Deloitte.

Enabling Smart Products and Smart Manufacturing by Security

The IT, OT and Product Security Triad

Security trends, opportunities and challenges

Smart manufacturing in the operational technology (OT) environment and smart products are changing the balance in the cyber security industrial landscape.

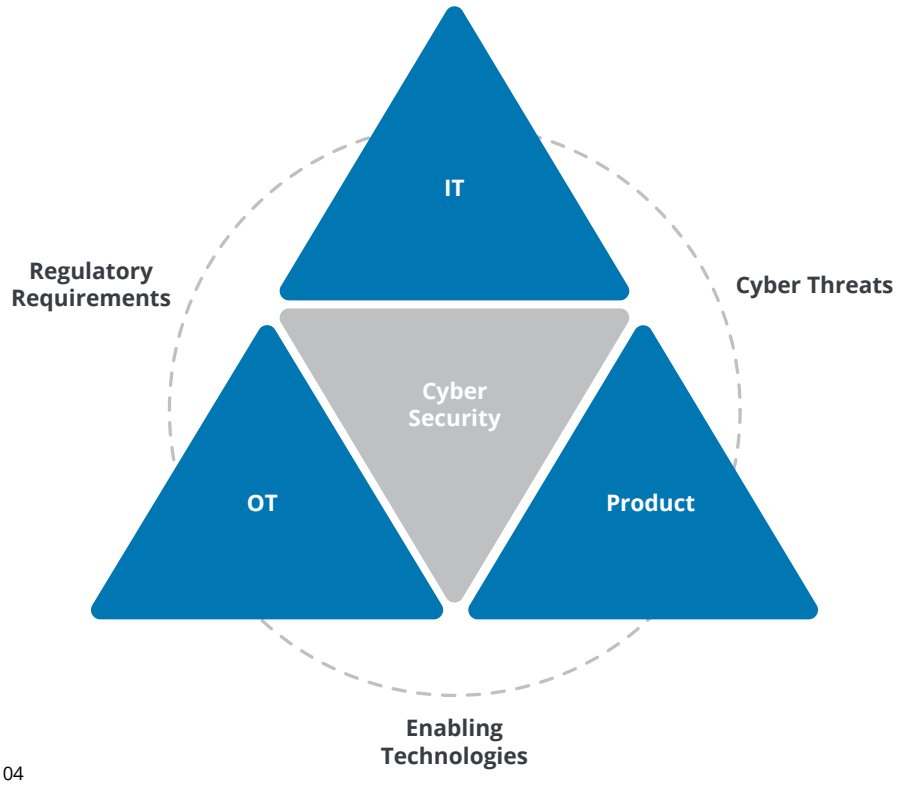
The interconnected nature of Industry 4.0 – driven operations and the pace of the digital transformation shed light on new operational risks created by the Fourth Industrial Revolution. One consequence is that cyber attacks can have far more extensive effects than ever before.

Industry leaders need to consider the actor in cyber security when it comes to smart manufacturing, smart products and digital supply networks.

We believe that companies should balance their security focus by strengthening their often mature security IT strategy and building initial security strategies for smart manufacturing and smart products.

The following pages focus on how to tackle the security challenges for smart manufacturing in the OT environment and for smart products by leveraging the experience gathered in cyber security.

Fig. 1 – The Cyber Security Triad



Smart Manufacturing Trends

Deloitte structures current trends based on the following three pillars:

Increased Danger of Cyber Threats
Both conventional malware or ransomware (like WannaCry) and attacks specially designed for production environments have increased the impact of security threats in the industry. Specific cyber threats are targeting industrial control systems (ICS) such as programmable logic controllers (PLC), supervisory control and data acquisition systems (SCADA), and human machine interfaces (HMI). The increased connectivity between those industrial devices related to the adoption of an IP-based connectivity, as well as their sophisticated microprocessors, has strongly increased the attack surface in production.

The list of examples of cyber attacks on smart manufacturing is long (see map with examples on the next pages). The example of WannaCry is nevertheless probably the most broadly known: Ransomware takes advantage of some vulnerabilities in the Microsoft operating system used in the car manufacturing environment, causing several automakers to stop production.

