impossible to address; where research can usefully contribute lowering the difficulty of mass-certification is through the automation of cybersecurity evaluation tests;
- The challenge of preserving cybersecurity in the post-production phase of systems and products' lifecycle until their decommissioning; this engineering challenge can be easily overcome by taking care at the concept and development stage of cybersecurity maintenance and preservation in the operation phase of systems and products' lifecycle; research should focus on the how of this, and also on how to engage post-production stakeholders in a form of "good cyber behaviour" that would make them increasingly the actors of cybersecurity maintenance and of its preservation in the course of support activities and processes until decommissioning.

The cultural challenge

This smart manufacturing challenge has several key aspects:

- The likely under-awareness of cyber-risks associated with the IIoT;
- The lack of people with the appropriate knowledge and skills, evaluated for Europe only at around 350.000 (JOIN(2017) 450 final, 2017);
- Creating a societal culture of cybersecurity and cyber defence that does not entail global paranoid behaviours as citizens are more and more told their responsibility in preserving our society's cybersecurity (U.S. Department of Energy, 2013), (Shaikh, 2015), (Ottawa Citizen, 2017).

Cranfield Manufacturing Informatics Centre's research directions

Besides its existing activities, Cranfield Manufacturing Informatics Centre's new research and research-based post-graduate education directions include:

- First, the study of complex, massively interconnected systems of systems' dynamic (SOSDYN) behaviour, like the IIoT, of their degradation under strain, and of their state-space will be particularly useful to better characterise their patterns of degradation under cyber-attacks. Like Network Operations Centres are asked by Security Operations Centres' staff to check systems' state in order to confirm a cyber-attack is in progress,

*** https://www-01.ibm.com/software/rational/rationalsystemarchitect-departure and https://teamblue.unicomsi.com/products/system-architect

††† https://www.iso.org/obp/ui/#iso:std:iso-iec:13719:-1:ed-2:v1:en

‡‡‡ https://cordis.europa.eu/project/rcn/107018_pl.html

§§§ https://ec.europa.eu/jrc/en/publication/model-based-security-engineering-internet-things

future cyber defence technologies embarked in the IIoT will require this kind of information for a similar purpose, possibly in real time or nearly so. This will help to deliver resilient reactions that will seamlessly preserve the IIoT's continuity of operation. Our assumption is that, currently, we have very little knowledge about such complex systems' dynamic behaviour under cyber-attack circumstances. Systems dynamics, complexity theory, cybersecurity, graph theory, system modelling and simulation will be part of the foundational disciplines to mobilise under this first umbrella. In a word, we could say that we aim at establishing formal models of the complex systems' state variation dynamics and of cyber resilience dynamics, for use by future cyber defence technologies and by cyber defence industries and stakeholders.

