White Paper

Paradigms for Resilient Digitalization

10/2020

DETECON
CONSULTING

Table of Contents

The increased interconnectivity of technology today requires a high level of innovation and understanding of the specific needs of these new ecosystems. New data sources and technologies enable new business models and the potential for digital value creation. This paper describes how security concerns can be taken into account when legacy environments embrace digitalization through remote work and new IoT products to secure the value created.

Critical Infrastructure's New Critical Vulnerabilities

Industrial Control Systems (ICS), Industrial Automation and Control Systems (IACS), or more generically, Operational Technology (OT) are systems used to control and monitor functions pivotal to continuous operation of production plants as well as critical infrastructure including water purification, energy production, and transportation systems (KRITIS).[1] For the majority of the time that these systems have been in place, it would have been impossible to remotely access them. To monitor and control a factory or a nuclear plant, a person would need to physically be in the secure and isolated control room, which is physically protected by various access controls. That is increasingly no longer the case - industrial control systems are more connected than ever, and more vulnerable than they have ever been.

Information Technology (IT) and Operational Technology (OT) were traditionally separate areas within the companies and functioned completely independently of each other. This can be applied to the task definition, the system architecture, as well as the organizational structure and leadership model. IT systems use computers, storage and network devices to process and store data. They are usually based on an open, standardized architecture. On the other end of the spectrum are OT systems that tend to be closed systems, reliant on proprietary protocols and programmable logic controllers (PLC). The convergence of IT and OT systems has been discussed for quite some time, but current circumstances and trends have accelerated the convergence.

Today, industrial companies face the challenge of having to react to rapid market changes and volatile global economic conditions in an agile and short-term manner. Shorter development and production cycles, increasing customer demands and quality requirements, in addition to the ongoing COVID-19 pandemic have all contributed to the need to enable digitalization within the industrial and critical infrastructure ecosystems. To cope with these major shifts, and to keep pace with the competition, companies are rapidly putting in place digitalization measures that may not take into account the security of critical systems in their IT/OT environment. Now more than ever, the importance of industry resilience is clear. Industrial systems must be able to withstand emerging disruptions and ensure normal operations within minimal time and cost in order to keep losses and waste to a minimum.

ICS Security, and cybersecurity more generally, is becoming more top of mind for national and international regulators and as such securing networked physical equipment is essential not only to avoid any disruptions but also to comply with regulatory and customer requirements. In 2016, the EU published the NIS Directive which requires EU nations to implement requirements within national law.[2] In Germany, the IT Security regulation (§ 8a Absatz 5 BSIG[3] within the BSI Gesetz) has set a high standard for operators of critical infrastructure to manage

[1] Critical infrastructure sectors are decided upon by each EU state. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=EN
[2] https://www.enisa.europa.eu/topics/nis-directive
[3] https://www.gesetze-im-internet.de/bsig_2009/__8a.html

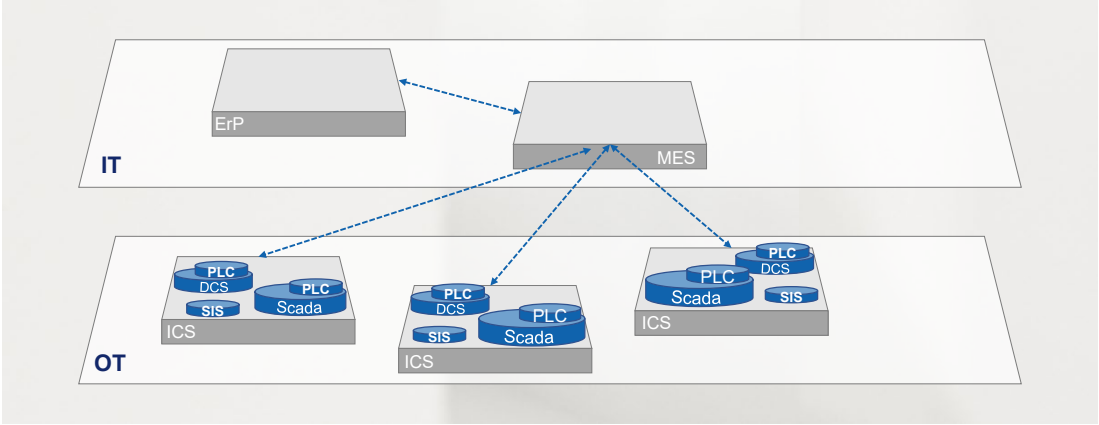
risk and security throughout their company ecosystems. It was augmented by the KRITIS provision to define which critical infrastructure providers are required to implement the IT Security regulation. A guide on how to concretely implement the regulation was released in March 2020.[4]

The challenge is to integrate the benefits of digitalization with the need for a robust, resilient, and secure IT/OT infrastructure. This paper explores the trends within industrial IT/OT convergence and offers a way forward for securing novel systems and working models.