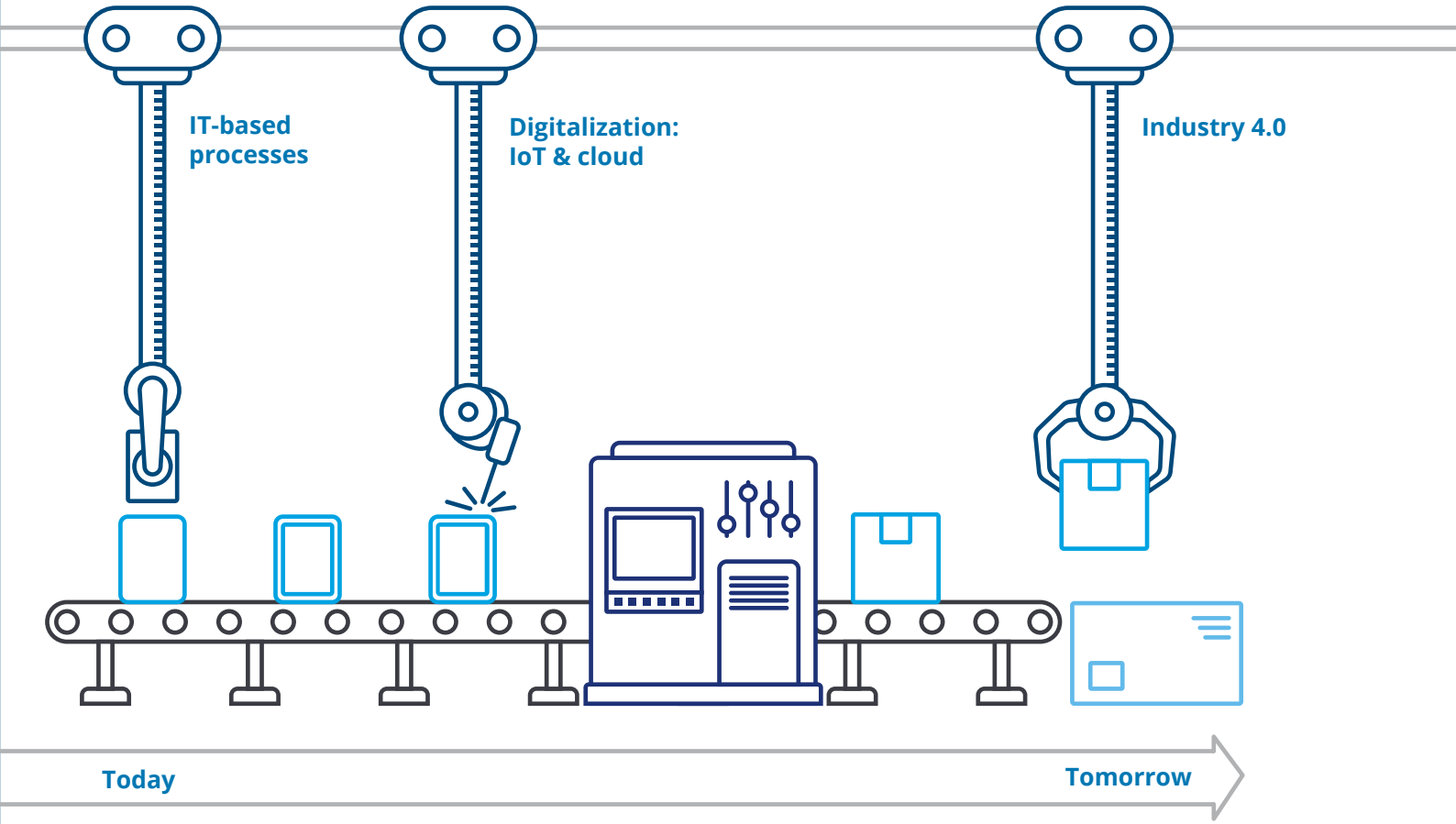
Enabling Technologies
The rapid evolution of hardware and software in ICS/OT has advanced tremendously over the last 50 years, moving toward an increasingly connected environment. Manufacturers who want to remain in the game must embrace the digital transformation and everything it has to offer.

The enabling technologies of this connected age are well known both from the public and the professional point of view: cloud computing, mobile apps, big data, machine learning, artificial intelligence, etc. Companies should not succumb to the siren´s call promising improved and efficient manufacturing without assessing cyber risks of these new technologies.

Regulatory & Compliance
The regulatory landscape is supporting the current trends. With smart manufacturing, several legal and regulatory aspects need to be strengthened, in particular the ownership of data. Answering questions such as who owns the data, who may process the data, where does the intellectual property lie is a new challenge.

The ISA/IEC-62443 "Industrial Network and Security Systems" and the NIST(1) "Guide to Industrial Control Systems" provide a framework and recommendations at both technical and organizational level.

