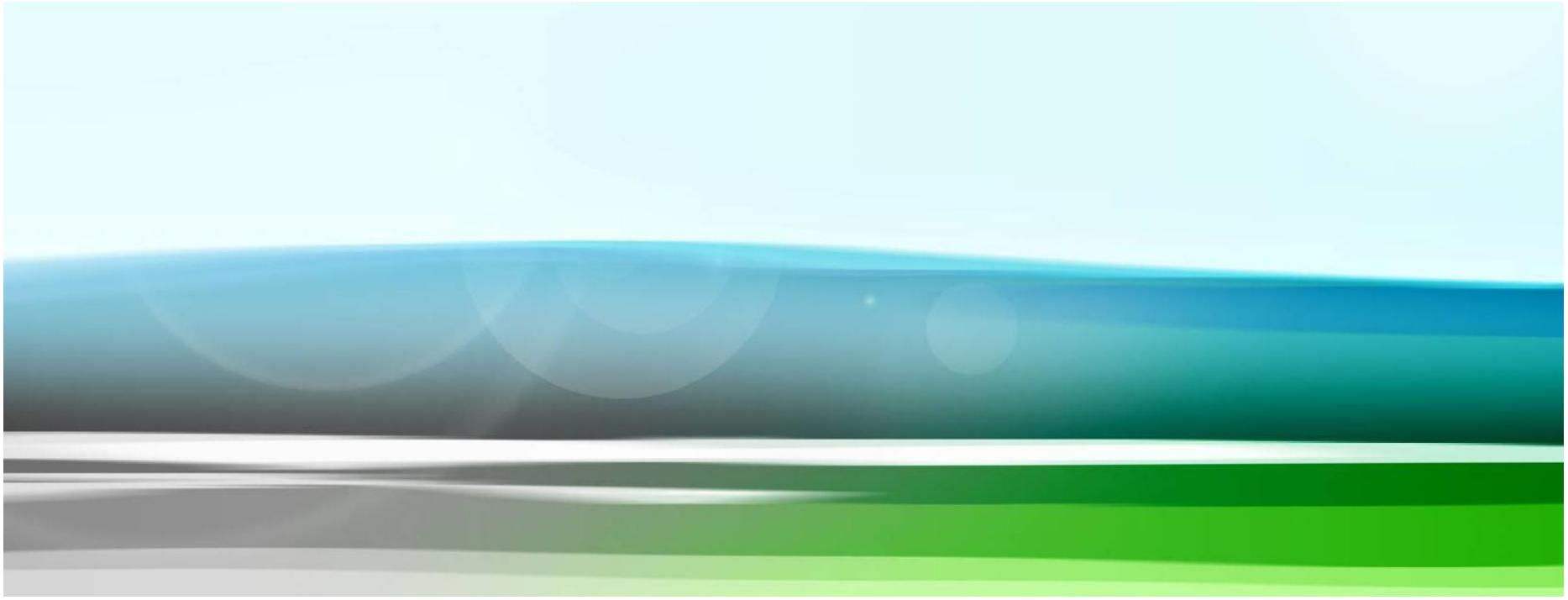


IKT-sikring, en forutsetning for olje og gass
HMS og anleggsintegritet

Arild Braathen Torjusen
(arild.braathen.torjusen@dnv.com)
Principal Consultant
Information Risk Management – Risk Management Solutions

22.05.2013

MANAGING RISK

Introduksjon

- IKT-sikring i et olje og gass perspektiv.
  - Sikkerhet: trygghet (mot fare, angrep e l)
  - Sikring: å gjøre sikker, verne, trygge
- Informasjonsikring = informasjonssikkerhet.
  - Fysisk sikring er en del av bildet.
  - ICS (Industrial Control Systems) (prosessanlegg)
  - PCSS (Process Control, Safety and Support) ICT system
    - IKT systemer---permanent eller midlertidig tilkoblet---med direkte påvirkning på O&G produksjon og IKT systemer som støtter disse.
- "Er det mulig se safety og security som to viktige elementer i en større sammenheng?"
  1. Safety og security fellestrekk og forskjeller.
  2. Hvordan DNV jobber med informasjonssikkerhet for prosessanlegg.
  3. Koblinger mellom safety og informasjonssikkerhet. (Krav og praksis)

Introduksjon

- **Anleggsintegritet**

En ønsket“integritet”(Asset Integrity) av et anlegg er oppnådd når, under de gitte operasjonelle forholdene, risikoen for personell, miljø og økonomiske verdier er akseptabel og er redusert til et nivå som er "reasonably practical""(økonomisk optimalt).

- Design - anlegg er designet i hht. krav og slik at operasjonskrav blir møtt
- Teknisk - vedlikehold og fortløpende håndtering av risiko
- Operasjonell - nødvendig bemanning og kompetanse til å operere og at systemer, data & dokumentasjon er tilgjengelig.

Innhold

1. Introduksjon
2. Safety & (information) security
3. Trusselbilde, myndighetenes fokus, regelverk og forventninger
4. Hvordan jobber DNV med informasjonssikkerhet
5. Koblinger mellom safety og informasjonssikkerhet
6. Oppsummering

Safety & Security

- Sikkerhet (Safety) sies ofte å være beskyttelse mot ikke-intenderte hendelser

- Sikkerhet (Security) sies ofte å være beskyttelse mot intenderte handlinger.

Safety & Security

- Safety – Sikkerhet
  - Beskyttelse mot vilkårlige hendelser, uønskete hendelser som er et resultat av en eller flere sammentreff.
- Security - Sikkerhet
  - Beskyttelse mot intendertete hendelser/handlinger, resultat av overveid og planlagt handling.
- Information Security - Informasjonssikkerhet
  - Bevare informasjonens konfidensialitet, integritet og tilgjengelighet (CIA).
  - Informasjon skal:
    - Holdes hemmelig om nødvendig.
    - Være korrekt
    - Holdes tilgjengelig
- Informasjonssikkerhet og IKT-sikkerhet
  - Beskyttelse av informasjonsaktiva er det primære.
  - Som oftest flyter denne informasjonen gjennom IKT baserte systemer.
- Europa: Information security
- USA: Cybersecurity (Kybersikkerhet)
  1. informasjonssikkerhet for datamaskiner og nettverk– spesielt for systemer på internett (cyberspace)
  2. informasjonssikkerhet for industrielle kontrollsystemer (cybernetics) (ICS)

	IT (Data)
1	Confidentiality
2	Integrity
3	Availability

Informasjonssikkerhet i prossessanlegg (ICS)

- Hovedforskjell mellom IT og ICS:
  - ICS styrer fysiske prosesser, feil har reelle konsekvenser med stort skadepotensial
  - ICS-risiko bør i større grad enn for IT koordinereres med fysisk sikkerhet og HSE
  - For ICS er det vanlig å reversere prioriteringen av fokus

	IT (Data)	ICS (Process)
1	Confidentiality	Availability
2	Integrity	Integrity
3	Availability	Confidentiality

- Integritet og tilgjengelighet
  - Prioritering fundert i IEC/ISA 62443-2-1, men problematisk,
  - Safety noder/PLCer
  - Network management

ICS = Industrial Control System

- Informasjonssikkerhet for ICS
  - uatoriserte personer eller systemer skal ikke kunne modifisere systemer eller data
  - uatoriserte personer eller systemer skal ikke ha tilgang til systemenes funksjoner
  - autorisert tilgang skal ikke hindres (både vanlig drift og i nødprosedyrer)

Safety vs. security (O&G)