- Research on Model-Integrated Co-Engineering of systems and cybersecurity (MICE), with a view to create a MICE engineering and innovation platform that will serve the manufacturing, defence and aviation sectors and their need to improve the inclusion of cybersecurity into smart manufacturing and other complex systems. Model-Based Engineering, cyber risk analysis and modelling, cyber-attack patterns and cyber-vulnerabilities classifications described for instance in MITRE's CAPEC (MITRE, 2018), simulation will stand at the theart of this research current.
- The first two domains of research require simulation. In effect, to understand complex large-scale systems and systems of systems' dynamic behaviour and the dynamics of cyber resilience in this context, one shall hardly be able to create a test bench at the size of a real one and with the activity of a real one. besides, in the context of the MICE research area, one of the difficulties to overcome will be to evaluate the impacts of architectural and cybersecurity design, operation and modification choices both on systems' performance and behaviour, and on their cybersecurity. For this double purpose, we shall create a Large-Scale Cyber Simulator (LSCS), capable of virtualising systems of systems comprised of up to hundreds of thousands and even millions of objects (software and hardware). High Performance Computing, complex systems, hybrid simulation, multi agent systems, visualisation, artificial intelligence, machine learning and big analytics, energy consumption optimisation will be all part of this research area. The LSCS will become a platform accessible to industrial and governmental partners and, in the future, we envisage to interconnect it to similar large-scale simulators around the globe to further advance research.
- As the need for cybersecurity certification is nowadays largely in question, and as it presents the challenge of mass certification in the context of a blossoming offering of connectable objects with which cyber risks may increase widely, our fourth area of research will relate to the possibility of automating cyber resilience tests and evaluations. We shall work to create the prototype of a Cybersecurity Evaluation & Testing Automation Platform (CETAP) that will aim to serve the needs of our partners and IT Security Evaluation Facilities (ITSEF) around the world. This domain will mobilise research competencies in cybersecurity, formal modelling, performance assurance, testing methods and technologies, artificial intelligence / machine learning.
- Finally, because future smart manufacturing systems, as well as other complex systems and infrastructures, will require a cyber defence that operates at the speed of systems and events rather than at the (slow) pace of human operators, we shall work to develop an autonomous intelligent Multi Agent System for Cyber defence (MASC) technology. MASC technology will deliver autonomous cyber defence for autonomous and highly complex systems. We aim to reach the point where it will act seamlessly on our behalf, our "goodware" fighting "malware" on its own terms, without our help. However, we assume that in given – extreme – circumstances, MASC swarms or cohorts may find their limits and require cooperation with a human operator. For this purpose, we shall develop a Cyber Cognitive Cooperation (C3) technology that will allow humans to help MASC agents to make decisions. If multi agent systems have been somehow marginalised in recent years to the benefit of the big wave of machine learning and big data, this branch of artificial intelligence will be mobilised along with cybersecurity, complex systems research and ergonomics to deliver in the longer term a technology that, we assume, attackers will also develop for their own, nasty, purpose. Working patiently towards this goal with our industrial and defence partners will be essential. Applications for MASC technologies that will emerge from this stream of research will also serve the wider public as more and more citizens will stand at the centre of a massive system of interconnected systems of objects.

In conclusion, the need for sustained industrial collaborations

The SOSDYN, MICE, LSCS, CETAP and MASC research areas do not belong in the same category:

- SOSDYN, research on highly complex systems' dynamics, belongs in the discovery type of research, with long-term goals and possibly short-term advances however hard to forecast today. Industrial collaboration will help the centre to create real-life use cases.
- MICE, research on Model-Integrated Co-Engineering of systems and their cybersecurity, is closer to innovation but requires serious research and close collaboration with model-based engineering platform suppliers and large engineering project procurers.
- LSCS, the Large Scale Cyber Simulator, is a mid-term innovative form of research. Such a large scale hybrid simulation capability is today required in order to research future highly complex systems. It will require not just investments but also real-size projects to test and validate it and its contribution to the industry, as well as to the SOSDYN and MICE research areas. And SOSDYN research findings will contribute to creating real life like patterns of behaviour and patterns of traffic generation in simulated systems.
- CETAP, research on the Cybersecurity Evaluation & Testing Automation Platform, belongs in innovation. Most of the tools are available today to advance this project. However, we assume that it requires elaborating use cases and a strong concept of operation, as well as creating a model-based approach to integrating these tools. This is a mid-term project that will require collaborating with ITSEFs, the manufacturing industry and cyber technology suppliers.
- MASC, the research on autonomous intelligent Multi Agent Systems for Cyber defence, is a discovery type of research and looks at the long term, a ten-year horizon probably. The MoD, the IoT and IIoT supply chain, as well as manufacturing industries and cybersecurity technology suppliers are invited to join this research stream. SOSDYN research findings will help augmenting agents' situation awareness. The LSCS will help testing and validating the developments of the MASC technology. And the MICE research stream will look at how to develop MASC agents. The CETAP platform will help testing how secure MASC agents will be.

To host this research, new labs and spaces are being set-up and will reach full power within the next two years.

References

Bassellier, G., Horner Reich, B. & Benbasat, I., 2001. Information Technology Competence of Business Managers: A Definition and Research Model. *Journal of Management Information Systems,* 17(4), pp. 159-182.

Bechtold, J., Kern, A., Lauenstein, C. & Bernhofer, L., 2014. *Industry 4.0 - The Capgemini Consulting View. Sharpening the Picture beyond the Hype,* Available from https://www.capgemini.com/consulting/resources/industry4-0/#: Capgemini Consulting.