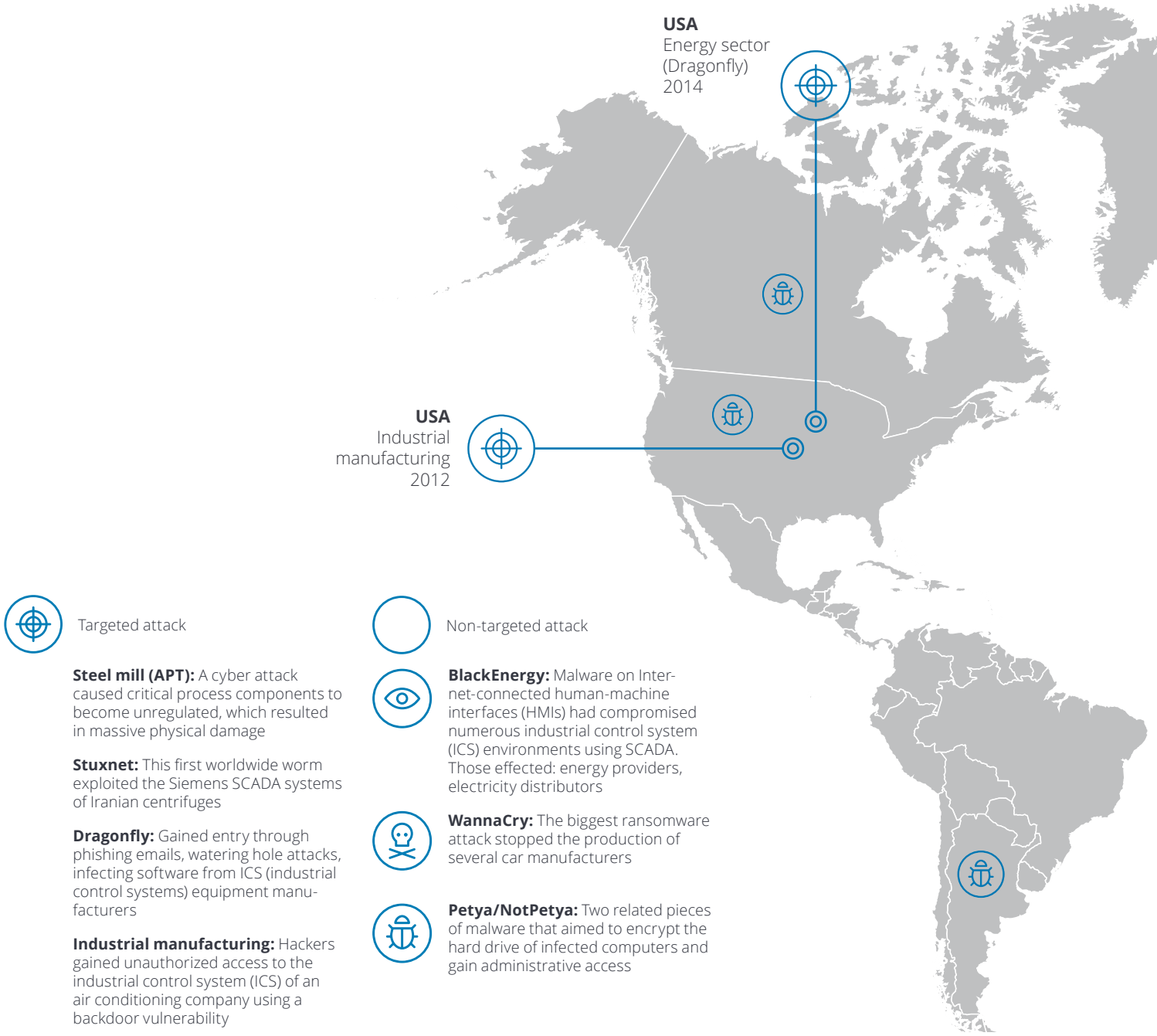
Smart Manufacturing in Operational Technology (OT)