The World of Operational Technology

Before understanding the security needs of IT/OT infrastructure, it is first essential to understand the terms used to describe these technologies and how they fit into a broader IoT context.

Whereas the term IT refers to enterprise devices, networks, and systems, the term OT covers all hardware and software used to monitor and control physical processes, equipment and infrastructure. An essential part of the operating technology is the Industrial Control Systems (ICS) or Industrial Automation and Control Systems (IACS).



These systems are used to control and monitor functions pivotal to continuous operation of production plants as well as critical infrastructure including water purification, energy production, and transportation systems (KRITIS).[1] According to the definition of the automation standard IEC 62443, an ICS/IACS involves various types of devices, systems, controllers and networks that control a wide range of industrial processes.

Most common are SCADA (Supervisory Control and Data Acquisition) systems for data acquisition, monitoring and control and DCS (Distributed Control Systems). DCS and SCADA systems control many physical operating systems running on programmable logic controllers (PLCs). They automate much of the work required to maintain extensive functionality. The difference between the two is that SCADA systems control PLCs over a large geographical area (multiple sites), while DCS systems are typically concentrated on one plant or industrial site.

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Konkretisierung_Anforderungen_Massnahmen_KRITIS.html

Safety Instrumented Systems (SIS) are particularly critical for industrial systems located in facilities with any hazardous materials as they are designed to detect potentially unsafe work environments and send alerts or shutdown commands. These control systems maintain a connection to the critical sensors and systems but are very intentionally separate from other control systems in order to prevent a malfunction in another system from impacting the safety of the employees.

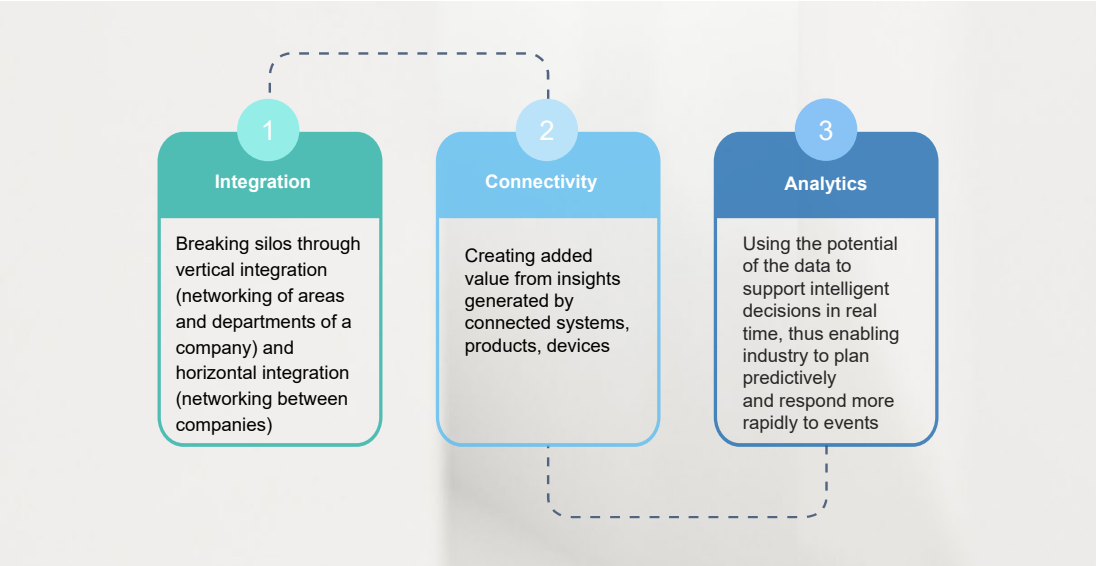
Compared to IT, OT is often considered a niche and overlooked field. A nuanced understanding of the function and construction of OT systems will contribute to a more seamless and secure integration of IT to enable the business to permit remote work, increase efficiency, reduce costs, and improve overall operational oversight.

