## Mikthan Security Technologies Limited

# Managing security, safety and privacy in Smart Factories

### Content

Preface ... 3
1. Why to consider IT-Security when implementing Smart Factories ... 4
2. Cyber espionage and Cyber sabotage ... 5
3. Data Ownership, Rights of Use and Privacy ... 7
4. Designing for IT-security in Smart Factories ... 9
5. Incident Management, Liability and Insurance ... 11
6. References and Recommended Reading ... 13
Imprint & Contacts ... 15

## 1. Why to consider IT-Security when implementing Smart Factories

**Smart Factories promise increased quality, efficiency and flexibility, by having more intelligent monitoring, steering and self-organizing capabilities than traditional factories** [1] [2] [3] [4]. Key enablers are:

- improved access to detailed information from the production process (from sensors or actual products in the making) and from all value chain partners
- 'clever' analysis of these large amounts of information (Big Data)
- direct control and inter-operability of machines in the production process, as well as possibly autonomous (decentralized) decisions by machines

This all becomes possible through intensive digital communication between machines and sensors (often referred to as "Machine-to-Machine communication" (**M2M**) or the "Internet of Things" (**IoT**)), not only within the walls of one factory or within one company but also between wider value chain partners, leveraging the ubiquitous Internet.

**Bringing the Internet into the factory offers opportunities but also new challenges** [2] [3]. The required information flow across many (external) communication networks raises questions about IT- and Data-Security that were not relevant in an era in which machines were only programmable locally and were not connected to any other (IT) infrastructure beyond the power plug. Especially in instances where an existing machine park (still running well with old but stable software) is being connected to the outside world, special measures are needed to protect valuable information from leaking out or malicious software disrupting fine-tuned production processes, potentially even causing harm to humans or the environment.

**It is imperative to deal with IT-security measures at an early planning stage**, as these often cannot be implemented as an "afterthought". This is essential to reap the benefits of Smart Factory concepts without exposing the business to serious risks.

**Serious top-management attention to IT-security is required,** driven by the CEO, CFO, CIO, and Heads of Production, Legal and Human Resources. Not only technical aspects need to be addressed, but also organizational, procedural, legal, and general awareness measures. This requires close cooperation between all departments, especially Office IT, Industrial IT and Operations.

*The CEO plays a crucial role in assuring IT-security is a top priority throughout the organization and should appoint an empowered CISO (Chief Information Security Officer) to drive security aspects.*

**Managing these risks pro-actively is required by Corporate Governance guidelines** such as SOX, Basel II or KonTraG, and increasingly by national or European IT-security Regulations [8] [9]. Management Teams should, therefore, understand not only the business potential but also the risks of Smart Factory implementations, actively managing both in order to assure sustainable growth.

This white paper provides a brief primer for those Executives who may not yet be wholly familiar with Smart Factory related IT-security issues and their potential impact. It should also help the reader to realize that IT Security is a business enabler and not just a cost item.

## 2. Cyber espionage and Cyber sabotage

The “smart” components that control the production process in a Smart Factory are IT-Systems with internet connectivity. They face the IT-security risks that are common to all IT-systems, comparable to home computers or office automation [10].

**Smart Factories, however, are very complex IT systems, facing a greater number of attack scenarios and the potential to cause much more severe impact than office automation systems, possibly even endangering the safety of people and the environment** [11]**.**

As every computer user knows, hackers can potentially break in via the internet or an infected USB-stick and steal sensitive information such as bank account details. Similarly hackers could tap into Smart Factory networks and steal valuable information about customers, product designs or production processes. This can cause commercial damage by unfairly helping competitors, while also invoking claims from customers whose sensitive information is being stolen (**Cyber espionage**) [12].

Computer users are also becoming increasingly aware of the risk that hackers hijack their computers, destroying their data or demanding a ransom to make data available again. In Smart Factories similar scenarios are possible, with a potentially far greater impact, such as the stopping of production, a decrease in product quality, the derailing of production processes or even damage being caused to machines remotely, possibly leading to personal injury or harm to the environment (**Cyber sabotage**).