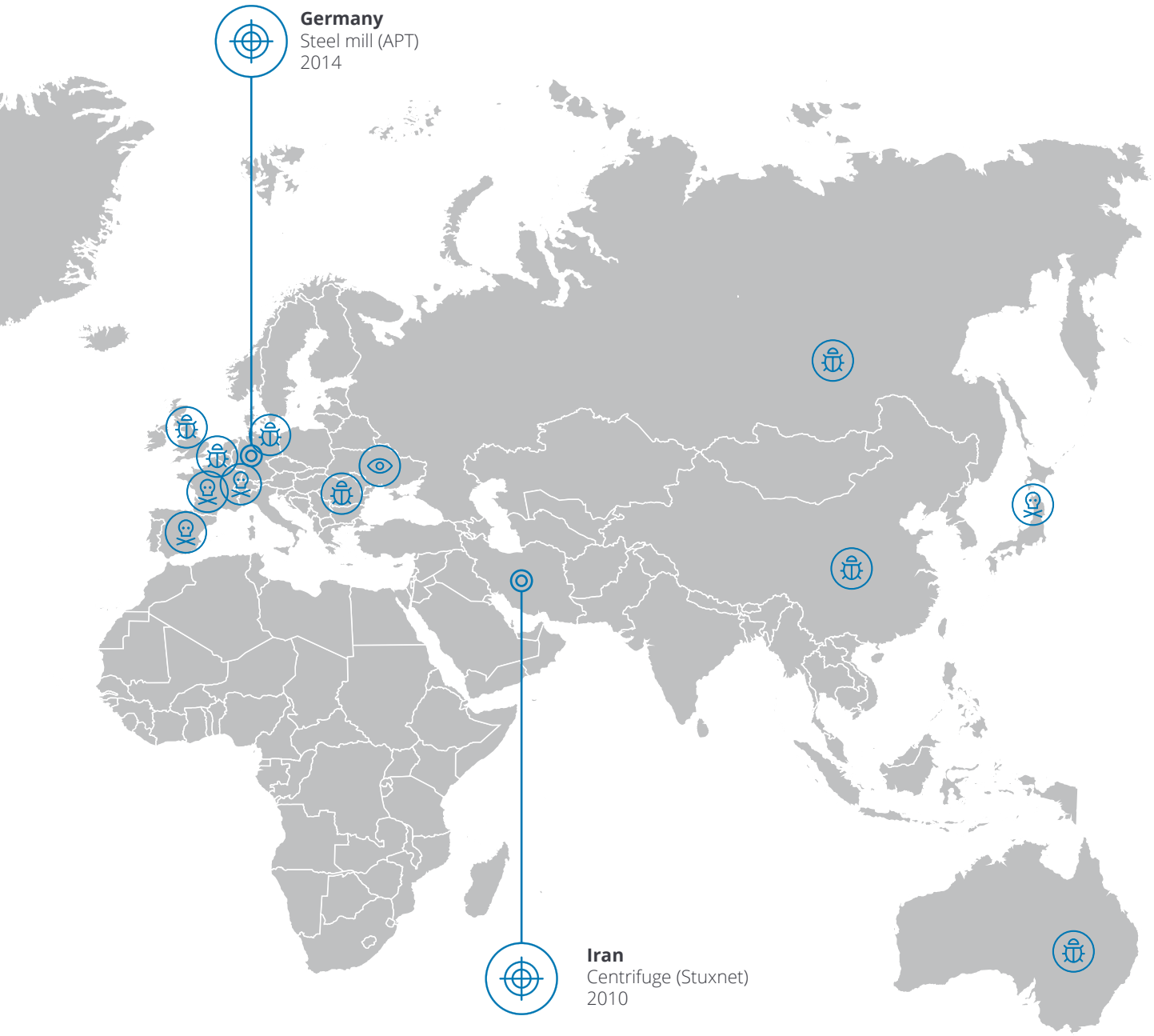


Worldwide Cyber Attacks in the Industry

Organizations need to have a detailed understanding of the potential impact of cyber incidents to manage cyber risks in Industry 4.0

Fig. 2 – Recent Worldwide Cyber Attacks in the Industry




Germany
Steel mill (APT)
2014
Iran
Centrifuge (Stuxnet)
2010

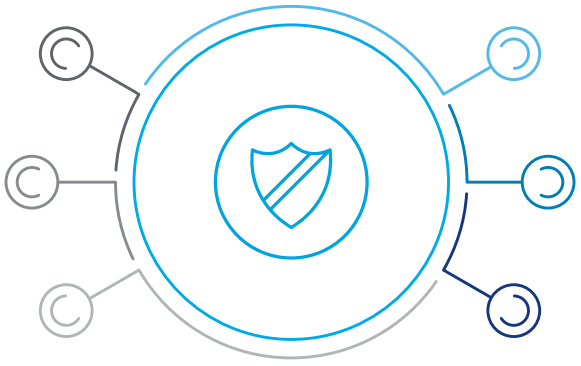
Smart Manufacturing

How to tackle the challenges of Smart Manufacturing in OT?

Cyber Threats

The creation of a Production Security Operations Center is essential to protect OT by guaranteeing efficient processes regarding the flexible and secure implementation of smart manufacturing. A Production SOC can leverage the knowledge gained in the IT environment while focusing on manufacturing-specific features. The log gathering of production device security is an example of OT challenges which can be overcome by means of a thorough analysis and deep understanding of the production architecture and review of potential market solutions. Use Case design should be developed in production by adapting and leveraging standard IT use cases (i.e., BruteForce and DoS, suspicious user behavior, inappropriate credential usage, etc.) and extending the production context knowledge. Furthermore, the design of an incident handling process enabling collaboration between IT and OT is critical. If the steps for incident handling in IT are to be followed (identification, containment, eradication, recovery, lessons learned), they should be closely adapted to the production constraints and priorities.

Fig. 3 – OT Use Case Framework



Module F – SCADA/ICS Advanced Threat Actor Detection
Attribution-based threat detection utilizing advanced adversary profiling (Deloitte TLM), Near Field Adaptive Threat Detection and other methods.

Module A – SCADA/ICS Campaign Kill (Chain) Threat Detection
Campaign-based SCADA/ICS kill chain. Where an actor utilizes multiple channels to target critical infrastructure or entities within the ESP or PSP.

Module E – SCADA/ICS Anomaly and Suspicious Activity Detection
Threat detection based on algorithms, behavior, outlier, rare event and other related detective methods. This threat detection technique moves beyond the "what an actor can do" use case threat modeling.

Module B – SCADA/ICS High Risk (Chain) Operator, Process Control and Rogue Activity
Activity that is associated with operators, contractors, rogue users and other entities. These are entities or identities that interoperate with PLCs, HMI, Ladder Logic or other related systems.

