Rome, 07/07/2023

Ernesto Del Prete

Email: e.delprete@inail.it

INAIL

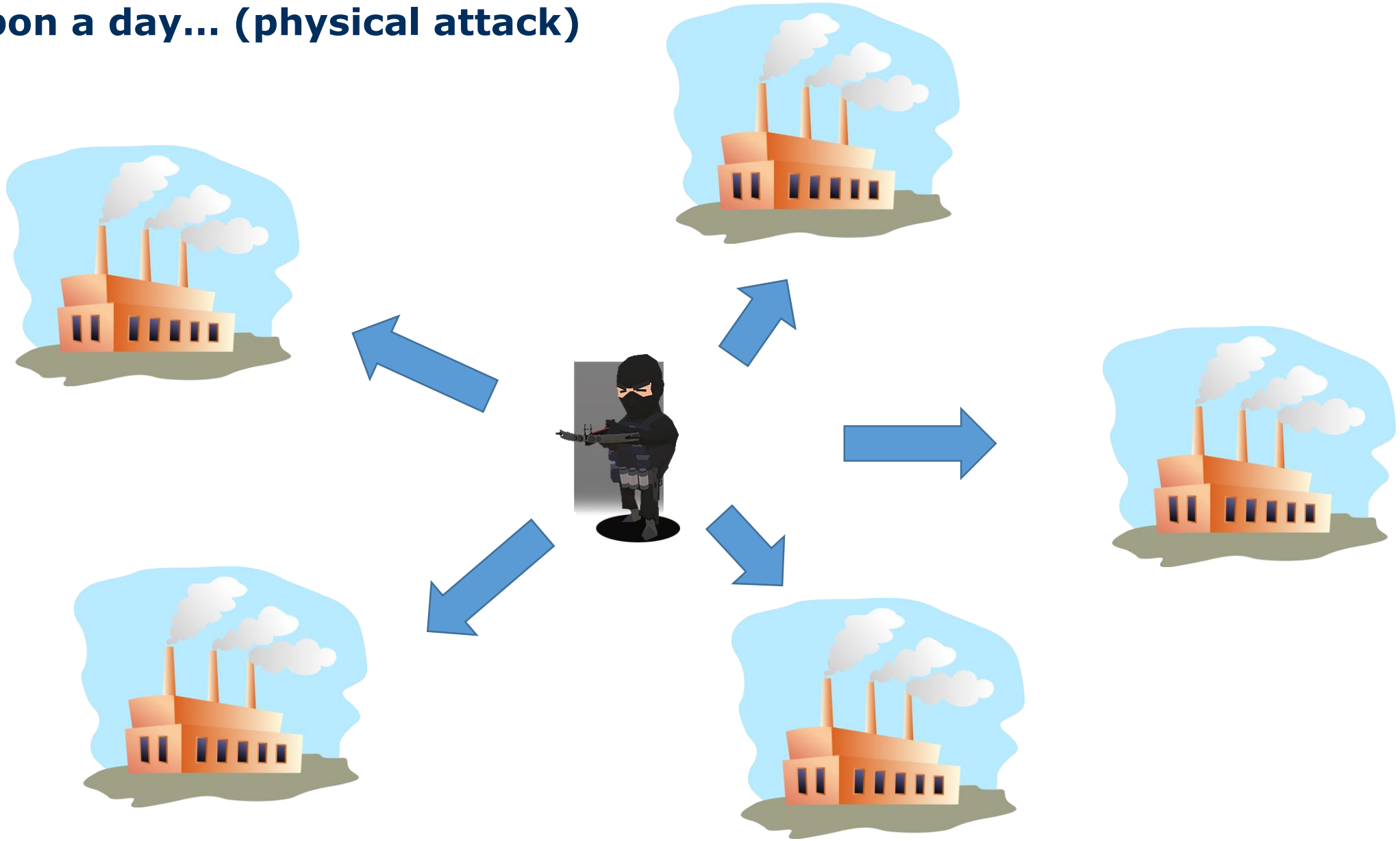
ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO

