Challenges of Safety Assurance for Industry 4.0

Omar Jaradat*, Irfan Sljivo*, Ibrahim Habli†, Richard Hawkins†
* Mälardalen Real-Time Research Centre, Mälardalen University, Västerås, Sweden
†Department of Computer Science, University of York, York, UK
{omar.jaradat, irfan.sljivo}@mdh.se, {ibrahim.habli, richard.hawkins}@york.ac.uk

***Abstract*—The Internet-of-Things (IoT) has enabled Industry 4.0 as a new manufacturing paradigm. The envisioned future of Industry 4.0 and Smart Factories is to be highly configurable and composed mainly of the 'things' that are expected to come with some, often partial, assurance guarantees. However, many factories are categorised as safety-critical, e.g. due to the use of heavy machinery or hazardous substances. As such, some of the guarantees provided by the 'things', e.g. related to performance and availability, are deemed as necessary in order to ensure the safety of the manufacturing processes and the resulting products. In this paper, we explore key safety challenges posed by Industry 4.0 and identify the characteristics that its safety assurance should exhibit. We propose a set of safety assurance responsibilities, e.g. system integrators, cloud service providers and 'things' suppliers. Finally, we reflect on the desirable modularity of such a safety assurance approach as a basis for cooperative, on-demand and continuous reasoning for Industry 4.0 architectures and services.**

***Keywords*—IoT, Industry 4.0, Cloud computing, Safety**

I. Introduction

The Internet-of-Things (IoT) can be seen as a system of inter-connected cyber-physical objects that collect and exchange data. More formally, IoT is defined as "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies*" [23]. This infrastructure allows the things to be sensed and controlled remotely so that their integration into the physical world leads to different ways to utilise the things in various reconfigurable applications. Cloud Computing is a fundamental infrastructural element for IoT, enabling different types of *X as a Service* (*XaaS*) [18], where X is a software, platform, infrastructure, etc. In this paper, we adopt the NIST definition of Cloud Computing: "*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*" [16].

The marriage of the IoT and Cloud services (e.g., cloud XaaS) has paved the way towards the fourth industrial generation, Industry 4.0 (aka Industrie 4.0), as a new trend of automation and data exchange in the manufacturing industry. This new industrial paradigm is characterised by its ability to reconfigure and often optimise autonomously, particularly during the operational stages. Moving certain manufacturing services, e.g., scheduling and data storage and analytics, to the Cloud has potential benefits in cost reduction, energy efficiency, sharing of resources and increased flexibility. The use of Cloud Computing in critical applications has been highlighted as a significant area of research, especially for production and manufacturing systems [2], [6], [11], [24].

However, factories are often categorised as safety-critical systems as failures of these systems, under certain conditions, can lead to human harm or damage to property or the environment, e.g. due to the use of heavy machinery or hazardous substances. As such, the risk associated with the manufacturing processes and the resulting products has to be analysed, controlled and monitored. However, the reconfigurable, modular and dynamic nature of Smart Factories pose significant safety assurance challenges. For example, designers or operators of factories do not have much control over the design and evolution of the 'things' or Cloud-based services that are increasingly being used in manufacturing processes. This potentially weakens confidence in the safety of the factory and can undermine the overall safety case [20], i.e. due to high degrees of uncertainty about the actual performance or behaviour of these 'things' or Cloud-based services.

Most of the reviewed published literature on IoT and Cloud Computing reveals focus on security in particular and dependability in general but without much focus on safety. For example, the German automation technology supplier 'PILZ' [17] stated that the Industry 4.0 vision entails modular plants being reconfigured quickly and flexibly. They view the control and decision making process in Industry 4.0 becoming more decentralised and highlight safety, in particular, as a fundamental challenge, with emphasis on the necessary modular certification of the individual factory devices (PILZ uses the term Safety 4.0 to indicate modular safety solutions).

In this paper, we introduce a common Industry 4.0 architectural style (Section II) and explore its safety assurance characteristics (Section III). We then propose a three types of assurance responsibilities, e.g. system integrators, cloud service providers and 'things' suppliers (Section IV). Finally, we reflect on the challenges of Industry 4.0 assurance (Section V).