Module D – SCADA/ICS Disruption and Sabotage Threat Detection
Contnet to detect TTP used to disrupt ICS/SCADA operations. This can be caused accidentally or by intentional activities, including those related to multi kill chain smoke screens (distractive techniques).

Module C – SCADA/ICS Attributable Cyber Threats against Critical Infrastructure
Attributable atomic exploit conditions against critical infrastructure, access points, data historian, MES components and supporting infrastructure. These exploit detection methods roll up into other modules to contextualize higher-level behavior or campaign-based (kill chain) analysis.

Enabling Technologies

To benefit from enabling technologies, it is recommended to ensure:

- an appropriate mandate of the stakeholders: Organizations should redesign their security organization to ensure that OT security is integrated into the global structure. The choice of the responsible teams and their roles as well as the interfaces should be carefully designed to avoid pushbacks from the organization and instead foster knowledge exchange. If broadly used designations such as "IT/OT Convergence" may raise suspicion and shielding, companies should keep their primary focus on building collaboration and trust to increase cyber security.

- a clear understanding of the production architecture: Organizations should be able to map their architecture to known frameworks like the Purdue Enterprise Reference Architecture. From these models, architectural decisions can be made regarding enabling technologies. For example, capitalizing on the functionality of next-generation ICS firewalls, providing service platforms for the operational technology and control networks, while shielding sensitive devices from direct threat exposure.

Regulatory & Compliance

Understanding the new regulatory requirements applicable to the sector (e.g., German IT Security Act, GDPR) and leveraging existing security standards for ICS (e.g., IEC 62443) is essential. It also enables firms to forward such requirements to suppliers and vendors in order to request certified products. Such security frameworks provide best practices and guide through the complexity of required security capabilities in production.

Regarding data protection, information protection and intellectual property, data in transfer in the production environment needs attention. It is critical to have well-defined agreements and contracts to protect the use of the manufacturing data. Data use agreements should be defined and contain the determination of the scope of the data use and its purpose. Further, these should include obligations regarding security and organizational measures, as well as delete and return requirements.

The other essential part of the picture in terms of protection of data protection is awareness of the stakeholders. Bringing teams from different backgrounds on to the same level of understanding of cyber risk facilitates data protection as well as an increase in the overall security level.

Smart Products Trends

Deloitte structures current trends based on the following 3 pillars:

Increased danger of cyber threats
Cyber threats specifically targeting smart products are increasing. The steps to an attack are made simple by:

- widely available tools for reconnaissance: Freely available online tools advertise their features to explore the Internet of Things, discover connected devices and qualify them.

- combined with a lack of smart products: Security by design or risk and vulnerability assessment are not fostered enough.

Several examples of cyber attacks are worth mentioning. In May 2018, a huge botnet known as VPNFilter led to the infection of at least 500,000 networking devices worldwide with a focus on hacking IoT devices and network access storage (NAS) devices. It is speculated that the attack was conducted in preparation for an allegedly planned cyber attack in Ukraine. A very different case is the vulnerability found in smart locks: A software engineer found vulnerabilities, qualified as trivial, to hack into smart locks (e.g., for offices, plants, safes, etc.)

