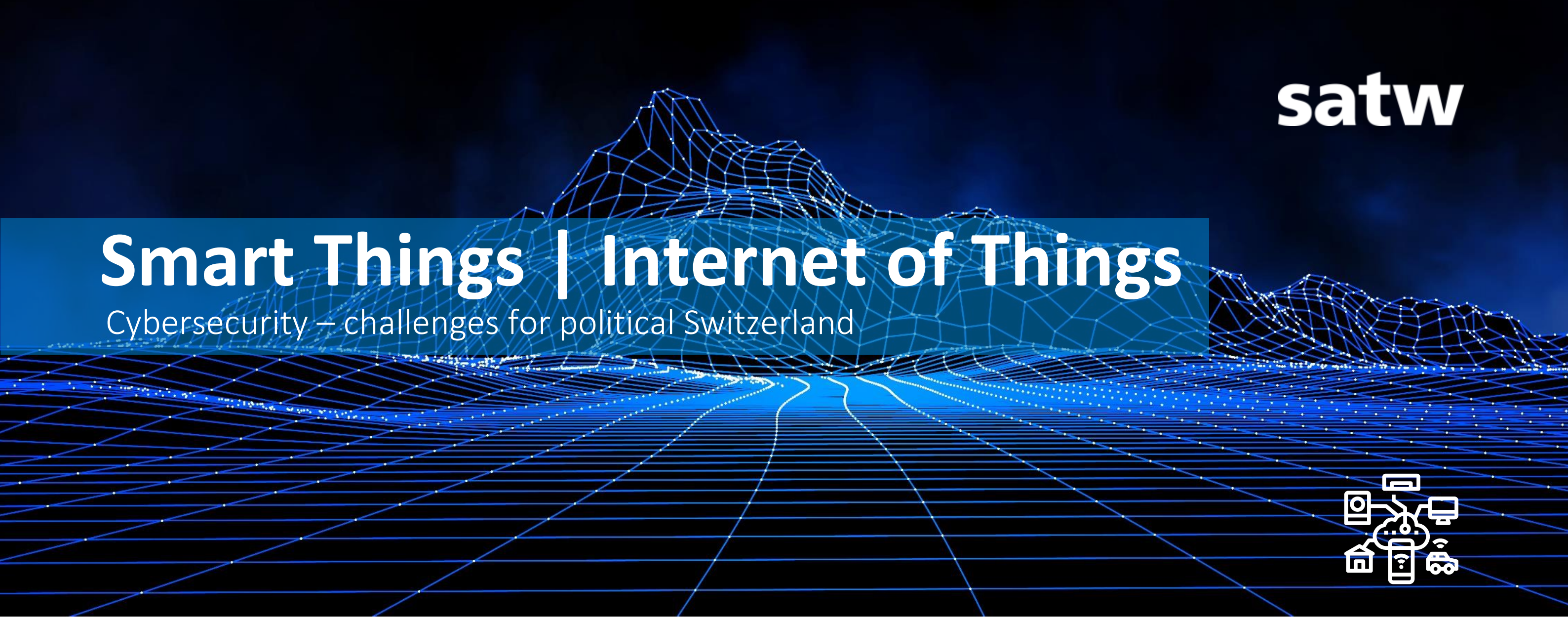

Smart Things | Internet of Things

Cybersecurity – challenges for political Switzerland

State of the art

The Internet of Things (IoT) can be defined as the intelligent networking of a global infrastructure of various smart things that fulfil all kinds of functions (e.g. temperature sensors, cars, loudspeakers, machines, etc.). Intelligent networking enables a new connection of physical and virtual resources with common interactions. The opportunities created also enable the performance of automated actions and the gathering and further use of information.

The terms Industry 4.0 and Operational Technology (OT) bring together on the one hand the Fourth Industrial Revolution and on the other the use of new technologies and technical opportunities. «Industry 4.0»[1] is the umbrella term for the new industrial world where machines are connected to one other and form a network with state-of-the-art information and communication technologies. The different worlds and architectures of traditional business IT and OT are increasingly being interconnected through digitalisation. Whereas traditional IT is used for information processing, physical processes in industrial manufacturing and logistics are controlled with OT. This connection of highly critical OT systems (e.g. nuclear power plants) with IT systems that are exposed to the internet creates new damage potential and risks. Their control and management entail great challenges and require new concepts.

Recommendations

1. Creating and circulating an overview of the current situation and future developments in IoT, which best practices exist (any existing standards and frameworks).
2. In-depth research on IoT/OT security must be driven forward so that security can also be ensured in future through new concepts and architectures in the highly heterogeneous environment.
3. The creation and standardisation of minimum norms in the areas of IoT/OT, which must be implemented through appropriate regulations. Cooperation with the relevant bodies in the EU would achieve a greater impact.

The new technologies and extensive linking of OT and IT will result in major advancements, new application opportunities and innovative business models in the economy, administration and society, provided we manage the risks involved appropriately and systematically.

[1] The term «Industry 4.0» concerns IT/OT technology far more and mainly refers to new overall concepts such as the «smart factory», with extensive interconnectivity of systems and sensors and optimisation based on comprehensive data or predictive maintenance as a further topic.