*The impact of an IT-security incident in a Smart Factory can be very severe, even endangering people and the environment.*

Not only hackers pose a threat but also (ex-) employees or service personnel can create IT-security incidents, either by accident or on purpose.

Such attacks or accidents could have a major impact on society, especially when this concerns so called Critical Infrastructure companies, such as energy and water suppliers, network operators, as well as financial institutions and food supply [13].

**IT-security regulations are, therefore, planned by many governments**, for example:

- proposed EU Directive on Network and Information Security [14]
- US regulation proposals [15]
- draft “IT-Sicherheitsgesetz” in Germany [16]

Most of these require Critical Infrastructure operators to take comprehensive IT-security measures, including a reporting obligation regarding security breaches. In addition, for operators of non-critical infrastructures like most Smart Factories, the new legislation may create indirect effects, as the resulting security standards could establish an industry-wide best practice.

*The Head of Legal should assure that all relevant regulations are understood and implemented throughout the organization.*

## IT-SECURITY RISKS

There are many ways the IT-infrastructure in a Smart Factory can be compromised, either on purpose or accidentally [11].

**While firewalls and virus scanners are basic protection mechanisms in Office IT systems, they have limited value in Smart Factories.** How can a virus scanner be Implemented on a 10-year old production machine with, for example, Windows 3.0 as the operating system, no updating possibility and real-time performance requirements? In addition, virus scanners provide no protection against unknown cyber threats (e.g. Zero Day Trojans), which are often designed for a specific attack, are far more difficult to detect and require (real-time) analysis of large amounts of data, looking for anomalies and isolating suspect data quickly [17] [18].

**Even a machine that is not directly connected to the internet may be targeted**, for example by using a service engineer's PC or laptop as a relay station. Furthermore, simple USB-Sticks used for monitoring, maintenance or programming machines can infect not only one machine but entire networks, as illustrated by the well-published STUXNET attack [19] [20].

*Smart Factory IT is exposed to far more complex IT-security risks than Office IT. As both are connected, they need to be secured as one system.*

**Remote maintenance by equipment suppliers or subcontractors creates another potential risk,** as it requires a connection to their network and computers. Network access by subcontractors or temporary staff often goes unnoticed and is not always disabled after they leave, thus risking uncontrolled access.

**Existing production machines often lack digital identification and authentication functionality**, which is important in a connected system. Traditional machines can often only be operated by somebody directly touching the control panel and are thus protected by physical security (entry into the factory). However, when a machine receives operating instructions via the network, how can it be sure that they are originating from an authorized person or computer? Is it certain that the instructions are not corrupted by some malicious software on that computer or in the network?

**In a true Industry 4.0 implementation, the smart tags attached to components or the final product in production may be manipulated by an attacker** and then travel through the supply chain, carrying their malicious contents from one company to another. The more autonomous decisions Smart Factory machines can make, the more serious this risk becomes.

## 3. Data Ownership, Rights of Use and Privacy

Exchange of data and information plays a key role in the Smart Factory business model, which requires enormous amounts of data to be generated and processed ("**Big Data**"). In this context, the following questions are of particular relevance:

- Who "owns" the data generated, exchanged and analyzed by Smart Factories, and how should this business data be protected (“**Data Ownership**”)?
- How can protection of personal data of employees and customers be assured in a Smart Factory environment (**Privacy**)?

### WHO "OWNS" THE DATA?

A crucial question is whether the operator of a Smart Factory has any legal rights in the generated or exchanged data, including any right to prohibit other parties from using or transferring the data. Most legal concepts in the world, however, do not provide for an ownership right in data as such.

**Smart Factories must, therefore, protect and control the use of data by suitable organizational, technical and contractual measures**.

Only exceptionally and to a very limited extent will data generated and processed in a Smart Factory environment be eligible to enjoy intellectual property rights and protection (such as database or patent rights). In addition, data and information are not subject to (tangible) property rights. There is some criticism of this and certain commentators ask for legislative changes to improve the legal protection of information and data. However, there are arguably very good reasons for not doing so, as the legal protection of information might dramatically hamper technological and economic development in times of social media, open source and open innovation.

