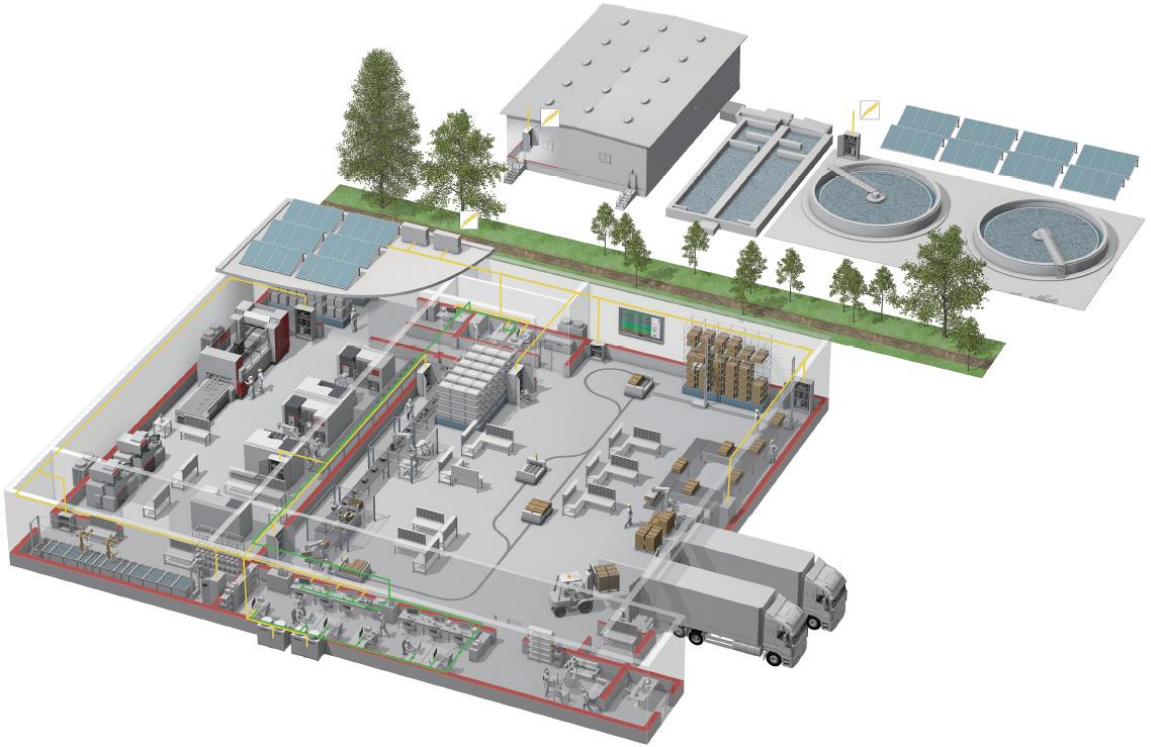
Safety and Cyber Security for Packaging applications