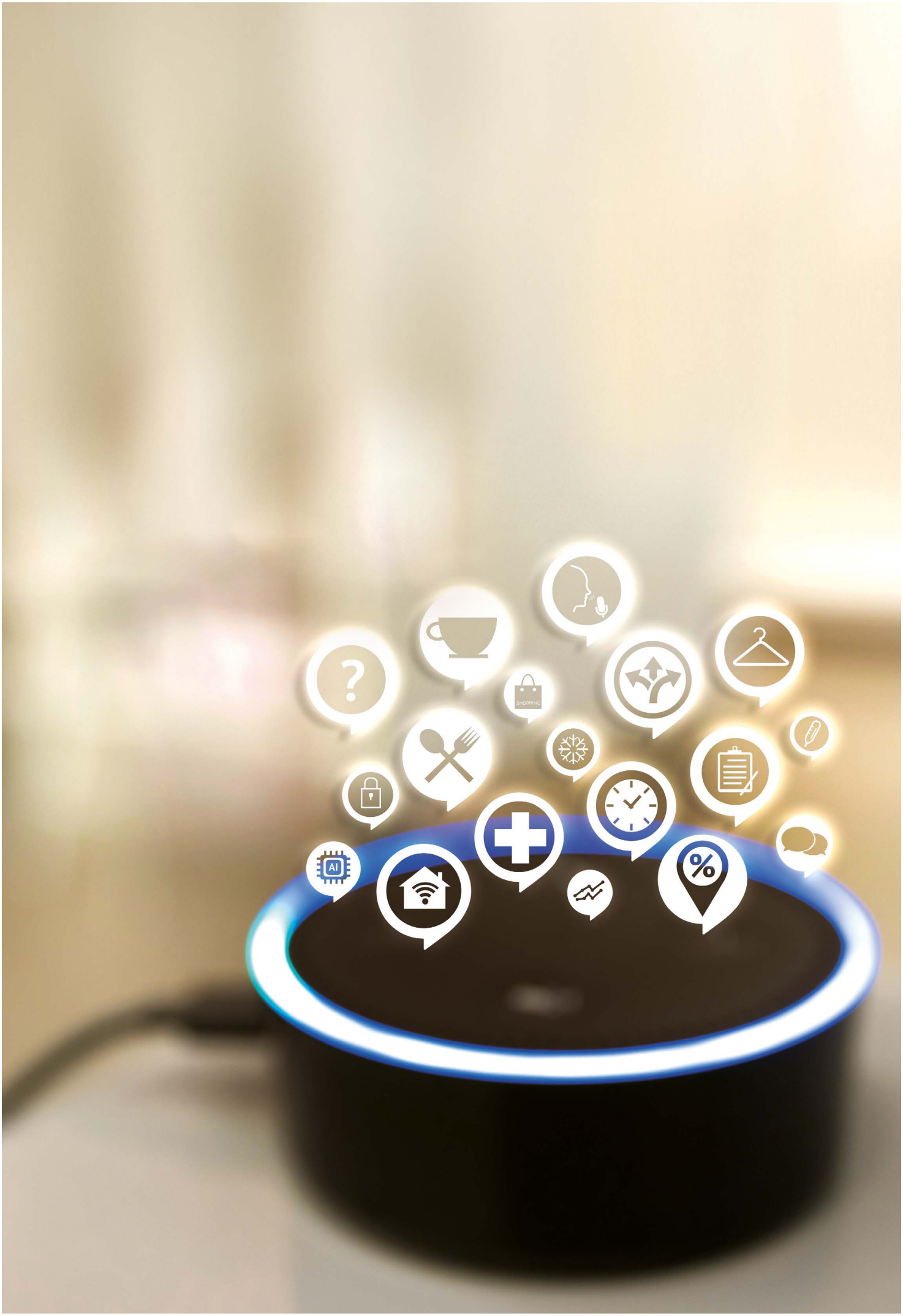
Enabling Technologies
Smart products can be found in our daily environment: in our homes with smart home devices, in our garages with the new car features, in our offices with connected tools and IoT devices, in our plants with connected products, etc. Cloud technology is the main enabling technology of smart products.

Smart products are products and assets embedded with processors, sensors, software and connectivity that allow data to be exchanged between the product on the one hand and its environment, manufacturer, operator/user, and other products and systems on the other. These smart products are enabled by vast improvements in processing power, miniaturization and network capability. However, the permanent connectivity between smart products increases the attack surface. Attackers are therefore taking advantage of these increased opportunities.

Regulatory & Compliance
Announced at the Munich Security Conference (MSC) in February 2018 and signed by a group of nine founding companies, the Charter of Trust (CoT) calls for binding rules and standards to ensure greater digital security and integrity in both the public and private sectors.

In addition to this initiative, several well-known standards have an impact on product security. GDPR regulation has a considerable impact on the usage and the exchange of personal data in the framework of smart product functionalities. Some IoT use cases rely on analysis, exchanging and processing data in/with the cloud, which increases the compliance challenges. The security community is also trying to improve standards through ongoing research. For example, the IEC 62443-4-1:2018 Security for Industrial Automation and Control Systems has released a chapter on secure product development lifecycle requirements. Similarly, the UL 2900 standard defines requirements for software in network-connectable products, aiming to provide a reasonable level of confidence[1].

[1] The list of standards is not comprehensive. NIST also published in 2016 NIST Special Publication 800-160 on implementing security in IoT


