Herbert Dirnberger

True Cost and Real Benefits of IIoT Security

@bsidesvienna 07e1

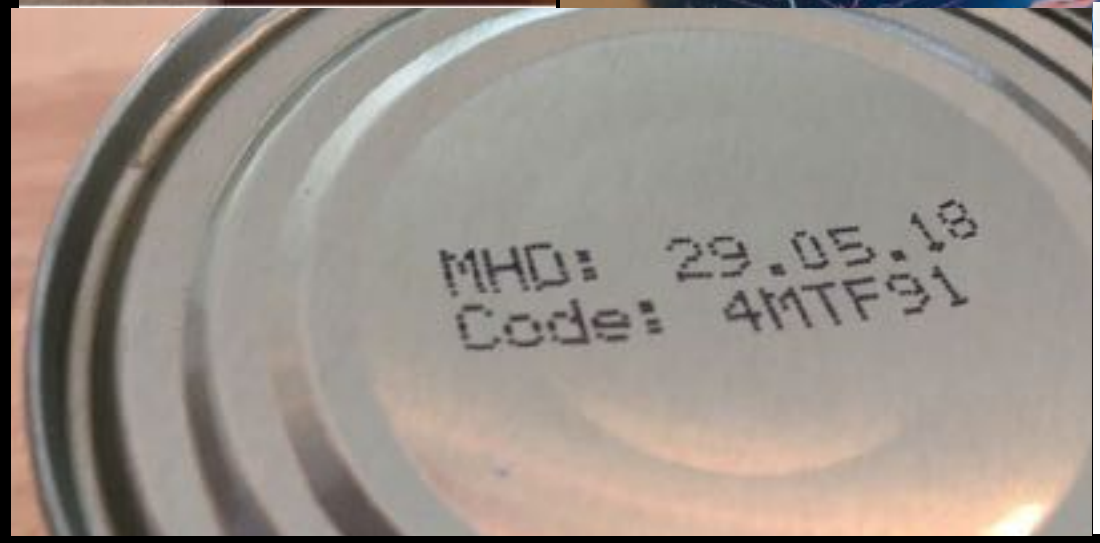
CYBER SECURITY AUSTRIA

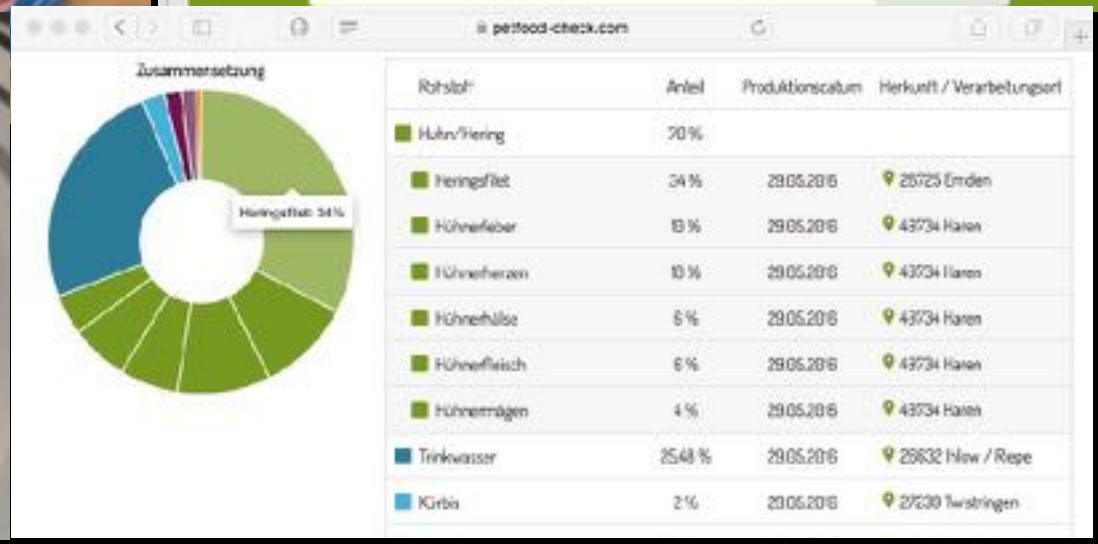
Verein zur Förderung der Sicherheit in Österreichs strategischer Infrastruktur

Agenda

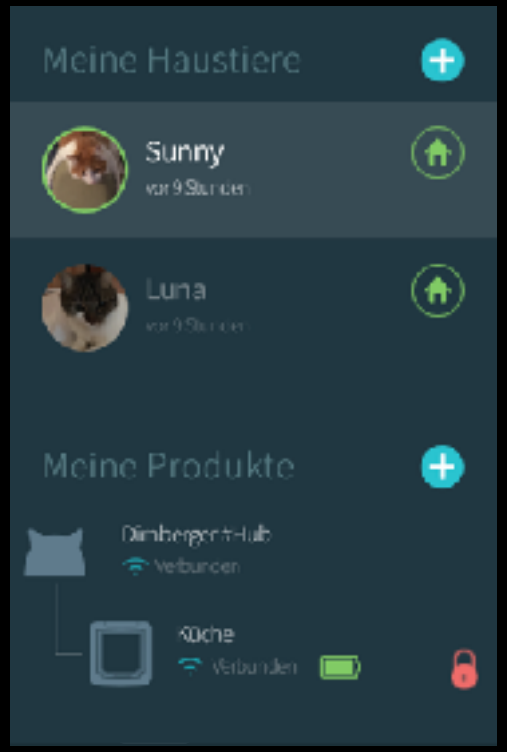
- Digital Darwinism
- Risks
- Scenario based IIoT Security
- Use Case
- Summary

