PLASMA – Platform for Service Management in Digital Remote Maintenance Applications

Natascha Stumpp[1], Doris Aschenbrenner[2], Manuel Stahl[3] and Andreas Aßmuth[4]

[1]ESSERT GmbH, Ubstadt-Weiher, Germany, Email: n.stumpp@essert.com
[2]Technische Universiteit Delft, Delft, Netherlands, Email: d.aschenbrenner@tudelft.nl
[3]Awesome Technologies Innovationslabor GmbH, Würzburg, Germany,
Email: manuel.stahl@awesome-technologies.de
[4]Technical University of Applied Sciences OTH Amberg-Weiden, Amberg, Germany, Email: a.assmuth@oth-aw.de

***Abstract*—To support maintenance and servicing of industrial machines, service processes are even today often performed manually and analogously, although supportive technologies such as augmented reality, virtual reality and digital platforms already exist. In many cases, neither technicians on-site nor remote experts have all the essential information and options for suitable actions available. Existing service products and platforms do not cover all the required functions in practice in order to map end-to-end processes. PLASMA is a concept for a Cloud-based remote maintenance platform designed to meet these demands. But for a real-life implementation of PLASMA, security measures are essential as we show in this paper.**

Keywords*–*Remote Maintenance; Cloud Solution; IoT; Security.

I. Introduction

A major competitive factor for manufacturing companies is a high and reliable availability of their production facilities. Despite already existing technology like Augmented Reality (AR) or Virtual Reality (VR), which has the potential to improve the service processes, a lot maintenance even today happens manually involving expert personnel. The common course of actions is depicted in Figure 1. Imagine that production in a company suddenly succumbs because one of their machines stops working. At first, the workers try to find the reason for the malfunction themselves. Maybe, the company employs their own technicians for the maintenance of their systems. In this case, the workers call for one of these technicians. In most cases, these technicians do not have the same knowledge of the machine that specialists employed by the manufacturer of the machines have. In many cases, neither the technician nor the worker have all essential information or know about possible actions to solve the problem the right away. Therefore, if the technicians are not able to solve the problem, e.g., they cannot find a solution in the manual of the machine, the company contacts the manufacturer using their hotline or website. This is when classic remote maintenance comes into play. If the machine is connected to the Internet, one of the manufacturer's specialists connects to the system, e.g., via VPN, and tries to gather more information about the malfunction. There are numerous cases in which one of the specialists has to travel to a broken machine to repair it in on-site. An essential part of the machine might be physically broken and only the manufacturer is capable of installing a spare part. Assuming the manufacturer is situated in Europe and the company with the broken system is, e.g., in Australia, the travel might take days causing high costs for the company due to the outage.

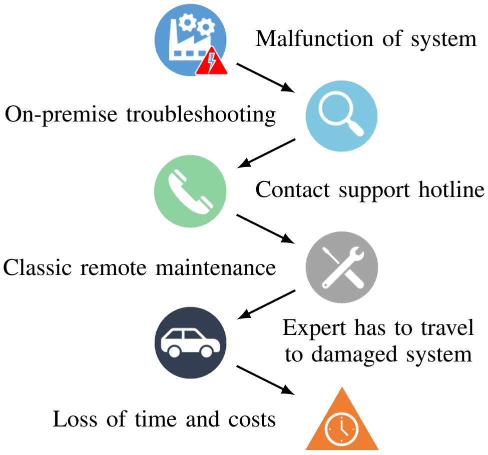
Malfunction of system
On-premise troubleshooting
Contact support hotline
Classic remote maintenance
Expert has to travel to damaged system
Loss of time and costs

Figure 1. Course of actions without an intelligent maintenance platform.

A small or medium-sized company today faces the challenge to implement their whole digital service processes in their existing environment, but only the currently available solutions usually cover just a small number of isolated use cases. Additionally, even though there is a large variety of such very specialised services, encapsulated platforms or IoT solutions readily available it is difficult to choose the ones the company really needs and that can be used in combination with services for other partial tasks of their digital service processes. For a complete mapping of application-driven end-to-end processes, it is necessary to realise a combination of these different platforms for small and middle-sized businesses which could probably struggle with the implementation by themselves. And these different platforms in practice do not necessarily interact properly with each other.

A. *Objective*

The joint project PLASMA aims for a holistic solution, which complements existing end-to-end business processes and supports the development of new service concepts, e.g., pay-per-x or x-as-a-service. Within the project an intelligent linkage between systems and platforms will be developed to allow integrated support and innovative business models all around service for production processes and facilities.