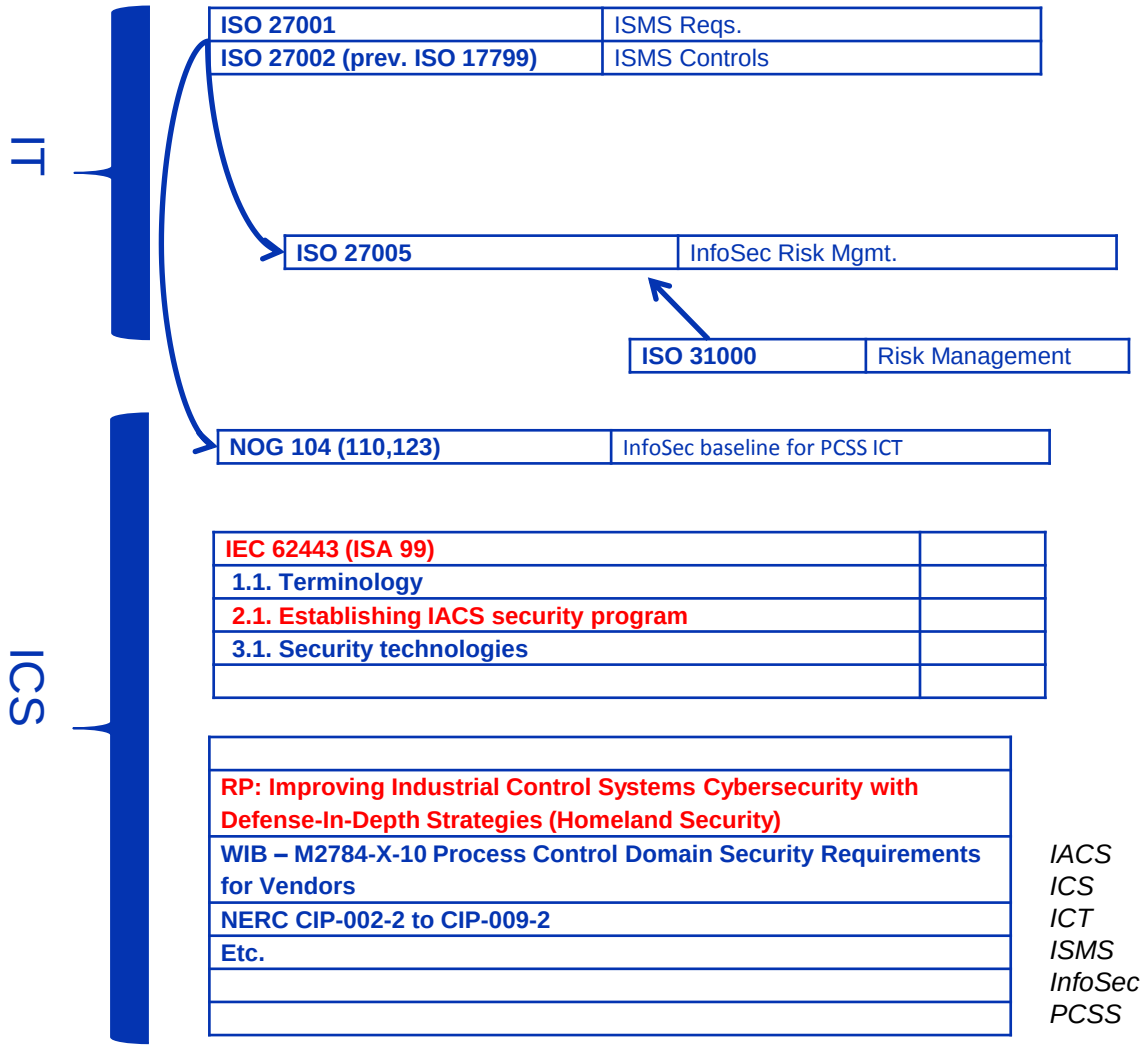
Safety	Information Security
- Primært fysiske aktiva (assets)	- Primært logiske aktiva (systemer og funksjoner) (noe hardware)

- Risikostyring:
  - Kvalitativt og kvantitativt
	- Risikostyring:
	  - Primært kvalitativt

- Kjenn dine aktiva og deres egenskaper:
  - Weaknesses
  - Operating parameters
	- Kjenn dine aktiva og deres egenskaper:
	  - Vulnerabilities
	  - **Threats**
	  - Operating parameters

- Meget høyt fokus på norsk sokkel	- Moderat, men økende fokus
- Formaliserte, aksepterte og obligatoriske metoder (f.eks. QRA & SIL)	- Mindre formalisert og ikke like detaljert kravgjennomgang som for Safety.
- Moden og standard teknologi	- Mindre moden teknologi i utvikling.
- God forståelse av verdi og viktighet.	- "Jeg vil ha Facebook!!!"
- Integrert i de fleste (engineering) disipliner.	- Mindre kompetanse i andre disipliner.
- Forankring i engineering disipliner.	- Forankring i informasjons og IKT sikkerhet.

IT og kontrollsystem (ICS) standarder

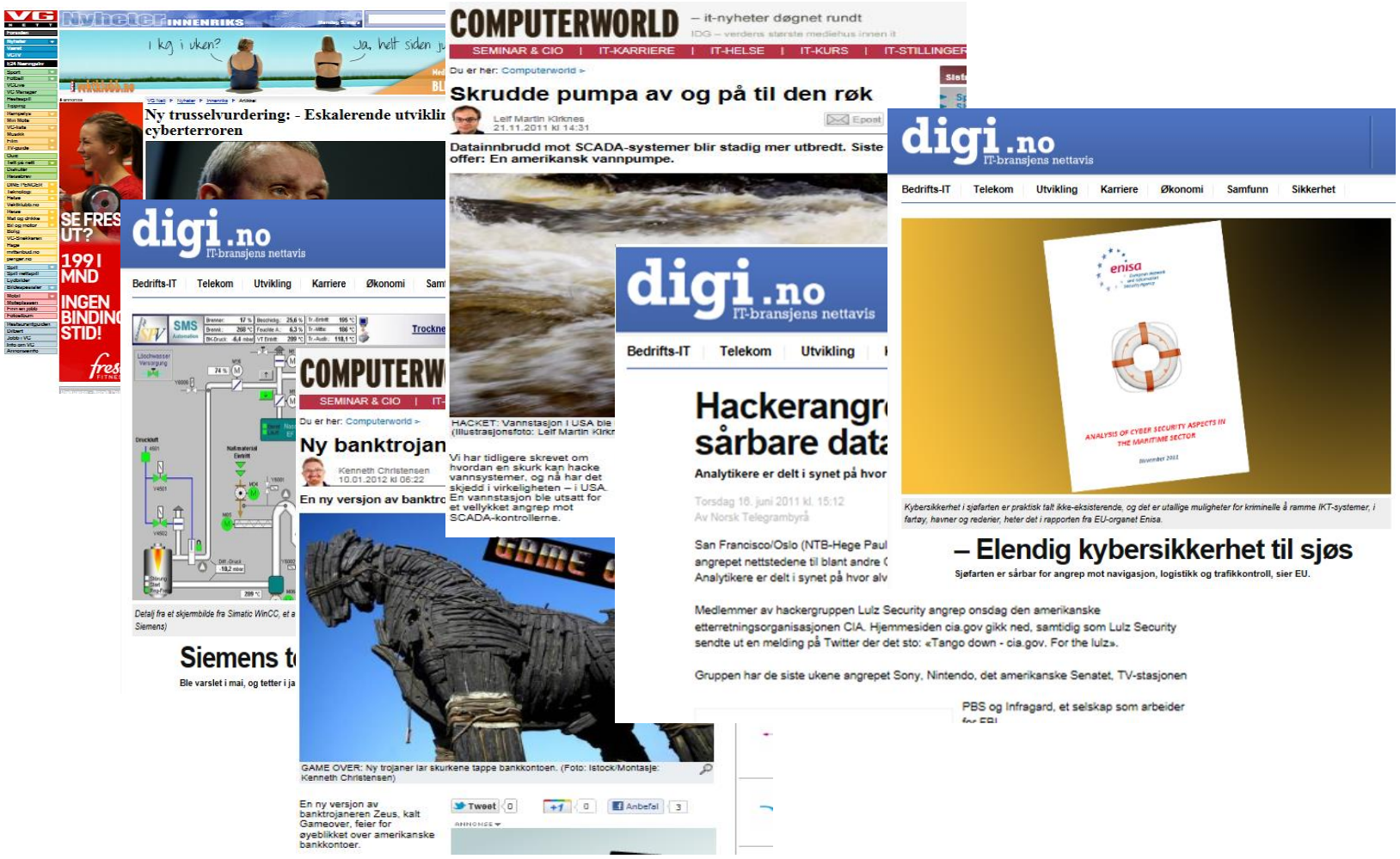


NIST 800-53	**Information Security** Recommended Security Controls for Federal Information Systems and Organizations
NIST 800-53A	*Guide for Assessing the Security Controls in Federal Information Systems*
NIST 800-83	**Guide to Malware Incident Prevention and Handling**
NIST 800-94	**Guide to Intrusion Detection and Prevention Systems (IDPS)**
NIST 800-123	**Guide to General Server Security**
COBIT 5 Framework	
ISF Standard of Good Practice	

NIST 800-82	Guide to ICS Security
Apendix I in revision 3. of NIST 800-53	ICS Security Controls.

IACS	*Industrial Automation and Control System*
ICS	*Industrial Control System*
ICT	*Information and communication technology.*
ISMS	*Information Security Management System*
InfoSec	*Information Security*
PCSS	*Process Control, Safety and Support*

Økende fokus på informasjonssikkerhet.



Økt trusselnivå og bevissthet internasjonalt

- Obamas "executive order" om forbedring av sikkerhet i kritisk infrastruktur:

> Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. (February 12, 2013)

- Worldwide threat Assessment of the US Intelligence Community (March 12, 2013)
  - *Cyber threats* and *cyber espionage på topp.*
- Konsekvenser av Stuxnet (2010)
  1. Økt bevissthet om sårbarhet i ICS – både fra forsvarere og angripere.
     - Flere sårbarheter publisert (med angrepskode), exploit kits.
  2. Flere Advanced Persistent Threats (APT) mot industrielle mål (spionasje, ødeleggelse)
  3. Bruk av kyber-krigføring er blitt legitimert og alminneliggjort.
- Økt grad av konnektivitet: ønske om å utnytte ny teknologi gir nye sårbarheter:
  - Mobile (trådløse) enheter
  - Fjernoperasjon og vedlikehold (egen og tredjeparts)
  - Deling av data mellom ICS og office.
  - Integrerte operasjoner gir økte krav til tilgjengelighet, (og integritet)

Advanced Persistent Threats (APT)

- **Avansert**: Dekker hele spekteret fra enkle exploits til egen forskning (profesjonelle utviklere/organisasjoner)
- **Vedvarende**: Ikke tilfeldig, eller opportunistisk. Men vedvarende aktivitet for å oppnå mål, gjerne på vegne av oppdragsgiver.
- **Trussel**: Bevisste aktører står bak, ikke kode.