Digitalization @home





Smart Cats @home



Mobile

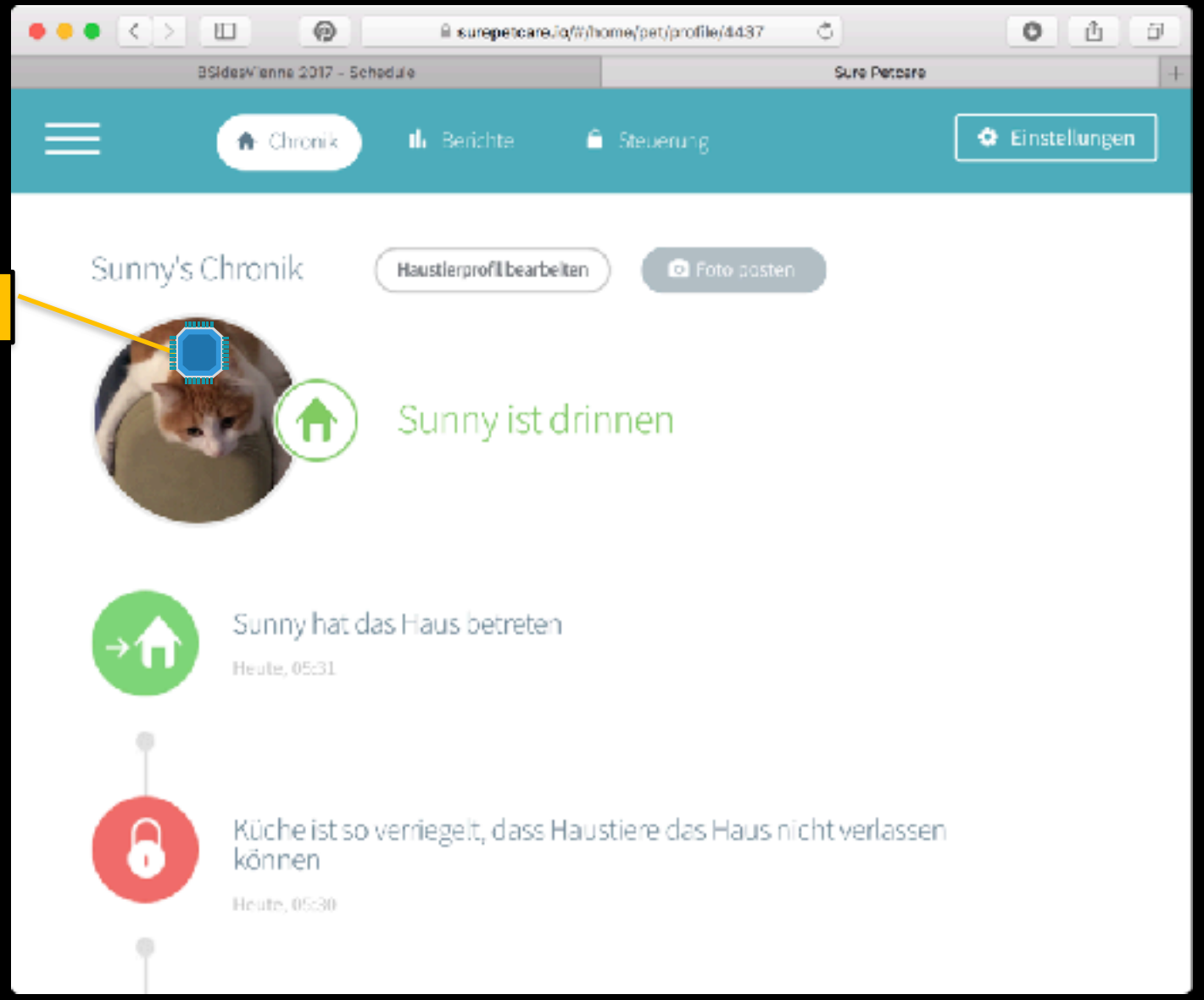
RFID-Reader

Smart Door

IoT Hub

Cloud

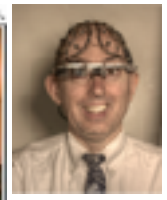
RFID



Smart Humans @world

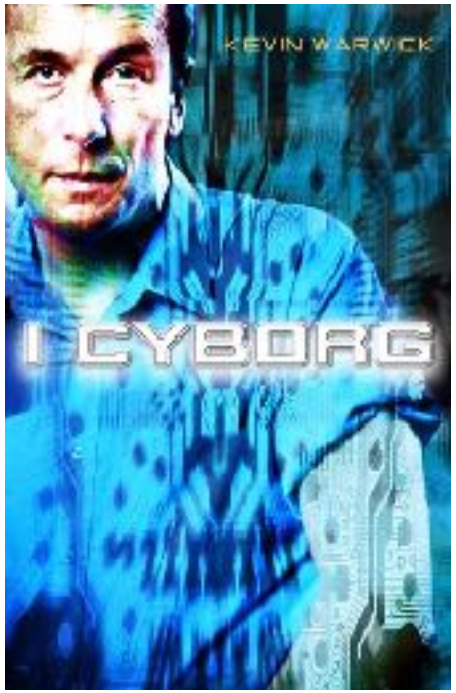
I CYBORG

Steve Mann



Google Glass

Kevin Marvick



http://www.csmonitor.com/Innovation/Latest-News-Wires/2012/0718/Cyborg-allegedly-attacked-over-camera-implants
http://www.zeit.de/digital/internet/2012-08/cyborg-neil-harbisson-biohacking-campus-party
http://dailynoise.blogspot.co.at/2011/10/what-is-cyborg-anthropology.html
http://en.wikipedia.org/wiki/Steve_Mann
http://www.kevinwarwick.com/ICyborg.htm

b0111 1110 0001: 0.15

7 E 1

1024 + 512 + 256 +128+ 64+32 + 1

Technical Progress of Industry

200 years digital, 70 years computer, 6 years Industrie 4.0/IIoT

Loom with punched cards

Markus Schweiß [GFDL (http://www.gnu.org/copyleft/fdl.html) or CC-BY-SA-3.0 (http://creativecommons.org/licenses/by-sa/3.0/)], via Wikimedia Commons

How do we call this kind of nerds and geeks in the industry?