The solution should seamlessly fit into all process models and should be integrable into existing system landscapes as

ISBN: 978-1-61208-703-0

well as Enterprise Resource Planning (ERP) systems. Additionally, PLASMA contains an information and knowledge management component to store and document instructions, tutorials, service reports, master data and offers a device- and location-independent visualization of it. PLASMA enables the user to handle complex machine data and real-time simulations presented in an intuitive way. With AR- and VR-support it will be possible to offer almost real guidance for maintenance and service cases. The service management platform can connect customers and suppliers and is intended to reshape the whole transparent life cycle of a product without exposing sensible data.

B. Related work

Currently, there is a vast change within automation industry which is attributed to be the "fourth industrial revolution"; although this name is mainly used in a European context, there are similar movements in the USA and Asia. [1] The goal of all these approaches is nearly the same: Whereas information and communication technology has advanced rapidly in recent years, the discovered trends and possibilities shall be transferred, so that the production industry can benefit from it. Although electronics and network infrastructure have of course been used for a long time in an industrial production setting, it is important to realise that plants and production machines are high investment goods which go together with slower innovation cycles. This means that while in the customer off-the-shelf segment, this year's "new" hardware or software will be already considered "old" in half a year (and eventually even out of stack in a very short time span), the production eco-system has a relatively long usage period of hardware and software.

But what is exactly changing due to "Industry 4.0"? Next to individualised production, the core issues of Industry 4.0 can be formulated according to [2] as the integration of Internet and networking systems, smart objects and human machine interaction. This already emphasises the need for higher security requirements. Internet and Cloud applications [3] come with the need to integrate production systems in larger network infrastructures or even in the common Internet. The latter is strengthened by the trend to enable new kinds of human-machine interaction: Bring Your Own Device (BYOD) and remote access on industrial infrastructure with the help of mobile devices can without doubt offer new services or help to decrease costs. But they are also prone to attack scenarios.

The general challenges of cybersecurity are already widely known. According to the 2017 Global State of Information Security Survey [4], at least 80 % of companies in Europe have experienced at least one incident in 2016 and the number increased by 38 % compared to the preceding year. At the same time, approximately 69 % of European companies have either no or only basic understanding of their exposure to cyber risks and small and medium-sized companies tend to pay a higher price for this than larger companies. [5]

This topic increasingly receives the necessary political attention, for example, within the currently discussed European legislation regarding cybersecurity and vulnerability reporting. The above mentioned surveys mainly focus on "common" office and server infrastructure, although the current transition of the production industry towards "Industry 4.0" opens a large field of additional vulnerabilities. At the latest, since the Stuxnet [6] malware, the possibility of damage on industrial infrastructure through the Internet has received worldwide attention. In order to understand where additional concern of security research should focus on in the upcoming years, we provide an overview over the current changes within the production industry and the resulting possible vulnerabilities.

Due to the above explained transformation towards "Industry 4.0" a multitude of devices become connected to the common Internet; IBM estimates that the number will increase to 40 billion by 2020. [7] To conclude from the above remarks, it cannot be expected that those devices have a sufficient amount of security protection. Rather, a lot of devices might consist of old, most probably unpatched equipment, but are wired to critical infrastructures. Practical proof of this problem can be, for example, obtained with tools, which automatically detect and index Internet-facing industrial systems. The Shodan computer search engine [8] has been successfully tested to be able to index and identify Programmable Logic Controllers (PLCs). As those devices are standard components of industrial machines, several thousand devices can be found. As they are automatically tested on the running firmware and indexed accordingly, known vulnerabilities can be exploited easily.

In a 2015 overview, Sadeghi et al. [9] lists a couple of cyberattacks on IIoT (Industrial Internet of Things) and emphasize the fundamental difference between CPPS (Cyber-Physical Production System) compared to classical enterprise IT systems. In the tradeoff between security and availibility, the CPPS requirements are fundamentally different. They mention numerous possible attacks on intellectual property, product piracy. After providing an overview to different security architectures for CPS (Cyber-Physical System), the article concludes with the following statement: "However, existing security solutions are inappropriate since they do not scale to large networks of heterogeneous devices and cyber-physical systems with constrained resources and/or real-time requirements."