Marco Filippis – Oscar Arienti – Cristian Sartori

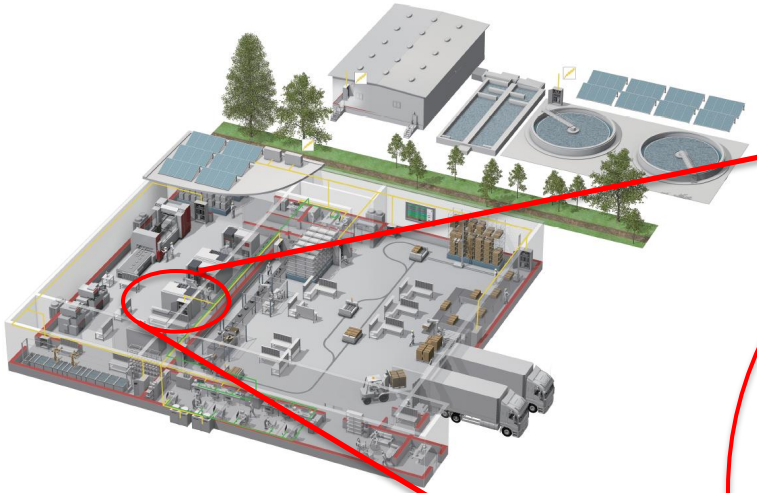
Smart Factory Concept

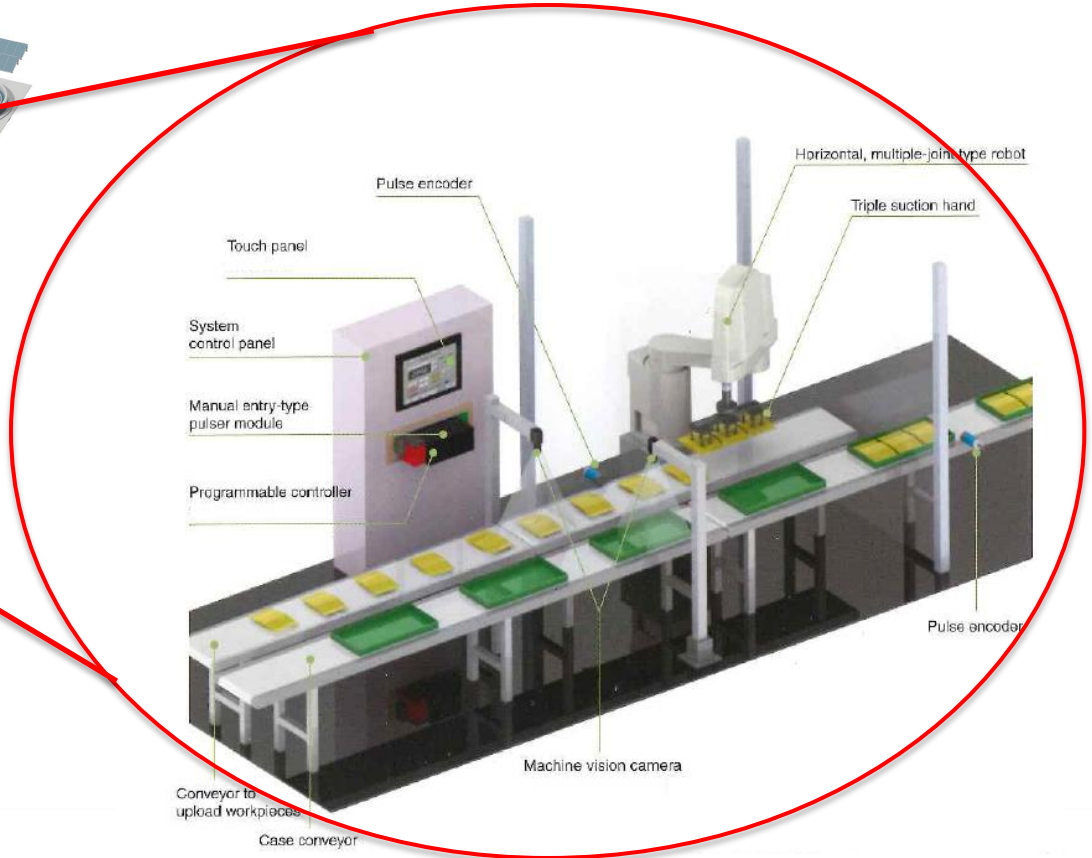


Industry 4.0 paradigm is a way of automation and data exchange in manufacturing technologies including IOT, Cloud Computing and Cyber-phisical systems

Safety and Cyber Security

Packaging Application

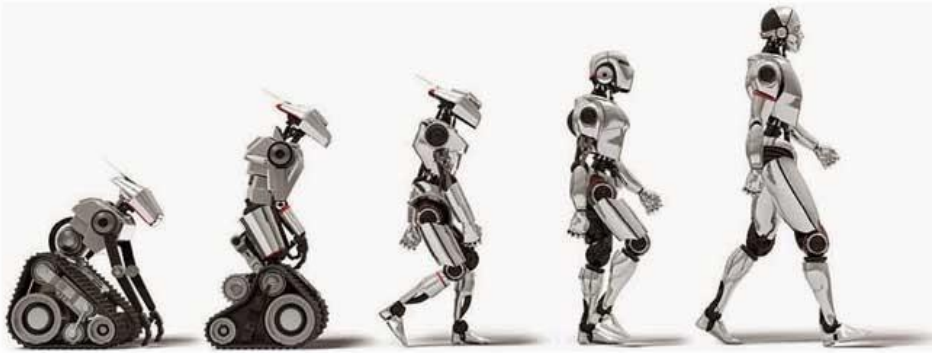




All-in-one solution integrating logic, motion robot and external devices for tracking