Industrial Internet of Things and Services

Industrie 4.0

Apollo 11

Zuse Z3 1805

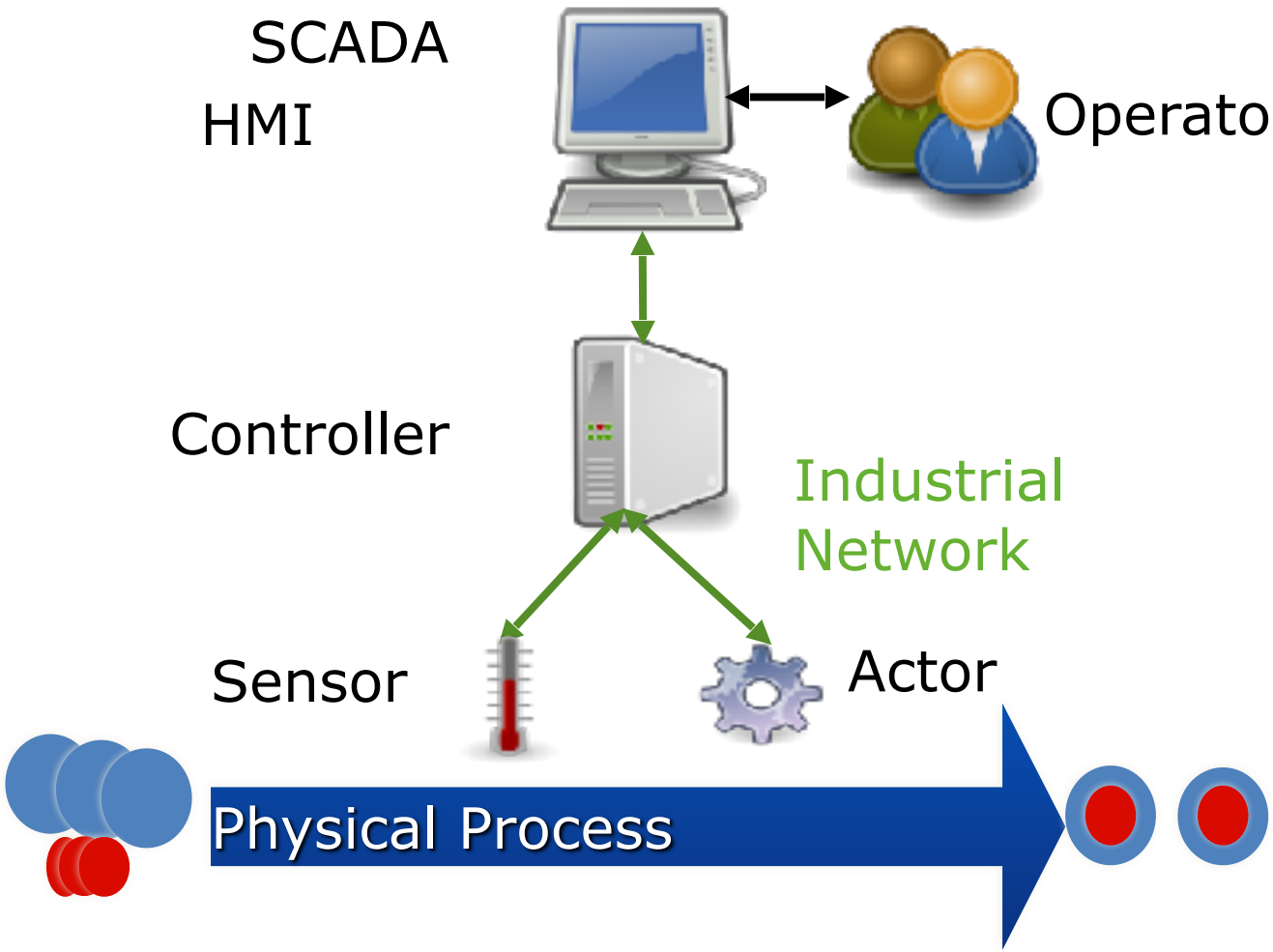
PLC 1941

Robot 1969

PC

Internet mobil Cloud IIoT 2011 2017

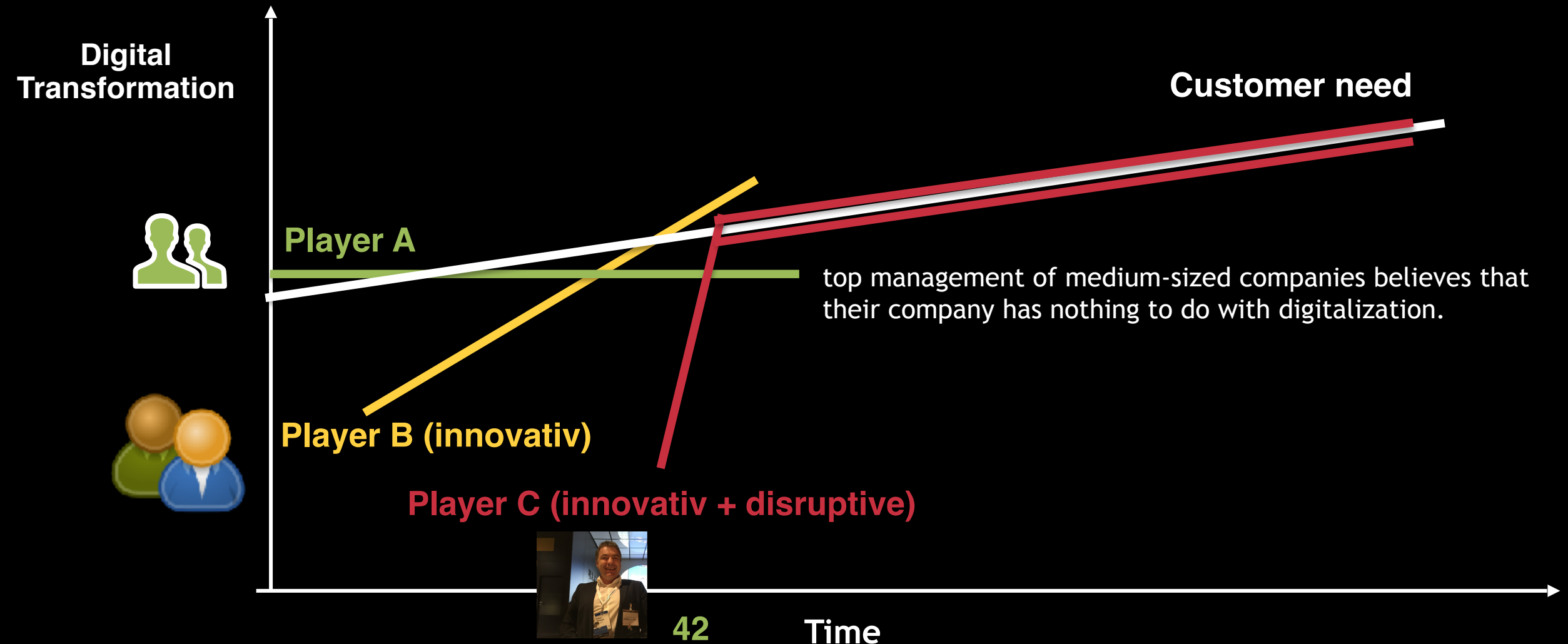
Industrial Automation in 2 min



Industrial Actors

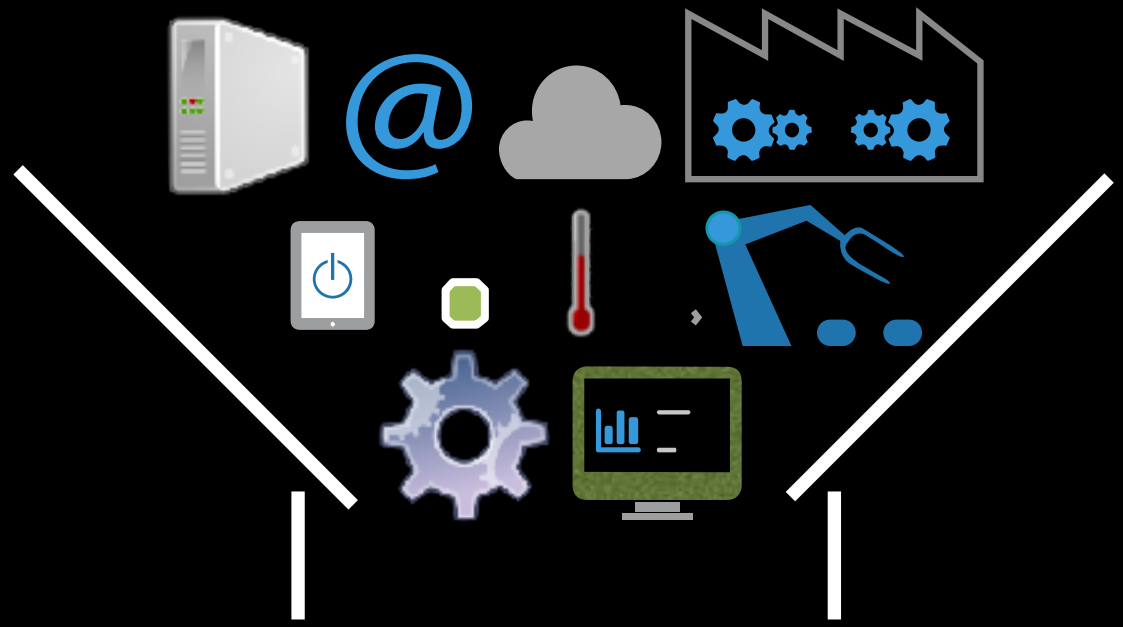
Robots **Power Plants** **…**

Disruption and Digital Darwinism



The new form of creative destruction "Disruptive self-attack!"
Let us ask ourselves, what is the business model that would destroy us ?!

Don’t think in Camps and Silos!