The book "Cybersecurity for Industry 4.0" [10] provides the technological foundations of cybersecurity for the production domain. It addresses existing threats caused by (A) humans, (B) technical insufficiencies, and (C) physical attacks of the actual IoT hardware. [11][12]

Recently, NIST published a draft with considerations for managing Internet of Things cybersecurity and privacy rights. [13] The main challenges are seen to protect device security, protect data security and protect individual's privacy. The publication focusses on "Internet of Things" in the sense explained above and does not cover specific production topics.

Are companies already aware of this topic? In the 2018 Global State of Information Security Survey (GSISS), 81 % of the companies judge IoT to be a critical part of at least some of their businesses. But only 39 % of survey respondents are confident that they have established "sufficient digital trust – security, privacy and data ethics– into their adoption of IoT". Furthermore, the replies from organisations using robotics or automation show that 40 % fear a disruption of operations due to a cyberattack on those systems.

II. The PLASMA Approach

To implement a holistic interactive support for service processes in production environments with the goal to reduce time- and resource-consuming error search and troubleshooting it is necessary to evaluate the following features:

1) Autonomous or automated event reporting in case of malfunction with digital communication tools like messengers or automated ticket systems,
2) Automated delivery of context-sensitive data sheets, videos, reports, statistics or other helpful stored information on a large variety of devices with different presentation models (textual, 2D, 3D, virtual, augmented, simulated, etc.)
3) An interactive remote support assistance with a far-off specialist,
4) A gateway to existing online-shop systems to automate the procurement of spare parts, and finally,
5) A complete connection to well-known ERP and Customer Relationship Management (CRM) systems.

With these features we aim to solve common use cases like a malfunctioning robot within an industrial plant. The goal is to find concrete solutions to elaborate a use case shown in Figure 2. The malfunction triggers the troubleshooting progress and tickets are created in an instant. A smart workflow manager can classify the incident and is able to suggests a solution depending on the severity of the error and archived data. The on-site worker gets useful information like data sheets, log files, instruction videos, virtual representations etc. to solve the issue by himself or receives remote support from a far-off specialist. All progress is documented and serves as new input for the smart workflow manager to sharpen its classification and support skills (cf. Figure 2).

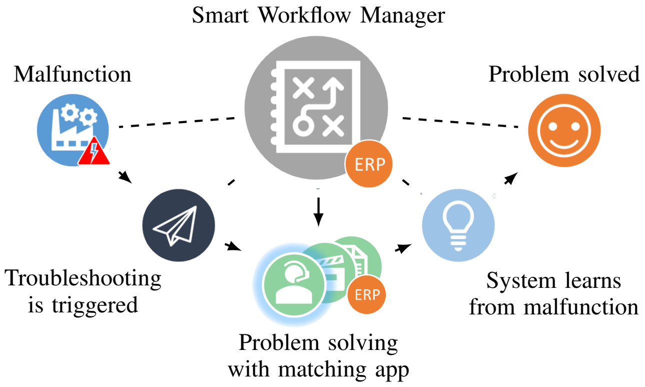
Smart Workflow Manager
Malfunction
Problem solved
ERP
Troubleshooting is triggered
ERP
System learns from malfunction
Problem solving with matching app

Figure 2. PLASMA workflow integrated in business processes

III. Security challenges

The amount of information, as well as the aggregation of information makes a remote maintenance platform like PLASMA a high-value target for attackers. Because of the key knowledge on technologies, machines and algorithms stored in the system, economic espionage funded by competitors certainly is an issue. In case the attacker is not capable of extracting the desired information from the platform, for example, he could also try to bring the system down using a Distributed Denial of Service (DDoS) attack. This would lead to high financial losses for the providers of the platform and the customers relying on the system alike. Organised crime should also be taken into account because these attackers could also try to bring the system down and demand ransom money to be paid. Last but not least, secret services might become attackers, too, if the information stored in the platform is essential for companies or industrial branches in that country.

To put it in a nutshell: since the remote maintenance platform is intended to be hosted in the Cloud, all of the already known security issues of Cloud services, e.g., documented by the Cloud Security Alliance in [14], apply to PLASMA as well. The necessity to keep the platform available and accessible has already been stated. Considering additional security services, e.g., as recommended by CCITT X.800 [15], it can be stated that their importance for the system security of PLASMA is equally essential:

Authentication: It must be ensured that every entity communicating with the platform is properly authenticated. This means, the capability to perfectly identify users as well as attached machines is needed in order to prevent Spoofing or masquerading attacks.