It is, therefore, in the hands of operators of Smart Factories to safeguard their sensitive data by appropriate technical and contractual measures. Practice shows that a large number of companies are still too careless in this regard.

**Data Use Agreements should determine the scope of the data use and its purpose**, similarly to Confidentiality and Non-Disclosure Agreements. They should contain obligations with respect to security and organizational measures, as well as erasure and return requirements.

**Continuous monitoring of data generation and data use by a designated “Data Manager” is important** to assure contractual and regulatory obligations are properly implemented in daily operations by all stakeholders.

*Executive management and legal professionals should ensure that data ownership and usage rights are adequately and explicitly covered in all contracts.*

**Technical measures can also help to reduce uncertainty** about the origin, manipulation and usage of data. Electronic signature of data and authentication of machines and operators can enable proper authorization and verification, in line with Data Use Agreements.

## PRIVACY REQUIREMENTS IN SMART FACTORIES

Whereas legal concepts more or less ignore the ownership aspect with respect to data, a totally different situation applies to protection of personal data and privacy. However, data protection rights and privacy obligations primarily favour the data subjects (natural persons) and their interests. European and national data protection laws provide for a comprehensive regulatory framework, in which the generation, use, processing and exchange of personal data generally requires the permission of the person concerned, unless otherwise allowed by statutory provisions.

**Personal Data Protection legislation is struggling with the challenges of Big Data, which leaves considerable uncertainty of what can and cannot be done.**

An interesting aspect of the discussion is to what extent machine data contains personal data. For instance, machine performance data (e.g. generated for the purpose of performance optimisation in Smart Factories) could potentially be linked with data relating to time and attendance of employees working on such machine and, therefore, additionally allow for monitoring such employees´ performance. Accordingly, either the employee´s or, where applicable, the works council's consent to such data processing would be required.

The EU Data Protection “Article 29” Working Party has published its view that, in times of Big Data and associated technical analysis capabilities, even anonymized data could be subject to privacy requirements [21] [22].

**On the (end-) customer side, product and process data may very well fall under the Data Protection regulations**, if such data is linked to specific natural persons (e.g. in "batch size one”-concepts, i.e. individually manufactured products to meet the needs of a specific customer).

*Heads of Production and Human Resources must ensure that personal data protection is considered in the overall design and implementation, and that all stakeholders are involved early on.*

**Data processing requires a global approach in terms of data protection and privacy**, as the exchange and processing of data across borders and various legislative regimes is an inherent consideration in the design of Smart Factory models. Efficient structuring of the supply chain often creates a global network of production sites, logistic centres and sales units. Accordingly, under European data protection laws, transfer of personal data outside of the EU requires compliance with specific rules.

Companies planning to establish Smart Factories must be aware of this "minefield" and take the appropriate measures to comply with applicable laws. Data Protection compliance should be considered from the early planning stage of Smart Factory implementations.

## 4. Designing for IT-security in Smart Factories

### PREVENTIVE MEASURES

100% effective IT-security is not possible in any environment but, with the right design and measures, the risks can be reduced to an acceptable level [23] [24]. Which risks are the most relevant, how much risk is acceptable and how much the appropriate measures can cost, should be analyzed before the Smart Factory implementation starts.

**Such an IT-security Target Analysis** is best done together with IT-security experts that help assess the most valuable assets (customer data, process know-how, critical equipment, etc.), compliance obligations, main IT- and business- risks, and appropriate IT-security mechanisms. Based on such analysis, the right IT-implementation, risk management systems and management processes can be planned.

*The Head of Production plays a key role in assessing what needs to be protected and in assuring appropriate measures are implemented and understood by all employees.*

**Regular IT-security awareness campaigns and training** throughout the company are crucial to prevent the most common problems, often completely unintentionally created by loyal employees. Such campaigns might include leaving a prepared USB-stick in the company restaurant and waiting until some employee plugs this into their computer out of interest, triggering an alert to the IT department to confront the employee regarding this risky behavior. Extensive and regular training, possibly with realistic simulations, is important to assure the right level of preparedness of the full organization.

