Analyse av Cyber security

Bjørn Axel Gran
Department Head: Risk, Safety & Security
Prof II: MTP, NTNU
bjorn.axel.gran@ife.no
(47) 909 55 295

Digital Systems
Research for a better future

Gunnar Randers, IFE's founder

Key Figures:

Annual turnover:
1
BNOK

Annual scientific publications with referee:
120

1948: IFA

1980: IFE

No. of employees:
650

Nationalities: 37

Researchers: 218

PhDs: 105

14000
Visitors a year

National Centres for Environment-friendly Energy Research
2

Advanced Laboratories:
24

International projects:
> 120

IFE, three organisations in one

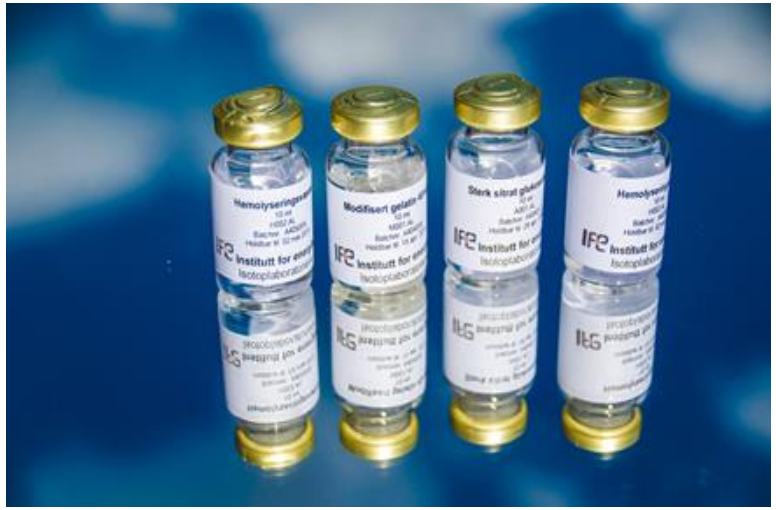
Research & Development

- Material and Process Technology
- Flow Technology and Environmental Analysis
- Digital Systems

Nuclear Technology

- Two research reactors
- Research within physics, materials, nuclides for medicines, nuclear safety, denuclearization, nuclear waste and decommissioning

Radiopharmacy

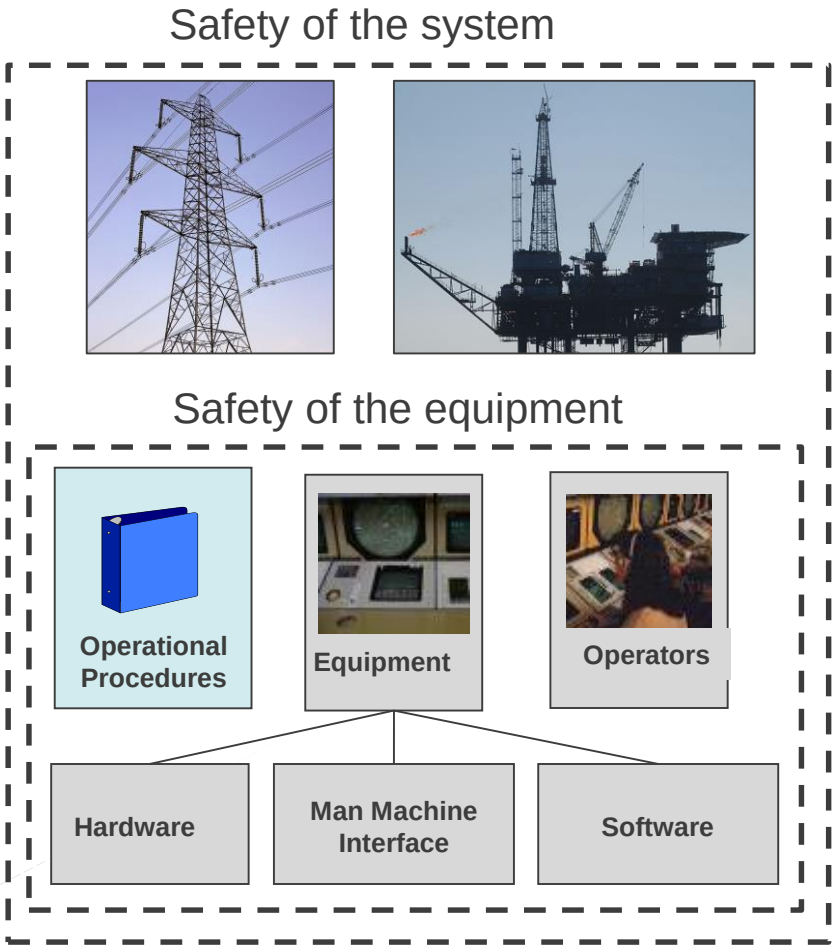


- Development of radiopharmaceuticals
- Production of Xofigo for Bayer
- Production of other radiopharmaceuticals
- Pharmacy and distribution of radiopharmaceuticals

Why risk, safety and security?