?
SHOPPING
AI
%

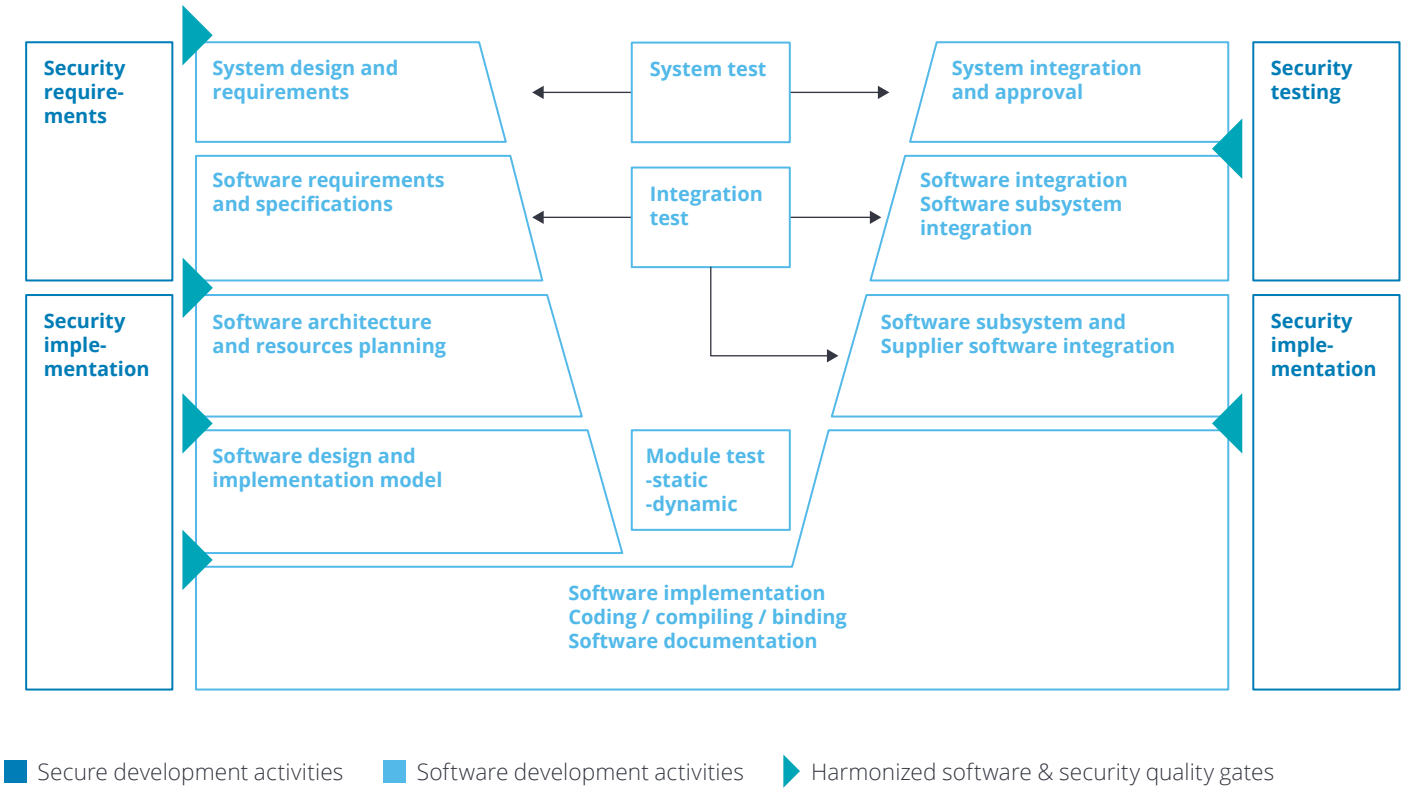
Smart Products

How to tackle the challenges of Smart Products?

Cyber Threats

The best way to prevent cyber attacks on smart products is to include security throughout the product development lifecycle. This secure lifecycle development (SLCD) should be used as a framework to reduce security risks in all steps. It should contain quality metrics and indicators as well as benchmarking tools to ensure code quality and overall security quality. In addition, standard IT security services should be leveraged in the SLCD: penetration tests, threat and vulnerability management, security event logging and, monitoring and in particular, incident handling. Product CERT should, for instance, be built to coordinate and communicate with all parties in order to identify potential vulnerabilities and IoC and define appropriate responses.

Fig. 4 – Smart Products Security Framework based on V-Model



Enabling Technologies

A smart products protection framework (SPPF) should be used to help companies assess and mature their handling of smart products throughout the product lifecycle. Such a framework includes both organizational (i.e. roles and responsibility, processes operating model) and technical aspects (i.e., secure communication & cryptography, hardening IoT, security monitoring, patch management, consumer and IoT identity access management). The last aspect, consumer and IoT identity access management, is particularly interesting to raise as the IAM solutions will have to securely handle the access not only of large numbers of consumers but also huge amounts of smart products connecting to a network. Moreover, the data integrity between smart products and the consumed service is a related challenge worth mentioning: If smart products send data without first establishing a secure session, they should nevertheless use sign-in information to ensure the information is not altered on the way to the consuming service. IAM solutions will have to handle the secure registration of new devices including registration of built-in product keys and data proof signing for the devices. The smart products protection framework should be used as a quality gateway to release products for the next level of development.

Regulatory & Compliance

Since smart products are relatively new phenomena in digitalization, know-ledge of existing fields such as life sciences (i.e., taking into account the different regulatory aspects in several countries) should be leveraged.

A significant contribution can also be made to product security by the design and development of software and interfaces in vehicles. “Privacy by design” is the key term in this context. Most functions that require data, such as autonomous driving or additional user services, can be achieved without the transfer of personal data. This is at least the case if it is already considered and implemented at the conceptual stage. Therefore, security in regulatory and contract management should be integrated at an early stage.

