Security Challenges for Cloud Manufacturing: A Case Study in the Space Domain

Diana Peters and Thomas S. Heinze

Institute of Data Science
German Aerospace Center (DLR)
[diana.peters,thomas.heinze]@dlr.de

Abstract. Industry 4.0 and cloud manufacturing are emerging trends to advance the automation and digitization of manufacturing systems. Both share cloud computing as key enabling technology. However, the increase in interconnectedness comes with crucial security issues. In this position paper, we consider a production process in the space domain and highlight the security challenges which arise when adapting the process for the Industry 4.0 and cloud manufacturing paradigm.

1 Introduction

Industry 4.0 and cloud manufacturing have lately drawn much attention in industry and academia, as is demonstrated by the amount of respective literature in recent years [1,5]. Industry 4.0 is used as an umbrella term covering digitization and automation in industry and relating to technologies like internet of things, big data analytic, or cloud computing. Cloud manufacturing transfers cloud computing to manufacturing by providing a platform for distributed access to a pool of shared manufacturing resources encapsulated as services. Customers are then able to send their requirements to the platform to request services covering all stages of a product life cycle, ranging from product design to maintenance.

While Industry 4.0 and cloud manufacturing promise substantial improvements of the production process in terms of production efficiency and flexibility, they also pose various challenges. Due to increased automation and interconnectedness of components, security in particular is a major obstacle. In this position paper, we investigate the security issues arising for a collaborative cloud production platform, which we are developing in the space domain.

2 Production Platform for the Space Domain

2.1 Product Lifecycle

The European Space Agency divides the life cycle of a spacecraft into seven phases: *0, A, B, C, D, E*, and *F* [2]. In phase *0*, the aim is to find out if a mission is possible at all, which is refined in phase *A* by an initial plan and feasibility studies. This is refined in phases *B* and *C*, resulting in the detailed definition

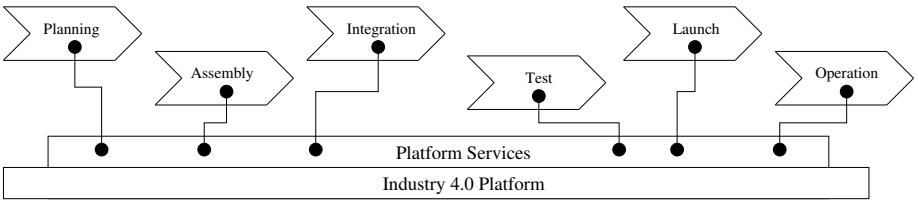

Fig. 1. Platform for Spacecraft Production

of the spacecraft and all its components. Assembly, integration, and test are conducted in phase *D*, which includes not only the spacecraft but also its ground segment. During phase *E*, the spacecraft is launched and operated. Eventually, the spacecraft is safely disposed in phase *F* (cf. Fig. 1).

2.2 Collaborative Production Platform

Our long-term development goal is a production platform covering the entire spacecraft life cycle. We currently focus on planning, which happens in phases *0, A, B, C*. Planning involves several stakeholders, e.g. project initiator, customers, and manufacturers, and continuous information exchange between them.

DLR's *Concurrent Engineering Facility* provides "a guided procedure, the simultaneous access to multidisciplinary groups of experts to a shared database, and the direct verbal and medial communication between all the experts" [6]. Together with the tool *Virtual Satellite* [4], it is used for planning spacecraft at DLR. Data exchange with manufacturers or other parties in later phases of a spacecraft life cycle is currently not covered by that collaborative process. To remedy that, we propose a production platform that allows uniform and standardized information exchange and is thus freeing stakeholders from the burden of manually seeking information and tracing the information flow. The platform enables the flexibility required to meet the needs of the distributed and multi-level supply chains of the DLR.

There will not be a sudden shift from the current system and, especially, from current processes and workflows, to the new platform. We think, however, that working on tools, methods, and standards conjointly with the different stakeholders is a process which will eventually lead to a platform that all parties are willing to use. We see the platform as an assembly of services, interfaces, and tools that enable data exchange in an standardized and automated way.

As a representative example of a process that currently involves a lot of manual work and which would benefit from automation by machine-readable information exchange via our platform, we consider the offer management between a manufacturer and a (potential) customer. In the process, the customer asks for information (in terms of *Request for Information (RFI)*). The manufacturer assembles existing documents, experiences, etc. into a first answer. If the customer is interested, they agree on a proposal request (*Request for proposal (RFP)*). This request already includes information from the customer, like specifications,

requirements, or timetables. The manufacturer then generates an offer, including a technical specification of the product. This process involves the frequent interchange of documents between both sites, even more due to often unique products or small batches thereof. Compared to other industries, which usually sell a lot more off-the-shelf products, there is more effort needed to create an offer. A machine-readable format of the customer's requirements would allow for automatically generating and processing offers in a standardized fashion, implying advantages in terms of elasticity, resource pooling, and self-service.