physical process

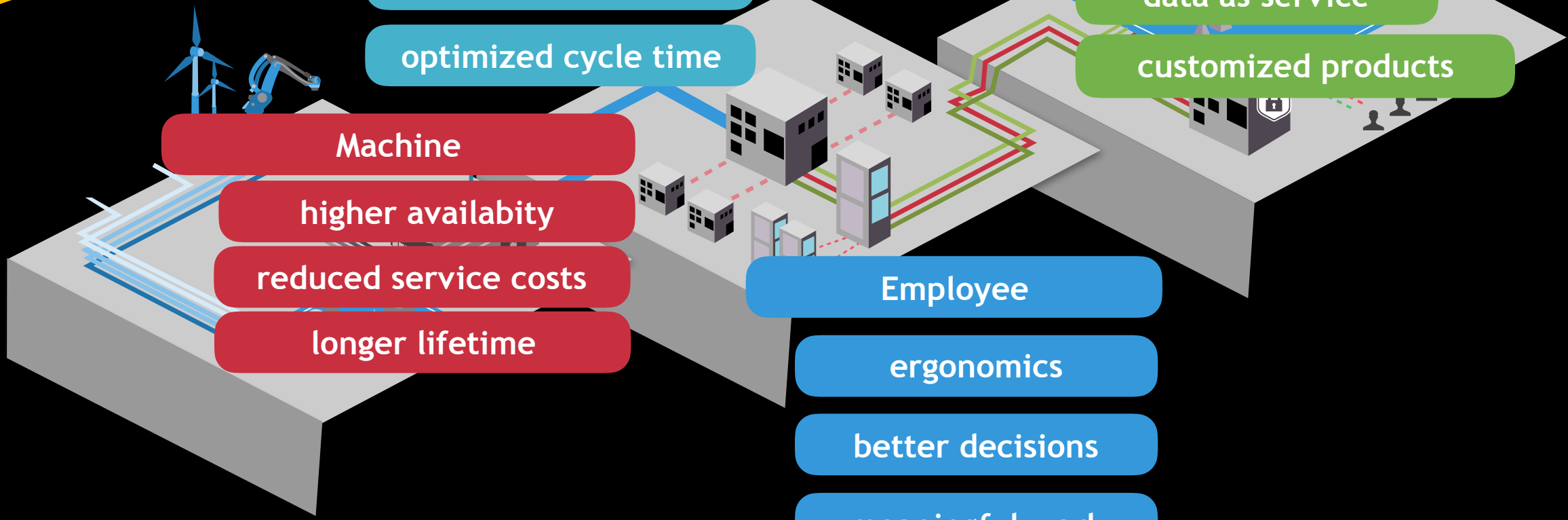
business process

services

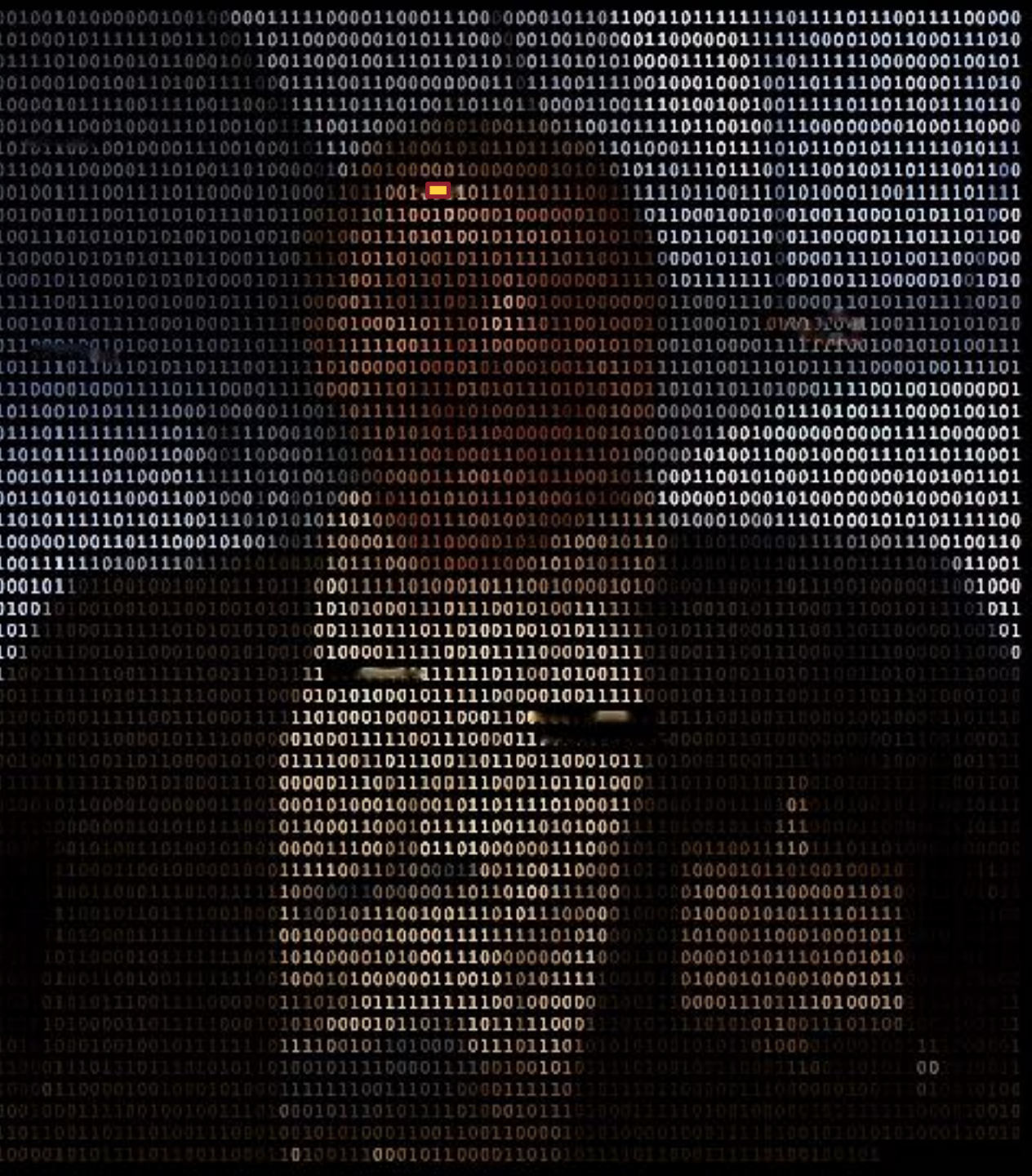
IIoT

(some) IIoT Benefits

Slide to flip very fast over!!



- Process
  - reduced costs
  - better quality
  - optimized cycle time
- Machine
  - higher availabity
  - reduced service costs
  - longer lifetime
- Employee
  - ergonomics
  - better decisions
  - meaningful work
- Business Model
  - pay per use
  - contracting
  - data as service
  - customized products