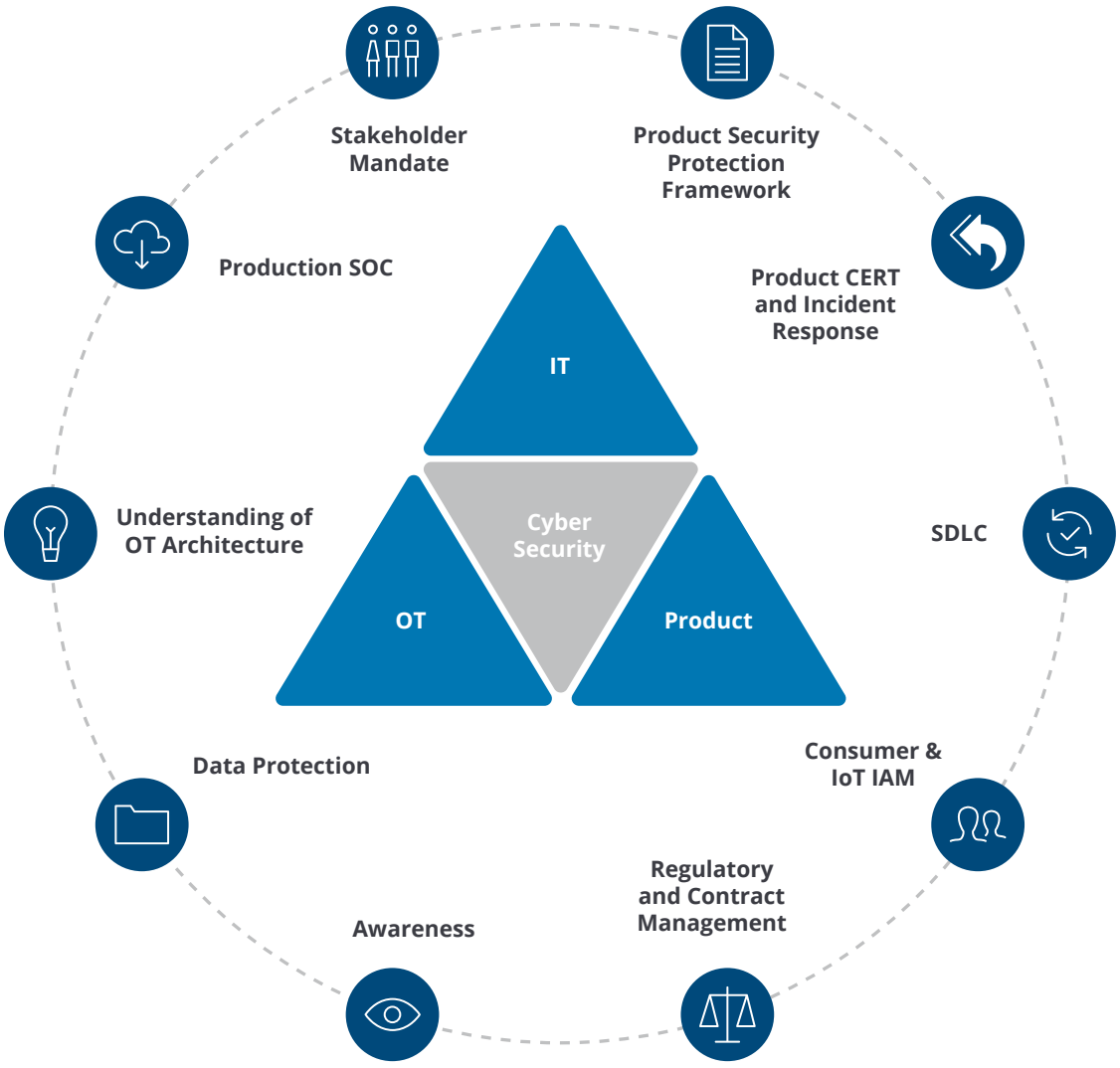
Conclusion

Recent developments in the smart manufacturing and smart products world have demonstrated that it is vital to raise security standards to cope with cyber attacks by leveraging experience gained in cyber security. The interconnection and combination of smart manufacturing and smart products will keep growing because smart manufacturing in the industry is increasingly based on smart products. Creating the appropriate security foundation will provide a valuable source of strength for future development.

Deloitte believes that the positive impact of security preparation and readiness of employees, customers and users should not be underestimated in the case of both smart manufacturing and smart products.

Building a comprehensive strategy and cyber transformation roadmap is the most effective way to reduce cyber risks in OT and product security while reaching the next maturity level. The magnitude of the task should not discourage organizations from moving forward step by step. Based on the motto "thinking big but starting small", representative lighthouse projects can be organized to prove the effectiveness of the solutions, to gain support in organizations and to ensure continuous and agile improvement.

Fig. 5 – Key Aspects of Cyber Security in Smart Manufacturing and Smart Products



Your Contacts

Peter J. Wirnsperger
Cyber Risk Leader
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Ingo Dassow
Director Cyber Risk
Tel: +49 (0)30 2546 8451
idassow@deloitte.de

Special thanks to our contributors:
Christian Franzen, Letitia Combes

Deloitte.

Issue 11/2018