**An Information Security Management System (ISMS)** helps assure continuous monitoring and improvement of IT-security aspects and should be installed as early as possible. It addresses organizational, process and technical aspects, and must be managed by a specialized employee or outsourced. International standards like ISO/IEC 27001 [25] or IEC 62443 [26] help assure that the right processes are installed and followed.

*The CIO or CISO is responsible for regularly analyzing potential IT risks and continuously improving IT-security measures, both technically and organizationally.*

**IT-security Audits** should be performed by an accredited certification body once all IT-security aspects are implemented properly. It is expected that customers and business partners will increasingly ask for such IT-security certifications before connecting a Smart Factory to their systems, which is crucial for reaping the full benefits of Smart Factory concepts [27].

**Penetration Tests (Pen Tests)** are meant to find security weaknesses that will exist in every complex IT-system, even with the best IT-security design and processes in place. In order to spot those weaknesses before "bad hackers" do, it is important to regularly have “good hackers” from specialized companies perform such Penetration Tests of the complete Smart Factory IT Infrastructure (Office IT and Operational IT). These experts think like hackers and are aware of what is happening in the hacker world, but instead use this know-how for preventive purposes.

## TECHNICAL DESIGN PRINCIPLES

Several Technical Design Principles are established in other IT-security domains (such as classified government IT) and can also guide the design of Smart Factories [24].

**End-to-End Encryption and Electronic Signing of sensitive communications**, whether originating from a person, a control system or a sensor, is an important principle, although not always easy to implement in, for example, real-time control environments. As the Smart Factory is connected through multiple, partially external networks, it cannot be assumed that these networks are secure. Only end-to-end encryption can ensure that:

- unauthorized persons or machines cannot effectively steal the information being transmitted
- the information cannot be tampered with (e.g. to sabotage the factory)
- the receiver can be sure the information originates from a trustworthy source (the message is electronically signed)

This can prevent, for example, an attack whereby a hacker changes the information coming from a temperature sensor to suggest a chemical mixing machine is too cold, while in reality it is already overheating, creating a potential explosion risk.

**Strong Authentication of all people, machines and processes** involved in potentially critical systems is a second design principle. This means, for example, that every machine operator, maintenance engineer and order desk employee should identify themselves before performing an activity, and it should be checked whether this person is authorized to perform this specific action. This is preferably a 2-factor authentication, i.e. based on some possession (e.g. Employee Smartcard) and knowledge (e.g. Password). Similarly, each machine and software process, and ultimately even each sensor, should identify itself in a way that cannot be tampered with, ideally based on a built-in hardware key, in order to enable trust in the messages coming from such a sensor.

*The Head of Production and the CISO or CIO should assure the overall Smart Factory is designed for optimal IT-Security.*

**Separation of subsystems in the overall Smart Factory architecture**, e.g. single production lines or specific production processes, assures that potential attacks can be constrained to one subsystem, by decoupling it from the rest of the Smart Factory. This is similar to isolating patients with an infectious disease from the rest of the population. It can also reduce the resources necessary to secure the smart factory, as it allows for distinguishing between more critical and less critical systems. This principle is also mandated by the upcoming standard for automation security, ISO 62443, as "network zoning" [26].

**"IT-security by Design" is the most important design principle**, meaning that IT-security should be a key consideration in all stages of planning a Smart Factory, rather than an after-thought. It should have the same weight as other crucial business factors such as cost, efficiency and flexibility.

## 5. Incident Management, Liability and Insurance

After taking all appropriate measures to design, implement and operate a Smart Factory according to state-of-the-art IT-security, there remains a risk that something goes wrong. As is the case with fire protection, even the best preventive measures do not make obsolete such things as fire extinguishers and an evacuation plan that is practised regularly. Furthermore, of course, most factories are insured against fire damage.

### IT-SECURITY INCIDENT MANAGEMENT

As part of the Information Security Management System, the complete organization needs to be prepared for dealing with an IT-security incident, to assure proper business continuity planning.