web access with cross site scripting

open system found in shodan.io

Business Risks
Risk Management

exposed wireless networks

exposed physical access

no backups

The IoT is extremely insecure and not patchable

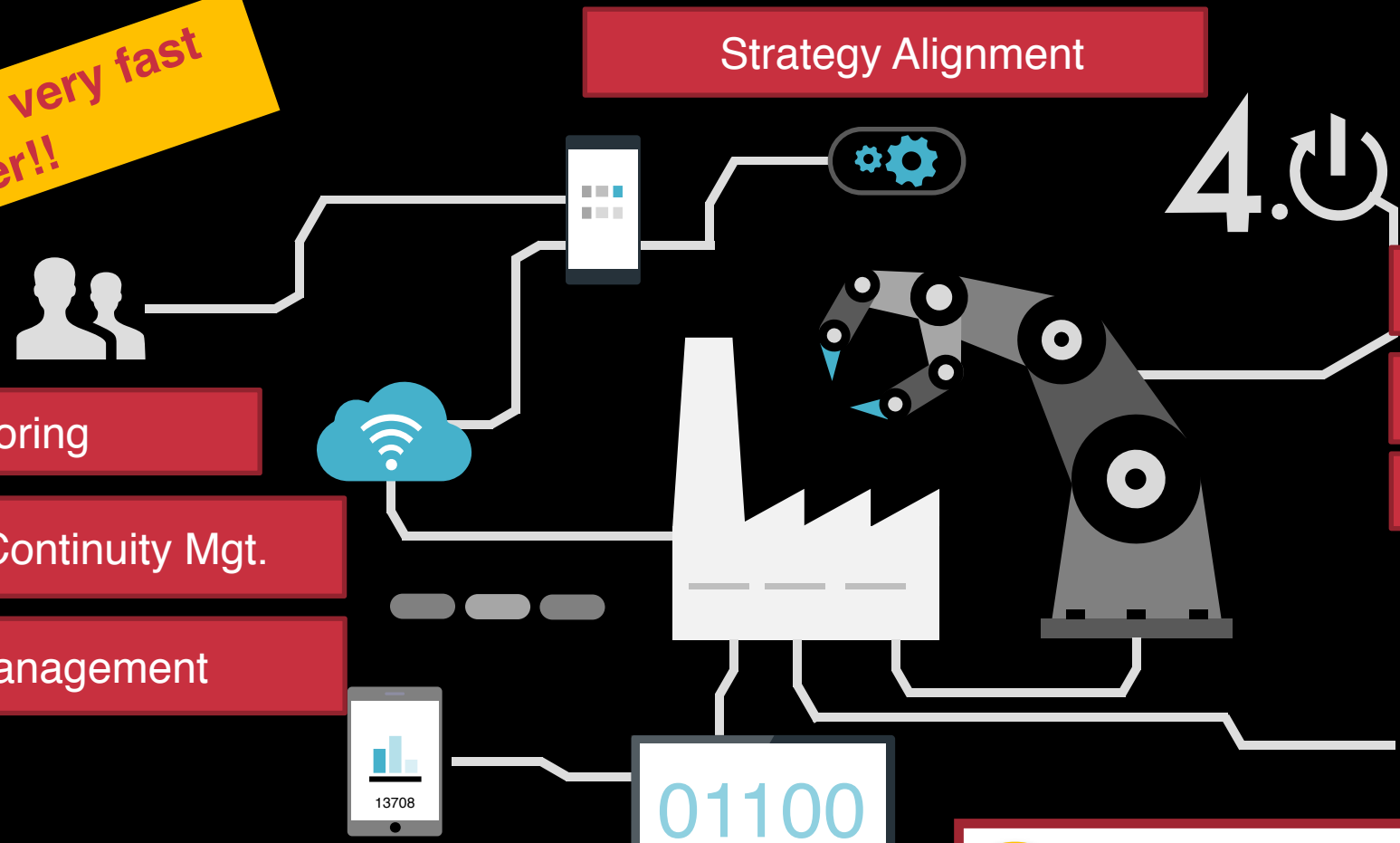
no secure passwords

Bruce Schneier

Backup

Traditional Risk Management Program

Slide to flip very fast over!!



Strategy Alignment

Risk Monitoring

Business Continuity Mgt.