Bista, S., Bista, P. & Rana, V. K., 2013. *The impact of Software Defined Networking on the network infrastructures of enterprise networks and the growing ISP industry of Nepal.* Park Village Resort, Nepal, 7th NASCoIT conference, 28th September 2013, https://nascoit.org.np/papers/The%20impact%20of%20Software%20Defined%20Networking.pdf.

Blakely, B. & Theron, P., 2018. *Decision flow-based Agent Action Planning.* Prague, 18-20 October 2017: https://export.arxiv.org/pdf/1804.07646.

Bodeau, D. J. & Graubart, R., 2011. *Cyber resiliency engineering framework,* Bedford, MA: MITRE, MITRE Technical Report MTR110237.

CISCO, 2014. *Addressing the Full Attack Continuum. A New Security Model for Before, During, and After an Attack,* http://www.cisco.com/go/security: CISCO.

COM(2017) 477 final, 2017. *Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"),* Brussels: European Commission.

ETSI, 2017. *Quantum Safe Cryptography; Case Studies and Deployment Scenarios,* Nice Sophia Antipolis, France: ETSI - ETSI GR QSC 003 V1.1.1 (2017-02).

European Commission - DG JLS, 2011. *A study on measures to analyse and improve European emergency preparedness in the field of fixed and mobile telecommunications and Internet.,* Brussels: European Commission, EC JLS/2008/D1/018 study, http://ec.europa.eu/information_society/policy/nis/strategy/prep_study/index_en.htm.

European Commission, 2017. *EU cybersecurity initiatives. Working towards a more secure online environment,* Brussels: European Commission, http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf.
Evans, S., 2016. *Manufacturing and Industrial Evolution – the future.* Cranfield, UK, Manufacturing 2075 conference, Cranfield University, December 7th 2016.
Fairbanks, R. J. & Caplan, S., 2004. Poor Interface Design and Lack of Usability Testing Facilitate Medical Error. *The Joint Commission Journal on Quality and Safety,* 30(10), pp. 579-584.
Ferber, S., 2012. *Industry 4.0: Agility in production?.* [Online]
Available at: https://blog.bosch-si.com/industry40/industry-4-0-agility-in-production
[Accessed 11 July 2018].
Ganek, A. G. & Corbi, T. A., 2003. The dawning of the autonomic computing era. *IBM Systems Journal,* 42(1), pp. 5-18.
Gates, D. & Bremicker, M., 2017. *Beyond the hype. Separating ambition from reality in i4.0,* Switzerland: KPMG International.
Guth, J. et al., 2018. A Detailed Analysis of IoT Platform Architectures: Concepts, Similarities, and Differences. In: B. Di Martino, K. Li, L. T. Yang & A. Esposito, eds. *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives.* Singapore: Springer-Verlag, pp. 81-101.
JOIN(2017) 450 final, 2017. *JOIN(2017) 450 final - Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,* Brussels: European Commission - High Representative of the Union for Foreign Affairs and Security policy.
Kott, A. et al., 2018. *Initial Reference Architecture of an Intelligent Autonomous Agent for Cyber Defense,* Adelphi, MD: US Army Research Laboratory, ARL-TR-8337, March 2018, available from https://arxiv.org/abs/1803.10664.
LeBlanc, B., Losiewicz, P. & Hourlier, S., 2017. *A Program for effective and secure operations by Autonomous Agents and Human Operators in communications constrained tactical environments.* Prague: NATO IST-152 workshop.
Liang, C.-W. & Hsu, J. Y.-j., 2014. *Auction-Based Resource Access Protocols in IoT Service Systems.* IEEE, IEEE 7th International Conference on Service-Oriented Computing and Applications.
Lie, E., Macmillan, R. & Keck, R., 2009. *The Role and Responsibilities of an Effective Regulator,* Geneva, Switzerland: International Telecommunication Union, www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/papers.html.
Lopez, D., Reid, A., Manzalini, A. & Odini, M.-P., 2016. Impact of SDN/NFV on Business Models. *IEEE Softwarization,* 2016(January), pp. online at https://sdn.ieee.org/newsletter/january-2016/impact-of-sdn-nfv-on-business-models.
Mahmud, R., Kotagiri, R. & Buyya, R., 2018. Fog Computing: A Taxonomy, Survey and Future Directions. In: K. L. L. T. Y. &. A. E. B. Di Martino, ed. *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives.* Singapore: Springer-Verlag, pp. 103-130.
Marsh, P., 2016. *Global manufacturing: the next 100 years.* Cranfield, UK, Manufacturing 2075 conference, Cranfield University, December 7th 2016 .
Mikolic-Torreira, I. et al., 2016. *A framework for exploring cybersecurity policy options,* Santa Monica, CA: RAND Corporation.
MITRE, 2018. *Cybersecurity Standards.* [Online]
Available at: https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-resources/standards
[Accessed 23 May 2018].
NIST, 2014. *Framework for Improving Critical Infrastructure Cybersecurity,* U.S. Department of Commerce: National Institute of Standards and Technology.
NIST, 2018. *Draft NISTIR 8200. Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT),* Gaithersburg, MD: NIST - Interagency International Cybersecurity Standardization Working Group (IICS WG).
Ottawa Citizen, 2017. *Why you should be 'suitably paranoid' about your home devices' cybersecurity.* [Online]
Available at: https://ottawacitizen.com/news/canada/are-you-suitably-paranoid-about-your-home-devices-cybersecurity/wcm/8b34e06b-2930-4099-b390-4cb6e1c0bb48
[Accessed 10 July 2018].
Shaikh, S., 2015. *Cyber Security, an Age of Paranoia?.* [Online]