**IT-security Incident Management requires a fast response**, not only on the technical side but also through immediate top-management involvement, ensuring appropriate internal and external communication, including with relevant authorities and insurers. Legal requirements need to be considered, e.g. reporting obligations in case of breach of confidentiality or data protection provisions.

> *The CEO should assure that proper IT-Security Incident Management processes are implemented and practised regularly.*

IT-security Incident Management generally includes three aspects:

- **containing the threat** as quickly as possible to minimize direct and indirect damage
- **informing top-management** and relevant staff to enable rapid assessment of the potential impact and required actions, especially external communication
- **establishing an Incident Team** and central point of contact to avoid chaotic actions

The Incident Team is usually responsible for:

- **preparing and executing a communication plan**, to inform relevant employees, customers, suppliers, authorities, legal and insurance experts (even if at this stage only a suspected breach can be communicated)
- **performing a root cause and impact analysis**, in order to understand what happened, what damage has been or could be done (scenarios), who is affected and how to limit further damage
- **developing and executing a proper action plan** to fix the root cause, restart systems and deal with direct and consequential damages to business partners

**Regular practising of IT-security Incident Management is as crucial as fire drills**, as incidents hopefully don´t happen so often that all relevant people already have experience with the process. All functions and departments need to be involved in this.

**The question of responsibility can be addressed once the incident is under control**, by considering: how this could happen, who has to pay for the costs and damages and what needs to be improved in systems and processes. Due consideration of such “lessons learned” is crucial for a business' brand and reputation. Most business partners show understanding that incidents can happen, but only if they are managed very well and are shown not to occur a second time.

## WHO IS LIABLE WHEN SOMETHING GOES WRONG?

The Smart Factory model leads to substantial new challenges with respect to the liability exposure of all involved parties. In a connected IT-based production environment, a more comprehensive and accurate documentation of all processes and production steps is possible and, therefore, it could be expected that the identification of the root cause of an incident is easier.

**However, it often requires the help of Forensic IT Experts** to perform an in-depth technical analysis in order to search for any traces of an attack or accidental error. The complexity of widely connected, highly interdependent and partially autonomously decision-making systems, many supply chain partners and the sophistication of hackers, can make it difficult to identify the true source of an incident.

There is, therefore, usually a multitude of partners who might have been the cause of an IT-incident, which makes it difficult to avoid or handle "finger-pointing" scenarios. For example, it is often not clear which party is responsible for the connectivity of the systems.

Moreover, telecom providers' liability for connectivity outages is capped in many jurisdictions (e.g. under German law).

*Executive Management should assure appropriate liability arrangements in contracts with all supply chain partners.*

**Smart Factories need to clarify liabilities in contracts with value chain partners**. A balanced share of the risks is essential to ensure the success of the Smart Factory model. For example, IT Suppliers are confronted with new liability risks, as a failure of a single IT Application may lead to substantial damages for the Smart Factory and its business partners. A production interruption of just a few days could put the IT Supplier's economic sustainability at risk, if it has not agreed to suitable and reasonable liability caps.

## INSURANCE

After taking suitable preventive IT-security measures and properly managing Incidents, certain costs remain after the Incident. This can include internal costs for handling the incident, cost for external experts (technical, legal, and communication), claims from customers or partners, and possibly fines.

*The CEO should organize appropriate Cyber security Insurance, and assure all conditions for coverage are fulfilled.*

**Some of those costs can be insured through Cyber security Insurance**.

However, such insurance only covers costs within certain limits and only if preventive measures are properly implemented by the insured Smart Factory. An insurer usually checks this both before accepting a client and after a claim is submitted. Such preventive measures include not only technical IT-security provisions and an ISMS implementation but also awareness, training and a well-implemented Incident Management or Business Continuity process.

**Insurers often require preventive consulting by IT-security experts**. It is, therefore, recommended that insurers are involved early on in the planning of a Smart Factory implementation. This needs to be driven by Executive Management, as an IT-Security Incident is not just an IT issue but also a Top Management affair.

## Imprint & Contacts