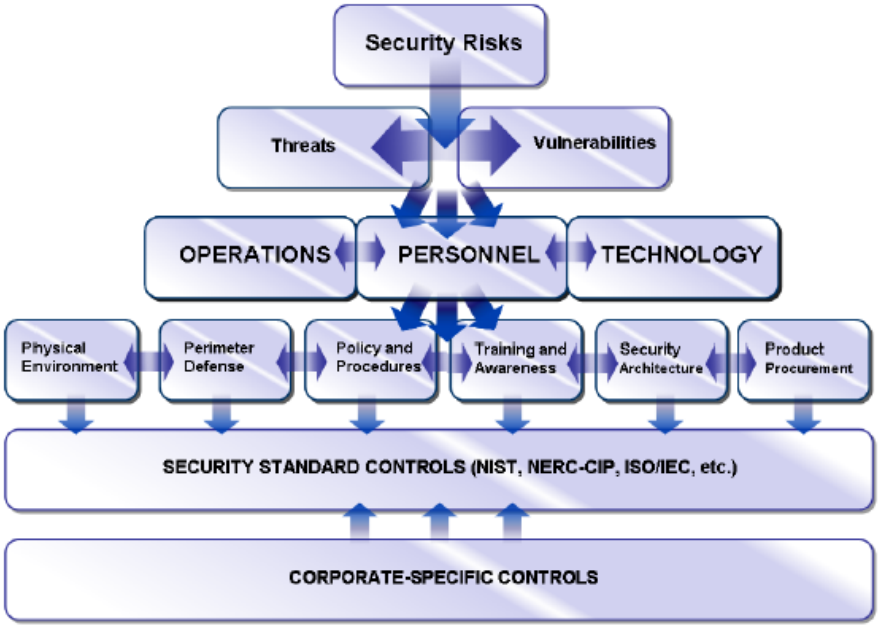
> This decade is setting up to be the exponential jumping off point. The adversaries are rapidly leveraging productized malware toolkits that let them develop more malware than in all prior years combined, and they have matured from the prior decade to release the most insidious and persistent cyberthreats ever known.
> (McAfee whitepaper Feb 2011)

- Duqu: Neste generasjons Stuxnet?
- Night Dragon: Rettet mot olje, energy og petrokjemiske firma. (Ikke ICS, men tyveri av

> Today it is clearly a game with the advantage going to the attacker, millions of decades-old systems that were **never designed to be secure**, **increasing connectivity of SCADA and ICS**, and a growing **library of free tools and techniques to attack SCADA and ICS**. (Tofino Security blog May 2013)

Hvordan håndtere trusselbildet: "Defence in depth"

- Defence in depth:
  - Personell, operasjon og teknologi.
  - Tekniske/logiske barrierer (flere lag)
    - soner/dmz
    - rutere/brannmurer
    - IDS
  - Fysiske barrierer
  - Prosedyrebarrierer
  - Opplæring og bevisstgjøring.
  - Beskytt "kronjuvelene"



Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies (Dept. of Homeland Security)

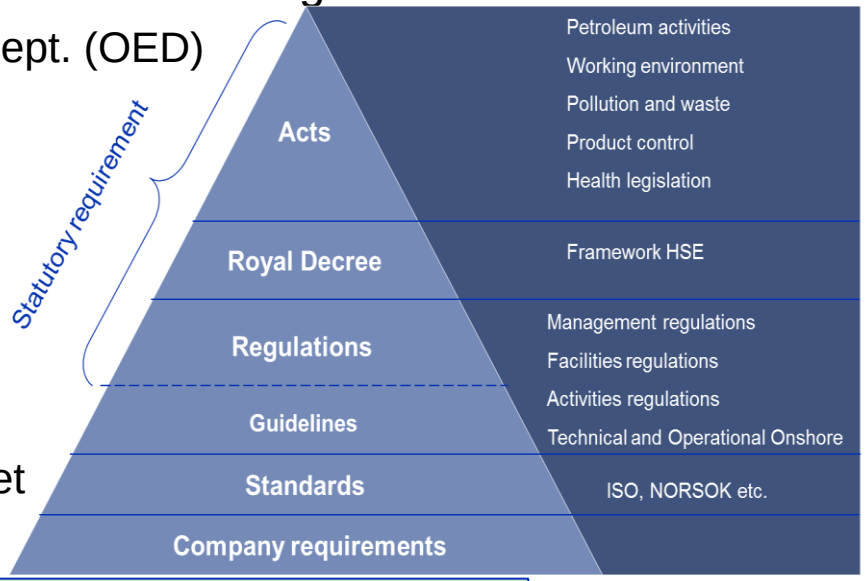
Personell: Operasjon: (aktiviteter som opprettholder sikkerhetsevnen fra dag til dag)

Teknologi:

- Engasjement fra toppledelse
- Arkitektur og segregering i soner
- Prinsipper (policy) og prosedyrer
- Brannmurer, rutere, switcher
- Opplæring og sikkerhetsbevissthet
- IDS - (intrusion detection system)
- Administrasjon av sikkerhetsanlegg
- Hendelseshåndteringssystem
- Rutiner for kontroll og overvåking av tilgang (også fysisk)
- Overvåking av trusler
- Avdekke angrep og respondere adekvat
- Gjenopprettning etter hendelser

Økt fokus på informasjonssikkerhet fra norske myndigheter.

- PTIL har økt fokus på informasjonssikkerhet for O&G næringen.
  - Pålegg fra Arbeidsdept. (AD) via Olje og Energi Dept. (OED)
- PTIL tilsyn i 2012
  - Dramatisk økning i mengden av angrep
  - Endringer i trusselbildet: IT ➔ kontrollsystemer
  - IO og økende fjernstøtte fra leverandører
- IKT-sikkerhet er forankret i HMS forskrifter:
  - virkemiddel for å redusere risiko, ivareta sikkerhet og redusere skade feil- og ulykkessituasjoner.



Rammeforskriften: § 10 Forsvarlig virksomhet

Virksomheten skal være forsvarlig både ut fra en enkeltvis og samlet vurdering av alle faktorer som har betydning for planlegging og gjennomføring av virksomheten når det gjelder helse, miljø og sikkerhet. Det skal også tas hensyn til de enkelte virksomhetenes egenart, stedlige forhold og operasjonelle forutsetninger.

Et høyt nivå for helse, miljø og sikkerhet skal etableres, opprettholdes og videreutvikles.

Styringsforskriften:§ 4 Risikoreduksjon

Ved reduksjon av risiko som nevnt i rammeforskriften § 11, skal den ansvarlige velge tekniske, operasjonelle og organisatoriske løsninger som reduserer sannsynligheten for at det oppstår skade, feil og fare- og ulykkessituasjoner.

Det skal dessuten etableres barrierer som nevnt i § 5.

De løsningene og barrierene som har størst risikoreduserende effekt, skal velges ut fra en enkeltvis og samlet vurdering. Kollektive vernetiltak skal foretrekkes framfor vernetiltak som er rettet mot enkeltpersoner.

NOG (OLF) Guideline 104: Information Security Baseline Requirements (ISBR) for process control, safety and support ICT systems.

- 16 krav danner basis for et *Information Security Mgmt. System* (ISMS (ISO 27000))
- Cyber Security Management System (CSMS - IEC 62443)
- Grunnleggende:
  - 1. Forankring i organisasjonen
  - 2. Riskobasert tilnærming.
- Organisatoriske krav (personell/operasjon):
  - 3,5,7,8,9,10,15,16
- Teknologiske krav til PCSS/ICT systemer:
  - 4,11,13
- Krav med begge aspekter:
  - 6,12,14
- NOG 123 støtter ISBR 2 ved å gi retningslinjer for kritikalitetsvurdering..

ISBR	Keywords
ISBR 1	**Policy**
ISBR 2	**Risk assessment (NOG 123)**
ISBR 3	System & Data Owners
ISBR 4	Network segregation & communication control
ISBR 5	User training
ISBR 6	Designated purpose/hardening
ISBR 7	Disaster recovery
ISBR 8	**Integration of IS-requirements in life cycle (NOG 110)**
ISBR 9	Service & Support levels
ISBR 10	Change Mgmt./Work permits
ISBR 11	Updated Topology
ISBR 12	Updates/Patches
ISBR 13	Protection against malicious Software
ISBR 14	Access Control
ISBR 15	Documentation of procedures
ISBR 16	Incident reporting

PCSS/ICT : process control, safety and support ICT systems

- NOG 110 støtter ISBR 8 ved å relatere NOG 104 til livsløpet for prosjekt og operasjons organisasjonen.

Resultat av tilsyn 2012

- Tilsynet omfattet: landanlegg, produksjonsanlegg, borerigger
- Svakeste punkter samlet sett:
  - ISBR #5: Users of process control, safety, and support ICT systems shall be educated in the information security requirements and acceptable use of the ICT systems.
    - Manglende forståelse for sikkerhetsrisiko og akseptabel bruk av systemene
  - ISBR #7: Disaster recovery plans shall be documented and tested for critical process control, safety, and support ICT systems.
- Spesielt for produksjonsanlegg også:
  - ISBR #6: Process control, safety, and support ICT systems shall be used for designated purposes only.
    - Systemene brukes også til andre formål
  - ISBR #13: Process control, safety, and support ICT systems shall have adequate, updated, and active protection against malicious software.
    - Krevende å ha oppdatert beskyttelse mot virus o.l.

