Digitisation of Production: General Targets of Cyberattacks and Prevention Strategy

New technologies offer unimaginable potential: they can increase safety in the workplace, better protect workers, make workplaces more ergonomic and promote good health. However, the global networking of machine controls, databases and software services also brings new threats that need to be identified and assessed. As digitalization progresses, innovation accelerates tremendously and development times of new products and manufacturing facilities are getting shorter and shorter. The disadvantage is that these systems often cannot be adequately tested and the necessary risk analysis is poorly developed, which can lead to new hazards in the workplace.
In the age of digitization, employee protection can be regarded as the combination of safety (machine safety) and security (IT security). However, these two security areas traditionally have very different strategies, which necessitates coordination to ensure the safety and health of workers.
Consequently, the role of the safety expert in the company is upgraded. Communication and increased teamwork with network and IT specialists are indispensable. With digitization and new technologies, it is more essential than ever to work across departments to ensure occupational safety in companies. Today, a holistic expert risk assessment can only be carried out in close cooperation between IT specialists and safety experts.

General targets of cyberattacks

Cyber-attacks can be carried out by individuals, groups or government-funded institutions, and may have different goals. The methods and attack scenarios used often depend on the:

- size of the company;
- product portfolio ;
- question whether intruders seek to steel know-how regarding technology
- question if critical infrastructure is being targeted

Therefore, it is necessary to develop company-specific security strategies and define appropriate measures.
In general, s. Fig. 1, cyber-attacks can pursue the following goals:

1.) building and energy supply
    - Attack on general infrastructure, aiming to paralyze the production partially or completely
    - Emergence of environmental catastrophes through manipulations, e.g. in the chemical industry. Due to long production processes in the chemical industry, parameter changes are only visible after many hours, sometimes only the next day. This complicates timely detection of possible manipulation by cyber-attacks.

Fig. 1 Objectives of cyber-attacks on productions

2.) Individual machines and production equipment
- should be disrupted to bring about a loss of production
- error frequency of a machine is increased in order to damage the machine manufacturer
- new machines are infected with malware that can attack the IT network from the inside after commissioning

3.) Employees
- Information to employees is manipulated in order to specifically disrupt processes
- Targeted deactivation of safety equipment provokes accidents. This causes the company an image damage
- Devices on humans are used to damage a machine or the IT network from the inside or to steal know-how

4.) Product
- Processes are manipulated in such a way that the product properties are altered: damage to the image of the company
- Process manipulation leads to a reduction in the quality of the product. Damage occurs at the customer such as unrecognized errors in a spare part for aircraft
- Mass products, such as food, are contaminated to cause harm to health: means terror

Defence strategies

All possible scenarios Cyber-attacks are now incorporated into a multi-level defense system and integrated into a management system (such as EN ISO / IEC 27001). The following are some general measures against malware and spyware malware attacks that should be self-evident in every business:

- All employees should be informed regularly about IT security
- The instruction should also cover cyber security at the workplace
- Raise employees' awareness of cyber incidents, privacy and use of personal devices in the workplace
- The guests as well as staff of external companies should be prohibited from using personal devices on their premises, including mobile phones and laptops, and the use of USB sticks should be prohibited
- Unnecessary USB ports on machine controls, PCs and other electronic devices should be turned off
- During the evaluation, Occupational safety expert together with IT experts in the machine park are to identify, assess and implement threats due to IT networking. The cooperation between security specialist and IT specialist has become very important and should be intensified in companies.

Grouping of new technologies according to safety relevance

From the point of view of machine safety and employee protection, or the expected impact of IT security on safety, the new technologies of digitization are divided into five main groups by IVSS (see Fig. 2):

1) Smart Human (employee uses portable computers incl. sensors and various devices)
2) Cloud & Internet (direct communication of machine controls and software via the Internet or cloud services)
3) Artificial intelligence (self-changing algorithms with integrated database and self-learning control programs)
4) Digital Factory (mathematical models of real production with various simulation and analysis tools)
5) Robots (industrial robots, mobile robots, drones, autonomous vehicles and other mobile machines)

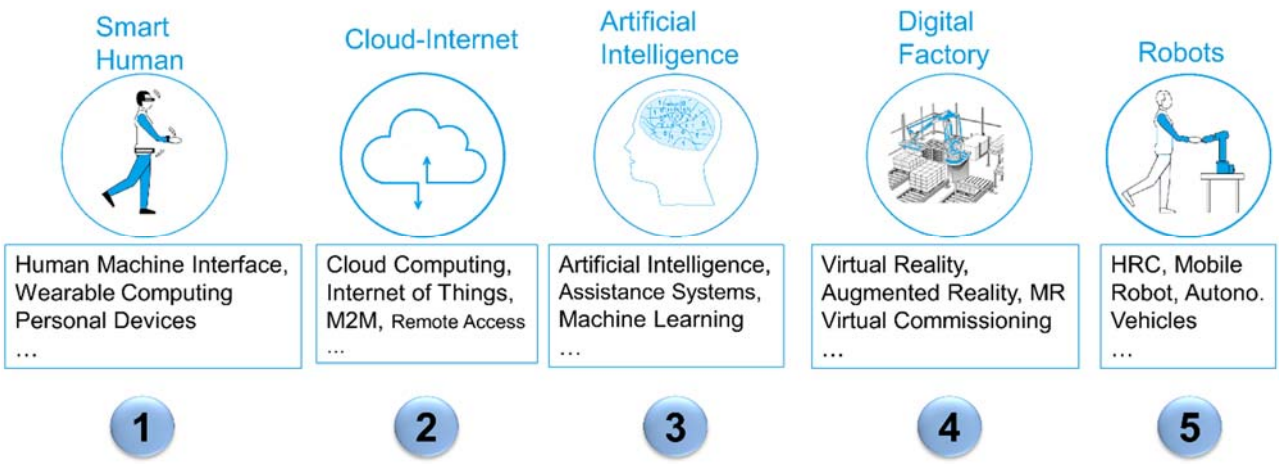

Fig. 2. Grouping of new technologies according to safety relevance

This division of the new technologies into five groups should facilitate the consideration of the links between safety and security as well as the impact on employee protection. It makes sense to bundle prevention activities and use them selectively.

The Partners of IVSS: AUVA, SUVA, DGUV, INAIL helps companies to implement the new technologies created by digitalisation, to set up workplaces 4.0, to integrate safety and security as well as appropriate management systems and to train responsible personnel as part of the training program.

Viktorijo Malisa

AUVA - Vienna