The evolution of robotics

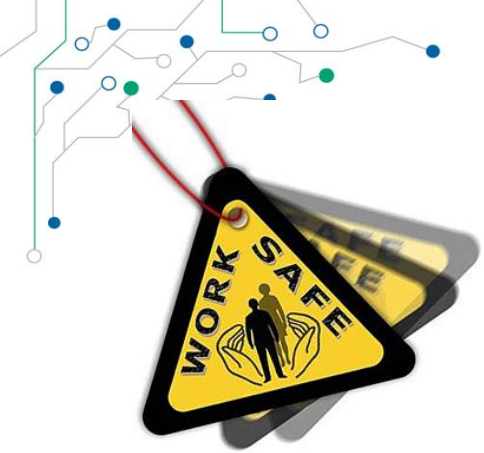
…from single robotic cell to integrated, safe and complete solutions



The most important challanges:

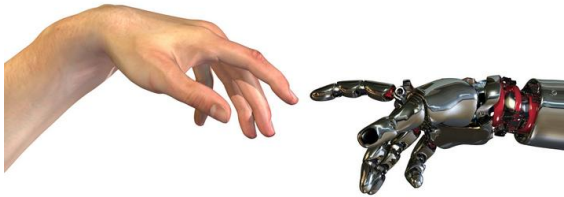
- Sharing the workspace with human beings mantaining unchanged the productivity at the end of line.
- Exchange of large quantity data with the external.
- Fitting with critical working environmental

The evolution of robotics



Create different working areas with safe different speedm; limiting the action areas using virtual safety planes ; torque control on every single joint are the secrets to allow industrial standard robots a collaborative approach.

Pure collaborative robotics can be an opening door for new application fields, sometimes very far from original uses



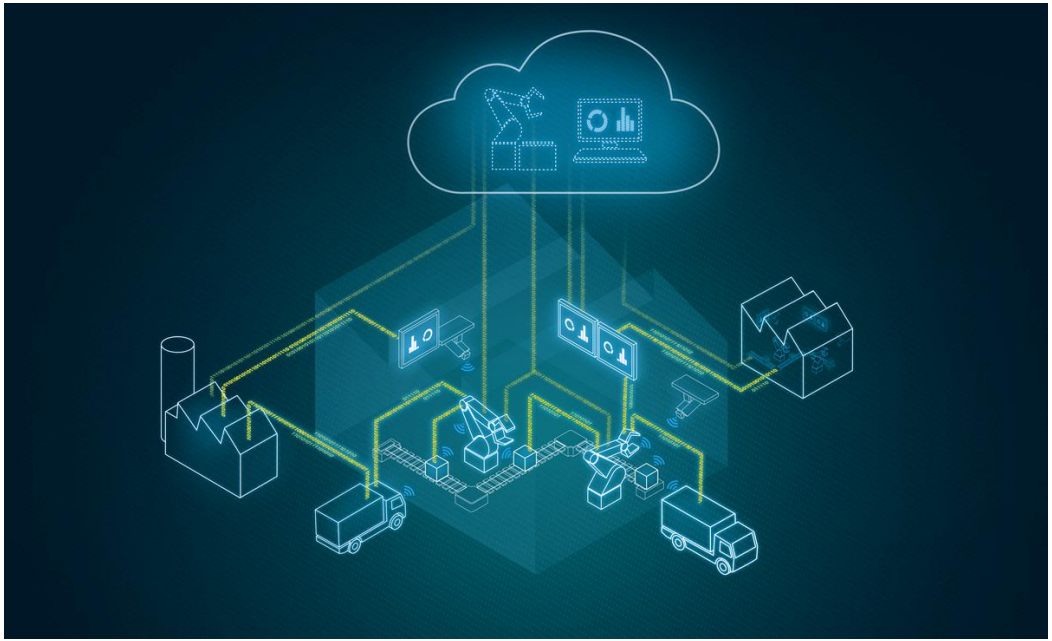
Critical Environments

Certifications and compliance with the international standard means that robot must to change skin to be resistant to corrosive agents (Ex. H2O2)

What means complaince with standard?