Cybersecurity for safety

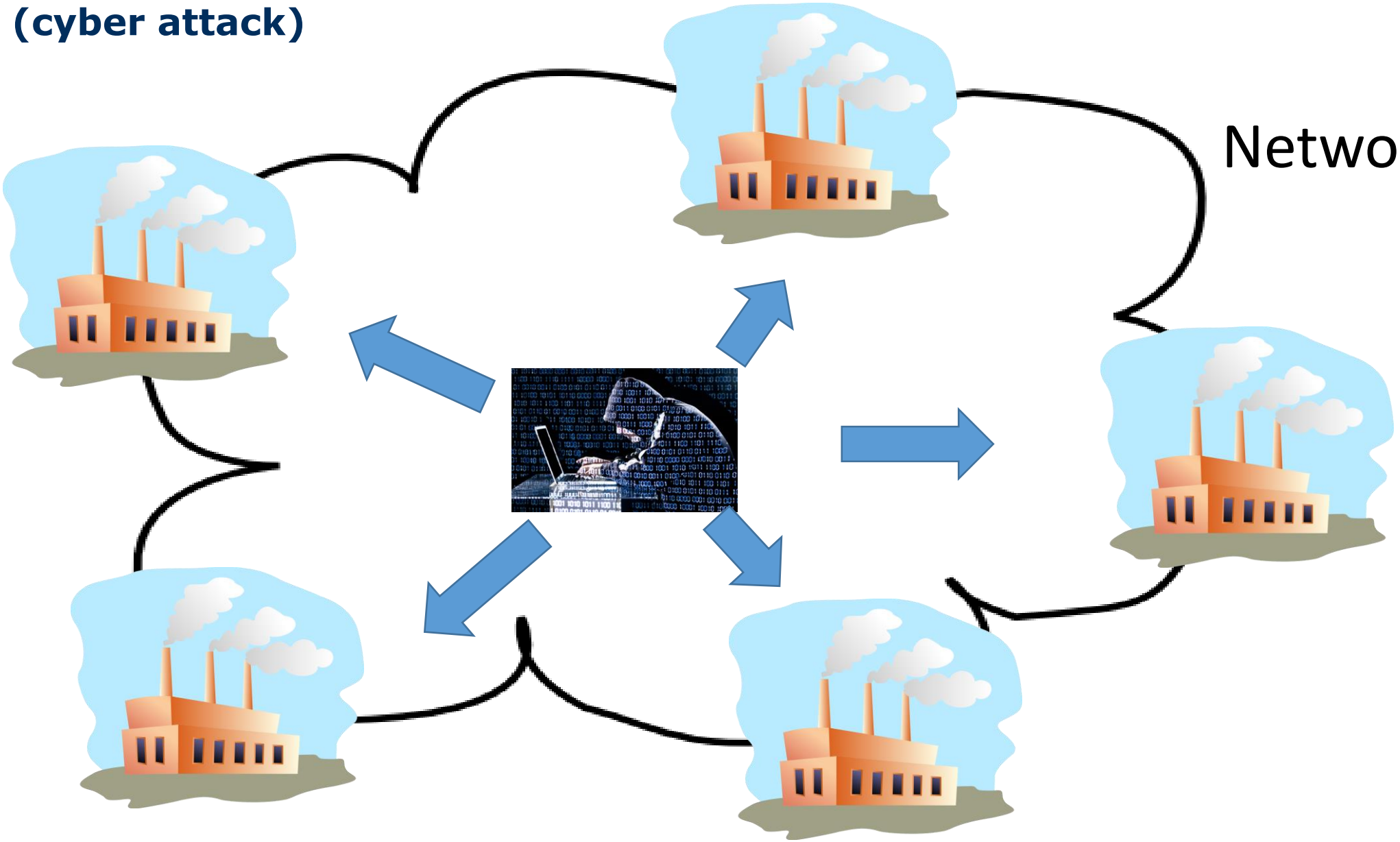
Department of technological innovations and safety of plants, products and anthropic settlements

Once upon a day… (damage)

Once upon a day… (physical attack)



Today… (cyber attack)



Why cyber-security in industry?