II. Industry 4.0 Architecture

In this section, we introduce a generic architecture for Industry 4.0. This architecture comprises three levels, as depicted in Fig. 1, where the things and Fog/Edge levels typically represent the local part of the system, while the Cloud represents a remote infrastructure that is usually owned by a third-party service provider:

- *Things Level* is composed of a set of things that enable interaction with the physical environment via different sensing/actuating devices. We consider a thing as an object capable of communicating with other networked devices [1]. Due to the limited storage and processing

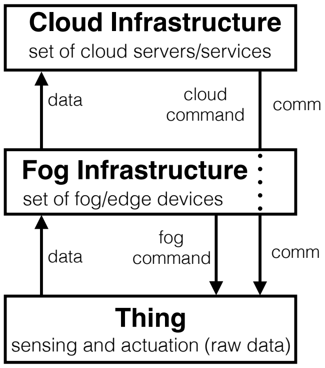

Fig. 1. Industry 4.0 Generic Architecture

power, devices from this level rely on the Fog or Cloud infrastructures for storage and processing services.

- *Fog Level* is composed of a set of Fog/Edge devices that are directly connected to things or/and Cloud infrastructure. We consider Fog devices to be local computational devices that offer advanced storage and processing power to the things and rely on remote Cloud infrastructure for high-power computing and storage. The Fog devices receive data from the things and, depending on the system configuration, might forward the data to the Cloud infrastructure. Moreover, the Fog devices may perform partial processing of the data and directly instruct commands to the things.
- *Cloud Level* is composed of a set of remote servers providing on-demand capabilities. The Cloud infrastructure typically receives data from the Fog devices, processes the data and forwards commands to the things via Fog devices.

The distribution of control, authority and responsibility between the things and the Fog and Cloud infrastructures depends on factors such as (1) performance, e.g. avoiding the Cloud for hard real-time requirements, (2) global and adaptive services, e.g. Big Data analytics via the Cloud and (3) local situational awareness, e.g. via smart IoT-based devices. Understanding the behaviour and integrity of the individual things and infrastructural elements, and their interactions, is a prerequisite for assuring the safety of Industry 4.0.

III. Safety Assurance Characteristics for Industry 4.0

Considering the capabilities of Industry 4.0, in this Section, we explore key characteristics of its safety assurance.

1) Modular and Cooperative: The safety assurance for Industry 4.0 will often have to be cooperative in a sense that a safety or assurance case cannot be built by a single stakeholder or organisation. Since the implementation of the business models is shifting from a single company to a network of service providers [13], so does the resulting system shift from a standalone system to a network of devices and services, performing, cooperatively, a number of functionalities. Each business participating in the integrated system, e.g. as a thing supplier (be it a “dumb” or a “smart” connected device), should accompany the provided thing with a set of safety assurances for different usages. However, since the suppliers cannot provide all the needed safety assurances out-of-context, certain properties should be assured by the integrator in the context of the particular usage of the thing.

2) Continuous: Safety cases are used to justify how the risk of each identified hazard has been eliminated or adequately mitigated. Industry 4.0 assumes that a modular factory can be reconfigured quickly and flexibly. The safety assurance of such a factory is expected to be in a position to accommodate this widening of flexibility. For safety cases, they should comprise evidence to make a convincing argument to support the relevant safety claims [14]. However, some claims and pieces of evidence might get invalidated due to reconfigurations that commonly take place in the factory, e.g. changes to the manufacturing processes and services. Hence, safety cases might be out of date and no longer reflect the actual safety performance of the system. To this end, the safety cases should be proactively reviewed and continuously maintained in order to justify the evolving status of the factory [5].

3) On-demand: As motivated in the previous characteristic, safety cases should be maintained after changing the associated factory to continuously demonstrate the status of the safety performance. Sometimes, however, updating the safety cases is not feasible because of the nature of the changes. That is, there might be drastic changes to the factory that could introduce new and different type of hazards that require repeating the entire safety assurance process and generating more and/or new pieces of evidence. Here, re-constructing the safety cases might be necessary as a more cost-effective option compared to updating the existing cases [21].

In this paper, we limit our focus to the modular and cooperative characteristics of safety assurance for Industry 4.0, considering the overall safety case for Smart Factories and future needs for continuous and on-demand assurance.

