Industry 4.0 Smart Factory & Safety Monitoring system

Safety & Security
Decentralisation
From Industry 1.0 to Industry 4.0
The Internet comes to the production floor

Industry 4.0:
- The objective is an intelligent (smart) factory. Characterised by high adaptability, resource efficiency and the integration of customers and suppliers into the value stream.
- Cyber-physical systems and the Internet of Things (IoT) are the technological basis.
- Data defines the production process – production data represents the actual value in the process chain.
Industry 4.0
What are the drivers

- Growing importance of the added value chain (incl. supplier)
- Demographic change
- Skills shortage
- Growing number of product types
- Individualisation
- Market changes Cost pressure
- Resource-efficient production Urban production
- Shorter product lifecycles

Industry 4.0
**Definitions**

- **Internet of Things (IoT)**
  - Computers are increasingly disappearing as individual devices - and their function is being replaced by "intelligent objects"
  - Rather than being the object of human attention itself – as it currently is – the "Internet of Things" is intended to support human activity unnoticed. The ever smaller embedded computer systems are intended to support humans in their work without causing a distraction or even coming to anyone's attention.
  - The Internet of Things connects clearly identifiable physical objects (things) to a virtual representation in an Internet-like structure. It no longer consists only of human subscribers but also things – or in the language of the automation world – intelligent and highly networked end devices.
  - Internet Protocol Version 6 (IPv6): Much higher number of IP addresses compared with IPv4 - prerequisite for networking a significantly higher number of intelligent end devices.

- **Cyber-physical production systems**
  - A cyber-physical system describes the network of IT-based software components with mechanical and electronic parts, which communicate via a common data model and a common infrastructure.
  - A cyber-physical system is characterised by a high degree of complexity. Cyber-physical systems are formed from networking embedded systems through wired or wireless communication networks.

- **Smart factory**
  - Research in the field of manufacturing technology
  - Element of the high-tech strategy of the German government as part of the Industry 4.0 initiative.
  - Vision of a production environment in which manufacturing plants and logistics systems largely organise and optimise themselves. Technically it is based on cyber-physical systems, which communicate with each other via the Internet of Things.
  - Part of this future scenario is communication between the product (e.g. workpiece) and manufacturing plant: the product brings its manufacturing information with it in machine readable form, e.g. on an RFID chip. The product's route through the manufacturing plant and the individual manufacturing stages are controlled based on this data.
  - Universities and research institutions are working on the smart factory within so-called model factories.
With Industry 4.0, **highly networked system structures** emerge, which include all automation devices, IT systems and the whole network infrastructure.

Logical consequence is:

- Increasing demand for
  - Communication
  - Security mechanisms
    (safety and security)

- A very flat hierarchy for the "automation pyramid"
  - A high degree of **modularisation** for machines and equipment
  - Exclusively functional orientation rather than device orientation
Industry 4.0
Protection targets for safety & security

**Safety – for the safety of man and machine**
- Protect persons & machines from the hazards of operating machinery

**Security – for safeguarding productivity**
- Protect machines or systems from unauthorised access
- Protect sensitive data from unauthorised change or loss or unauthorised access
Industry 4.0
Safety and security – the differences

Safety – for the safety of man and machine

Safety Intensity Level (SIL)

Security – for safeguarding productivity

Security Assurance Level (SL)

Diagram:
- Safety measures (shearing, crushing, protective fence, protected area, machinery, cutting)
- Security measures (internal staff, access control, integrity monitoring, staff training, secure zone, electrical and physical scenarios, staff training, segmentation, hardening, espionage, remote access, trojans, production loss)

September 2014
### Industry 4.0 Commonalities

**Safety and security** –

<table>
<thead>
<tr>
<th>Process</th>
<th>Safety</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>System limits</td>
<td>Plant, machine, machine elements...</td>
<td>Zone, subzone, network, ...</td>
</tr>
<tr>
<td>Threats</td>
<td>Material feed, maintenance gates, ...</td>
<td>ERP data exchange, Remote maintenance access, IPC, ...</td>
</tr>
<tr>
<td>Result of risk analysis</td>
<td>Cutting, crushing, shearing ...</td>
<td>Non-authorised access, unauthorised reading of data, manipulation ...</td>
</tr>
<tr>
<td>Measures</td>
<td>E-STOP, light grid, speed monitoring ...</td>
<td>Firewall, virtual networks, VPN, authentication, coding, encryption, SNMP, ...</td>
</tr>
<tr>
<td>Validation</td>
<td>Approvals, auditing, test, ...</td>
<td>Verification, monitoring, recording, ...</td>
</tr>
</tbody>
</table>

**SIL: Safety Integrity Level**  
IEC 61508

**SL: Security Acceptance Level**  
ISA99 / IEC 62443 draft standard

> Safety and security have clear parallels in the standardisation and structuring of the design process.
> Aim:
> - Benefits of safety experiences used for industrial security
### Industry 4.0