Business needs

Efficiency needs

Production monitoring

Interconnection

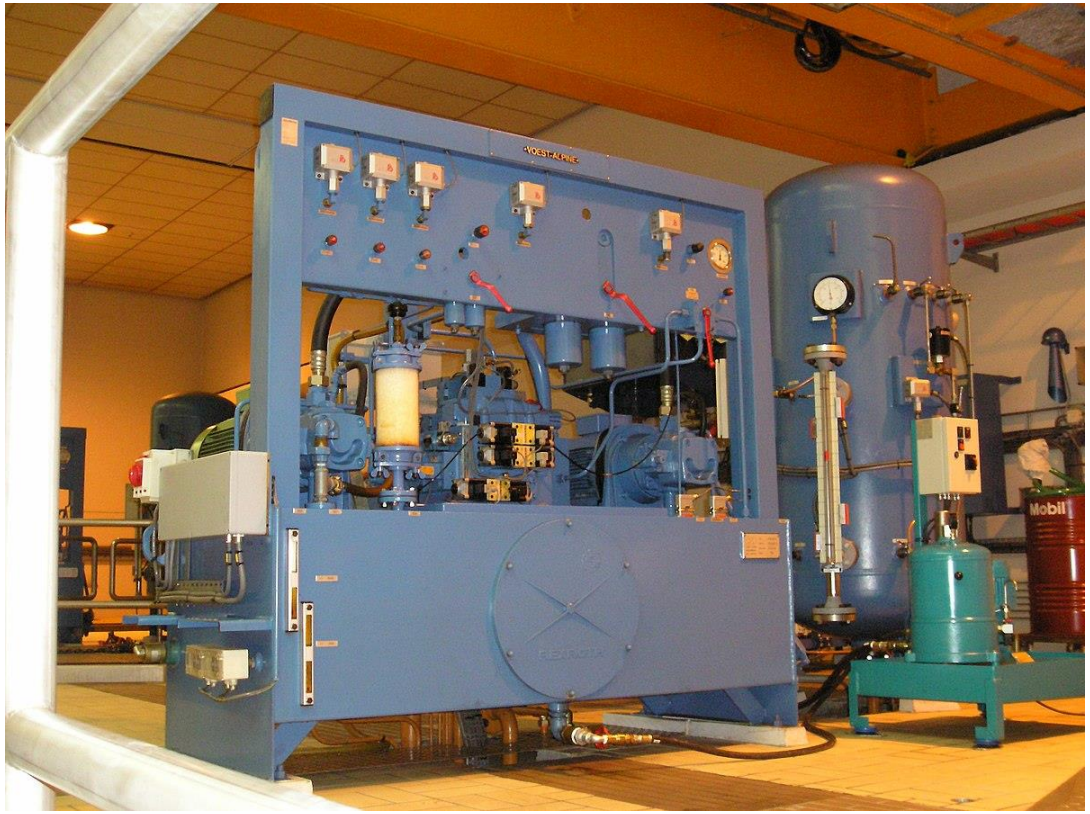
Increasing complexity → n **objects** → $\frac{n(n-1)}{2}$ **connections**

IT security problems

When does a cyber-security risk imply a safety risk directly?