- ✓ Special coating of the surface
- ✓ Stainless steel joints
- ✓ Seals resistant to chemical agents
- ✓ Special shape of the screws avoiding accumulation of contaminated meterials

Industrial Security – prerequisite for Digitalization



- Total Connectivity : every real component has a digital twin in the IIoT ➔ every component, every production- and network-level is connected and needs to communicate.
- Big data: transfer and storage of all machine and plant data – real-time, process data, diagnostics, quality data, IT data.
- Use of open Standards: required for a barrier-free data exchange

But these Trends increase also the vulnerability of production plants against cyber attacks and require effective and suitable security concepts and measures.

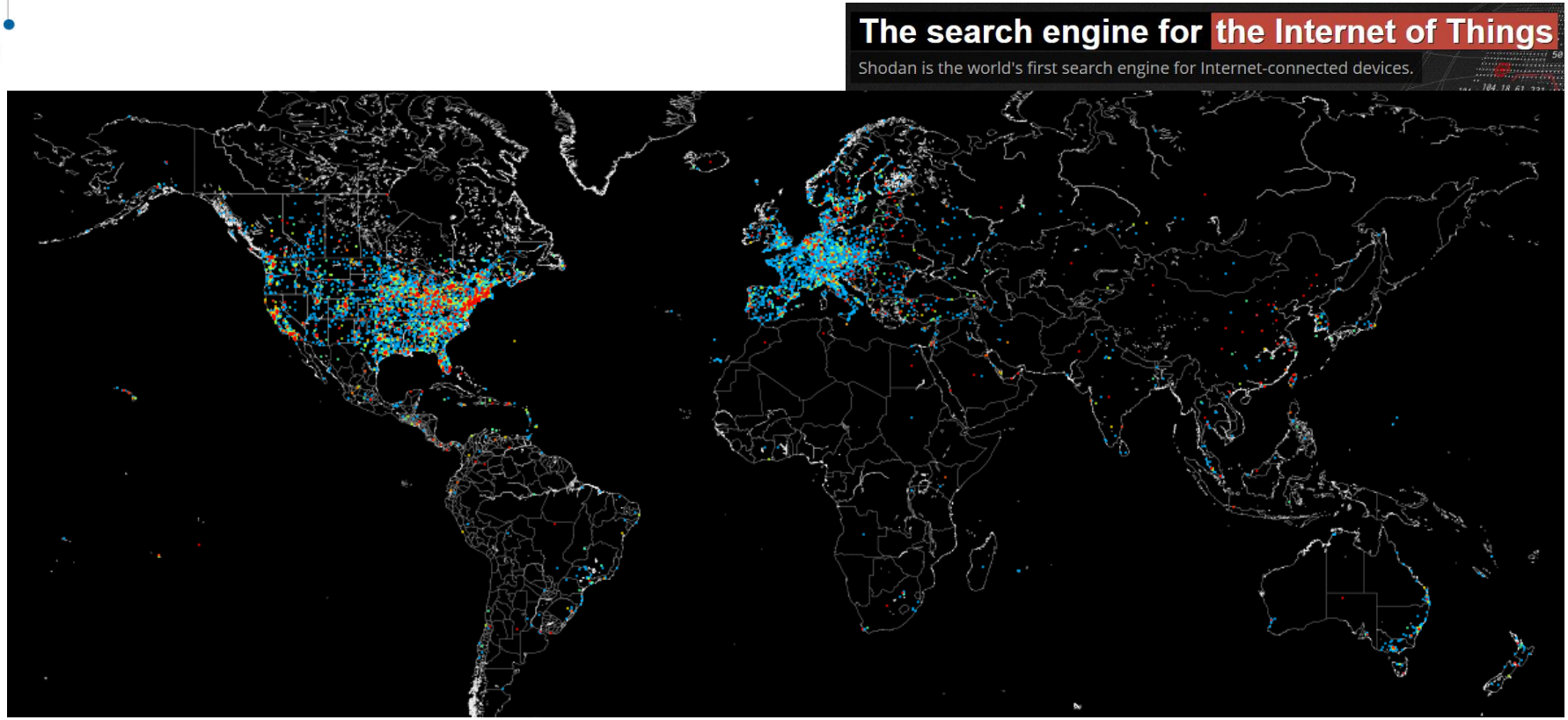
Cyber vulnerabilities

