“To be safe you need to be secure”

Hans Hansson
2016-03-16

FIA-PiiA

[Funktions och intrångssäkerhet i automationsindustrin]

joint work with

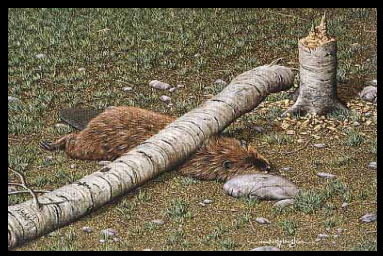
Kaj Hänninen, Henrik Thane & Mehrdad Saadatmand

Safety and security

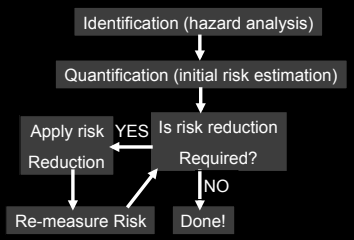
Safety
“Freedom from unacceptable risk”

Security
“The degree of resistance to harm”

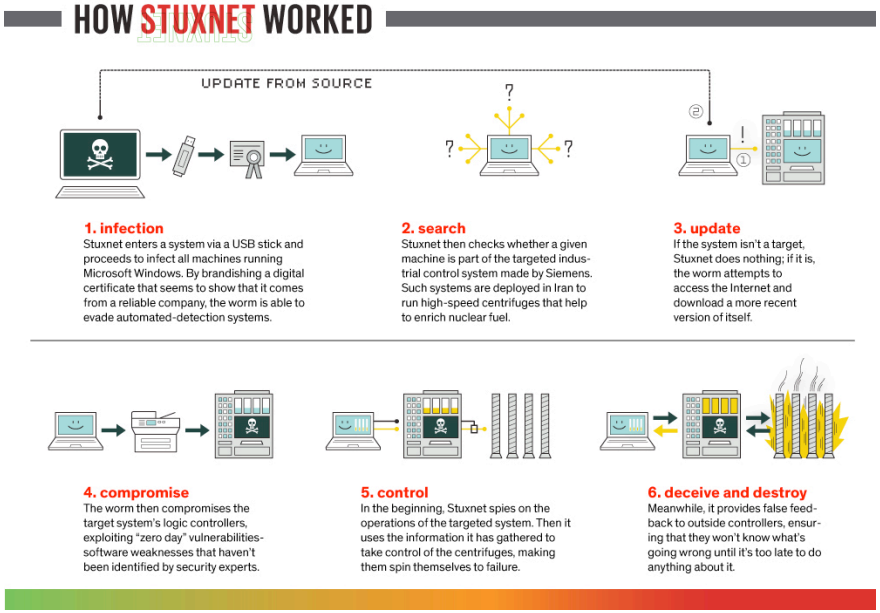
Safety is about avoiding accidents



Risks have to be managed



Risk Lifecycle



Organisation
SICS

Contact person:
Prof Hans Hansson

E-mail:
hansh@sics.se

Phone:
+46-21-103163

PiiA
PROCESS INDUSTRIAL IT AND AUTOMATION

Dagens industri

LÖRDAG DEN 2 MAJ

DIMENSION

BROTTSPLATS INTERNET

Cyberbrottslingarna blir alltmer sofistikerade, men it-säkerheten släpar efter. Säkerhetsexperterna sliter sitt hår medan hackarna angriper från allt fler håll.

Allowing external communication is an enabler for many useful and exciting functions and services, but is also potentially dangerous, as it opens up for a whole range of security threats.