Hvordan jobber DNV med informasjonssikkerhet (ICS)

1. **Risikostyring for informasjonsikkerhet**
2. Nettverk og topologi – design og implementasjon (teknologi)
3. Rammeverk og forankring (personell og operasjon)

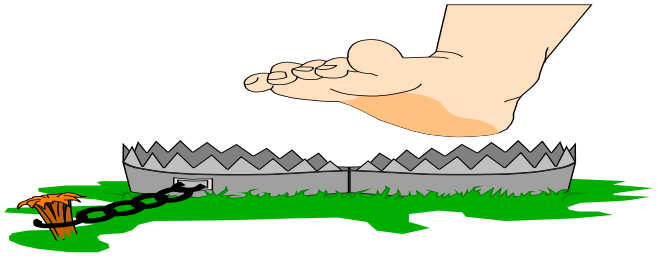
Risikoanalyse

"En strukturert analyse som omfatter systematisk indentifisering og kategorisering av risiko for mennesker, miljø og økonomisk verdi"

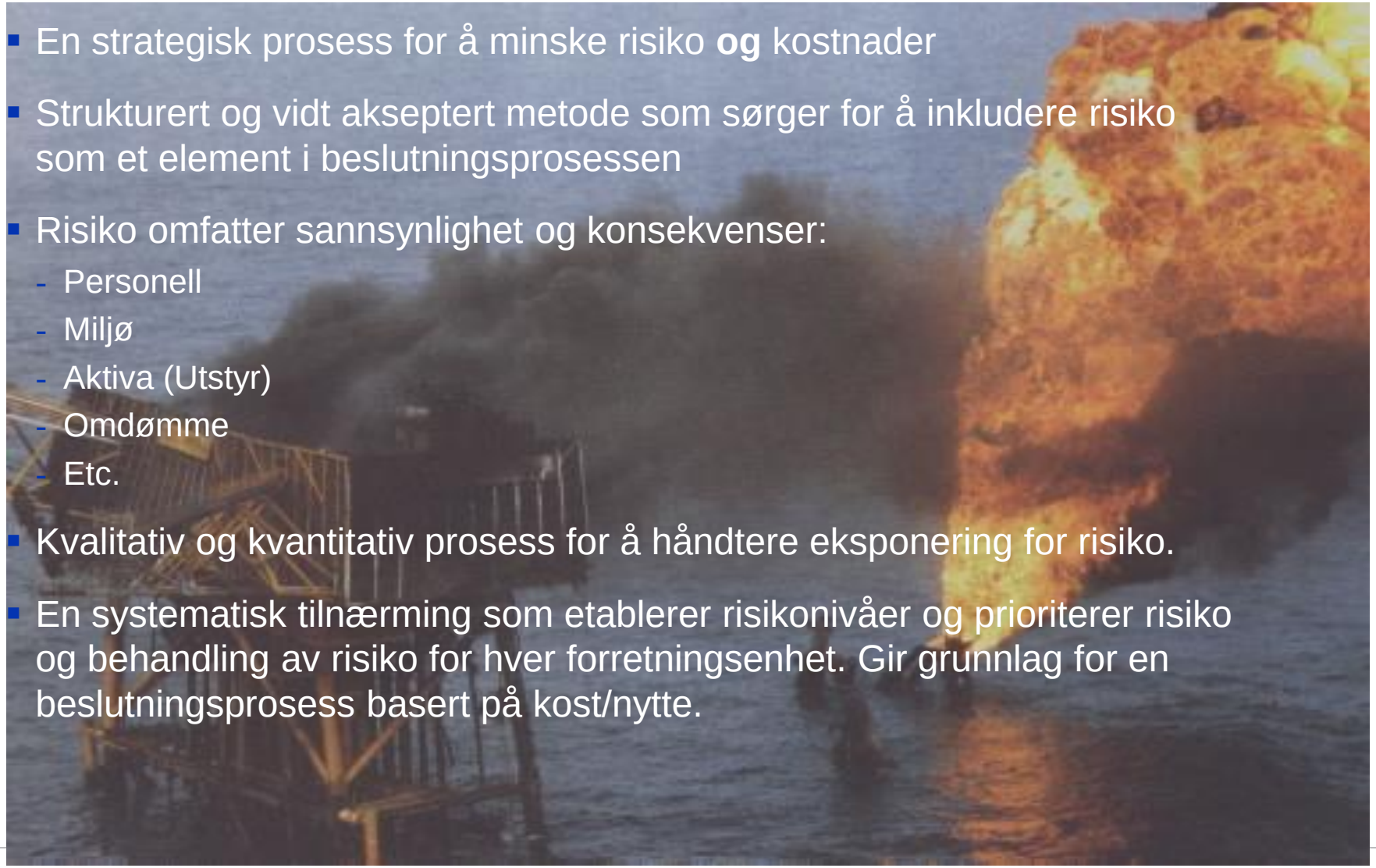
Dette gjelder for Safety "people" and Security "people"

RISK =

Sannsynlighet **x** **Konsekvens**

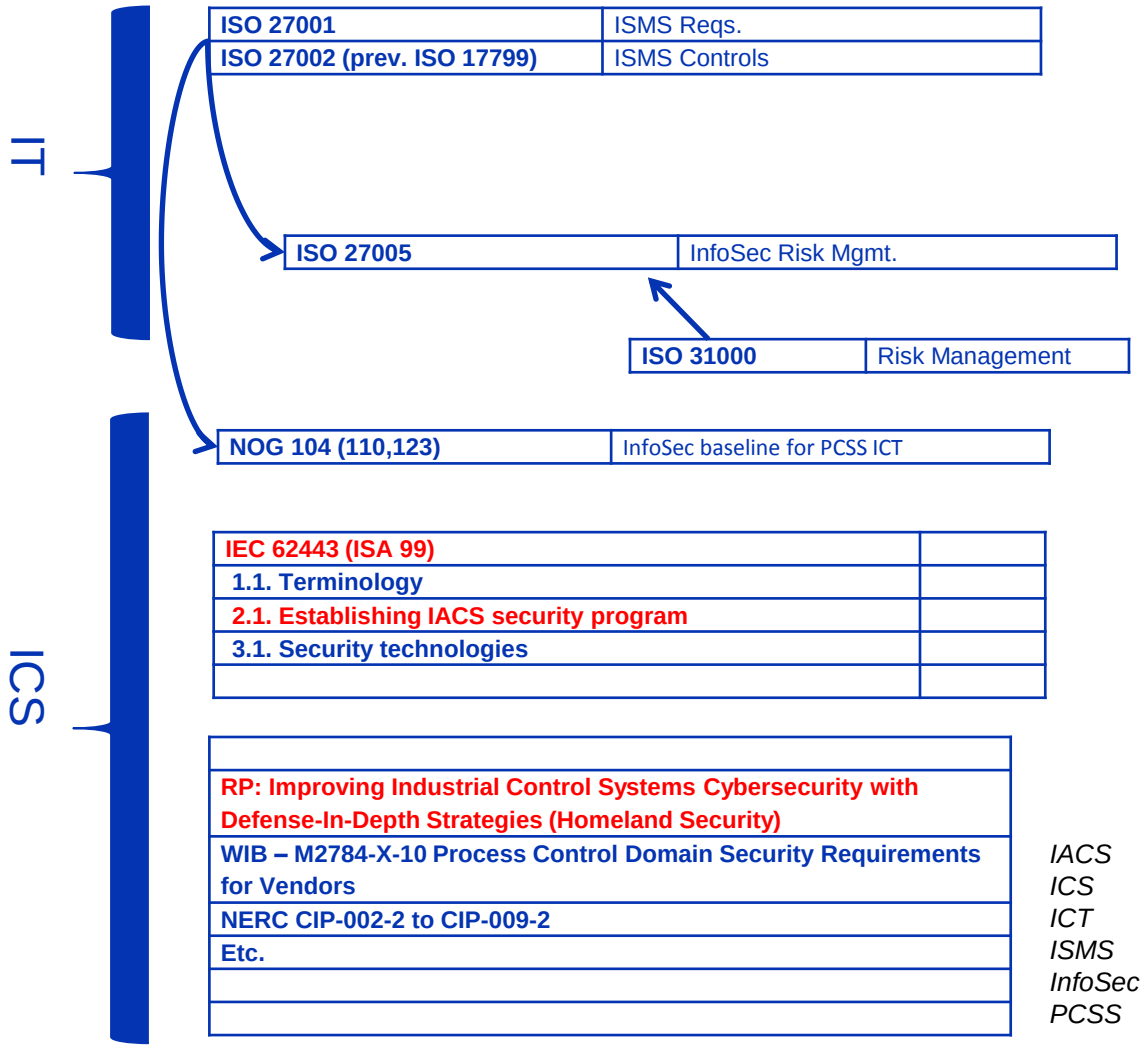


Risikostyring



- En strategisk prosess for å minske risiko **og** kostnader
- Strukturert og vidt akseptert metode som sørger for å inkludere risiko som et element i beslutningsprosessen
- Risiko omfatter sannsynlighet og konsekvenser:
  - Personell
  - Miljø
  - Aktiva (Utstyr)
  - Omdømme
  - Etc.
- Kvalitativ og kvantitativ prosess for å håndtere eksponering for risiko.
- En systematisk tilnærming som etablerer risikonivåer og prioriterer risiko og behandling av risiko for hver forretningsenhet. Gir grunnlag for en beslutningsprosess basert på kost/nytte.