}

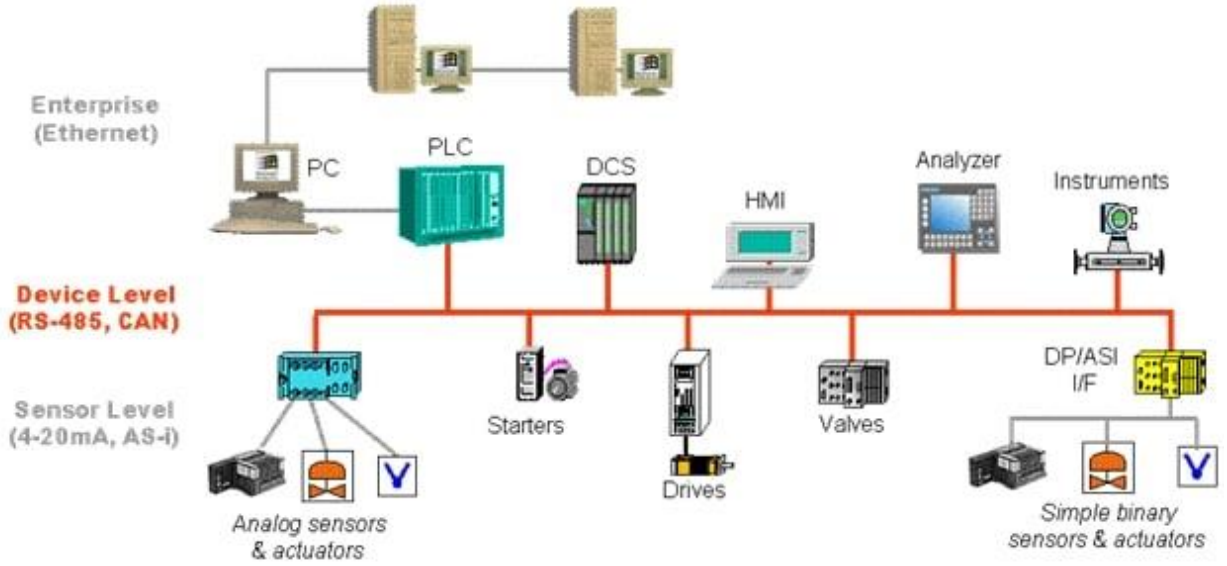
+



Where do problems come from?

When you connect industrial control systems together you get the same problems of cyber-security:

- Network
- People
- Computer systems

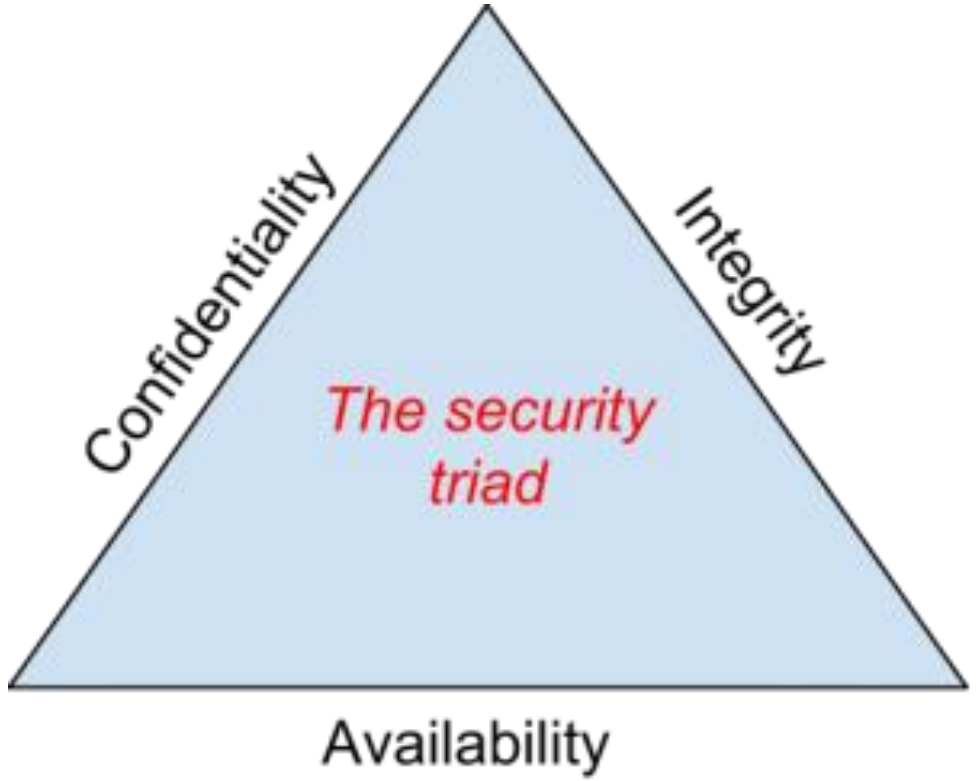


Some effects of intrusions

- Loss of availability and production
- Damages
- Personal injury
- Public health
- Publication of sensitive information
- Violation of regulatory and legal requirements
- Compromised image (reputation)
- …