Incident Management

Asset Management

Business Impact Analysis

Risk Management

Threat Analysis

Vuln Analysis

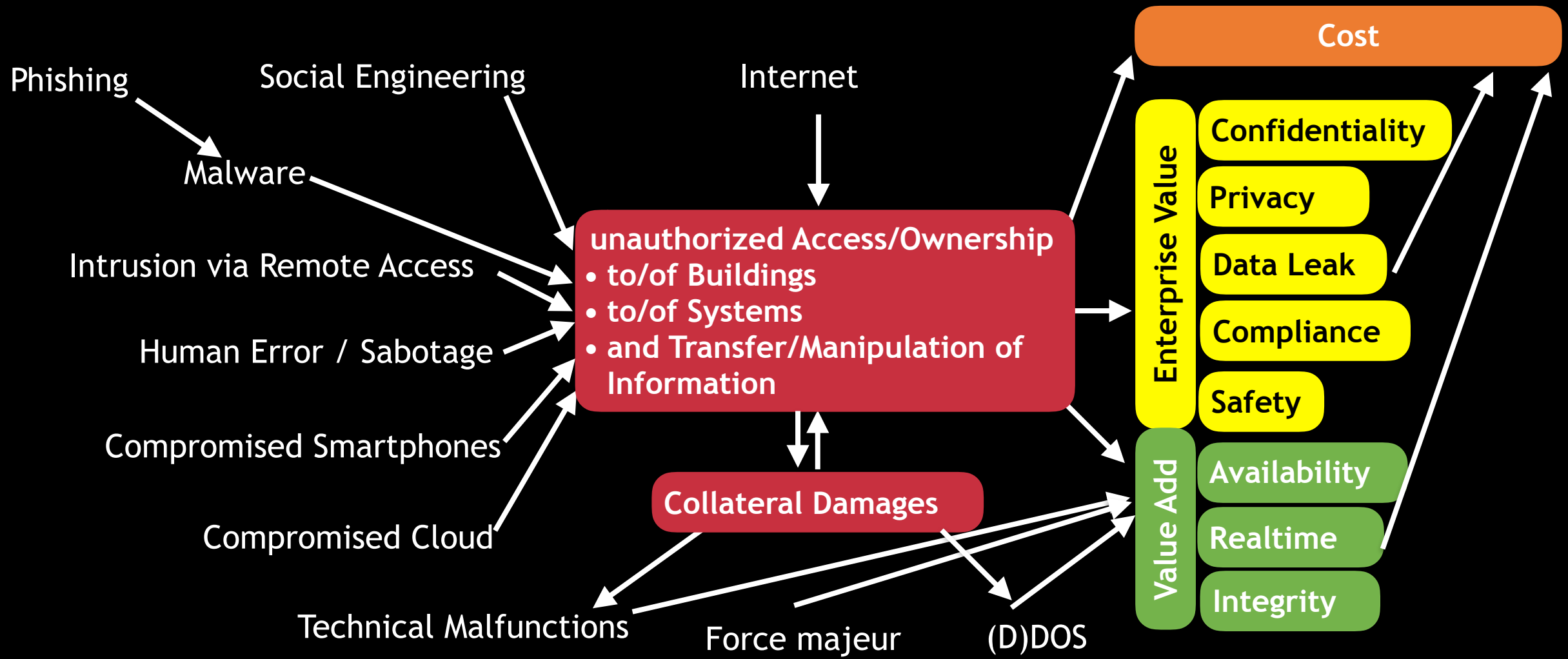
Controls

€ Program ROI

Risk Mitigation

Typical Scope: 1 year - balancing cost and risk

BSI Top 10 Threats to IIoT/ICS Systems



BSI: Top 10 Threats and Countermeasure 2016

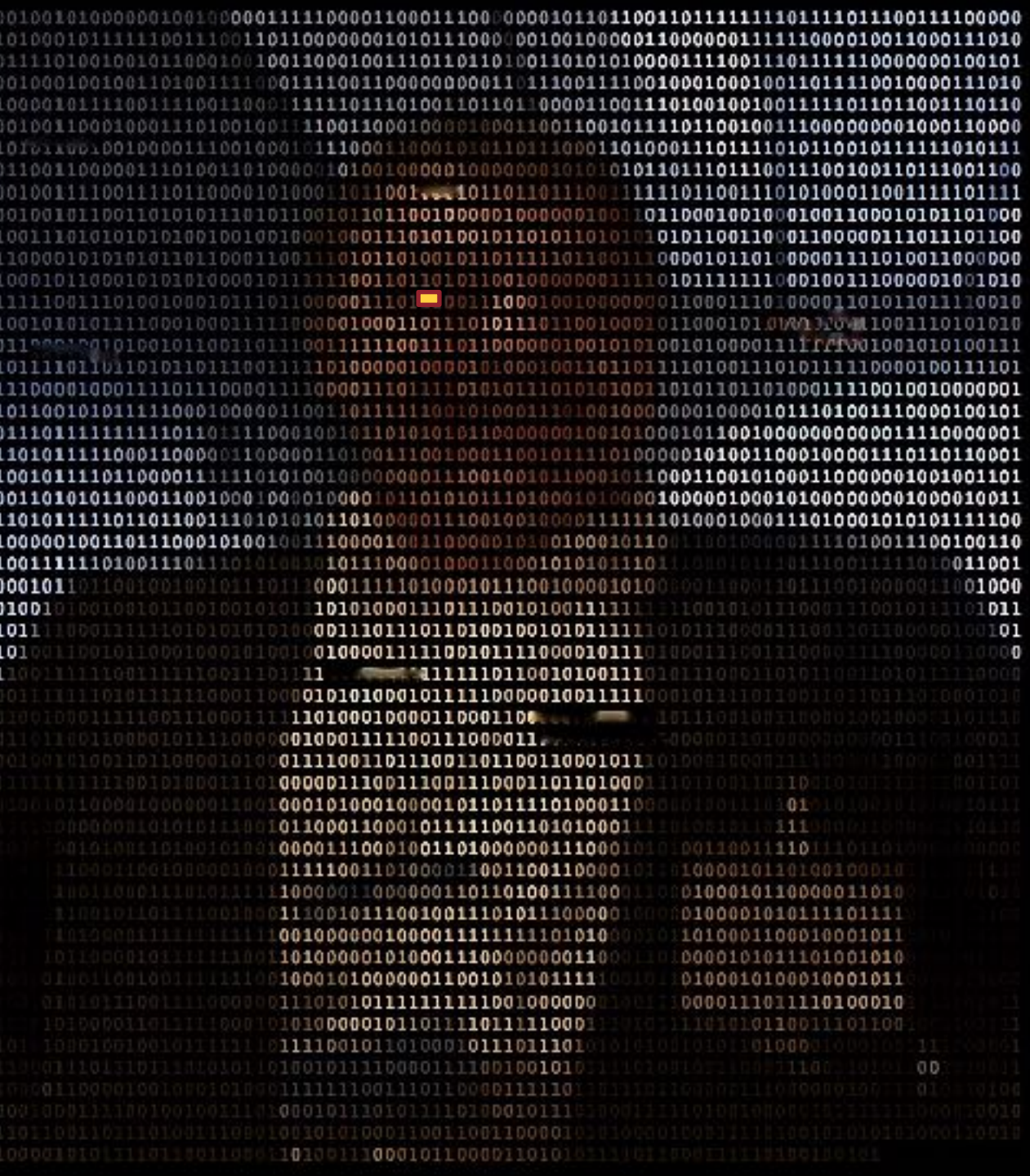
Backup

Controls for IIoT Security

Restricted Access to Internet, VPN, Industrial Firewalls (micro Segmentation) are the basics.

	Fences, Guards	SLA, NDA Vendor Management	restricted Internet for Control Network	Need to Know Passwords, Files, DB	Awareness Training	Anti Malware Sandbox, Whitelists	Policies, Procedures Business Continuity	Scan, Log, IDS Monitoring, Audits	Hardening	Security Updates Patches	VPN, 2 Faktor Encryption	DMZ, Network Segments, Firewall	Backup, Diversity Redundancy	Secure Appstores MDM
Social Engineering / Phisihing	+	+	+	+	+	+	+	+	+	+				
Human Error / Sabotage			+	+	+	+	+	+	+	+		+		
Malware			+	+	+	+	+	+	+	+		+		
Malfunctions / Force Majeur		+					+	+					+	
Compromised Cloud		+					+	+			+			
Intrusion via Remote Access		+					+	+			+	+		
Compromised Smartphones							+	+	+		+			+
DDOS								+	+				+	

BSI: Top 10 Threats and Countermeasure 2016



Use Case: IIoT in manufacturing

Focus: Business Interruption and Cyber Security

- IT Security
- Information Security
- ICS Security
- IIOT Security
- Physical Security

IIoT Security is about DEFENSE and ENABLER

Industrial Users

Processes

Ressources

Safety &

C

Costs

VA

Value Add

Service

Maintenance

- IT Security
- Information Security
- Physical Security
- ICS/IOT Security
- Cyber Security

Business Continuity Management

Incident Management

Risk Management

Attacks
(Scan, Tests, Enumeration, … Exploits)

Unauthorised use

Human Misbehaviour

Sabotage, Theft, Fraud

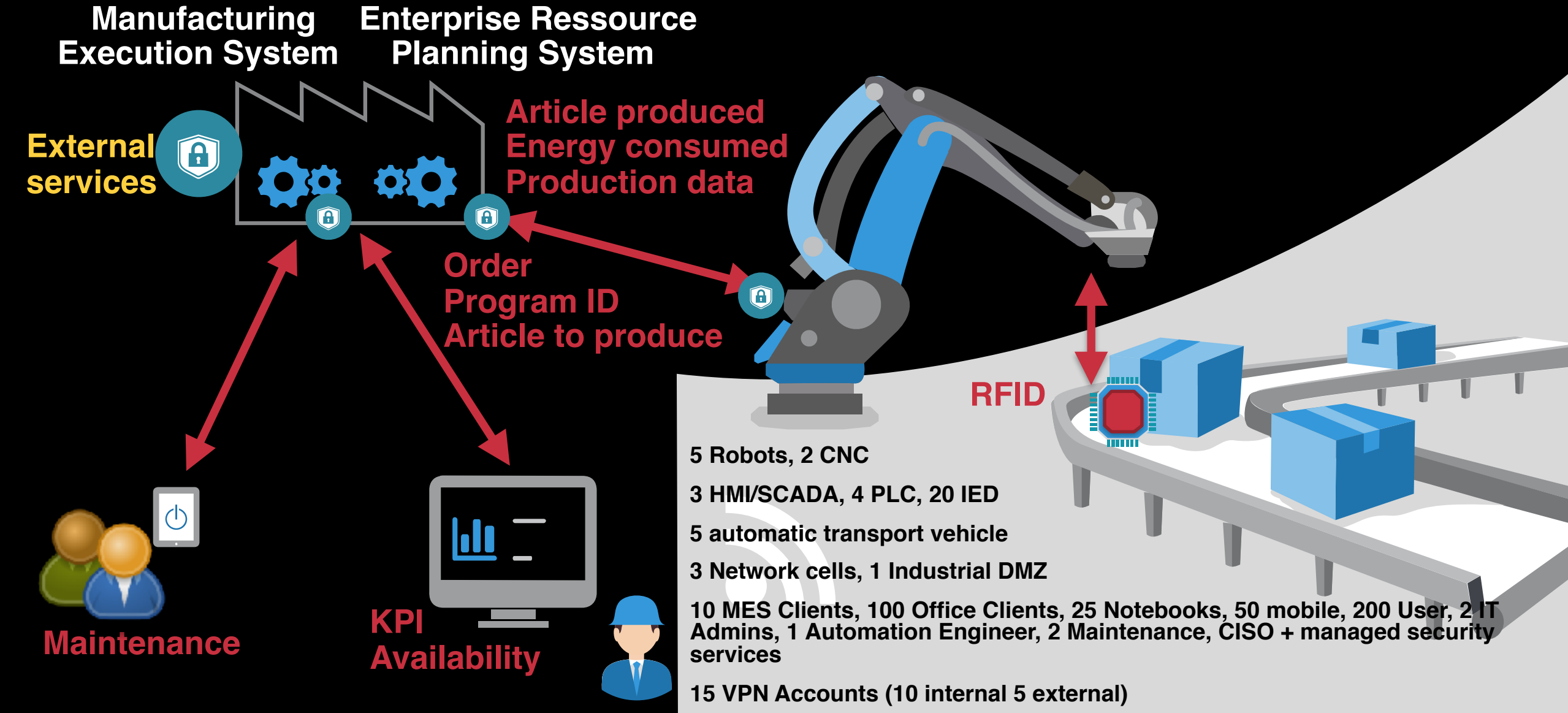
Malicious Code

Technical Misbehaviour
(uncontrolled Patches, Software Bugs, Protocol Error)

Force majeure

Use Case: IIoT in manufacturing

Industrial user, 200 employees, 50 m € sales/year, 1 m € profit/year



What we will expect, because it happened last years

Industrial user, 200 employees, 50 m € sales/year, 1 m € profit/year

20 hardware malfunctions	20 malware / Crypto	45 software defects / updates
4 orders in Junk	40 locked User (10 leaks)	25 network outage > 1d
1 data breach > 15000 EUR		
20 lost - 5 stolen devices		
10 power breakdown		
10 lost encryption keys		
20 problems with VPN		

Comparing Costs and Value Add

Industrial user, 200 employees, 50 m € sales/year, 1 m € profit/year

	Costs		in TSD €
20	CAPEX	Industrial FWs, VPN Router incl. Config and Licenses	8
		Enterprise FW inkl. Config and Licenses	12
100	OPEX	Managed prof. ICS Security Services	24
		Managed basic ICS Security Services	6
		Managed Client Security Services	60
		Managed mobile Security Services	10
		CISO as a Service	Incl.