IT og kontrollsystem (ICS) standarder

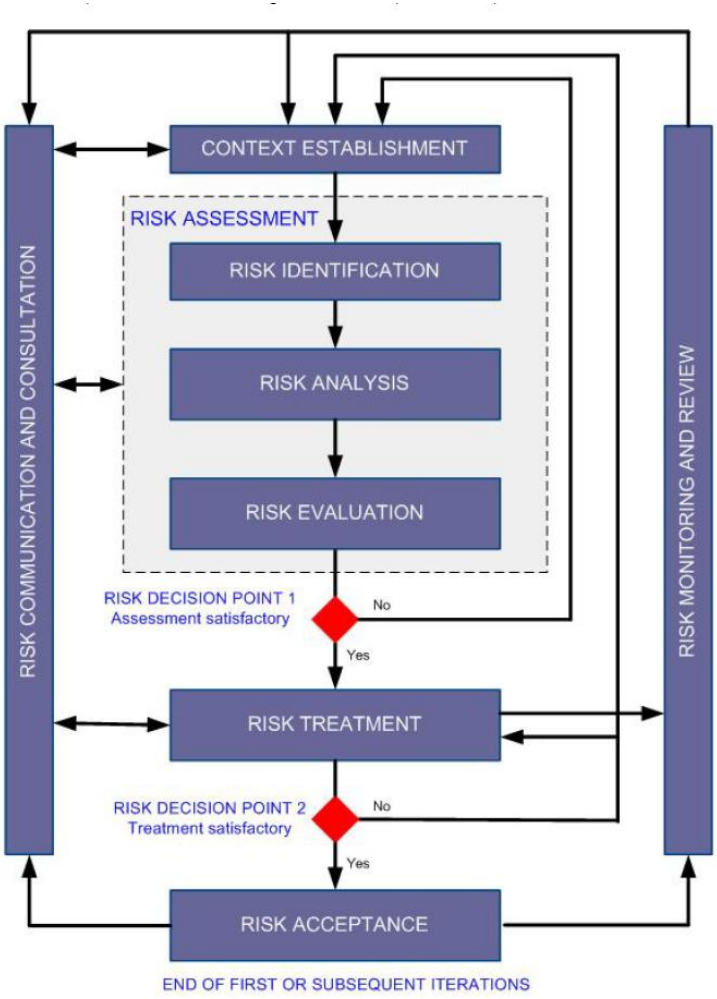


NIST 800-53	**Information Security** Recommended Security Controls for Federal Information Systems and Organizations
NIST 800-53A	*Guide for Assessing the Security Controls in Federal Information Systems*
NIST 800-83	**Guide to Malware Incident Prevention and Handling**
NIST 800-94	**Guide to Intrusion Detection and Prevention Systems (IDPS)**
NIST 800-123	**Guide to General Server Security**
COBIT 5 Framework	
ISF Standard of Good Practice	

NIST 800-82	Guide to ICS Security
Apendix I in revision 3. of NIST 800-53	ICS Security Controls.

IACS	*Industrial Automation and Control System*
ICS	*Industrial Control System*
ICT	*Information and communication technology.*
ISMS	*Information Security Management System*
InfoSec	*Information Security*
PCSS	*Process Control, Safety and Support*

Risikostyring for informasjonssikkerhet (ISO 27005)



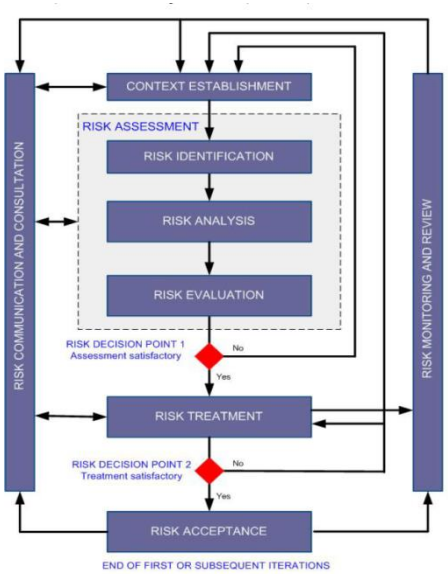
ISO 27005 information security risk management process

Risikovurdering (assessment) som påkrevet av ISBR #2 bruker metodologi utledet fra:

- ISO/IEC 27005
- Bruker NOG 123 for kritikalitetsvurdering.

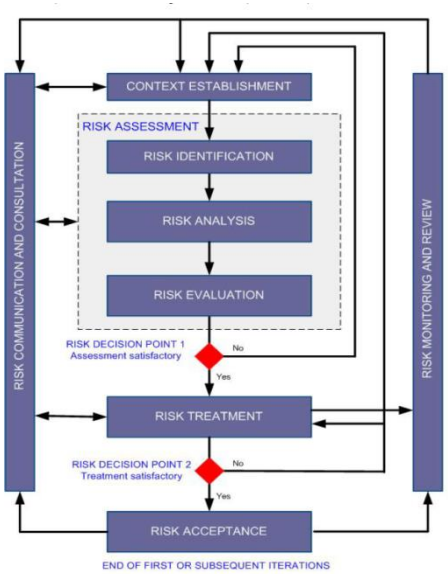
Risikostyring for informasjonssikkerhet (ISO 27005)

1. Initiering
   - Spesifisere og forberede grunnlaget for risikostyringen.
2. Identifikasjon;
   - Identifisere og vurdere aktiva, kritikalitetsvurdering.
   - Eksisterende kontroller
   - Sårbarheter og trusler som kan utnytte sårbarheter og medføre risiko.
3. Analyse og evaluering
   - Evaluere risiko, effekt på forretningsmål, etablere eierskap, prioritere risiko.
   - Spesielt fokus på relasjon til evt. safety-barriere risiko.
   - Kvantifisering av risk kan være en utfordring.
     - Hendelse med ukjent sannsynlighet og alvorlig konsekvens. (Stuxnet, Terrorisme) – forvente det uventedet.
4. Risikobehandling
   - Identifisere og beslutte handlinger, utarbeide handlingsplaner. Ytterligere sikkerhetskontroller.
5. Implementasjon og oppfølging
   - Effektiv oppfølging av handlingsplaner, og av risikobilde. Vedlikehold av kontroller og sikkerhetsmekanismer.



Risikostyring for informasjonssikkerhet (ISO 27005)

1. Initiering
   - Spesifisere og forberede grunnlaget for risikostyringen.
2. Identifikasjon;
   - Identifisere og vurdere aktiva, sårbarheter og trusler som kan utnytte sårbarheter og medføre risiko.
3. Analyse og evaluering
   - Evaluere risiko: sannsynlighet og konskevens for forretningens mål, etablere eierskap, prioritere risiko.
   - Spesielt fokus på relasjon til evt. safety-barriere risiko.
4. Risikobehandling
   - Identifisere og beslutte handlinger, utarbeide handlingsplaner. Ytterligere sikkerhetskontroller.
5. Implementasjon og oppfølging
   - Effektiv oppfølging av handlingsplaner, og av risikobilde. Vedlikehold av kontroller og sikkerhetsmekanismer.