Objectives of IT security (CIA)

- Confidentiality
  - set of rules that limits access to information
- Integrity
  - assurance that the information is trustworthy and accurate
- Availability
  - guarantee of reliable access to the information by authorized people



Objectives priorities

Pure IT

Industry

Data-centric architecture (Industry 4.0+)

Remote maintenance attacks and counter-measures

- Unsecured networks -> network segmentation, VPN
- Unsecured communications -> encrypted protocols
- Unauthorized access -> dedicated and limited accounts, no shared accounts, time-limited connections
- Phishing -> cybersecurity awareness

Attacks on equipment monitoring and counter-measures

- Denial of Service -> use a separate network, data diodes
- Unsecured communications -> encrypted protocols
- Altered data -> use data integrity
- Spoofing -> use data authentication and encryption

Attacks on Human-Machine Interface and counter-measures

- Unsecured communications -> encrypted protocols
- Altered data -> use data integrity
- Spoofing -> use data authentication and encryption
- Use a separate network (different from corporate network)

Attacks on agriculture machinery and counter-measures

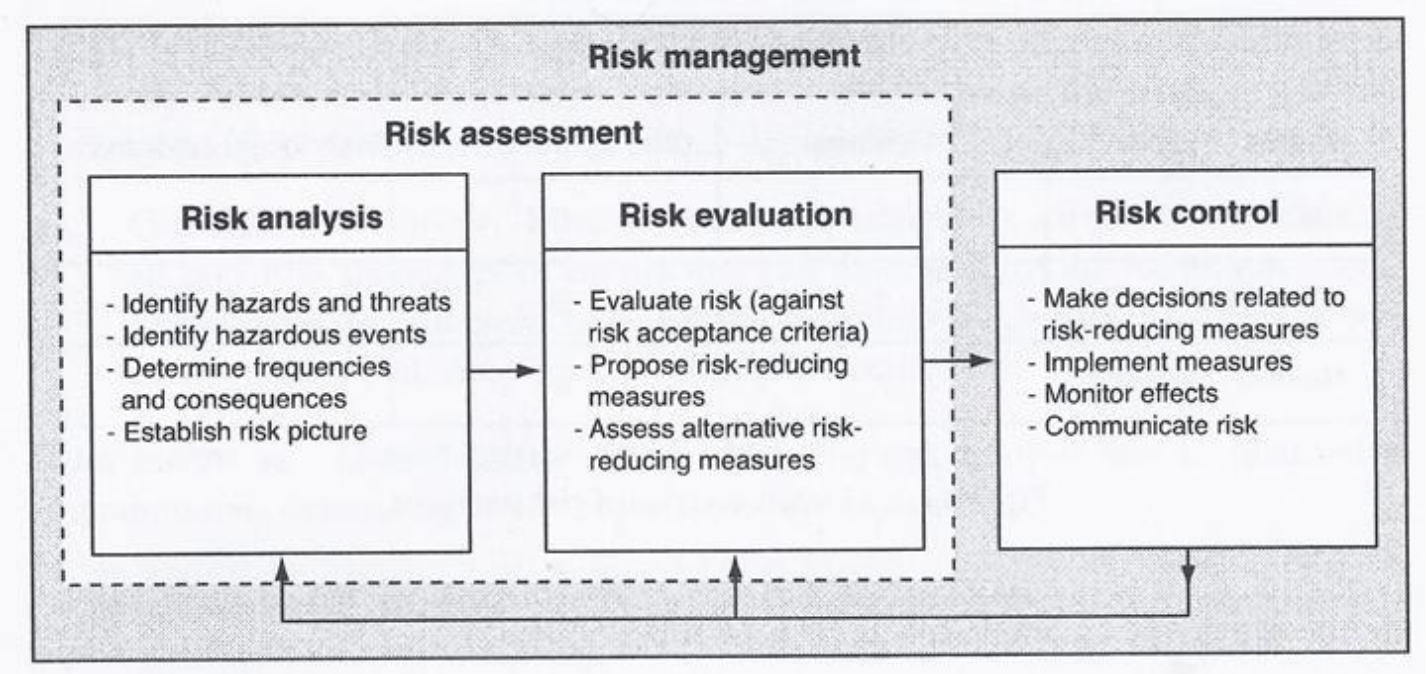
- ROPS: firmware upgrade -> signed firmware
- ROPS: altered data -> use data integrity
- ROPS: Spoofing -> use data authentication and encryption
- Disabled rural mobility: firmware upgrade -> signed firmware
- Disabled rural mobility: altered data on GUI -> use data integrity
- Disabled rural mobility: spoofing -> use data authentication and encryption