Damage Costs	in TSD €
Hardware/Software Malfunctions	40
Power Breakdown/Network Outage	10
Unrealized Orders	10
Data Breach	15
Stolen Devices	5
Crypto/Ransomware	15
Mini Problems	5

100

Scope: 5 years

Value add	in TSD €
Value Add	250
CAPEX	-20
OPEX	-100
Damage Costs	-100
Real Benefit Value add > Costs	+30

Direct „measurable" Value Add ~ 0.1% of sales/year

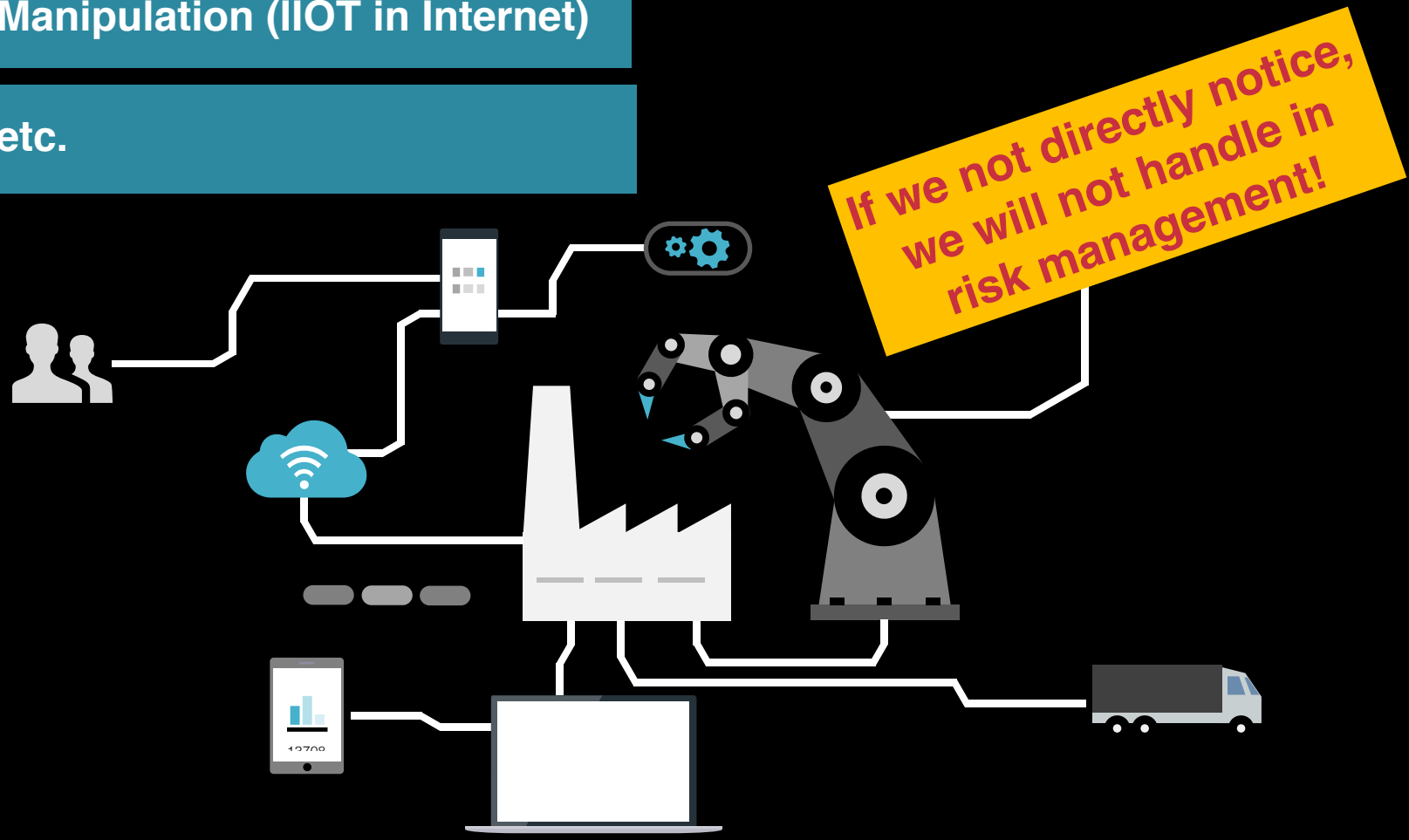
Realtime | Availability | Integrity

Privacy | Safety | Compliance | no Data Leak | Confidentiality

What we will not see, but it will happen.

Industrial user, 200 employees, 50 m € sales/year, 1 m € profit/year

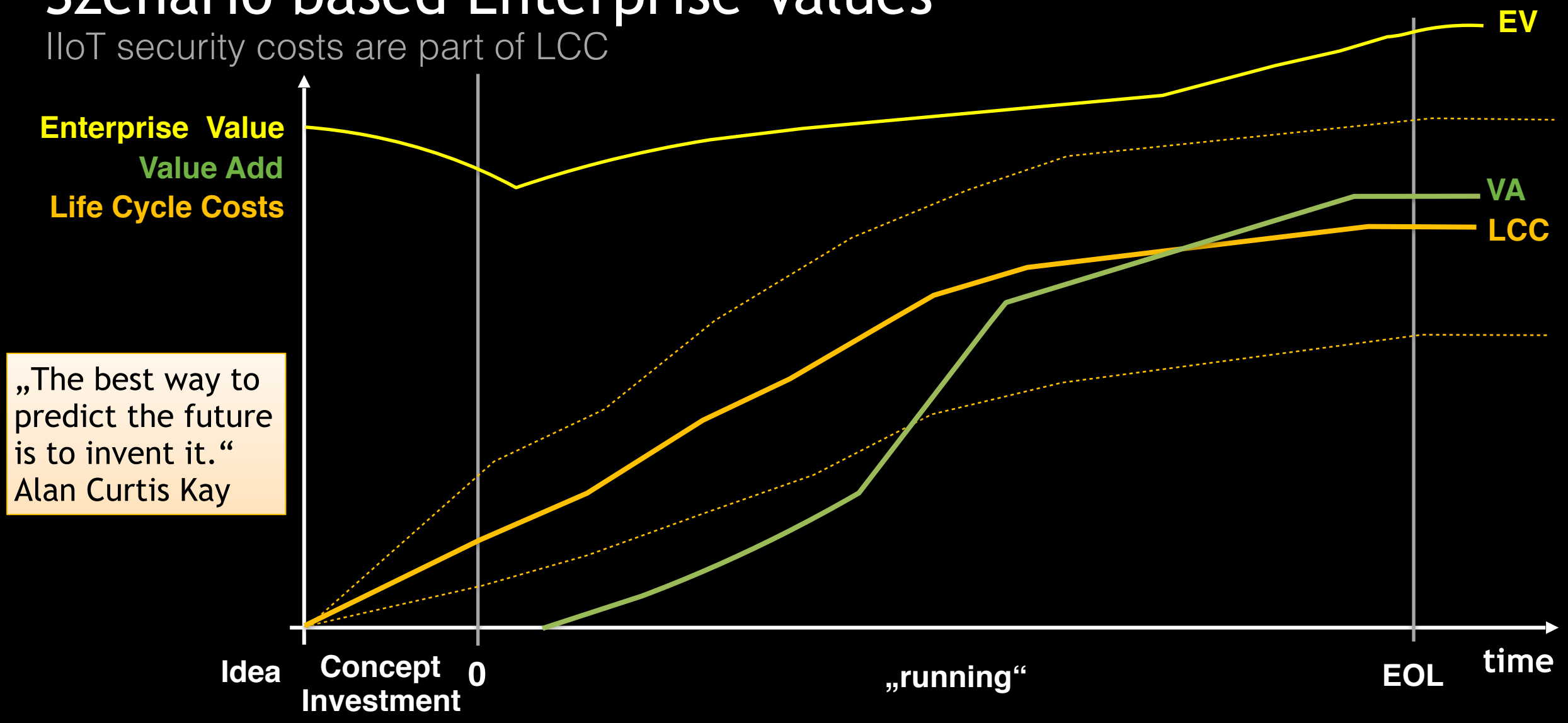
- Social Engineering
- Phishing (Accounts)
- Industrial Spionage
- Sabotage (Availability)
- Manipulation (Integrity)
- DDOS (Availability)
- Friendly Malware
- Manipulation (IIOT in Internet)
- etc.