Access Control: In addition to authentication it must be ensured that authenticated users and machines alike are only able to access data they are allowed to. Due to the involvement of many different companies and roles, Role-based Access Control (RBAC) systems that have been adapted for use in Cloud environments, as proposed by Tang et al. [16] or Balamurugan et al. [17], seem to meet this demand.

Confidentiality: For big remote maintenance platforms, it seems likely that they will have competing companies as customers. This means, all data must be kept confidential such that, for instance, one company cannot get access to data from its competitor. As stated before, a remote maintenance platform stores and aggregates different types of information, like algorithms, procedures, etc., from manufacturers and customers or machine data about outages and errors. The system potentially gathers data that is relevant concerning the EU General Data Protection Regulation (GDPR), like working hours of operators or maybe errors made by certain operators. If technicians or experts use smartglasses during the error searching process, it is possible that other personnel might get recorded as well. This must be considered when it comes to GDPR-compliant saving of the data.

Integrity: PLASMA is intended to learn from previous errors and outages and if a malfunction occurs it is supposed to automatically suggest the most suitable action to deal with this scenario. An attacker might want to tamper with data in a way that leads to wrong suggestions, either to derogate trust in the remote maintenance platform or to harm an affected company. Other targets might be stored sensor data that lead to wrong simulation results when modified or falsified documentation on machines or manuals which could mislead technicians in case of a malfunction and cause even greater (physical) damage to the machine. Weir, Aßmuth and Jäger have proposed strategies for intrusion monitoring in Cloud services and for managing forensic recovery in the Cloud. [19] It is planned to realise and evaluate these concepts for the remote maintenance platform.

Nonrepudiation: It must be ensured that no party is capable of denying its involvement in any communication with or in the system. One reason to keep track of all actions in the system is to monitor the security of the system itself. But, of course, the provider of a remote maintenance platform wants to earn money with the system, too. Depending on the chosen business model the amount of messages or communication in general could be a metric to measure the usage of the system by a certain company and this may be used for billing.

In order to emphasise the necessity for appropriate security measures in a Cloud-based remote maintenance platform, we revisit the use case described in Section II and depicted in

Figure 2. Obviously, the Cloud-based remote maintenance platform needs to be protected against DDoS attacks, otherwise the system would not take notice of the malfunctioning robot in one of the customer's industrial plants. The triggering of the troubleshooting process might be related to another security issue. Imagine the situation that there is no malfunctioning robot, but the troubleshooting is triggered by a manipulated sensor. The attacker might want to stop production in the industrial plant or learn how the maintenance platform deals with such problems. The adversary might also try to tamper with the smart workflow manager which could lead to inappropriate solutions for detected malfunctions and eventually cause even greater damage. In addition to that, if information about malfunctions and errors, manuals or machine data gets manipulated, the system will not be capable of learning properly how to handle such issues. Less knowing technicians working in the industrial plant but also specialists might be tricked into wrong actions. Security is essential for a system like PLASMA.

IV. Involved Partners

The project core team consists of four parties: two industrial partners and two partners from academia.

ESSERT GmbH provides its multi-user remote support system and large user base as an important starting point for the development. It already offers a detailed user and permission administration, generates service reports for further documentation and is available for iOS, Android devices and smartglasses. [18]

Awesome Technologies is involved in a couple of Industry 4.0 projects which use Augmented and Virtual Reality with actual off-the shelf head-mounted displays, which also involves localization issues.

The cooperative setting of remote support is a very interesting topic within the framework of human supervisory control of smart cyber-physical production systems (smart factory) at TU Delft.

The research group of Prof. Dr. Aßmuth at OTH Amberg-Weiden has been working on concepts and solutions to ward off cyber-attacks aimed specifically at production facilities or vehicles for many years. In cooperation with international colleagues, concepts for increasing the security of Cloud services and securing forensic data in the Cloud have been published as well. [19]

The mentioned partners are currently looking for additional partners and funding programs for a PLASMA funding proposal.

V. Conclusion and Future Work

To compete on Cloud service markets SMEs need to focus on security challenges. Launching a great idea on the market may fail due to insufficient data security or privacy issues. Meeting a customer's high expectations for security is essential and a great challenge for SMEs because there are no negotiation opportunities. The authors are convinced that a Cloud-based remote maintenance platform, like PLASMA, will be needed in future. Therefore, they plan to realise such a system in a funded research project as a collaboration of industrial partners and partners from academia.

References

[1] Y. Liao, F. Deschamps, E. de Freitas Rocha Loures and L. F. Pierin Ramos, "Past, present and future of industry 4.0 – A systematic literature review and research agenda proposal." International journal of production research, vol. 55, no. 12, pp. 3609–3629, 2017.