Risk identification

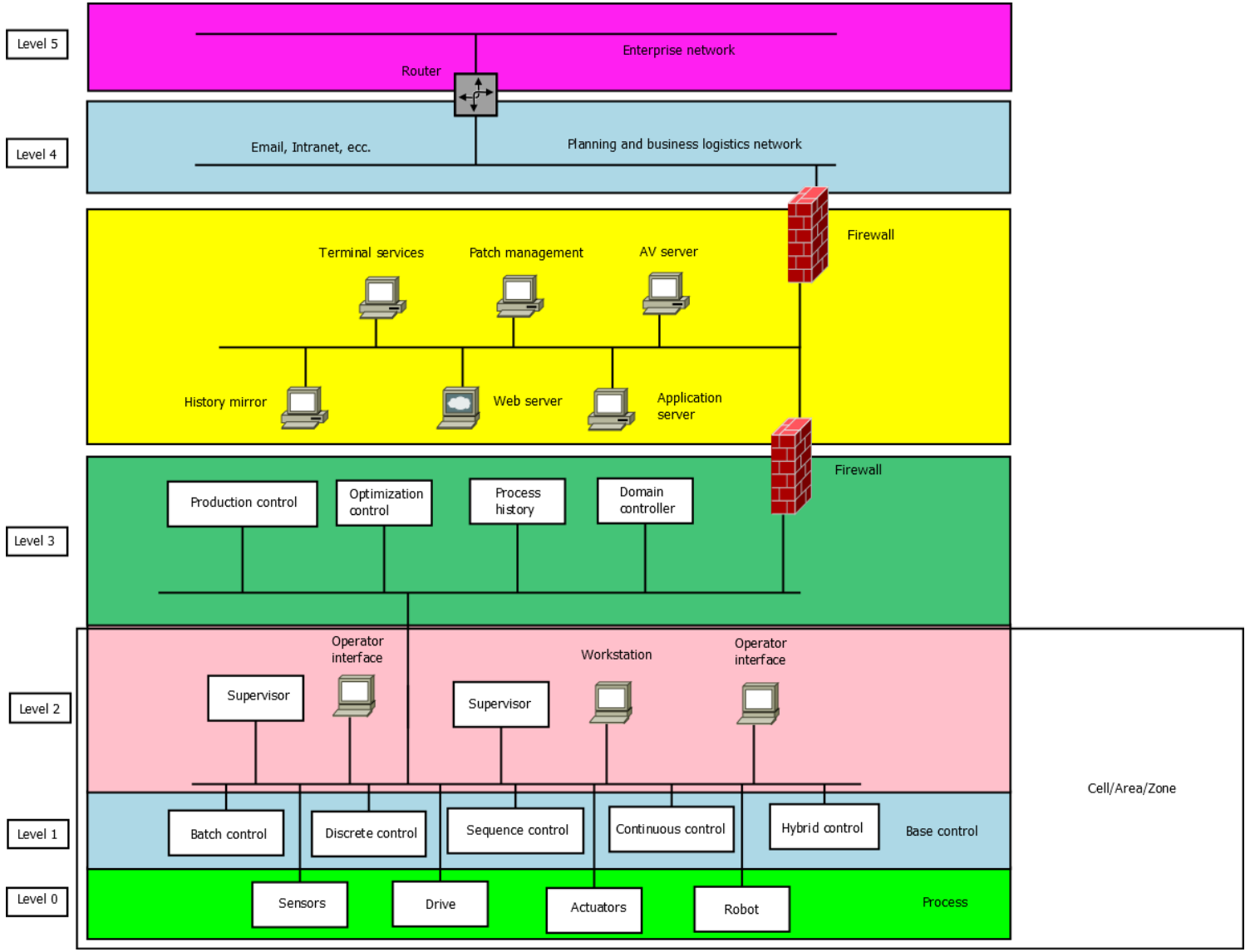
- Identify safety risk on every component
- Is this component connected to the network?
- Can this component be controlled remotely?
- Model production network (hidden indirect couplings)
- Relate components to each other
- And human factor?