Industry 4.0 – Increased Visibility, Efficiency, and Control

The operational environment in which IT and OT are converging is one of rapid development, digitization, and integration. These trends are an important aspect of why cybersecurity must now, more than ever, be considered throughout the evolution of IT/OT infrastructures.

Industrial companies must today deliver the conventional criteria (reliability, quality and price), while also accommodating the desire for flexibility and increasing individualization of products. For these reasons, the classical business IT and process/production IT (OT) must grow closer together both technically and organizationally. There is a great need to integrate data from all parts of the enterprise to create a more holistic control. The goal is a resilient, constantly optimized operation, high efficiency in resources, costs and productivity, stronger customer centricity and reduced system complexity.

The activities in the Industry 4.0 area that attempt to achieve these objectives can be clustered into three main areas: Integration, Connectivity and Analytics.



Integration:

The term integration is basically about breaking down the individual data silos and integrating the data in such a way that in the end a data flow is created that provides all systems with the right information at the right time.

The term **vertical integration** can be used synonymously to describe IT/OT convergence and describes the continuous networking of the individual hierarchical levels of the production systems (from the company management level to the sensor). Processes should become more transparent and flexible in order to adapt production tasks to changing customer requirements. On the other hand, data from the production facilities enable better steering and control of the entire process.

Horizontal integration is about the continuous, digital connection along the supply and value-added chain, with the intention of achieving greater transparency and increasing flexibility in production and service.

The importance of production **resilience** will increase significantly in the future, with a strong focus on the value network. Covid-19 has illustrated how vulnerable some supply chains are and will encourage companies to rethink their current strategy. **Ecosystems** and **platforms** will play a particularly important role in avoiding future bottlenecks and will enable rapid adaptation to changing market situations. The linear supply chain is gradually being replaced by ecosystems.

Connectivity & Communication:

Connectivity is the cornerstone of digital change in the industry and one of the most important topics when it comes to realizing Industry 4.0 use cases.

The **(industrial) Internet of Things (IoT)** plays a decisive role in networking operational technology with IT. In general, IoT is the technology that makes it possible to connect all kinds of devices and machines via the Internet and enables the use of data that was previously not accessible. The interplay between IoT and Cyber-Physical Systems allows the devices to interact and cooperate with each other.

A **Cyber-Physical System** is the combination of physical (e.g. mechanical machine) and information technology components (e.g. embedded system). The embedded systems collects data from the physical world through sensors, as well as controls and regulate them through actuators.

The cyber-physical system unfolds its full potential in combination with a **digital twin** and enables scenarios up to a self-regulating system. “A digital twin is the virtual representation of a physical object using operating data and other data sources to enable monitoring and dynamic control of the object. This covers the full scope from a life cycle phase to the complete product life cycle. The maturity of a digital twin is defined in dependence on the level of communication and the degree of standardization. The degree of communication describes the connection between the digital twin and the physical object. The degree of standardization reflects the modelling of the data and data sources.” (Source: Detecon Study: Digital Twins)

To ensure that new devices can be quickly integrated and applications are scalable, **interoperability** plays a major role. The open interface standard OPC Unified Architecture **(OPC UA)** is increasingly establishing itself for this purpose and is on the way to become the industry standard. OPC UA is an open interface standard for industrial communication that is designed to ensure the platform-independent exchange of data.

Analytics:

With the rapid growth of Internet-enabled devices, the amount of data generated in an automated and structured way is also increasing – the advent of **big data** offers the potential for more detailed insights. Managing and analyzing this data to create insights is the real value that IT/OT convergence can bring. Data within the company and from products is becoming an asset and must be treated as such.

In order to enable products, machines, applications and the corresponding digital twins to make smart decisions, the company must have the appropriate know-how in handling the data.

Various **AI** and **machine learning** methods make it possible to analyze this data in a target-oriented way in order to optimize products, to better understand and control the production process, realize predictive maintenance and thus minimize downtimes, or optimize energy management.

The trend towards the convergence of IT and OT offers many advantages for businesses around the world. These benefits, summarized below, are driving innovation and advancement in nearly every industry. Unfortunately, increased efficiency and usability also comes with a cost, IT/OT convergence has also created more interdependencies that may be exploited by malicious actors or even unwitting insiders.