[2] D. Zuehlke, "Smartfactory – towards a factory-of-things." Annual Reviews in Control, vol. 34, no. 1, pp. 129–138, 2010.

[3] P. Mell and T. Grance, "The NIST definition of Cloud Computing." SP 800-145, 2011, URL: https://doi.org/10.6028/NIST.SP.800-145 [accessed: 2019.04.12]

[4] PwC, Ed., "Key findings from The Global State of Information Security Survey 2017." Technical Report, 2017, URL: https://www.pwc.com/gx/en/issues/assets/2017-gsisss-bold-steps-to-manage-geopolitical-threats-final.pdf [accessed: 2019.04.12]

[5] K. Kertysova, E. Frinking, K. van den Dool, A. Maričić and K. Bhattacharyya, "Cybersecurity: Ensuring awareness and resilience of the private sector across europe in face of mounting cyber risks – Study." Technical Report, European Economic and Social Committee, March 2018, URL: https://www.eesc.europa.eu/en/our-work/publications-other-work/publications/cybersecurity-ensuring-awareness-and-resilience-private-sector-across-europe-face-mounting-cyber-risks-study [accessed: 2019.04.12]

[6] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon." IEEE Security & Privacy, vol. 9, no. 3, pp. 49–51, 2011.

[7] R. Baxter, "Bluemix and the Internet of Things", 2014, URL: https://developer.ibm.com/bluemix/2014/07/16/bluemix-internet-things [accessed: 2019.04.12]

[8] R. Bodenheim, J. Butts, S. Dunlap and B. Mullins, "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices." International Journal of Critical Infrastructure Protection, vol. 7, no. 2, pp. 114–123, 2014.

[9] A.-R. Sadeghi, C. Wachsmann and M. Waidner, "Security and privacy challenges in Industrial Internet of Things" in Proceedings of the 52nd Annual Design Automation Conference (DAC), June 07–11, 2015, San Francisco, USA. ACM, Article no. 54, ISBN: 978-1-4503-3520-1, 2015.

[10] L. Thames and D. Schaefer, Eds., "Cybersecurity for Industry 4.0. Analysis for Design and Manufacturing." Springer, ISBN: 978-3-319-50659-3, 2017.

[11] J. Dia and S. Smith, "A Hardware Threat Modeling Concept for Trustable Integrated Circuits" in Proceedings of the 2007 IEEE Region 5 Technical Conference, April 20–22, 2007, Fayetteville, USA. IEEE, Nov. 2007, pp. 354–357, ISBN: 978-1-4244-1279-2, 2007.

[12] A. B. Shahri and Z. Ismail, "A tree model for identification of threats as the first stage of risk assessment in HIS." Journal of Information Security, vol. 3, no. 2, pp. 169–176, 2012.

[13] K. Boeckl et. al, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks." Draft NISTIR 8228, September 2018, URL: https://doi.org/10.6028/NIST.IR.8228-draft [accessed: 2019.04.12]

[14] Cloud Security Alliance, Ed., The Treacherous 12, Top Threats to Cloud Computing + Industry Insights, 2017.

[15] The International Telegraph and Telephone Consultative Committee (CCITT), Ed., Security Architecture for Open Systems Interconnection for CCITT Applications, Recommendation X.800, March 1991.

[16] B. Tang, Q. Li and R. Sandhu, "A multi-tenant RBAC model for collaborative cloud services" in Proceedings of the Eleventh Annual Conference on Privacy, Security and Trust, July 10–12, 2013, Tarragona, Spain. IEEE, Sep. 2013, pp. 229–238, ISBN: 978-1-4673-5839-2.

[17] B. Balamurugan, E. Durga Chowdary and S. Linkesh, "A Combined Architecture for RBAC and DAC for Inter-cloud Communication" in Proceedings of the 3rd International Conference on Eco-friendly Computing and Communication Systems, December 18–21, 2014, Mangalore, India. IEEE, Aug. 2015, pp. 167–171, ISBN: 978-1-4799-7002-5.

[18] ESSERT GmbH, Ed., "Augmented Support", 2019, URL: https://www.essert.com/en/digital-processes [accessed: 2019.04.12]

[19] G. Weir, A. Aßmuth and N. Jäger, "Managing Forensic Recovery in the Cloud", International Journal on Advances in Security, vol. 11, no. 3 & 4, pp. 264–273, 2018.