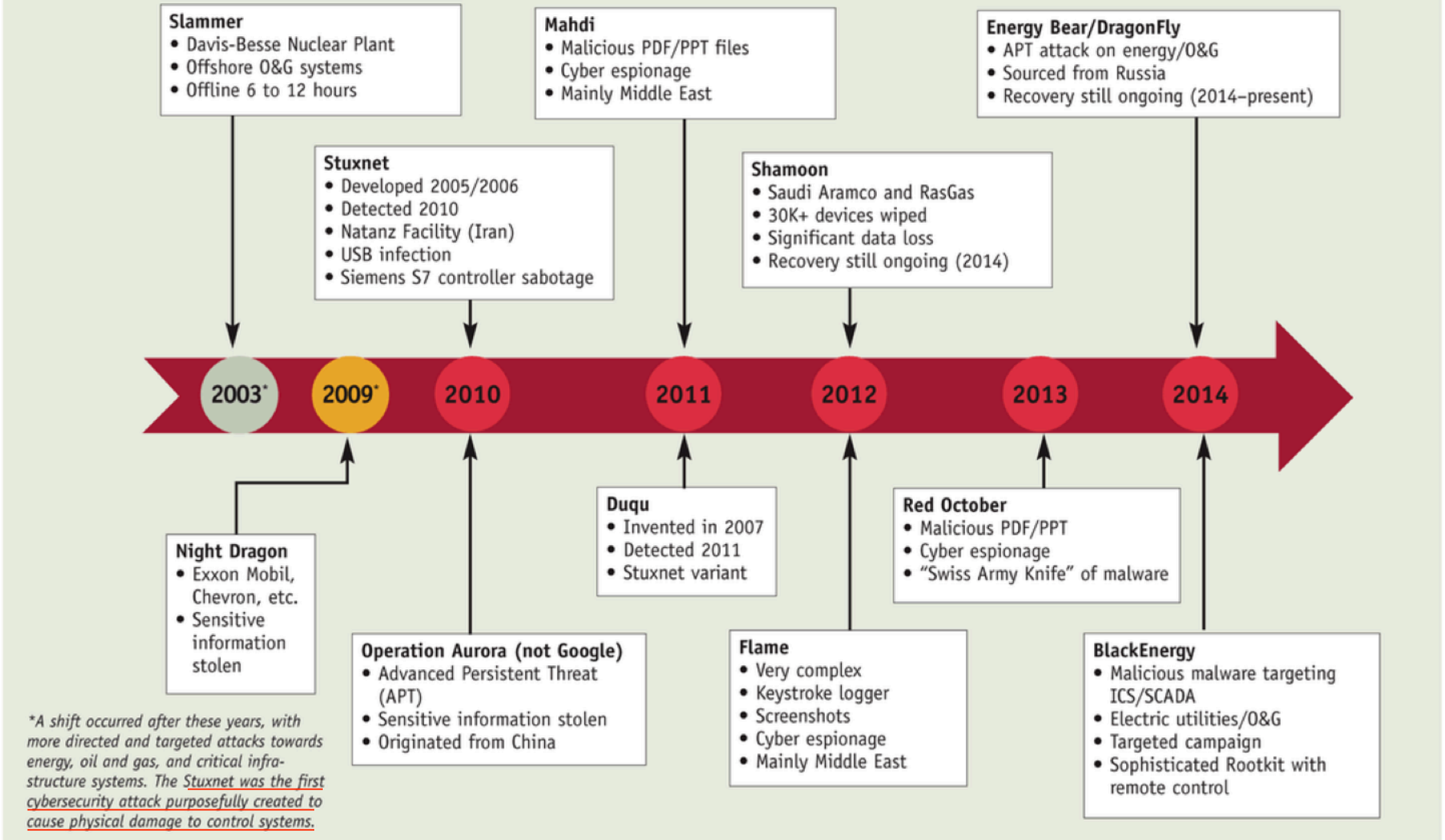
Other “solutions”

So you think you are safe?

- Stuxnet worm
- Hacked insulin pumps and drug infusion pumps
- Hacked water treatment facility
- Hacked ATMs
- Hacked Jeep
- … and more

Cyber attacks: Control systems are not immune

Figure 1. ICS cyberattack timeline by Red Tiger Security



*A shift occurred after these years, with more directed and targeted attacks towards energy, oil and gas, and critical infrastructure systems. The Stuxnet was the first cybersecurity attack purposefully created to cause physical damage to control systems.

http://www.valvemagazine-digital.com/valvemagazine/winter_2015?pg=15#pg15

So you think you are safe?

Examples

- Hacked Jeep (video)
- [https://www.youtube.com/watch?v=MK0SrxBC1xs]

Hacking is one of the problems

- Another (potentially worse) problem:
  - Current safety standards do not prescribe how to avoid security related risks

  $\Rightarrow$ Safety-certified systems may not be safe after all!