IV. Industry 4.0 Safety Assurance Responsibilities

In high-risk domains, assurance is typically demonstrated through the provision of an assurance case, consisting of a structured argument, i.e. justification, supported by evidence [14]. In this paper, the assurance case is for safety properties (aka safety case). As discussed in III, due to the co-operative nature of IoT, it is not possible for any single stakeholder to provide the assurance case for the entire system.

The constituent things, and the required infrastructure elements will be developed and provided by different organisations. It is these separate organisations that have the knowledge of the properties and characteristics of their components (i.e. things or infrastructure elements). However, these suppliers are only able to reason about the assurance of their own components, and can say little about the assurance of the IoT system as a whole, especially with regard to system-level conditions such as hazards, accidents and harm. The system integrator must therefore consider what is required for the assurance of system-level properties, which are primarily safety properties in this paper, and then show that the things or infrastructure elements being used are able to support this.

This leads us to propose a modular approach to assurance for IoT. The overall assurance case structure for the IoT system, is split into a number of modules, where each module reasons about a different aspect of the IoT system. There are assurance modules for each of the things and infrastructure elements, and modules dealing with the assurance of the integration of these into an IoT system.

The different stakeholders have assurance responsibilities. These responsibilities are discussed below.

1) Component supplier responsibility: The component suppliers need to provide a clearly defined context of their components in terms of the assured component properties under the given environmental conditions, and description of potentially failure behaviours. Each of the assured properties must be related to a set of conditions under which the property is assured, and the confidence in this assurance should be clearly communicated. To increase the confidence, the component supplier should assure with the necessary degree of confidence that if the set of conditions is satisfied, then the resulting property is also satisfied. Moreover, the component supplier shall provide assurance with high confidence that all failure behaviours have been identified. The failure behaviours may be due to violation of the conditions, or due to their incompletion. The list of failure behaviours should be continuously maintained by the supplier, hence the corresponding assurance should be accordingly updated.

2) Service supplier responsibility (including infrastructure): Similarly to the component suppliers, the service suppliers also need to define the context for using the service and the descriptions of their failure behaviours. But unlike for component suppliers, the specification of the properties and conditions is more complex and requires structures such as degradation cascades to fully describe the interaction. Just as the component suppliers, service suppliers should also assure with high confidence the properties and the list of failure behaviours. Moreover, due to the complex interaction and active participation of the supplier in providing the service, continuous evaluation of the interaction is needed to both allow for adaptivity of the connected systems and the cooperative functionality as a whole, and also to evaluate the confidence of the specification describing the interaction. Hence the service supplier needs to assure with high confidence that the list failure behaviours and the interaction specification is continuously maintained.

3) Integrator responsibility: Since the integrated system is dynamic and configurable, the integrator should be ready to assure that every permitted configuration and the assembly of the components is acceptably safe. For a particular configuration, the integrator should identify the internet-enabled things, and the accompanying IoT infrastructure. Since such components come with certain safety analysis results performed independently, the integrator should perform the additional analysis to identify ways in which the things can contribute to each hazard. The safety requirements derived form such analysis should be either satisfied by the properties assured for the things under the current configuration, or an alternative safety mechanism should be specified to address the safety requirement. Depending on the nature of the thing and involvement of its supplier, the required properties can be subject to negotiation. For example, under the current configuration the smart factory might use lidar sensors for visual input processing, which puts high demands on the cloud service processing the input. If the cloud service cannot be configured to comply with the demanding requirements, either a new service configuration can be negotiated with the provider, or local mechanisms may be employed to reduce the demands to acceptable levels.

V. Discussion and Challenges

We have highlighted a number of safety challenges posed by Industry 4.0 and proposed a modular assurance approach that has the potential to address some of these challenges, particularly with regard to the compositional and configurable nature of IoT-based architectures. In essence, our preliminary approach builds on past and current research on assume-guarantee reasoning, contract-based assurance and modular certification for safety-critical applications [19] [15] [7]. Historically, these approaches formed the basis for safety cases and certification for systems in various domains including automotive [22] and aviation [4].

However, some fundamental safety assurance problems remain and have to be addressed as a prerequisite for realising the general-purpose vision of Industry 4.0. We explore, and reflect on, these in the rest of this section.