Available at: https://www.btplc.com/Innovation/Innovationnews/BTTowerTalk/index.htm
[Accessed 10 July 2018].
Sniderman, B., Mahto, M. & Cotteleer, M. J., 2016. *Industry 4.0 and manufacturing ecosystems. Exploring the world of connected enterprises,* Deloitte Touche Tohmatsu Limited: Deloitte University Press.
Sterbenz, J. et al., September 2002. *Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions,* Atlanta, Georgia: Paper presented at WiSe'02.
Sterbenz, J. P. et al., 2010. Resilience and Survivability in Communication Networks: Strategies, Principles, and Survey of Disciplines. *Computer Networks,* June, 54(8), pp. 1245-1265.
Theron, P., 2013. ICT Resilience as Dynamic Process and Cumulative Aptitude. In: P. Theron & S. Bologna, eds. *Critical Information Infrastructure Protection and Resilience in the ICT Sector.* Hershey, PA: IGI Global, pp. 1-35.
Theron, P., 2016. *Introduction to the European IACS components Cybersecurity Certification Framework (ICCF),* Luxembourg: Publications Office of the European Union.
Theron, P., 2016. Lessons and Needs for Improving Critical Infrastructures' Resilience. 10 August.pp. Available at http://cip.gmu.edu/2016/08/10/lessons-needs-improving-critical-infrastructures-resilience/.
Theron, P. et al., 2019. For an autonomous cyber defense of autonomous and complex military systems. NATO's AICARA reference architecture for autonomous intelligent cyber defense agents. In: E. t. b. confirmed, ed. *Foundations of Autonomous Adaptive Cyber Systems (Provisional title).* Berlin, Germany: Springer, p. TBD.
Theron, P. & Lazari, A., 2018. *IACS Cybersecurity Certification Framework (ICCF): Lessons and enhancements from 2017 experiments,* Luxembourg: Publications Office of the European Union.
Trimintzios, P. et al., 2017. *Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU,* Brussels: European Parliamentary Research Service, Scientific Foresight Unit (STOA), http://www.europarl.europa.eu/stoa.
U.S. Department of Energy, 2013. *Cybersecurity Is Every Citizen's Responsibility.* [Online]
Available at: https://www.energy.gov/articles/cybersecurity-every-citizens-responsibility
[Accessed 10 July 2018].
UN-DESA, 2011. *Cybersecurity: A global issue demanding a global approach.* [Online]
Available at: http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html
[Accessed 10 July 2018].
Vicino, D., Lung, C.-H., Wainer, G. & Dalle, O., 2014. Evaluating the impact of Software-Defined Networks' Reactive Routing on BitTorrent performance. *Procedia Computer Science,* 34(2014), pp. 668 – 673, proceedings of the International Workshop on Software Defined Networks for a New Generation of Applications and Services (SDN-NGAS-2014).
Wikipedia, 27 March 2018. *List of automation protocols.* [Online]
Available at: https://en.wikipedia.org/wiki/List_of_automation_protocols
[Accessed 28 June 2018].