Safety vs. Security

Safety

- Protection against hazards

Functional safety

- Protection against failures causing hazards
- Absence of unacceptable risk due to hazards caused by **malfunctional** behavior of control system

Failure ➔ Hazard ➔ Accident

Security

- Protection against threats. Where people cause losses intentionally.

Functional security

- Protection against intentional failures (sabotage) causing accidents
- Absence of unacceptable risk due to hazards caused by **intentional failures**

Intentional Failure ➔ Hazard ➔ Accident

\+

Functional Safety with Security

- Protection against intentional and non intentional failures causing hazards that may lead to accidents.

Failure/Intentional Failure ➔ Hazard ➔ Accident

The FIA-PiiA project

"Funktions- och intrångssäkerhet för Automationsinustrin"

(Oct 2014 - Dec 2015)

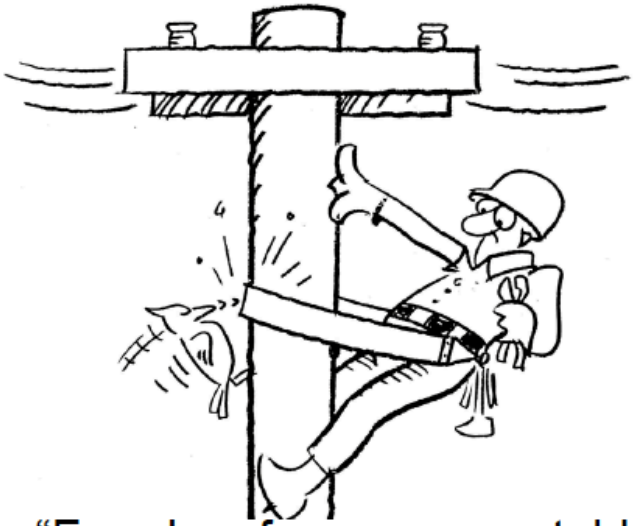
Strategic research project within the

Process-industrial IT and Automation (PiiA)

Vinnova funded Strategic Innovation pgm

FIA – the strategic project

- Strategic aims
  - Increasing awareness of safety and security within PiiA and involved companies
  - Strategic plans for safety and security within PiiA
  - Guidelines for efficient handling of safety and security



Safety “Freedom from unacceptable risk”

Security “The degree of resistance to harm”

What did we do?

- Talk to companies
- Read safety & security standards
- Studied a remote controlled vehicle case
  - Developed in a related research project (WROOM)

⇒ Problem identified!

\+ Remedy proposed

\+ Guidelines for companies developed

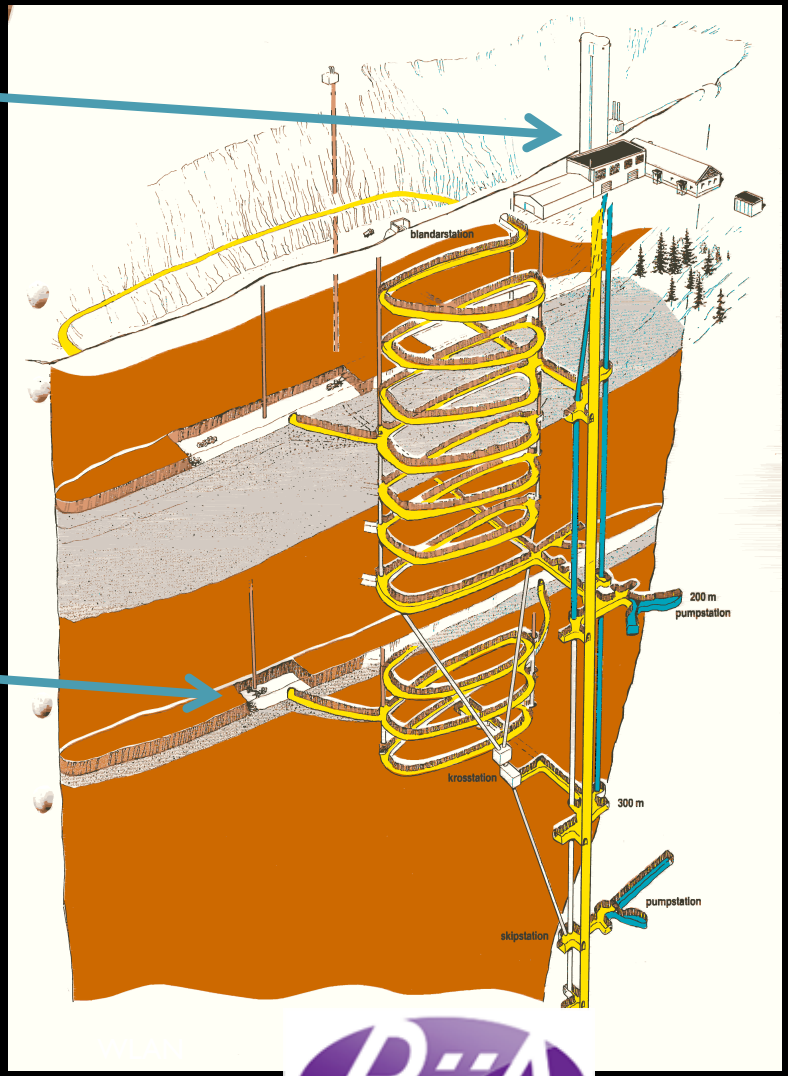
  - Yet not at a very detailed level (more research needed)