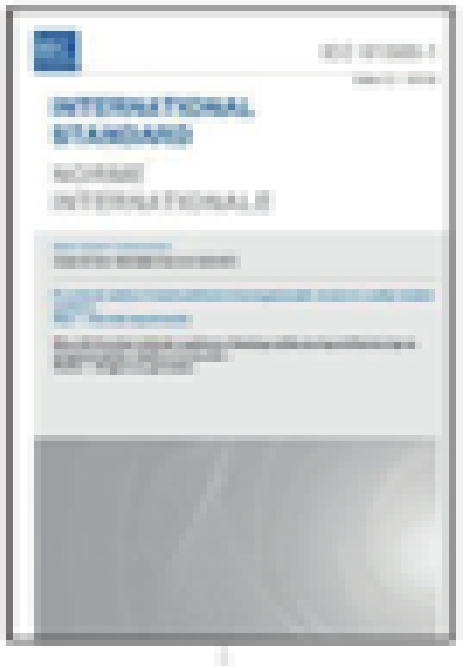
- Lack of well defined and tested requirements for the management system can lead to unforeseen downtime and inefficient services.
- Lack of safety and risk assessment can lead to hazardous incidents working with high energy sources.
- Leak of privacy data will potentially be breach of laws and regulations, and will undermine the trust in the services.
- Manipulation of data or denial of service attacks will besides having costs, also undermine the trust in the services.

How to: risk, safety & security



- Hazards and failures
  - Conduct failure and hazard analyses and follow ups
- Requirements Engineering
  - Conduct requirement process
  - Quality management
- Safety and security
  - Combined assessments
- Safety Demonstration
  - Arguing the safety

IEC 61508 about security



Reference to:

- IEC 62443 series
- ISO/IEC/TR 19791

- requirement 7.4.2.3:
  - “If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out”
- requirement 7.5.2.2
  - “if security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements”
- The safety manual
  - “details of any security measures that may have been implemented against listed threats and vulnerabilities.”

Security assessment

Step1: **Value**

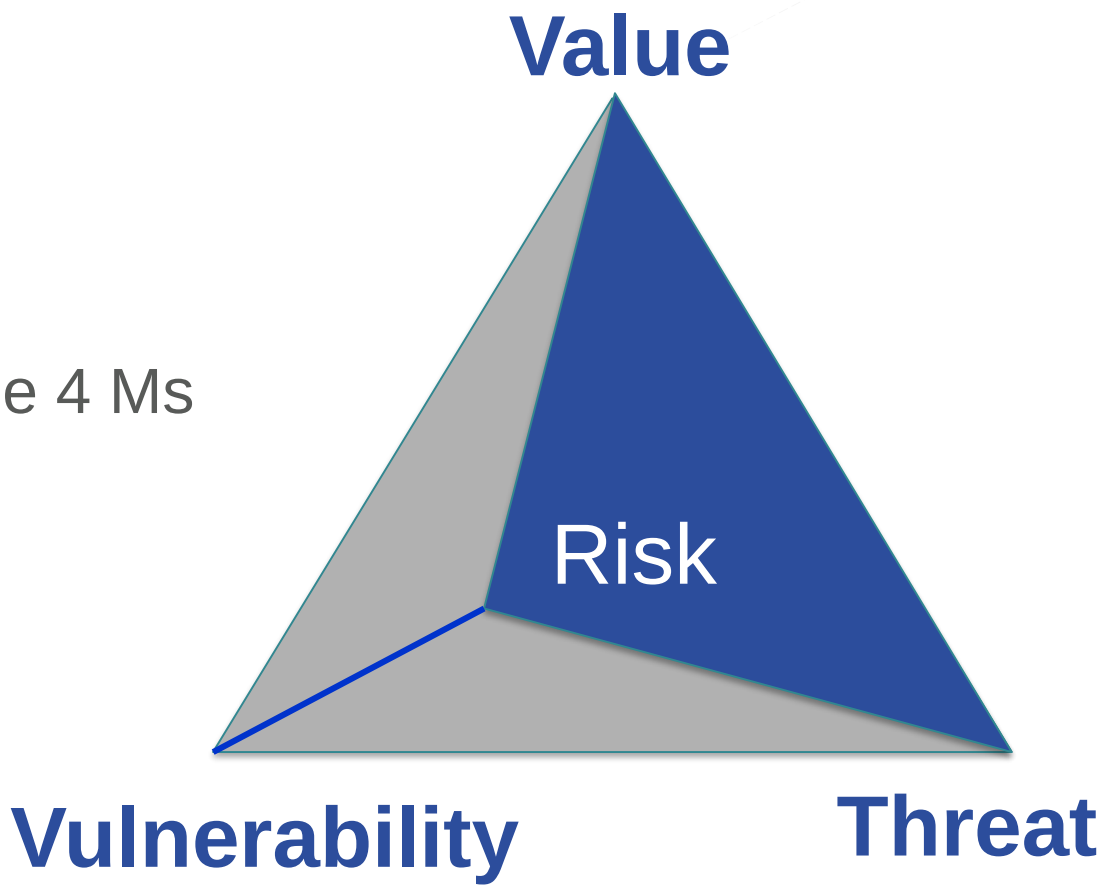
Which values do you have?