BSI[1]: Top 10 threats for Industrial Control Systems (ICS) - 2016

1. **Social engineering and phising**[2]
2. Introduction of **malware via removable media** and external hardware
3. Malware **infection via the Internet and Intranet**
4. Intrusion via **remote access**
5. Human error and sabotage
6. Control components connected to the Internet
7. Technical malfunctions and force majeure
8. Compromising of extranet and cloud components
9. (Distributed) **denial-of-service** ((D)DOS) attacks
10. Compromising of **smartphones in the production environment**

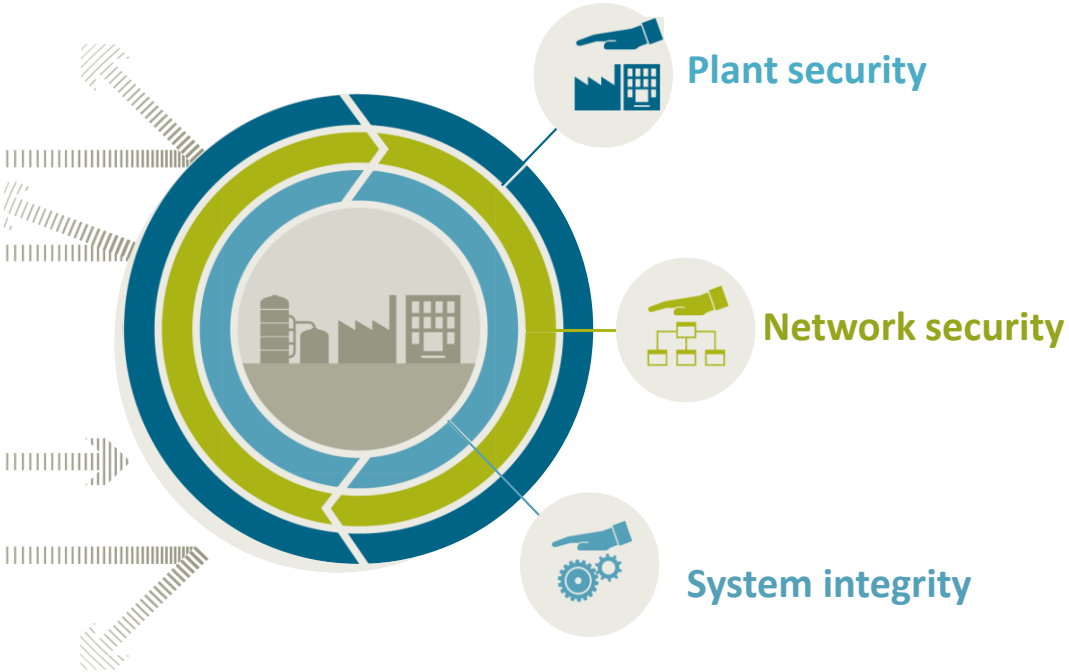
1 German Federal Office for Information Security
2 New
Source: BSI analysis on cyber security 2016

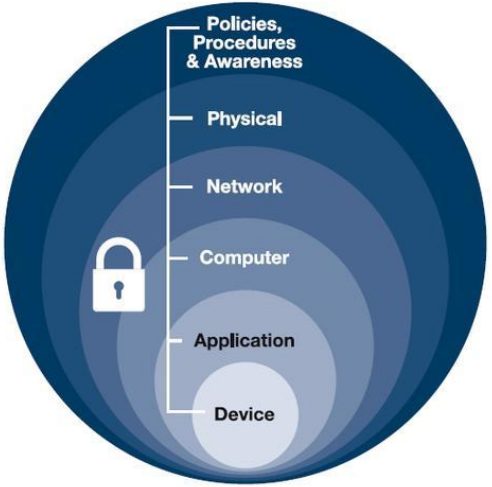
www.shodan.io



https://ics-radar.shodan.io/

“Defense in Depth”