The remote controlled vehicle

Operator station

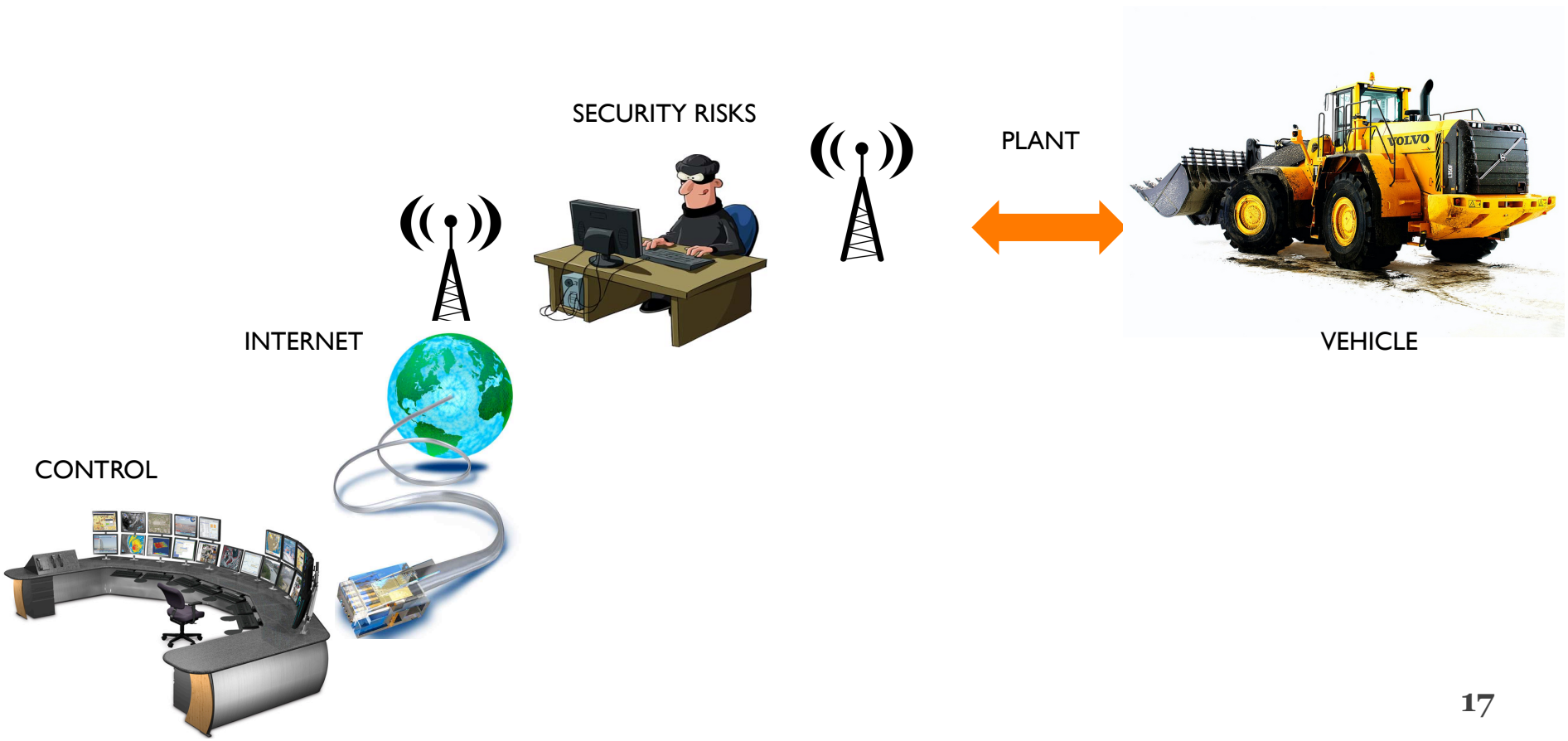
Wired/
Wireless
network

Excavation and loading place

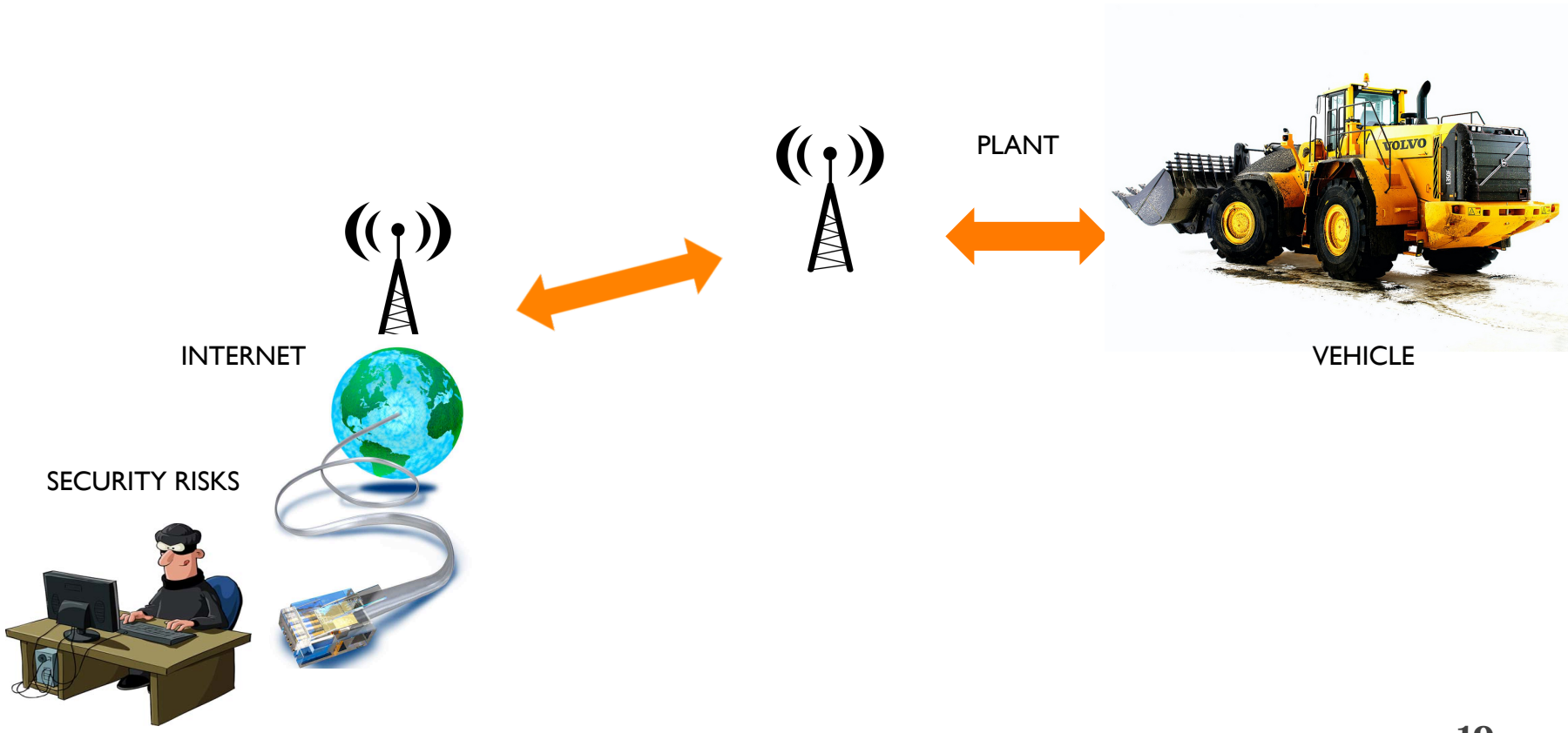


PiiA
PROCESS INDUSTRIAL IT AND AUTOMATION

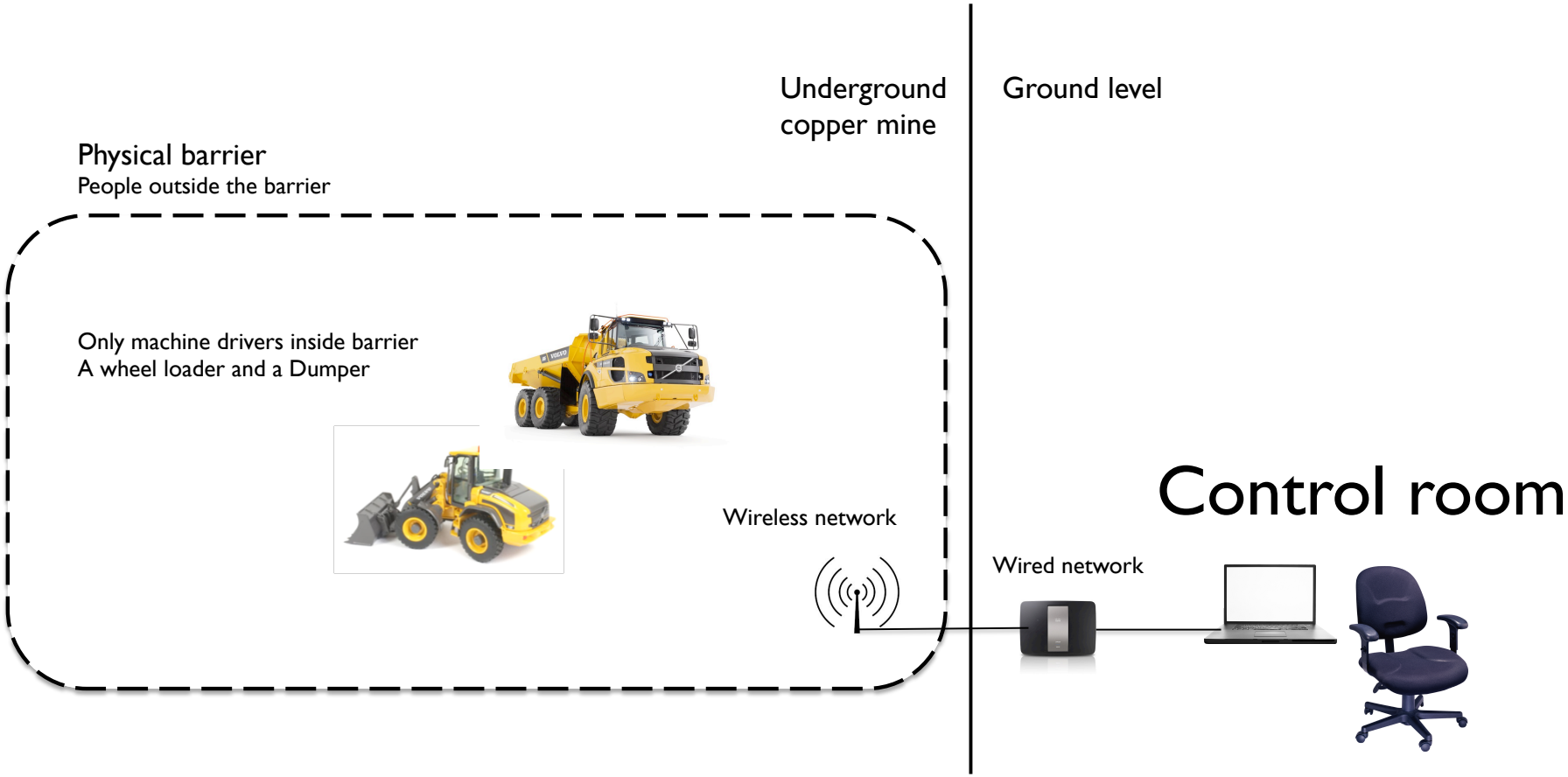
Security threats



Security threats



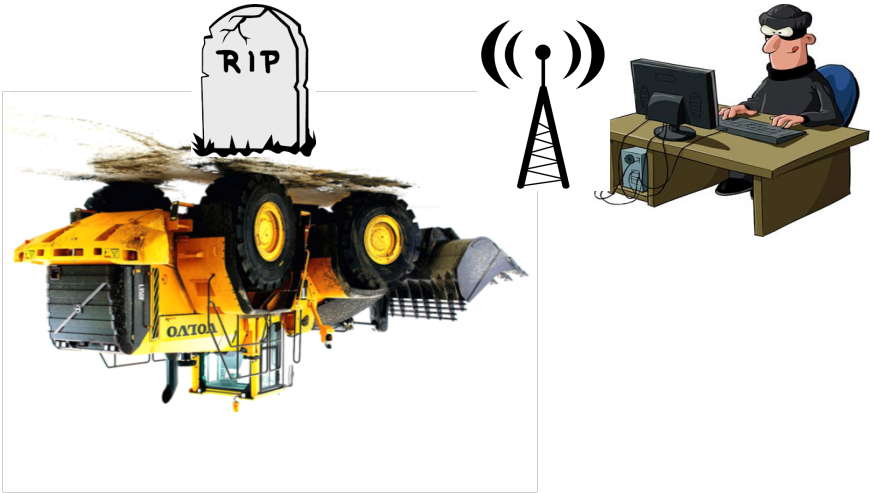
System definition



- **Wheel loader** can be **operated manually** (locally) by driver **or remotely** by operator in the control room
  - Remote operation due to: Gases from rock blasting and faster shifting of operators
- **Dumper** is **operated manually** (locally)

“Intruder” can cause accidents

- *Sample scenario:*
  1. *Driver is loading Dumper*
  2. *“Intruder” takes remote control of Wheel loader*