Step 2: **Threats**

The actors capacity and intention – the 4 Ms

Step 3: **Vulnerability**

Physical, Logical, Organizational



Cyber Security at IFE – Why?

- Expectation from the authorities:
  - Gjennomføring av Risiko og Sårbarhetsanalyse (ROS) i forbindelse med cybersikkerhet innen utgangen av Juni 2018.
  - Besvare spørsmål som:
    - Har IFE foretatt en grundig verdivurdering?
    - Hvilke trussel- / risikoscenarier står IFE ovenfor?
    - Hvor tett er IFE koblet? (er virksomheten styrt sentralt?)
    - I hvor stor grad er IFE avhengig av eksterne leveranser?
    - Hvordan har IFE organisert sikkerhetsarbeidet?
    - Har IFE kompetanse og kapasitet til å hente ut relevant informasjon?
    - Har IFE IDS-sensorer, netflow, et samarbeid med en CERT?
    - Har IFE PGP-kryptering?

Which risk matrix to use?

Description		1	2	3	4	5	6	7
		Ubetydelig			*Moderate*			Kritiske
1	Ubetydelige							
2								
3								
4	Moderate							
5								
6								
7	SVÆRT høy							

Description		1	2	3	4	5
		Ubetydelig	*Små*	*Moderate*	*Betydelige*	Kritiske
5	SVÆRT høy					
4	Høy					
3	Moderate					
2	Lav					
1	Ubetydelige					

Description		1	2	3	4
		Ubetydelig	*Moderate*	*Betydelige*	Kritiske
4	SVÆRT høy				
3	Høy				
2	Lav				
1	Ubetydelige				

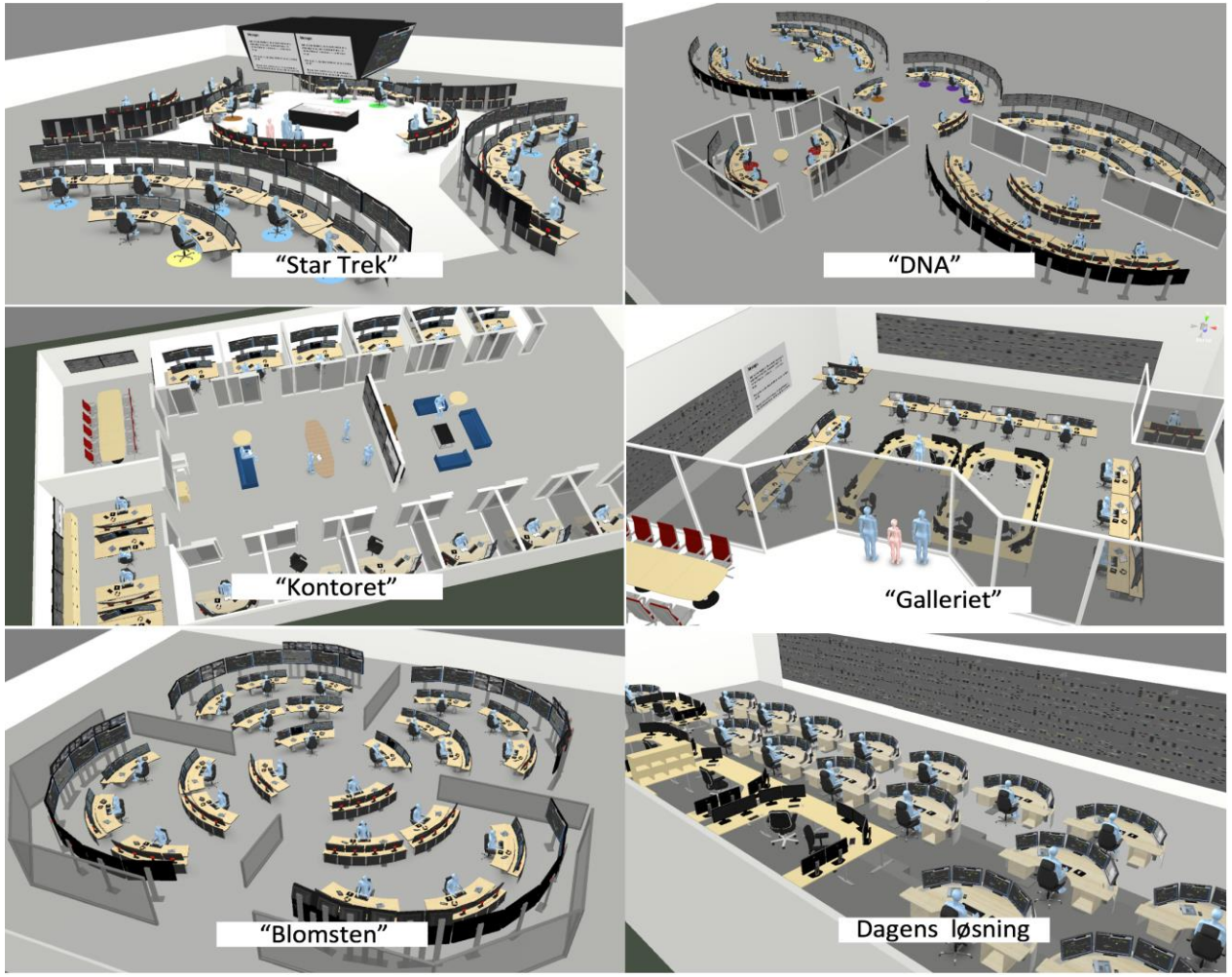
Description		1	2	3	4	5
		Ubetydelig	*Små*	*Moderate*	*Betydelige*	Kritiske
5	SVÆRT høy					
4	Høy					
3	Moderate					
2	Lav					
1	Ubetydelige					