- Holistic use of all data available in the company
- Improved control and automated steering of processes
- Creating better predictions and systems with better responses to events
- Improved automation by combining information acquisition from business and production
- Improved decision making based on more accurate and in time information.
- deliver the right information, at the right time, where it is needed
- Better customer experience through proactive services (maintenance, consulting, optimization, development)

Cybersecurity Threats to Industrial Environments – Dangers of Connectivity

Many cyber-physical systems are responsible for carrying out critical functions such as energy production, manufacturing, or public transit. While the trends highlighted in the previous section - increased remote-monitoring and configuration, and the introduction of new, relatively untested technologies, represent a significant increase in efficiency and maturity for many companies, they also pose a threat to the overall security of these systems. The risks of a cyber attack specifically against physical systems can have serious consequences for society in general as well as for companies in terms of overall business continuity and profits.

The danger of such attacks is no longer speculative or hypothetical; cyber-attacks on physical systems have been occurring with more and more frequency since the 2009 Stuxnet worm infiltrated Iranian uranium enrichment centrifuges to delay progress towards a nuclear weapons capability.[5] Stuxnet, a governmental project stemming from a collaboration between

[5] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

the United States and Israel, is presumed to have infiltrated the network via an infected USB key. From there the malicious program altered the speeds of the centrifuges to emulate common operational failures. The Stuxnet malware is estimate to have set back the Iranian nuclear program back by two years.[6]

In 2015, power operators went black in the middle of a cold December evening in Ukraine. The attackers had been in the power company's system for months; they initially gained access by sending infected Microsoft Word documents to targets within the company. From there they got access to the ICS/SCADA power systems located behind a firewall. The attack consisted of: disabling uninterrupted power systems (UPS), updating serial-to-ethernet converters with augmented firmware, and finally flooding the customer service telephone lines with fraudulent calls to prevent any customers impacted by the attack from reporting the incident. Tampering with the UPS meant that even the operators would be operating in the dark when the command to shut down operations was given. The augmented serial-to-ethernet converters were then no longer able to transmit commands from a larger control system to the substations. The attackers were furthermore already in the network, so the commands they gave to cut off power to a significant portion of Ukraine came from inside the network and would not be flagged as anomalous. The unavailability of the phone lines delayed reaction time, information gathering, and promoted a general uncertainty for all parties involved. It took approximately six hours to get power to the consumers after the attack but it is clear that such an attack could have fatal effects on a population.[7]

Another incident of targeted ICS malware occurred in 2017 within a Saudi Arabian petrochemical plant. The malware was identified after what is presumed to be an accidental shutdown of plant operations; Fireeye, a US-based Cyber Security company, has postulated that the attacker's intentions were to augment the Safety Instrumentation Systems (SIS) at the plant with more catastrophic consequences. Such an attack would theoretically be aimed at causing a chemical spill or malfunction at the plant which would then go unnoticed due to the manipulation of the SIS. The employees at such a plant would be in the most danger but the effects could extend to the broader community surrounding the facility. Malware targeting SIS is particularly notable because SIS are in place to protect employees and therefore any manipulation of such systems are intended to inflict personal harm to people, something often considered out of scope for cyber attacks.[8]

Core Principles for Securing Industrial IT/OT Environments

The core security goals within an IT setting are confidentiality, integrity, and availability, typically in that order. For an industrial setting, availability is the most critical goal to protect (with integrity being a close second). The priority is to ensure that the systems continue to operate and do not disrupt production which may cause delays and financial losses but can also result in the failure of integrated systems with even more dire consequences. Integrity must likewise be protected to ensure that the system commands are not altered to disrupt or destroy the system process.

---

[6] https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf; An estimate from Ralph Langer, one of the security experts involved in analyzing the Stuxnet worm.
[7] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[8] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html; https://www.darkreading.com/vulnerabilities---threats/triton-trisis-attacks-another-victim/d/d-id/1334388

Detecon has worked with many customers to introduce more connectivity, visibility, transparency and efficiency into their industrial environments. Topics that Detecon's team is currently exploring include:

- Secure networking of machines and plants
- Acquisition of machine data
- Integration of shopfloor technologies into current and future IT architectures

By creating an ecosystem of connected devices, it is clear that there is a significant risk to the underlying systems. A vulnerability in one system is a vulnerability to the entire platform, including individual input systems. To protect the security goals mentioned above, such a platform requires rigorous security standards, testing, and strategy.