BSI: Top 10 Threats and Countermeasure 2016

Szenario based Enterprise Values

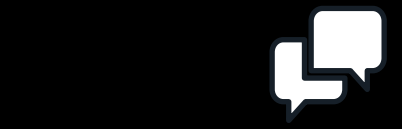
IIoT security costs are part of LCC



„The best way to predict the future is to invent it.“
Alan Curtis Kay

LCC, OPEX, service and security costs are mostly defined in the concept and investment.

The Reality about Industrial Security

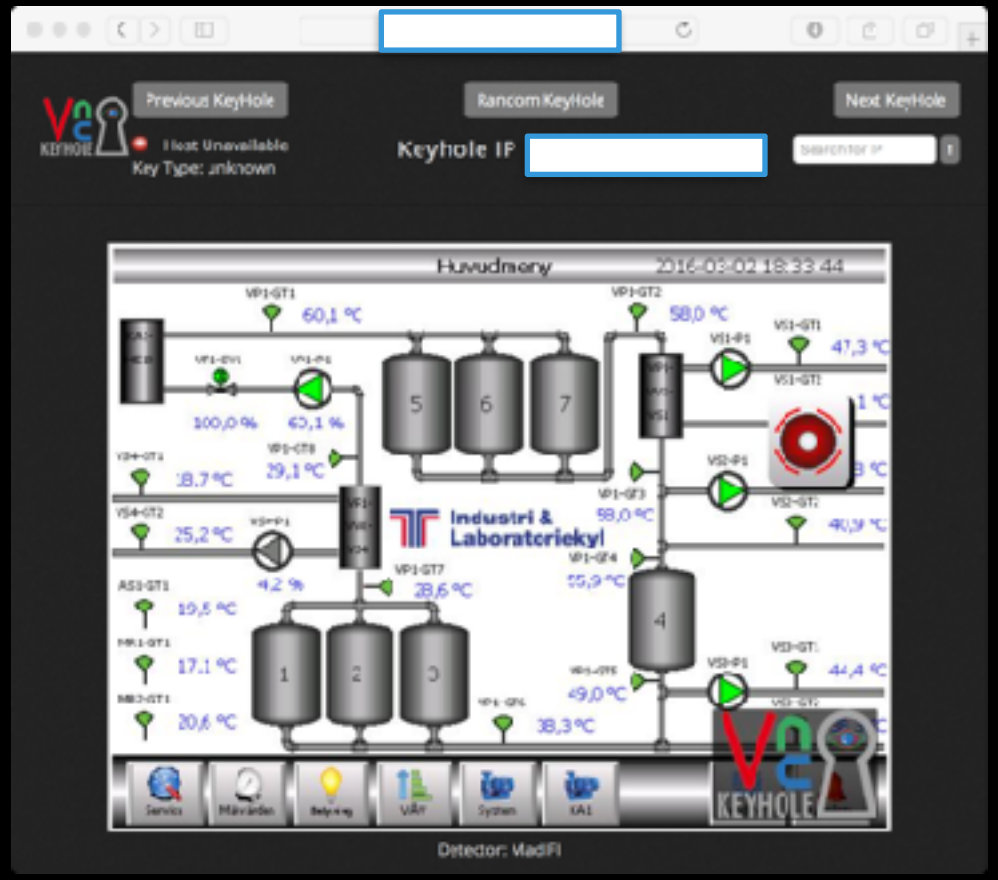


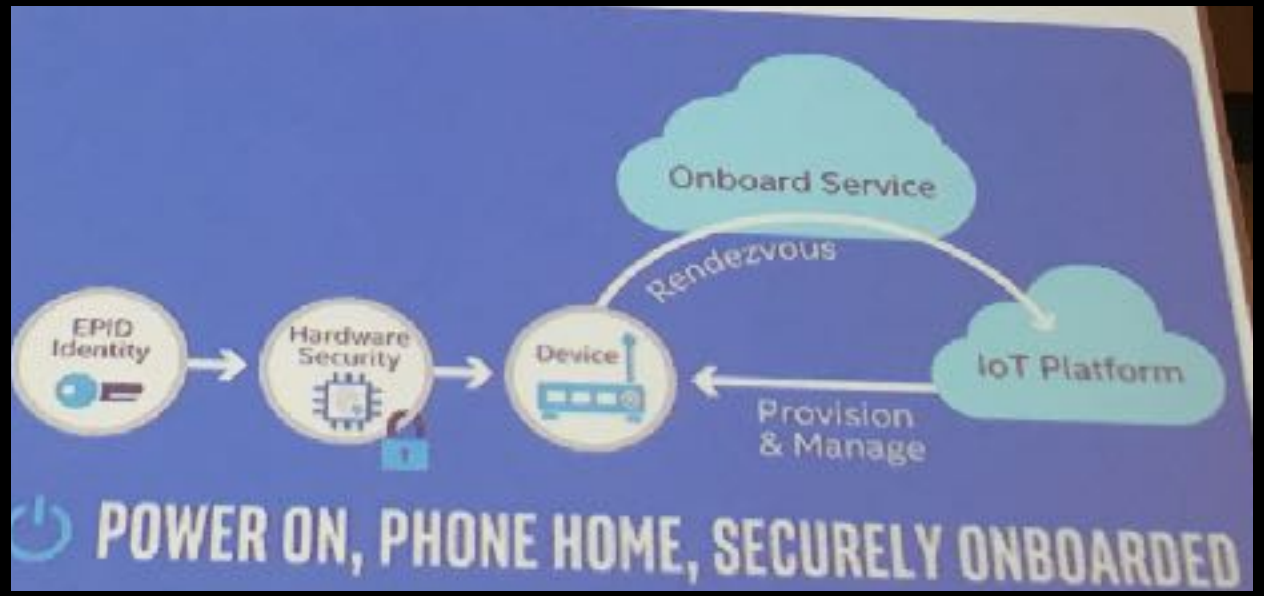
10% Hackers, Script Kiddies, APT, Cybercrime …

90% Wrong documentation, no backups, protocol errors, no time, no awareness, legacy …

2010 Stuxnet
2017 Wannacry, NonPeyta
~~2035~~ all problems solved
2042+

1 typical Lifecycle … 25 years





Picture taken at
Security of Things Conference 2017 - Berlin

Summary

Disruptive self-attack

Don’t think in camps and silos, but in lifecycle!

IIoT security is about defense and enabler.

What we will not see, but it will happen.

„The best way to predict the future is
to invent it.“

2042+

Think big, start small, secure and now