And is critical (safety) = critical (cyber) ?

- ***Kritiske:***
  - The asset is damaged/contaminated beyond safe use.
  - Safety functions are critically impaired and the effect on main facility components and functions is severe
  - The event can lead to loss of life or injury.
- ***Betydelige:***
  - Safety systems remains intact but the entire, or parts of the, facility might be closed for a period of up to 1 week pending resolution.
  - Some assets might need to be replaced or to undergo extensive maintenance or re-certification/verification before normal operation can resume.
  - The event requires a notification to governmental partners and might trigger emergency procedures.
  - The event can lead to significant negative publicity.
- ***Små:*** The asset is temporarily damaged or is impaired in performing its function, but will be restored within 1 hour. A limited number of assets may be damaged or impaired, but the majority of the assets are not affected. There is no reduction of safety systems and the impact on business for the company is minor/acceptable.
- ***Ubetydelige:*** The asset under consideration experiences no significant impact on operations (downtime is less than four hours) and there is no loss of major assets.

RAMS and Security for Bane NOR

- Different concepts for new traffic control centers for Bane NOR
- We have provided:
  - Security Risk Analysis
  - Hazard Identification
  - RAM requirements
- Applying
  - EN 50126 (2017)
- Cyber-security is also about having the right design, e.g.:
  - Access control
  - Security zones



«See it coming: The Four M's of Digital Espionage»

Ref:

Frode Hommedal

On LinkedIn 21. sep 2014

Former: Senior Advisor Difi

Now: Cyber security specialist, Telenor

- Motivation

  «These «viruses» are security incidents, and the results of deliberate actions from hostile entities»

  «Spying on you gives the threat actor – your adversary – some kind of advantage over you, or someone else through you»

- Mission

  «They are highly trained professionals – cyber special forces so to speak – who have been purposely deployed within the perimeters of your network»

- Mindset

  «How can we subvert this» and «what can we make this do», «how can we break into it» and «how can we hide within it».

- Methods

  «The list of methods employed by the wide range of possible cyber adversaries is way too long for me to even contemplate compiling»

Threat assessment – including cyber

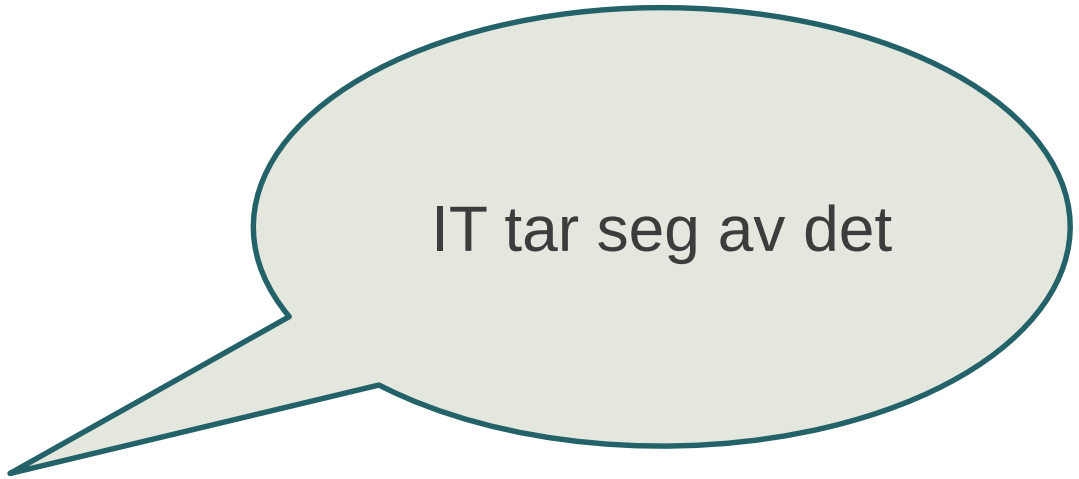
Cat.	Motive	Examples	Mode/means	Loc	Lik	Comment
Sabotage	Show capacity/strength to gain control and damage	Russia	Exploit weaknesses & Espionage			Has capacity and competence, but no history
		Org. Crime	Exploit weaknesses & Espionage			Has capacity and competence, but no history and other targets with more gain
	Gain control and damage in operation	Insiders Indra	Exploit weaknesses			
Terror (Harm)	Gain control and damage	Extremists	Exploit weaknesses			Easier access to weapons and bombs, as well as more gain in other targets
	Show strength/ spread fear	Extremists, Loan wolfs	Exploit weaknesses & Gain control			No history of incidents, but increased awareness
	"On wrong place at wrong time"	Extremists, Loan wolfs	Bombs, weapons			Terror
			Bombs, weapons			Hostage
All	All	Environmentalist	Exploit weaknesses			Very low gain and search publicity in other ways
	"On wrong place at wrong time"	Extremists, Loan wolfs	Bombs, weapons			
Crime	Burgarly/economic	Narco	Physical weaknesses			No history, Client not known for having values
		Crime	Physical weaknesses			Depending on where
						Normally no access, other places with more gain
Espionage	Espionage for later use	Industry, states	Act as burglary, to exploit weaknesses			There is a market
	Espionage for industrial crime	Industry, states	Act as burglary, to exploit weaknesses	All		There is a market