The principles described in this section are the core activities that need to be undertaken to maintain operational systems and businesses when more and more critical functions are being accessed via the

internet. These are general principles that can make a difference in a cyber-physical or IoT system constellation, however the ISA/IEC 62443 standard[9] provides a comprehensive overview of both organizational and technical security measures to secure ICS environments. That document defines further, more detailed measures that can be taken to ensure system security – for example, the enforcement of multifactor authentication, physical access control, or changing default passwords.

1. Deploy a risk-based strategy that targets the most critical systems.

Given limited resources, it is important to determine the services and systems that are most critical to the business in order to prioritize efforts. Once these core services or systems have been identified, you can determine the key functions that, if disrupted by a cyber attack, would impact the business the most. From there, determine which of those critical systems are most vulnerable to an attack. Controls to secure these components would therefore be implemented first within a prioritized security strategy that takes into account the needs of the business and inputs from all relevant stakeholders including management, IT, and OT employees. For example, to change a function critical to plant operations it is useful to implement dual control, in which two individuals separately have to confirm the change in order for it to be implemented on the system. This would ensure that no one person (a malicious insider or a sophisticated hacker) can, on their own, cause a major shutdown or incident.

The benefits of security controls, especially in legacy systems, needs to be carefully evaluated using a cost-benefit analysis. In some cases, while the intention of securing the device is good, the security control itself (e.g. patching or remote monitoring) can adversely impact the operational systems leading to a disruption in operations or the introduction of an additional vulnerability. OT systems are less likely to have a test environment for testing new configurations or patches. Whereas in traditional IT systems one can expect a system to be offline for a couple hours during the patch and update process, the same is not true for OT systems. This can produce a more severe incident than the risk that the patch would try to avoid.

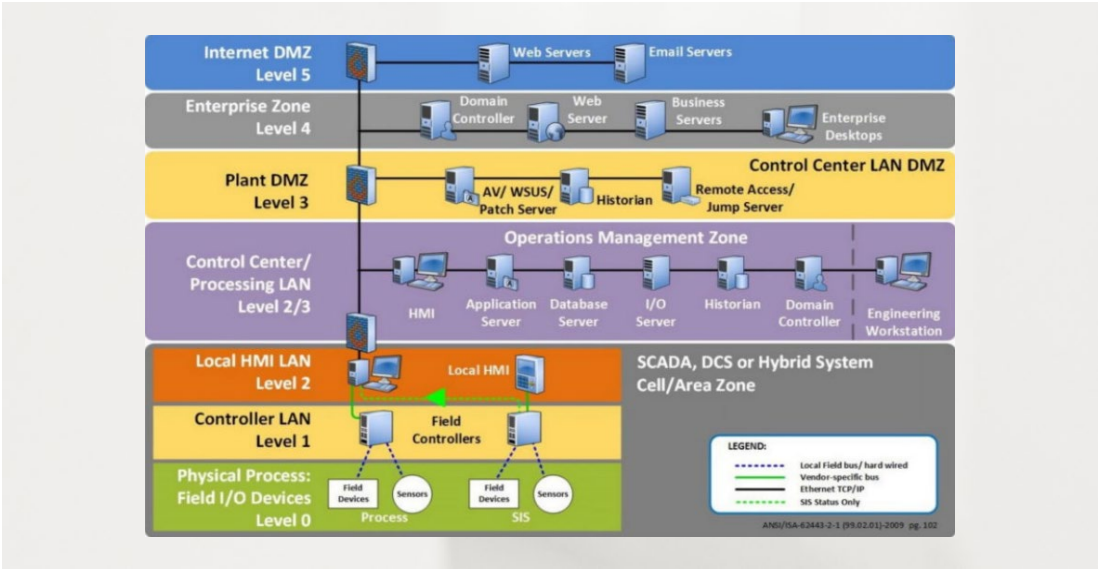
[9] https://www.isa.org/intech/201810standards/

Therefore, as with many security measures, there should be a consistent and documented procedure in place for determining when the risk of inaction outweighs the risk of control implementation.