#### Differences

<table>
<thead>
<tr>
<th></th>
<th>Safety – for the safety of man and machine</th>
<th>Security – for safeguarding productivity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Safety</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Origin of threat

- **Plant or machine**
- **Internal staff, external forces, malware (viruses, trojans, etc.)**

#### Threat

- **Can be localised and managed**
- **Diffuse, changing, with specialist knowledge, potentially criminal intent**

#### Impact

- **Injury or death, e.g. due to cutting or shearing**
- **Production failure, loss of expertise, data loss ...**

#### Remedies

- **Isolate the hazard: (enclosure)**
- **Protected zone, safety fence and continuous monitoring of all safeguards**
- **Immunisation: “Hardening” of communication, segmentation etc.**

#### Norms, standards

- **IEC 61508 and a wide range of A, B and C standards**
- **Machinery Directive, legally binding in the EU**
- **No standardisation! Common objectives emerge only through the coming together of the worlds of automation and IT**

---

*October 2014*
Challenge:
Conflict of interests in priorities

Automation
- TOP1: Availability, Productivity
- TOP2: Integrity, Reliability
- TOP3: Confidentiality

IT world
- TOP1: Confidentiality
- TOP2: Integrity, Reliability
- TOP3: Availability, Productivity

October 2014
Industry 4.0
Flat hierarchies and modular machines
Industry 4.0
Decentralisation of the control function

- Centralised I/Os (70s)
- Decentralised I/Os (80s)

Zentrale Ein- und Ausgänge (70er)
Centralised I/Os (70s)

Dezentrale Ein- und Ausgänge (80er)
Decentralised I/Os (80s)

Verbundene Systeme, zentrale Steuerungen (heute)
Connected systems, centralised controllers (today)

Modular architecture with decentralised control systems

Reduction of component-related costs (installation, handling)

Reduction of system-related costs (engineering, reusability, flexibility)
The mechatronic approach

A mechatronic module is:
- a simple device (e.g. cylinder)
- a machine element (e.g. drilling station)
- machine modules (e.g. machine centre)
- the whole machine

The mechatronic approach can be used at best if the machine can be split up into functional parts and functional modules…… Which is true for most of the machines!
Distributed architecture and decentralisation

- PSS 4000: first distributed system for safety and control
- Keep the centralised view of a distributed control architecture
- The controller is a function - not a device!
- In future: intelligent sensors will control the process
Automation system PSS 4000 – Simplify your Automation™

SafetyNETp (Real-time Ethernet) 기반의 네트워킹

다양한 제품군 및 광범위한 I/O module 로 뛰어난 확장성

하나의 헤드 모듈에 일반 I/O 모듈 및 Safety I/O 모듈 혼합하여 확장 가능.

다양한 I/O 모듈 지원으로 Safety 평선 및 일반 공정제어를 하나의 Safety PLC에서 처리 가능.
– Application

Gate monitoring & Access control system

I/O

Office
Network

PSSu PLC

Local Remote Panel

Ethernet Switch

Local Remote Panel

Ethemet Switch

I/O

I/O

I/O

Gate monitoring & Access control system

Local Remote Panel

Remote Panel

I/O

I/O

I/O

I/O

Gas & Fire detector

Plant 내의 각종 유해 Gas 검출 및 화재 감시 시스템

출입 인원 및 정보 관리

설비 관련 안전 부품 및 드라이브 관련 안전 기능

Safety components

Scan-1

Photo-1

Drive

Download

Download

Download

Download

Download
## Gate monitoring & Access control system

관련 시스템 및 주요 안전 부품

### PSS 4000 – Fail-safe 기능의 Safety PLC

- **Dual processor** 기반의 안전 PLC
- 이중화 모니터링 기능으로 고장에 대한 안전 확보
- 높은 신뢰성 및 최상위 안전 등급 만족

### Network components PSSnet – 산업용 이더넷 네트워크 장치

**Industrial Ethernet Switch**

- 산업용 Ethernet 기반의 Network 장치
- 최대 전송 가능 거리 32,5 km (Fiber-optic S/M), 5 km (Fiber-optic M/M)
- Ring redundancy

### PSENgate – Safety gate system

- 안전 게이트 감시 및 Safe 가드 락킹 장치
- 기구 적인 락킹 및 제어
- Bolt 파손 등에 대한 모니터링 기능
- 비상 탈출 기능

### PITmode – RFID key 기반의 출입 요청 장치

- RFID 기반의 Key 를 통한 출입 요청 장치
- 출입자 마다 접근 권한 부여 가능
- RFID 코드를 통해 출입자의 정보 인식 가능
Thank You!
Keep up-to-date on Pilz
www.pilz.com