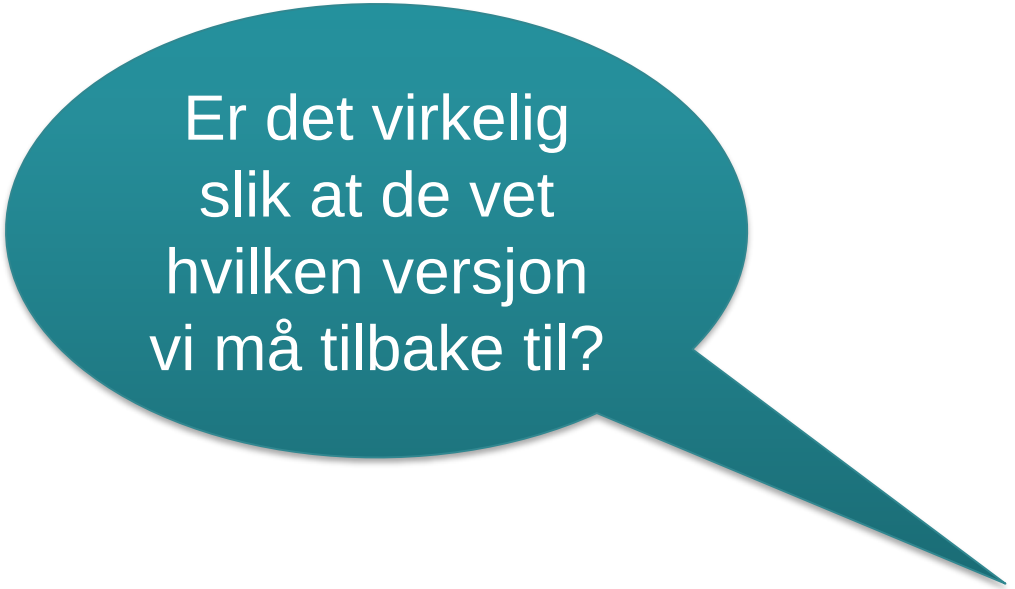
ISO 27001/27002 – walkthrough

- 114 controls divided on 14 areas
- Data collected through:
  - Interview
  - Walkthrough of management system
- Data assessed as
  - Green: covered by procedures / praxis
  - Yellow: weaknesses easy to address
  - Orange: weaknesses hard to address
  - Red: procedures / praxis is missing
  - Grey: not relevant now

Eksempel from Table-tob excersise:

Case: discovered that corrupted code have been checked in



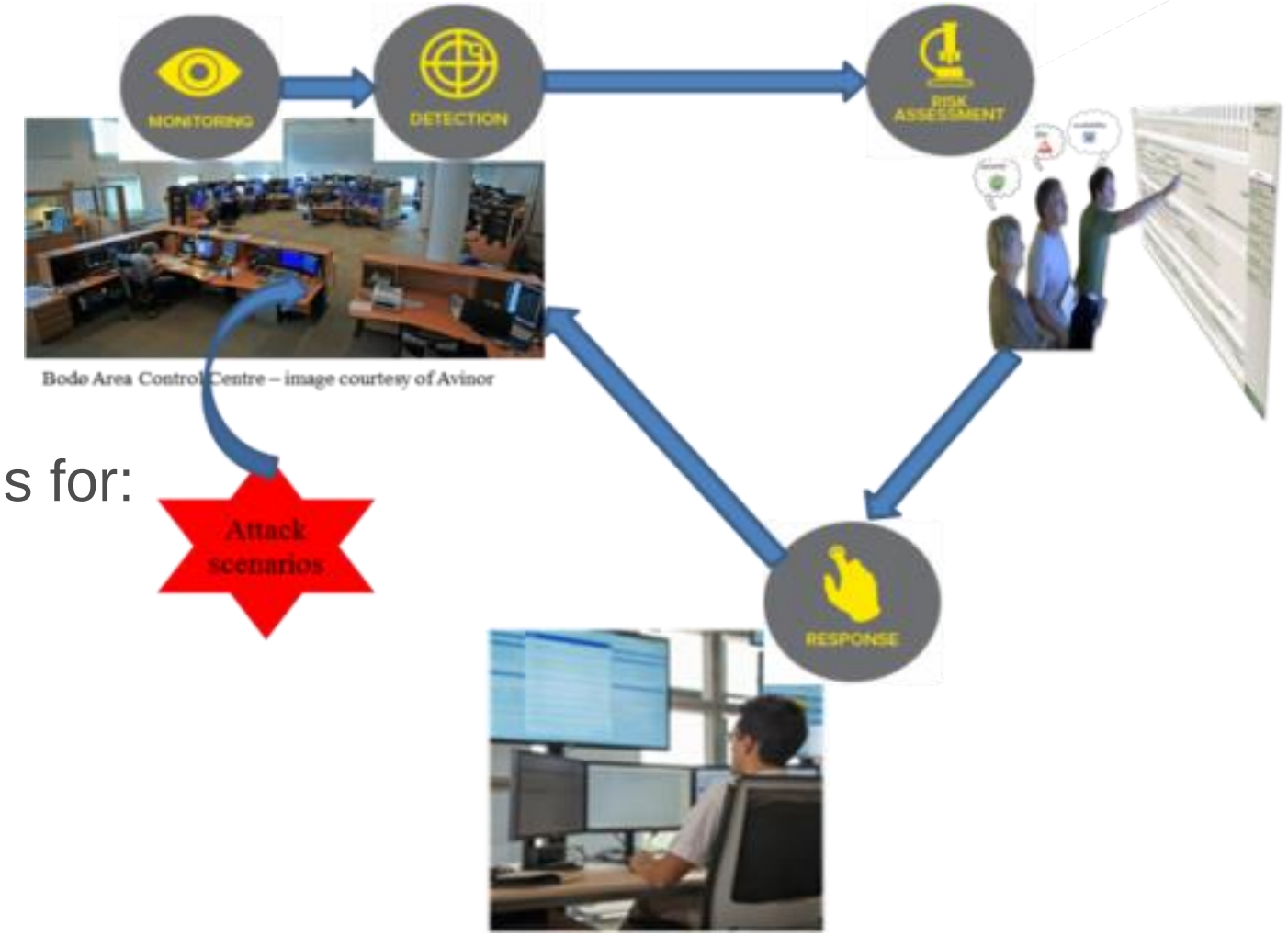


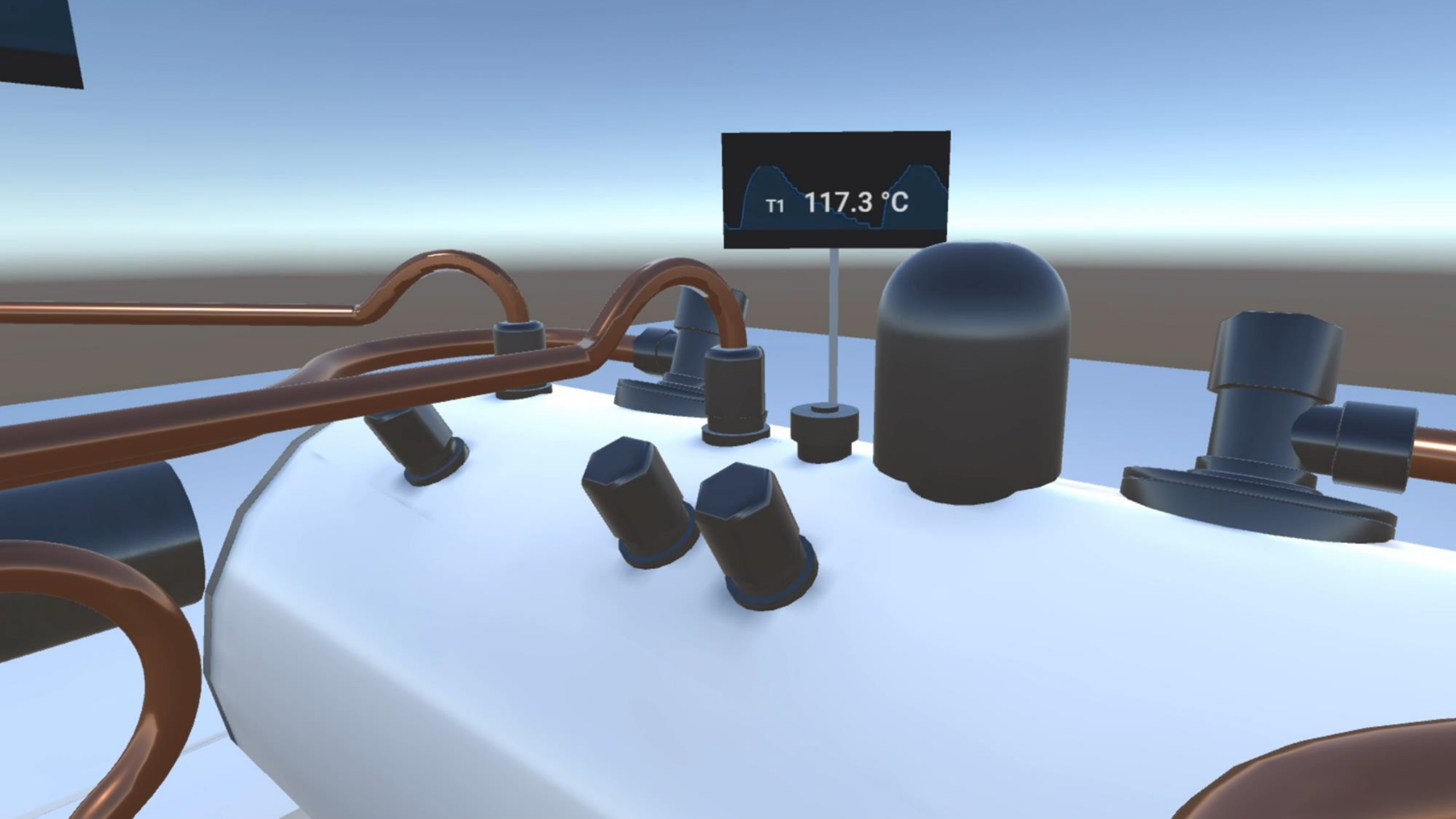
Providing a result like:

	40	43	19	8	4
5 Information security policies		1	1		
6 Organizing information security	3	2		2	
7 Human resource security	1	2	1	2	
8 Asset management	1	6	3		
9 Access control	6	4	3	1	
10 Cryptography	2				
11 Physical and environmental security	9	2	4		
12 Operations security	6	6	1	1	
13 Communications security	1	5	1		
14 System acquisition, development and maintenance	5	6	1		1
15 Supplier relationships	1	1	1		2
16 Information security incident management	1	3	1	2	
17 Information security aspects of business continuity management	1	1	2		
18 Compliance	3	4			1

Cyber Security Lab

- We address:
  - Assets
  - Threats
  - Vulnerabilities
- Partners contribute with tools for:
  - Monitoring
  - Detection
- Results:
  - Modelling of risk
  - Modelling of response




T1 117.3 °C

Is cyber a problem?

- The process is not connected.
- And if it is, they can not stop it.
- .. and other system protect the people from harm.


SYSTEM FAILURE

It is a problem!

- *My process is not connected.*
- *And if, they can not stop it.*
- *.. and other system protect the people from harm.*

- They studied the design
- … studied the vulnerabilities
- … used it for a DoS
- … and gained 1M$ on their stocks

GIKK I SVART: Ved 07.35-tiden torsdag morgen gikk hele Fredrikstad i svart som følge av strømbrudd. (MMS-FOTO: Erik Hagen)

- Dominoeffekt førte til strømstans i Fredrikstad

Ved 07.36-tiden torsdag morgen gikk hele Fredrikstad og store deler av Sarpsborg i svart som følge av strømbrudd. 37. 000 av Fredrikstad Energinetts abonnenter ble berørt.