2. Clearly define and protect network segments to prevent lateral movement.

Network segmentation is the process of limiting communication between defined zones within a network typically through the use of firewalls, VLANs, VPNs, and physical network device segregation. According to the NIST's publication on Industrial Control System security, "Network segmentation and segregation is one of the most effective architectural concepts that an organization can implement to protect its ICS."[10] The reasoning behind this is that even if a system is not directly relevant to business functions, it can be exploited to reach other, more critical, systems within the company. Historically, ICS environments are prone to the inadvertent or poorly designed integration of the business environment to the OT systems. For example, in the past many energy facilities did not have wireless internet connections. While this is unnecessary for the core business of the facility, there are supporting staff working in an office part of the building. To avoid this inconvenience, in one instance employees brought in a router and created a wireless access point. Unfortunately, the addition of this insecure network device opened up the entire facility to malicious hackers.

The implementation of network segmentation is complex and time-consuming; it must, furthermore, be impeccably tailored to each company. To identify the logical network segments, there are several factors to take into consideration including functionality, management access, risk, volume of network traffic, etc. Meanwhile, it is generally advisable to ensure that there are no connections that permit unnecessary communication (i.e. the human resources department does not need to access the management console of an OT system and therefore any connection should be completely disabled). Each segment should be organized to connect with systems within that zone, with as little cross-zone communication as possible. To assist in this organization, the broadly deployed Purdue Model acts as a reference model for large, non cloud-based environments. The introduction of cloud computing and storage to ICS environments requires very nuanced zoning considerations.



[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

(Source:[11])

This image, based on the ANSI/ISA 62443 standard, portrays a typical ICS network segmentation determined by function.

3. Integrate all stakeholders into security operations and overall protection of critical assets (IT/OT convergence).

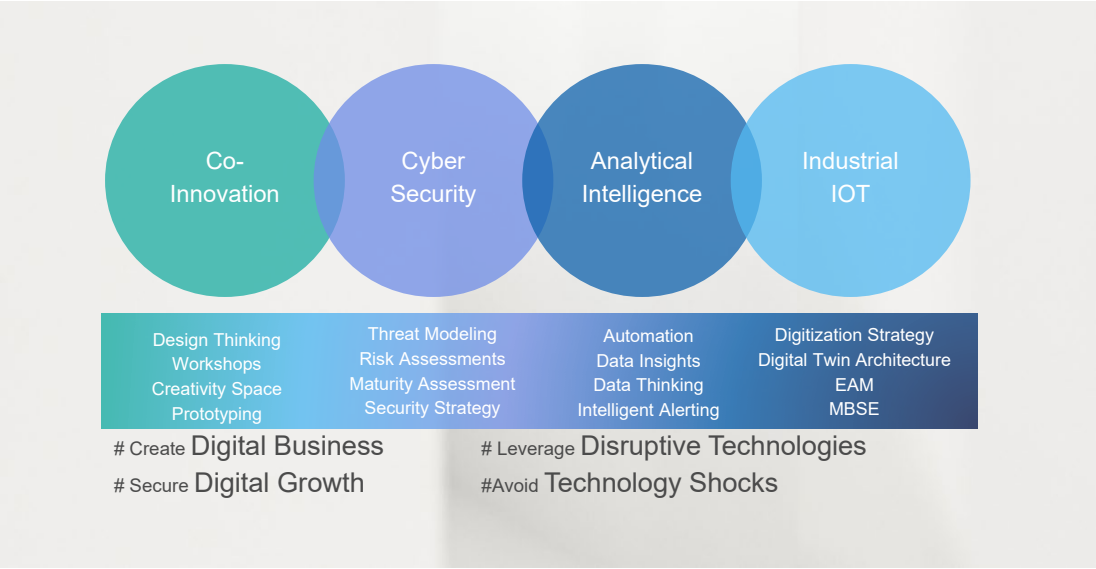
Remote management of OT systems has incontrovertibly changed the risk profile for presumably air-gapped physical systems. A win for convenience and quick reaction times, the control systems are at a higher likelihood of being exploited due to the connection with the outside world. As the principle of IT/OT convergence is applied generally, it must also be applied to the security efforts surrounding these systems. Those responsible for IT security must include the inputs of OT operators and experts in order to ensure that the IT security techniques typically applied are appropriate and sensible for IT/OT systems. The 2020 Study on the State of Industrial Security[12] found for 63% of respondents, risk management for IT and OT are not coordinated.

Security efforts for systems that are critical to operations must also include strict requirements and assessments of third-party providers. As shown many times in recent years, third parties with lower security standards but high amounts of access within the target system are often the perfect entry point for attackers. In the 2013 hack of the major shopping retailer Target, the attackers gained access to the network through a company installing heating, ventilation, and air conditioning systems.[13] For this reason third party security assessments, risk evaluations, and adequate SLAs must be in place for any company given access to IT networks to limit the chance of lateral movement within the network.