3 Security Challenges

The increased interconnectedness of customers and vendors in the collaborative production platform comes together with novel security risks, which can not only threaten individual parties but also the whole supply chain. We can align these risks using their relation to *confidentiality*, *integrity*, and *availability*.

3.1 Confidentiality

Most prominently, information exchange on the platform has to be reliable and safe with respect to data privacy. Multiple vendors are using the platform, sharing confidential information on component design and competitive pricing. The customers share confidential information in their *RFPs*, the manufacturers in their proposals. Information disclosure should not only be prevented using measures like encryption and access control, but should also be subject to incident management as governed by regulations and policies (e.g., *Non-Disclosure Agreement (NDA), Memorandum of Understanding (MoU)*) [3]. Access control is a requirement concerning the entire spacecraft life cycle. For example, data transmitted from a spacecraft during operation is differentiated into health and payload data, the latter only accessible to customers. Health data, on the other hand, must be only accessible to ground control and to manufacturers.

3.2 Integrity

Flexibly provisioning and releasing manufacturing services poses the question of trust. Trust management has thus to play a key role, addressing both services and exchanged data, in order to protect the platform from tampering, e.g., by using malicious components [7]. Related to trust is the tracking of information flow such that data provenance can be used as reliable measure for data integrity. This is also true for other industries, but there, in case of malicious components, components can be replaced, which is impossible for a spacecraft in operation.

3.3 Availability

Eventually, a supply chain on our collaborative production platform relies on the availability of its supplier services, such that threats to vendors can cause the

entire supply chain to halt, which needs to be subject to any risk-based analysis of the system's architecture. For instance, backup infrastructures need to handle data from different vendors, again raising questions on trust and data integrity. Furthermore, in the space domain, another aspect of availability is crucial: certain components and infrastructure are highly critical. As an example, spacecraft missions are planned with dedicated ground stations. Switching to a different station in case of defect, or just moving the ground station's time frame, is rather difficult due to irrevocable parameters like location, frequency, and bandwidth.

4 Related Work

Various surveys on Industry 4.0 and cloud manufacturing identify security as an obstacle [1,5]. Due to space constraints, we refer to those surveys and provide just a brief summary next. Data breaches are the most prominent security concern, due to data typically touching a company's core competencies. Besides confidentiality of shared data, integrity and availability of data or collaborating services have also been considered critical (e.g., [7]). Most similar to our work is [1], where the authors study security issues in the whole product life cycle. We see our paper as a complement to the more abstract and summarizing discussion of [1], in that we consider the concrete case of a production platform in the space domain.

5 Conclusion

In this paper, we have outlined security issues arising when developing a production platform in the space domain based on Industry 4.0 and cloud manufacturing. As advocated by the idea of secure-by-design, we believe that building security in – from the start – helps in developing a secure and reliable production platform.

References

1. Chhetri, S.R., Faezi, S., Rashid, N., Faruque, M.A.A.: Manufacturing Supply Chain and Product Lifecycle Security in the Era of Industry 4.0. J. Hardware and Systems Security **2**(1), 51–68 (2018)
2. Space project management – Project planning and implementation. ECSS Standard ECSS-M-ST-10C (2009)
3. Esposito, C., Castiglione, A., Martini, B., Choo, K.K.R.: Cloud Manufacturing: Security, Privacy, and Forensic Concerns. IEEE Cloud Comput. **3**(4), 16–22 (2016)
4. Fischer, P.M., Deshmukh, M., Maiwald, V., Quantius, D., Gomez, A.M., Gerndt, A.: Conceptual data model: A foundation for successful concurrent engineering. Conc. Eng. **26**(1), 55–76 (2017)
5. Henzel, R., Herzwurm, G.: Cloud Manufacturing: A state-of-the-art survey of current issues. Proc. CIRP **72**, 947–952 (2018)
6. Martelo, A., Jahnke, S.S., Braukhane, A., Quantius, D., Maiwald, V., Romberg, O.: Statistics and Evaluation of 60+ Concurrent Engineering Studies at DLR. In: IAC 2017. IAF (2017)
7. Turner, H., White, J., Camelio, J.A., Williams, C., Amos, B., Parker, R.: Bad Parts: Are Our Manufacturing Systems at Risk of Silent Cyberattacks? IEEE Security & Privacy **13**(3), 40–47 (2015)