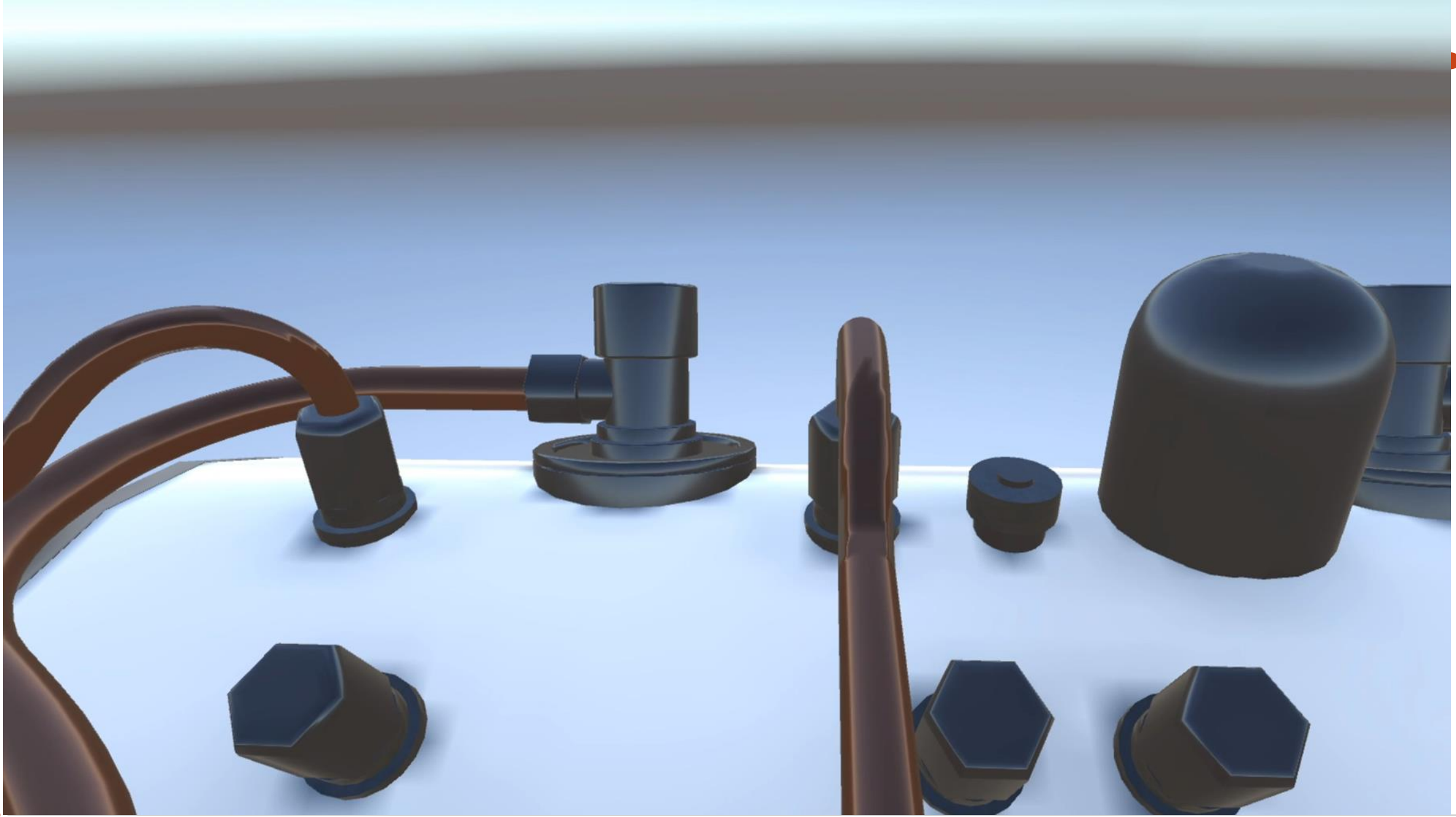
AV: HELGE NESS OG ESPEN NORMANN

PUBLISERT 16.12.2010 07:48

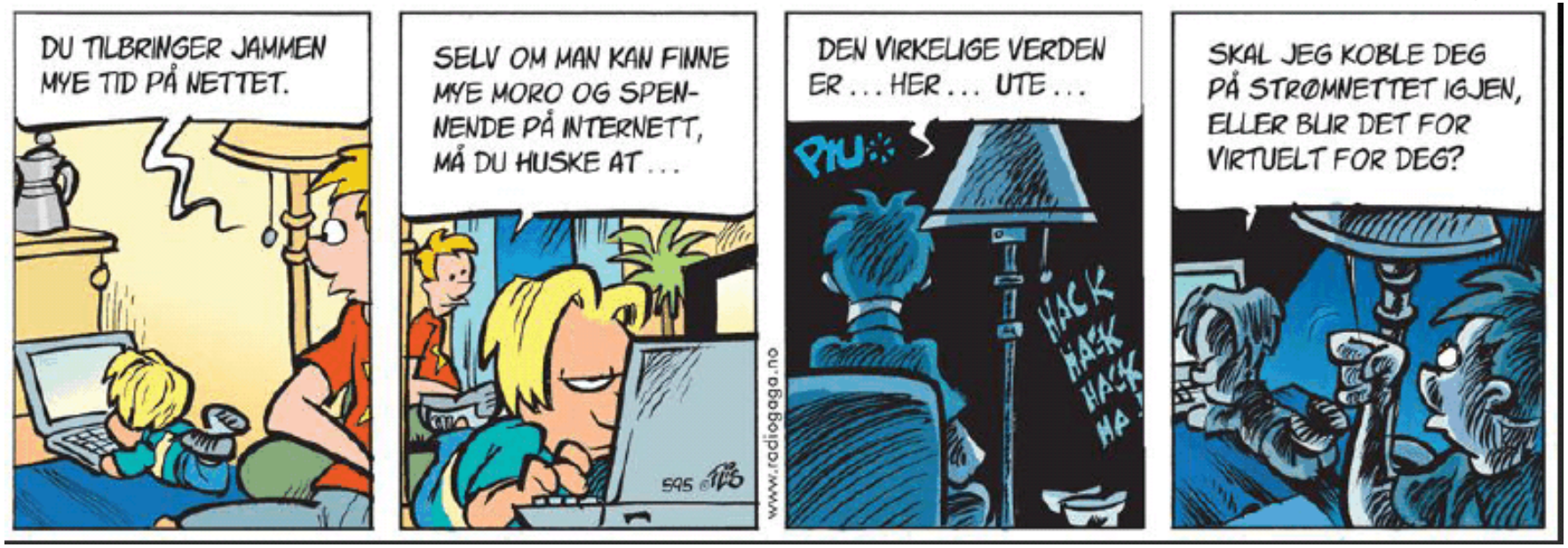
SIST OPPDATERT 16.12.2010 13:10

Why the cyber-problem is also about humans:

- Your conversation on the train made you an obvious target
- Your password was easy to guess
- Your e-mails showed us your critical contacts
- Your local files provided us with the design
- You provided us with an easy way into your customers systems




WEGA



Thank you – any questions?