Industrial Security Standard **ISA 99 / IEC 62443**

Critical Environments

When a machine tool is in setup mode of operation, there may be a person within the machine's work envelope. To avoid damage to persons, it must be ensured – for example - that:

Stationary axes do not start moving uncontrolledly

→ Safe operating stop

Driven axes move at low speed

→ Safely limited speed

- In europe safety requirements are regulated by law (Machinery directive - 2006/42/EG)
- Standards describe "how to reach safety"
- New standards with improved requirements are established (IEC 61508, EN 13849 - sucessor of EN 954-1)

PL PFHd SIL

Performance Level (PL - EN ISO 13849)	PFH_d Probability of a dangerous failure per hour [1/h]	Safety Integrity Level (SIL - EN 61508)
a	10^{-5} to 10^{-4}	No specific requirements
b	$3x10^{-6}$ to 10^{-5}	1
c	10^{-6} to $3x10^{-6}$	1
d	10^{-7} to 10^{-6}	2
e	10^{-8} to 10^{-7}	3

SIL2 / PL "d" = usual requirement on a machine tool (corresponds to category 3 as per EN 954-1)
A direct correlation of "old" categories as per EN 954-1 and the Performance Levels as per EN 13849 are possible only if the structure of the system (e.g. single-fault tolerance), the diagnostic coverage and the probability of failure are known.

Note: The PFH_d-value is only related to the failure of the safety function of a system not its general function.

Dependency between MTTF, MTTFD, FIT, DC and PFHD

PFH_d/PFH: Probability of a dangerous failure per hour [1/h]
PFH is often used instead of PFH_d. Both terms usually mean the same.

FIT: Failure in time [10^{-9}/h]
Used in EN ISO 61508
The FIT value is the reciprocal of the MTTF value

MTTF/MTBF: Mean time to(between) failure [h]
Used in EN ISO 13849

$MTTF_d$: Mean time to dangerous failure
The $MTTF_d$ value does not itself contain any diagnosis of the values.
Estimation from the MTTF value (according to EN ISO 13849): $MTTF_d = 2 \times MTTF$

DC: Diagnostic coverage
The DC indicates the probability with which certain faults can be detected. The percentage of non-detected faults leads to the PFH_d value.

Explanation of terms MTTF, MTTFD, FIT, DC and PFHD

- **Basic principle of calculation of a safe axis and the incorporation of the encoder:**

  $PFH_{d\ axis}$ = **$PFH_{d\ encoder}$** + $PFH_{d\ control}$ + $PFH_{d\ actor}$

  The PFH_d value of the encoder depends both on the failure behavior of the encoder as on the diagnostic capabilities in the control

- **PFH_d for certified EnDat 2.2 Encoders:**
  The PFH_d can be entered directly. Here the catalog of measures describes in detail how to evaluate the encoder data for the safe control (see D533095). This reveals the diagnostic coverage (DC) of the control, and the PFH_d value can be provided immediately to the customers.

- **PFH_D for non certified Encoders:**
  HEIDENHAIN cannot provide a PFH_d value for the encoder because the diagnostic possibilities of the control (DC) must be known. In this case, HEIDENHAIN provides the customer with a failure rate (MTTF value) for the encoder. The MTTF value includes both nonhazardous and hazardous failures of the encoder. According to EN ISO 13849, it is standard practice to assume that 50% of the faults are dangerous.

  $MTTF_{d\ encoder}$ **= 2 x $MTTF_{encoder}$** **(as per EN ISO 13849)**

  $PFH_{d\ encoder}$ $= \frac{(1 - DC_{control})}{MTTF_{D\_encoder}} = \frac{(1 - DC_{control})}{2\ x\ MTTF_{encoder}}$

Security And Safety

Security process

- Based on IEC 62443-2-4 and ISO27001
- Maturity Level 1 - 4

Protection Level (PL)

Security functions

- Based on IEC 62443-3-3
- Security Level 1 - 4

Protection Levels are the key criteria and cover security functionalities and processes