  3. *Wheel loader is driven into Dumper*
  4. *Drivers of Wheel loader and Dumper killed*
     - *2 deaths + equipment and mine damaged*



Wheel loader

Steering (preliminary hazard analysis)

Undetected hazard

Mode	Operation manual	Operation remote	Operation manual overtaken by remote
Hazard No.	1	2	3
Focus	Safety	Safety	Safety & Security
Failure	Steering capability lost	Steering capability lost	None
Intention	None	None	To crash
Situation	About to load dumper	About to load dumper	About to load dumper
Consequence	WL crashes into D 2 deaths	WL crashes into D 1 death	WL crashes into D 2 deaths

Hazards found using original scope of IEC62061

Considering security

- New hazards and additional ways in which a system might enter a hazardous state was revealed
- Could jeaopardize safety
  - E.g., remote overtake with vicious intent could lead to two deaths

Safety and security

- Standards are not flawed!
- But
  - The interdependencies of safety and security are not regulated or guided enough in normative safety standards

Safety standards are not really providing guidance how to consider security threats in the safety work

When will they do? (10 year revision periods)

Suggested remedy

- An extended safety approach
  - considering relevant aspects of security together with safety
- Must be compliant with current safety standards
  - Required for industrial acceptance

Our 

- Extend system definition
  - Intential misuse and sabotage
    - Bad guys and interfaces
- Extend hazard analysis to also consider security threats
- Extend risk classification and mitigation
  - Distinguish hazards discovered from
    - Safety perspectives, Security perspectives, S&S perspectives
  - Certification requires all mitigations to follow safety standards
    - Including security mitigations

Conclusions

- Security threats in modern systems/products could affect safety
- Safety standards are not prescribing solutions
- Proposed solution
  - Extend system definition, hazard analysis and mitigation to cover security related safety risks
- More research & standards development needed

Details at: https://www.sics.se/projects/fia

Questions or comments?

Thank you for your attention!

hans.hansson@mdh.se

https://www.sics.se/projects/fia