A. Industry 4.0 Safety Validation Challenge

We discussed the potential for modular reasoning to drive the structure of the overall safety case for Industry 4.0 architectures and meet the safety requirements. However, the fundamental problem does not lie in how the configurable architectures meet the safety requirements. Rather, the issue lies in the *generation* of these safety requirements in the first place. The ad hoc assemblage of things and infrastructures for Industry 4.0 architectures will likely result in new hazards and/or risk ratings and as such new safety requirements. These *emerging* hazards are due to expected, yet unpredictable, reconfigurations or redeployments of the architecture in multiple contexts (i.e. we cannot assume that the world is stable and variation only lies within our system). This will often mean that the hazard analysis, or at least a large part of it, will have to be manually repeated for each reconfiguration or deployment and should produce an updated set of safety requirements (i.e. each of these changes might be considered as a new factory). This can be seen as undermining the general-purpose and reusable nature of Industry 4.0 architectures, i.e. where rapid reconfiguration and deployment is seen as a unique selling point. In other words, modularity and contract-based reasoning largely deal with the *verification* issue whereas hazard analysis addresses the *validation* problem. Safety validation, against the intended real world usage, is the essence of safety assurance and how risk and harm are assessed, perceived and accepted.

B. Industry 4.0 Safety Confidence Challenge

In our example definition of assurance contracts for things and infrastructures within Industry 4.0 architectures, we highlighted the need to specify necessary *properties* that have to be provided (e.g. measurement of air pressure values) to a particular level of *integrity* (e.g. accuracy of 0.001%) and *confidence* (e.g. 99%). For large socio-technical IoT systems such as Smart Factories, confidence will inevitably be measured using different qualitative [10] and quantitative [5] indicators. Propagating confidence from the different qualitative and quantitative measures associated with the various things and infrastructures is necessary to assess confidence in the safety of the overall configured system [9]. This has to be performed dynamically and on-demand to address the particular reconfigurable characteristics of Industry 4.0 architectures. This is a grand safety challenge for Industry 4.0 (and safety engineering generally). Current approaches to specifying confidence and associating it with assume-guarantee contract specification for individual components is relatively straightforward compared to the challenge of *assessing*, dynamically, confidence for the different reconfigurations.

C. Industry 4.0 Commercial Pressure Challenge

The financial appeal of commercially available things and infrastructures, which *appear* to be dependable although they are not developed for safety-critical applications, should not be undermined. The business pressure is mounting on safety engineers to accept the use of, relatively *cheap*, consumer electronics and commercially available cloud-based services. Resistance from the safety community on the basis of difficulty or novelty (i.e. we do not do it this way in safety) could be counter-productive. This might result in aliening or excluding safety engineers when design decisions are made or more likely, and sometimes rightly so, appealing to reduction in overall risk despite increases in technological risks (e.g. a typical risk-benefit argument in clinical applications in which clinical benefits outweigh technological risks [12]).

D. Industry 4.0 Security-Informed Safety Challenge

There is now almost a consensus on the necessity to address cyber security in safety assurance [3]. This issue takes a greater significance for Industry 4.0 where remote connectivity and the use of commercially available infrastructures and things expose the system to a wide range of cyber threats (particularly Distributed Denial of Service [8]). Security risks tend to be more dynamic than safety risks. As such, exploring the extent to which an Industry 4.0 architecture might have to reconfigure in the event of a security breach is a significant challenge, particularly in how it might compromise safety assurance (i.e. a typical tradeoff between safety and security that has to be made more explicit in the safety assurance case).

VI. Conclusions

In conclusion, in this paper, we explored a number of characteristics for the safety assurance of Industry 4.0 and focused on modularity as a key characteristic of the overall assurance case for safety. We also highlighted some grand challenges that remain and will be a focus for our future work.

Acknowledgment

This work is supported by the Swedish Foundation for Strategic Research (SSF) via the project Future factories in the Cloud (FiC).

References

[1] L. Atzori, A. Iera, and G. Morabito. The internet of things: A survey. *Computer networks*, 54(15):2787–2805, 2010.