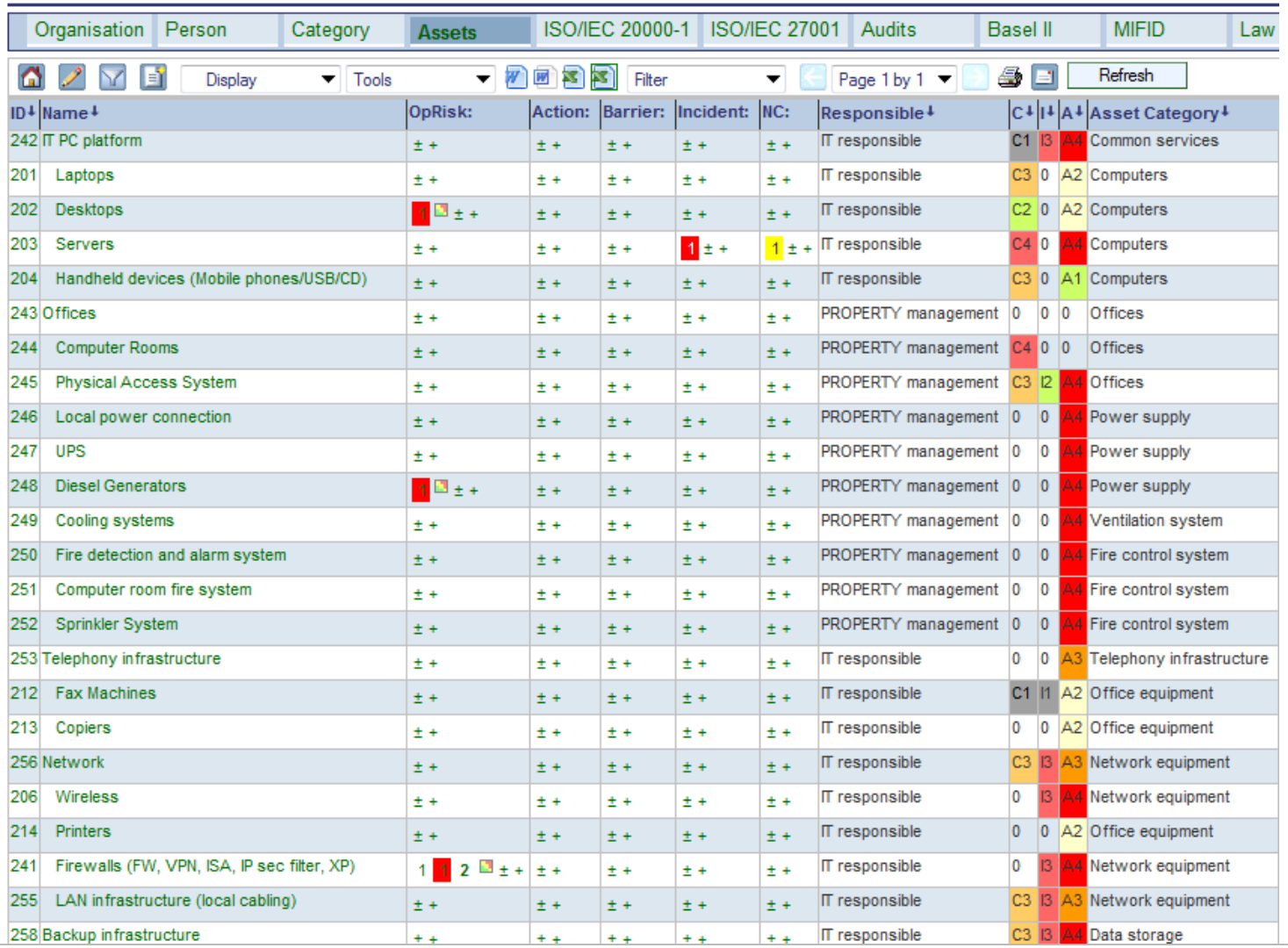
Risikostyring for informasjonssikkerhet og prosesskontroll (ISO 27005/NOG 104)

- Risikometodikken er spesifikk for informasjonssikkerhet, men har mye til felles med standard ISO 31000 tilnærming.
  - Hovedprosessen er den samme
  - Kritikalitetsvurdering er sentralt
  - Kartlegging av aktiva er utfordrende (sytstemer, funksjoner,nettverk)
  - Sårbarheter og trusler utenfra tillegges mer vekt i risikoanalysen
- Kritikalitetsvurdering med vekt på AIC
  - Hvilken effekt vil tap av tilgjengelighet, integritet og konfidensialitet ha.
- Risikostyring for PCSS/ICT (NOG104/123)
  - anbefaler å ta safety aspektet eksplisi

1. Helse og sikkerhet (safety)
   (inkludert SIL rating)
2. Miljø
3. Produksjonsregularitet , tilgjengelighet og integritet (AI)
4. Konfidensialitet (C)

System		Aggregated result
ESD/F&G System		Very high
Category	Criticality level	Rationale and comments
Health and Safety	Very high	The system handles health and safety related situations.
Environment	High	The system has impact on reducing spillages and emissions.
Regularity, Availability and Integrity	Medium	The fail safe nature of the system (e.g. automatic shutdown) can cause reduced production regularity.
Confidentiality	Low	The system does not handle production sensitive data.

Identifikasjon og vurdering av aktiva (EasyRisk Manager)



Organisation | Person | Category | **Assets** | ISO/IEC 20000-1 | ISO/IEC 27001 | Audits | Basel II | MIFID | Law

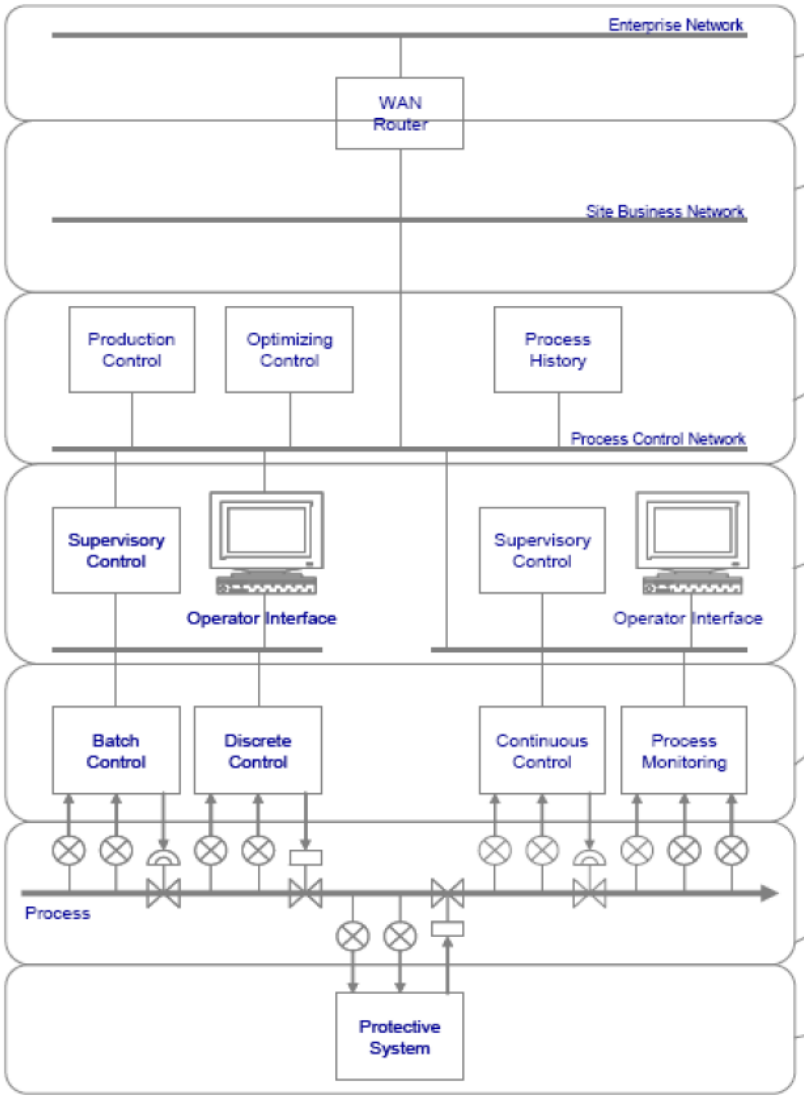
Display | Tools | Filter | Page 1 by 1 | Refresh

ID	Name	OpRisk:	Action:	Barrier:	Incident:	NC:	Responsible	C	I	A	Asset Category
242	IT PC platform	± +	± +	± +	± +	± +	IT responsible	C1	I3	A4	Common services
201	Laptops	± +	± +	± +	± +	± +	IT responsible	C3	0	A2	Computers
202	Desktops	1 ± +	± +	± +	± +	± +	IT responsible	C2	0	A2	Computers
203	Servers	± +	± +	± +	1 ± +	1 ± +	IT responsible	C4	0	A4	Computers
204	Handheld devices (Mobile phones/USB/CD)	± +	± +	± +	± +	± +	IT responsible	C3	0	A1	Computers
243	Offices	± +	± +	± +	± +	± +	PROPERTY management	0	0	0	Offices
244	Computer Rooms	± +	± +	± +	± +	± +	PROPERTY management	C4	0	0	Offices
245	Physical Access System	± +	± +	± +	± +	± +	PROPERTY management	C3	I2	A4	Offices
246	Local power connection	± +	± +	± +	± +	± +	PROPERTY management	0	0	A4	Power supply
247	UPS	± +	± +	± +	± +	± +	PROPERTY management	0	0	A4	Power supply
248	Diesel Generators	1 ± +	± +	± +	± +	± +	PROPERTY management	0	0	A4	Power supply
249	Cooling systems	± +	± +	± +	± +	± +	PROPERTY management	0	0	A4	Ventilation system
250	Fire detection and alarm system	± +	± +	± +	± +	± +	PROPERTY management	0	0	A4	Fire control system
251	Computer room fire system	± +	± +	± +	± +	± +	PROPERTY management	0	0	A4	Fire control system
252	Sprinkler System	± +	± +	± +	± +	± +	PROPERTY management	0	0	A4	Fire control system
253	Telephony infrastructure	± +	± +	± +	± +	± +	IT responsible	0	0	A3	Telephony infrastructure
212	Fax Machines	± +	± +	± +	± +	± +	IT responsible	C1	I1	A2	Office equipment
213	Copiers	± +	± +	± +	± +	± +	IT responsible	0	0	A2	Office equipment
256	Network	± +	± +	± +	± +	± +	IT responsible	C3	I3	A3	Network equipment
206	Wireless	± +	± +	± +	± +	± +	IT responsible	0	I3	A4	Network equipment
214	Printers	± +	± +	± +	± +	± +	IT responsible	0	0	A2	Office equipment
241	Firewalls (FW, VPN, ISA, IP sec filter, XP)	1 1 2 ± +	± +	± +	± +	± +	IT responsible	0	I3	A4	Network equipment
255	LAN infrastructure (local cabling)	± +	± +	± +	± +	± +	IT responsible	C3	I3	A3	Network equipment
258	Backup infrastructure	+ +	+ +	+ +	+ +	+ +	IT responsible	C3	I3	A4	Data storage