Challenges

It is generally recognised that the deployment of new technologies presents specific risks. The extensive interconnection of physical and virtual smart things increases security risks and the potential degree of damage owing to the significantly greater scope for attack and the increasing importance of OT and IT to value creation.

A successful attack on an IoT device can have a direct impact on the real/physical environment and, for example, result in power failures, stop pacemakers from working or damage industrial plants. This development is leading to more rigorous security requirements, for example in the form of more secure data communication and storage. The increased security requirements are often not recognised or deliberately overlooked today (e.g. in IoT for private application) in order to launch affordable and pseudo-innovative smart things on the market as quickly as possible. This situation means the security of devices and the privacy of users usually cannot be sufficiently guaranteed. Market failure in terms of sufficient security standards can be observed in the consumer IoT sector (products for private use).

It must also be noted that the emphasis is clearly placed on safety (e.g. accident prevention) and not primarily on security (e.g. measures to protect against attacks), especially in industry[2]. The lifespan of the devices used is designed for several decades, particularly in the field of OT, as they are often exposed to high levels of physical stress in harsh environments. By comparison, other smart things are sometimes updated after a few months (e.g. smart tags). This very wide range of requirements and framework conditions must be taken into account in order to develop and integrate sufficiently secure overall systems.

Current practice shows that common and established concepts (e.g. security/privacy by design) and standards (e.g. EN IEC 62443) are not systematically applied or do not even exist in the development of IoT and OT systems.

The testing and certification of IT components and systems is currently being discussed both in Switzerland and at EU level. Legal regulation of cybersecurity testing is being debated in the EU in the context of the Cybersecurity Act. The discussions in Switzerland focus on a concept to set up a cybersecurity testing institute for connected devices. The initiatives aim to ensure that the security and integrity of digital products are subject to mandatory regulations. This kind of quality testing by independent bodies has long been an established part of product authorisation in other critical sectors of industry such as medical technology.

Need for action

As mentioned above, the IoT world can be roughly divided into two parts:

- Interconnection of all possible smart things with all kinds of functions
- Operational Technology (OT) / Industry 4.0

Due to the division of the above-mentioned areas, different measures are required for each category. In view of the lack of security awareness of some manufacturers of smart things and the sometimes naive way they are used, these two issues need to be addressed using the following areas of action:

Smart things

- Application of international standardisation and device certification, particularly in the field of security, to increase transparency (which manufacturer is certified) and security (e.g. security/privacy by design). The provision of regulation based on this to make a sufficient level of security mandatory. This must be implemented extensively in at least one

[2] Safety: Being protected against unintentional dangers, such as floods or accidents, Security: Being protected against malicious actions, such as intentional human-induced threats, a robbery or a cyber attack. https://www.endpointprotector.de/blog/was-den-unterschied-zwischen-safety-und-security-ausmacht/

major economic area (e.g. EU) to make an impact on the large manufacturers.

– Supporting and driving forward, where possible, the concept currently being discussed in Switzerland for establishing a national cybersecurity testing institute for interconnected devices.

– Pursuing user-awareness initiatives in order to constantly increase security awareness.

– Research in the field of IoT/OT security, in particular on concepts and architectures, to guarantee security over very long periods of use (e.g. lifespan of 30 years).

OT/Industry 4.0

– The increasing degree of interconnectedness in the field of OT presents every sector of the economy with challenges, as it does not just concern the integration of new systems, but also the interconnection of existing (old) ones. Due to the high level of diversity in the systems to be connected – which also have fundamentally different requirements in terms of safety, availability and lifespan – suitable and feasible end-to-end security architectures (e.g. zero-trust concept[3], micro-segmenting) are essential. To prevent the possible spread of shadow IT, the existing IT processes and interfaces must be modified accordingly.

[3] The Zero Trust concept defines that all connections and users must be checked at all times, regardless of whether they are internal or external. A sole protection of the network perimeter is no longer sufficient. "Trust no one, check everything". See also column inside-IT by Roger Halbheer (in German only): https://www.inside-it.ch/de/post/satw-insights-zero-trust-sicherheit-in-zeiten-von-homeoffice-20200527

References

- EN IEC 62443 – industrial communication networks – network and system security
- Also the ISA standards: https://www.isa.org/intech/201810standards/

SATW-Blog: Die Sicherheit vernetzter Geräte prüfen:
https://www.satw.ch/de/cybersecurity/die-sicherheit-vernetzter-geraete-pruefen/

Contact

Nicole Wettstein
Head of priority programme Cybersecurity
+41 44 226 50 13

https://www.satw.ch/cybersecurity-challenges

Impressum
Swiss Academy of Engineering Sciences SATW
Expert contributions
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Board of Directors and Advisor | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Editing and graphics
Beatrice Huber, Claude Naville, Adrian Sulzer, Nicole Wettstein

The views expressed here are those of the members of the SATW Cyber Security Advisory Board and do not necessarily reflect the official position of SATW and its members.

www.satw.ch
September 2020