[2] A. Bessani, R. Kapitza, D. Petcu, P. Romano, S. V. Gogouvitis, D. Kyriazis, and R. G. Cascella. A look to the old-world sky: EU-funded dependability cloud computing research. *Operating Systems Review*, 46(2):43–56, July 2012.

[3] R. Bloomfield, K. Netkachova, and R. Stroud. Security-informed safety: if its not secure, its not safe. In *International Workshop on Software Engineering for Resilient Systems*, pages 17–32. Springer, 2013.

[4] P. Conmy, M. Nicholson, and J. McDermid. Safety assurance contracts for integrated modular avionics. In *Proceedings of the 8th Australian workshop on Safety critical systems and software-Volume 33*, pages 69–78. Australian Computer Society, Inc., 2003.

[5] E. Denney, G. Pai, and I. Habli. Dynamic safety cases for through-life safety assurance. In *Proceedings of the 37th International Conference on Software Engineering-Volume 2*, pages 587–590. IEEE Press, 2015.

[6] B. Esmaeilian, S. Behdad, and B. Wang. The evolution and future of manufacturing: A review. *Journal of Manufacturing Systems*, 39:79 – 100, 2016.

[7] J. Fenn, R. Hawkins, P. Williams, and T. Kelly. Safety case composition using contracts-refinements based on feedback from an industrial case study. In *The Safety of Systems*, pages 133–146. Springer London, 2007.

[8] Guardian. DDoS attack that disrupted internet was largest of its kind in history, experts say. www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[9] J. Guiochet, Q. A. Do Hoang, and M. Kaaniche. A model for safety case confidence assessment. In *International Conference on Computer Safety, Reliability, and Security*, pages 313–327. Springer, 2015.

[10] R. Hawkins, T. Kelly, J. Knight, and P. Graydon. A new approach to creating clear safety arguments. In *Advances in systems safety*, pages 3–23. Springer, 2011.

[11] W. He and L. Xu. A state-of-the-art survey of cloud manufacturing. *Int. J. Comput. Integr. Manuf.*, 28(3):239–250, Mar. 2015.

[12] ISO. *ISO 14971: medical devices-application of risk management to medical devices*. ISO, 2012.

[13] H. Kagermann, J. Helbig, A. Hellinger, and W. Wahlster. *Recommendations for Implementing the strategic initiative INDUSTRIE 4.0: Securing the future of German manufacturing industry*. Forschungsunion, 2013.

[14] T. P. Kelly. *Arguing safety: a systematic approach to managing safety cases*. University of York, 1999.

[15] T. P. Kelly. Concepts and principles of compositional safety case construction. *Contract Research Report for QinetiQ COMSA/2001/1/1*, 34, 2001.

[16] P. Mell, T. Grance, et al. The nist definition of cloud computing. 2011.

[17] PILZ. Industrie 4.0 – safe and smart (white paper), June 2016.

[18] B. P. Rimal, E. Choi, and I. Lumb. A taxonomy and survey of cloud computing systems. In *2009 Fifth International Joint Conference on INC, IMS and IDC*, pages 44–51, Aug 2009.

[19] J. Rushby. Modular certification. Technical report, Sept. 2001.

[20] J. Rushby. The interpretation and evaluation of assurance cases. Technical Report SRI-CSL-15-01, Computer Science Laboratory, SRI International, Menlo Park, CA, July 2015. Available at http://www.csl.sri.com/users/rushby/papers/sri-csl-15-1-assurance-cases.pdf.

[21] J. Rushby. Trustworthy self-integrating systems. In N. Bjørner, S. Prasad, and L. Parida, editors, *12th International Conference on Distributed Computing and Internet Technology, ICDCIT 2016*, volume 9581 of *Lecture Notes in Computer Science*, pages 19–29, Bhubaneswar, India, Jan. 2016. Springer-Verlag.

[22] D. Schneider and M. Trapp. Conditional safety certification of open adaptive systems. *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, 8(2):8, 2013.

[23] Telecommunication standardization sector of ITU. *Overview of the Internet of things*, Y.2060 edition, 6 2012.

[24] D. Wu, M. J. Greer, D. W. Rosen, and D. Schaefer. Cloud manufacturing: Strategic vision and state-of-the-art. *Journal of Manufacturing Systems*, 32(4):564 – 579, 2013.