Hvordan jobber DNV med informasjonssikkerhet (ICS)

1. Risikostyring for informasjonsikkerhet
2. **Nettverk og topologi – design og implementasjon (teknologi)**
3. Rammeverk og forankring (personell og operasjon)

Risikostyring – nettverk og topologi



Level 5 - Enterprise
- Enterprise Financial Systems

Level 4 - Site Business Planning
- Site Production Scheduling
- Site Accounting

Level 3 - Site Manufacturing Operations
- Production Control
- Optimizing Control
- Process History
- Windows Domains

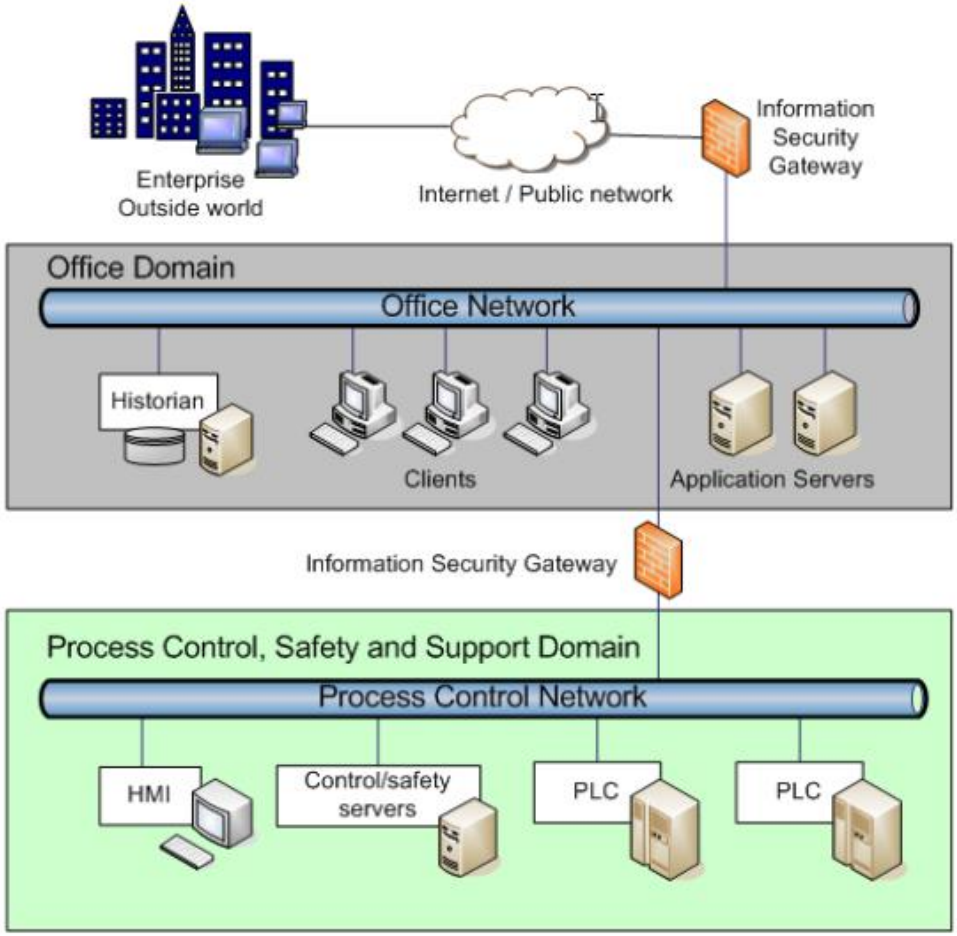
Level 2 - Area Supervisory Control
- Supervisory Controllers
- Primary Operator Interface

Level 1 - Basic Process Control
- Batch Controllers
- Continuous Controllers
- Discrete Controllers
- Process Monitoring

Level 0 - Field Instrumentation
- Sensors, Transmitters, Control Valves
- Field Networks (e.g. Foundation Fieldbus, Profibus)

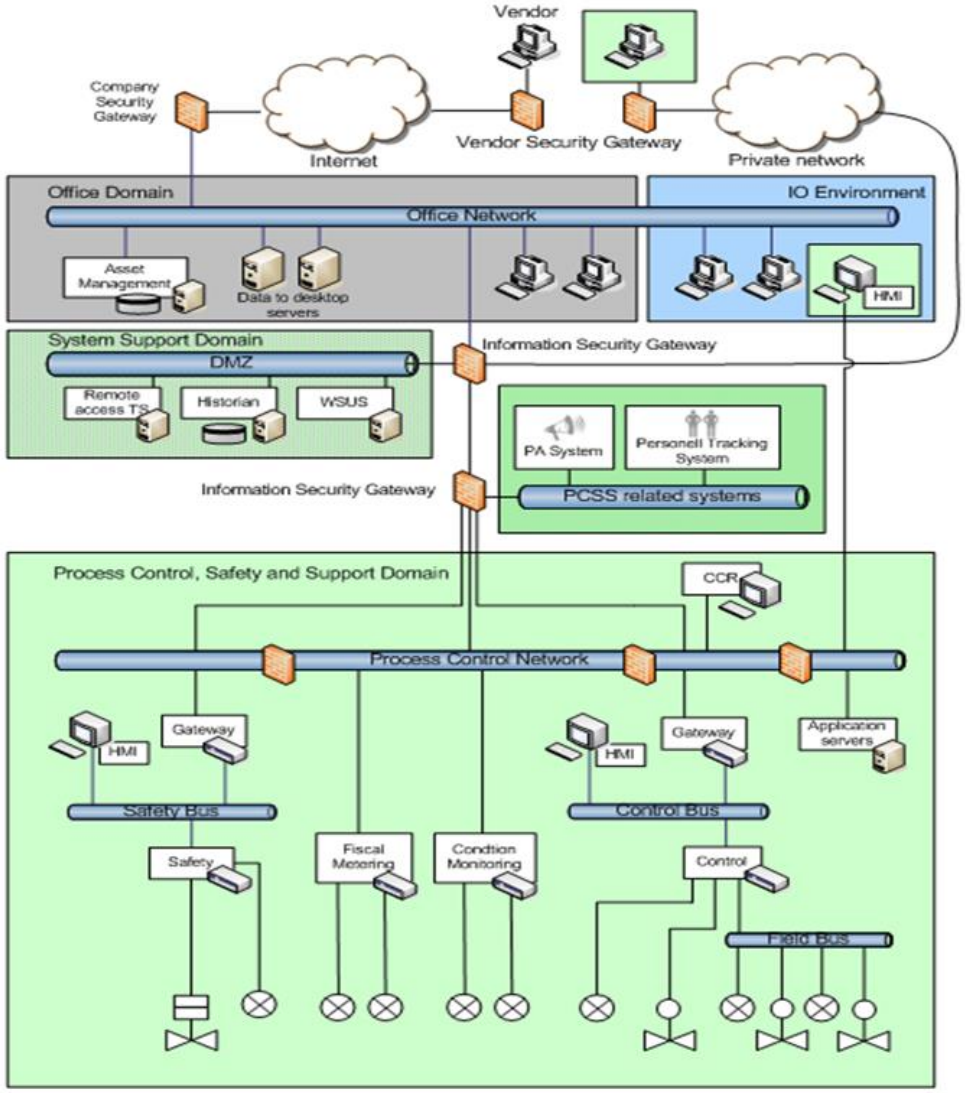
Safety-Critical
- Protective Systems
- Safety Instrumented Systems

Grunleggende arkitektur



- Behov for tilgang til data
- Beskyttelse av prosess

Teknologiske kontroller – nettverk og topologi



- soneinndeling og trafikk mellom soner (TCP/IP)
- brannmurer/dmz/routing
- tilgang fra onshore kontroll senter (IO) – inkl. kommunikasjonslinjer.
- kommunikasjon mellom office domene og ICS
- segregering av 3. parts systemer, og tilgang
- virusoppdatering og backup
- trådløst utstyr
- Intrusion Detection and Prevention Systems (IDS/IPS)
- hendelseshåndtering
- beskyttelse utenfra, og innenfra (misnøyd insider, men også manipulasjon, eller feil)

Hvordan jobber DNV med informasjonssikkerhet (ICS)

1. Risikostyring for informasjonsikkerhet
2. Nettverk og topologi – design og implementasjon (teknologi)
3. **Rammeverk og forankring (personell og operasjon)**

Rammeverk og forankring (personell og operasjon)

- Typiske tema:
  - Prinsipper (policy) og prosedyrer, og ledelsesengasjement.
  - Opplæring og sikkerhetsbevisthet
  - Adminstrasjon av sikkerhetsarbeid
  - Rutiner for kontroll og overvåking av tilgang (også fysisk)
  - Vedlikehold av prinsipper og prosedyrer
  - Endringshåndtering og kontroll
  - Disaster recovery
- Typiske sårbarheter
  - Svakheter/mangler i prinsipper (policy) og prosedyrer
  - Utilstrekkelige sikkerhetsprosedyrer
  - Utilstrekkelig sikkerhetsarkitektur og retningslinjer
  - Ingen eller svakt definerte operasjonelle prosesser
  - Utilstrekkelig opplæring/sikkerhetsbevissthet
  - Manglende audits