Risk evaluation

- Is risk acceptable? (check against risk attitude)
- If not acceptable, you have to find some actions in order to reduce risks:
  - Mitigation (network partitions, IDS, IPS, Firewall, redundancy, …)
  - Avoidance (data diodes, isolation, …)
  - Insurance (if possible)



Zones and conduits

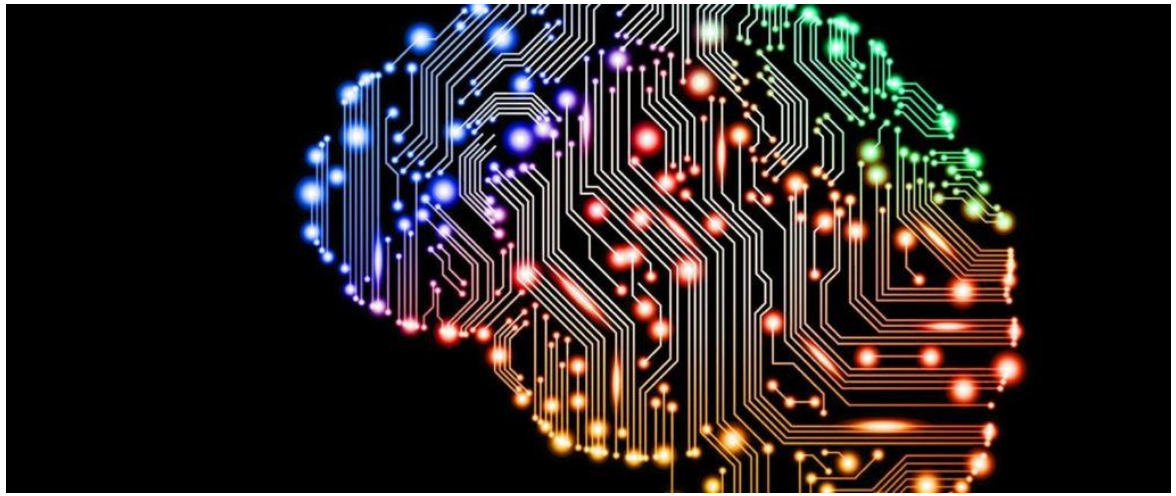


Zero Trust

- If the threat is inside your perimeter?
- Every equipment becomes potentially untrustable
- Principle: «Never trust, always verify»
- Use authentication for every connection
- Every equipment must be able to secure itself or must be included in a very small security perimeter

Uses of AI

- It is possible to use ChatGPT in order to create code or modules
- It is very easy to create a ransomware
- It is possible to use AI in order to attack
- It is possible to use AI in order to defend from attacks
- Examples:
  - Predicting passwords and PIN codes
  - Botnet coordination (no need for command and control servers)



Some advices…

- Firewall
  - Not a single system or a single appliance
  - A complex system to be built
- Software is a COMPLEX engineering product
  - Bugs
  - Use software EXPERTS!
- People
  - Security and safety awareness

ISSA-Section Machine and System Safety

Activities and Projects

Working Group „Digital Manufacturing“

"Digitalization is the business process of using digitization everywhere. The result of digitalization could lead to digital transformation."