The organizational aspects of security are not to be underestimated. By implementing clear processes, policies, and procedures, you limit opportunity for human error, and ensure that risk can be accurately evaluated. To secure a business' most critical assets the entire company must understand their role in securing them. This starts with a strong management commitment, consistent and practical user training, and a culture of security – which will maintain motivation among employees to use secure practices on a daily basis.

[11] https://dale-peterson.com/2019/02/11/is-the-purdue-model-dead/
[12] https://img06.en25.com/Web/TUVRheinlandAG/%7Ba68a7b58-1215-4c4a-8c4f-f0bada2c4738%7D_DE20_I07_2000214_en_Whitepaper_OT_Survey_A4_Web_final.pdf
[13] https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Detecon's Digital Engineering Center focuses on staying ahead of new trends in digitalization. With our four knowledge centers and technological experts from the field of industrial IoT, cyber security (ICS security), data analytics (AI) and co-innovation, we have established a hands-on innovation hub in the heart of Berlin. Our systematic customer-oriented approach combines consulting and innovation with high-tech expertise to ensure the transfer from the innovative ecosystem to the real world. By developing and providing prototypes and proofs-of-concept, we offer an accelerated, low-risk implementation of digital strategies. We support the full range of organizations and companies seeking to digitalize their operations by applying cutting-edge technologies using tested management methods. A snapshot of some of the specific services we provide are depicted below:



The Authors

Eve Hunter is a Senior Consultant in the Detecon Digital Engineering Center‘s Cybersecurity team. Her focus is on cybersecurity risk management techniques for critical infrastructure industries but previously worked in the field of nuclear security policy. She has a MSc in Cybersecurity from Tallinn University of Technology and a BA from Smith College.

She can be reached at eve.hunter@detecon.com.

Lino Lindner is a Business Analyst at Industrial IoT Center (Detecon Digital Engineering Center). His consulting focus is on IoT/Industry 4.0 technologies for the mechanical engineering, manufacturing and mobility sectors. He supports customers in concepts of the digital twin as well as data and knowledge driven use cases, which the digital twin enables in cyber-physical systems. Lino Lindner studied transport systems (B. Sc.) with a focus on aviation engineering at the Technical University of Berlin and mechanical engineering (M. Eng.), with focus on digital engineering, at the Brandenburg University of Applied Sciences.

He can be reached at Lino.Lindner@detecon.com.

The Company

Detecon is the leading, globally operating technology management consulting company with headquarters in Germany, which has been combining classic management consulting with high technological competence for over 40 years. The focus of its activities is on digital transformation: Detecon supports companies from all areas of business to adapt their business models and operational processes to the competitive conditions and customer requirements of the digitalized, globalized economy with state-of-the-art communication and information technology. Detecon's expertise bundles the knowledge from the successful conclusion of management and ICT consulting projects in over 160 countries.

Detecon is a subsidiary of T-Systems International, one of the world's leading vendor independent providers of digital services and subsidiary of Deutsche Telekom. Together with T-Systems Multimedia Solutions GmbH (MMS) and the digital areas of T-Systems Global Systems Integration (SI) the Detecon International GmbH forms one of the largest integrated digital providers in Germany as the portfolio unit "Digital Solutions".

As a member of this new alliance, Detecon is driving forward its consulting approach Beyond Consulting, a significant evolutionary step forward in traditional consulting methods adapted to meet the demands of digitalization today and in the future. The concept features top consulting that covers the entire spectrum from innovation to implementation. Groundbreaking digital consulting demands ever greater technology expertise and a high degree of agility that incorporates flexible, but precisely fitting networking of experts for complex, digital ecosystems in particular. At the same time, it is more and more important in digital consulting to accompany clients from innovation to prototyping to implementation.

This factor prompted Detecon to found the Digital Engineering Centers for Cyber Security, Analytical Intelligence, Co-Innovation, and Industrial IoT in Berlin in 2017 as facilities that extend the added-value chain of consulting and accelerate the realization of digital strategies and solutions by means of prototypes and proofs of concept.

Detecon International GmbH
Sternengasse 14 - 16
50676 Cologne
Phone: +49 221 9161 0
E-Mail: info@detecon.com
Internet: www.detecon.com

www.detecon.com