Activities

- extend the classical risk assessment including security risks
- develop practical examples from industry => industry guides for integrating industrial security and occupational safety and health
- create fact sheets on special topics of industrial security
- develop webinars for engineers, employees, prevention and IT-experts

Website: https://www.safe-machines-at-work.org

IFA
Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung

AUVA

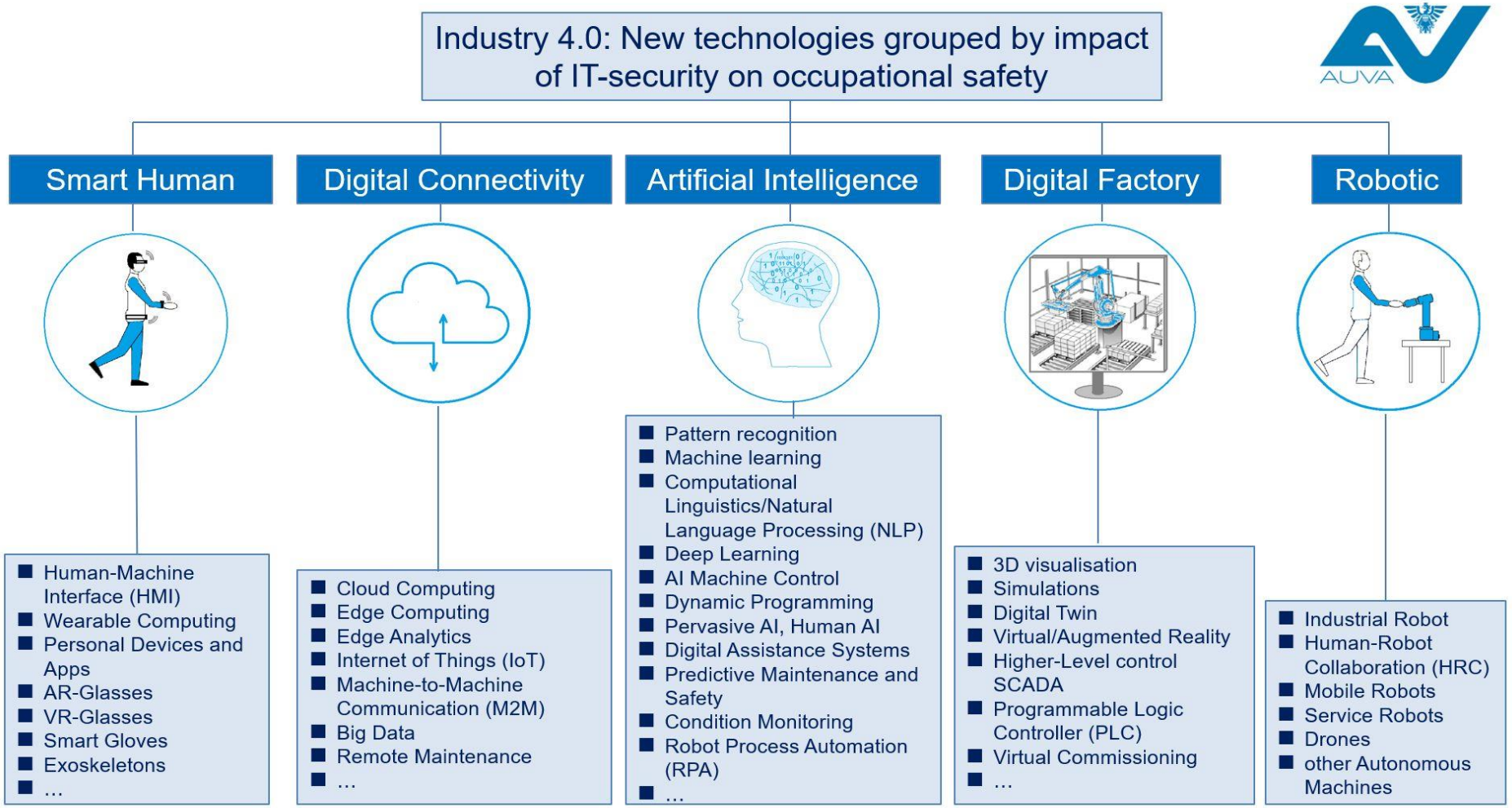
INAIL
ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO

UNIVERSITY of GREENWICH

VSB TECHNICAL UNIVERSITY OF OSTRAVA

BGN
Berufsgenossenschaft Nahrungsmittel und Gastgewerbe

Working Group „Digital Manufacturing“



THE END

Thank you very much for your attention