Innhold

1. Introduksjon
2. Safety & (information) security
3. Trusselbilde, myndighetenes fokus, regelverk og forventninger
4. Hvordan jobber DNV med informasjonssikkerhet
5. **Koblinger mellom safety og informasjonssikkerhet**
6. Oppsummering

Safety Risk Management in the Oil and Gas industry

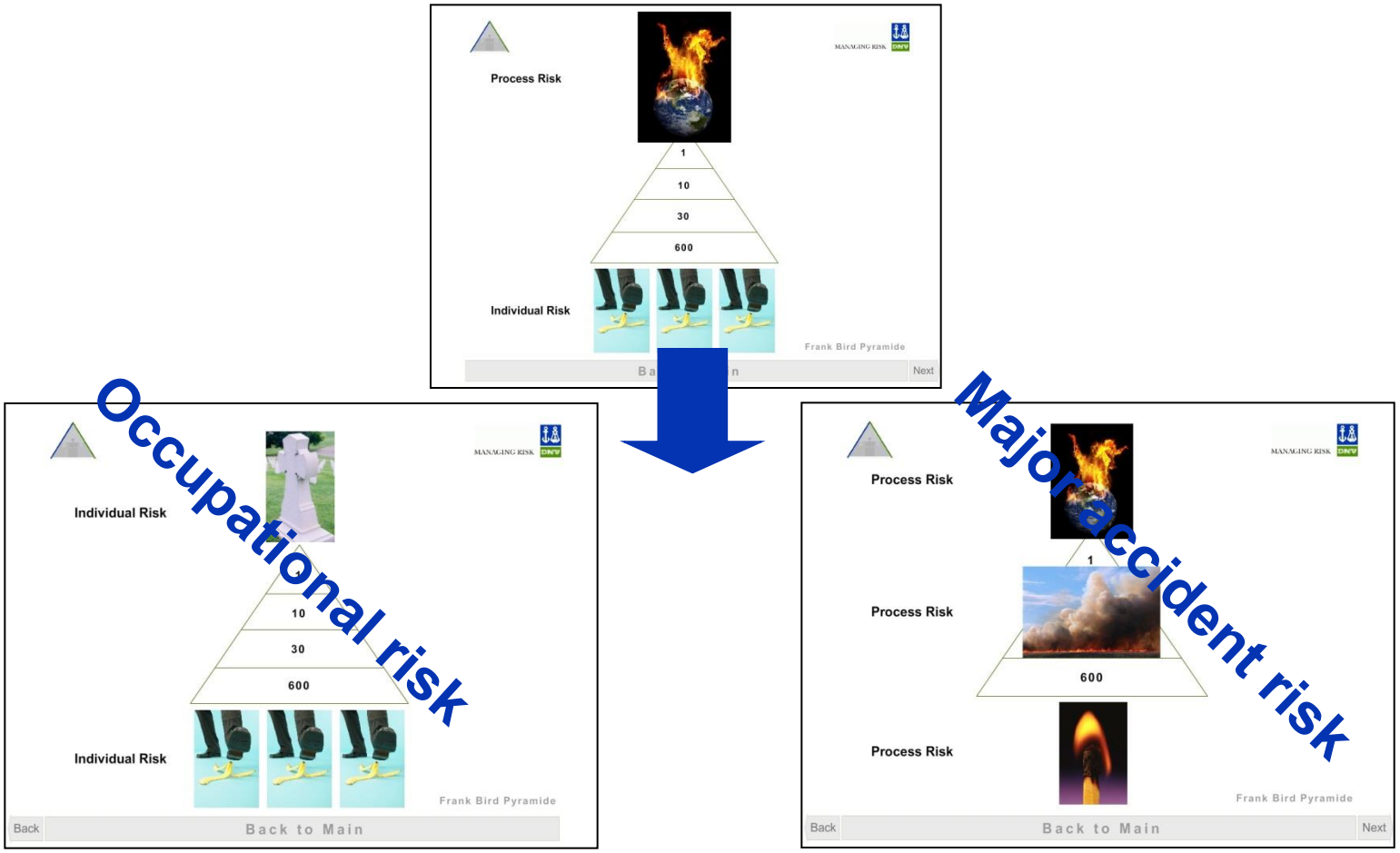
Major accidents…

- Complex set of causes
- Potentially catastrophic consequences
- Several barriers breached
- Potential for spreading and escalation

…and working accidents

- Simple cause and effect
- Normally limited consequences
- Few barriers breached
- A short «history»

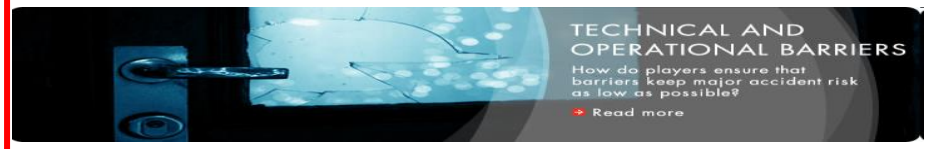
Storulykker styres av andre mekanismner enn de som styrer arbeidsulykke



Personal safety management

Prosess safety management

Barrierestyring er et element i (Safety) risikostyring



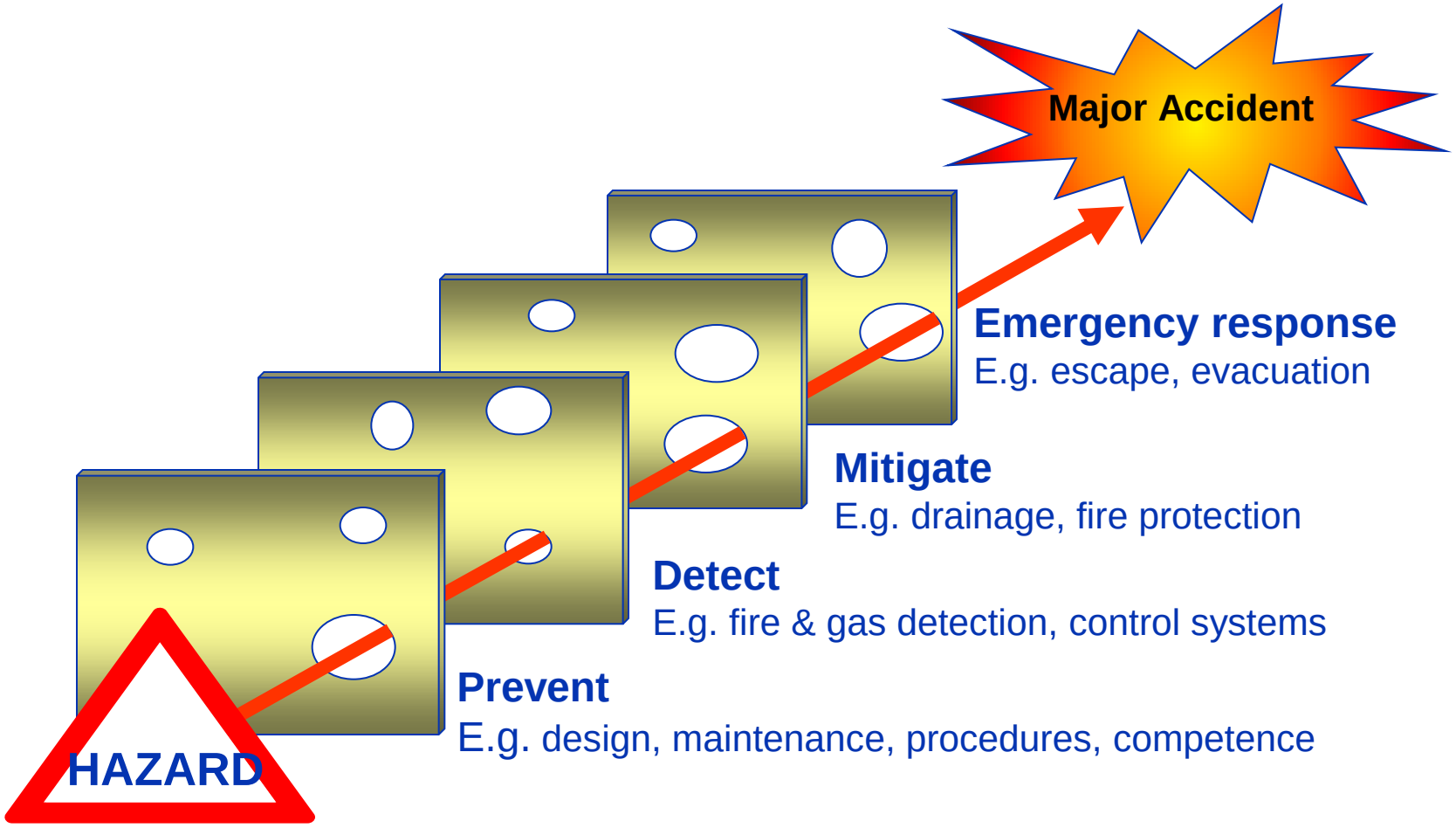
- **Barrierer**
  Barrierer skal ivaretas på en helhetlig og konsistent måte slik at risiko for storulykker reduseres så langt som mulig.

Hovedprioriteringer PTIL 2013

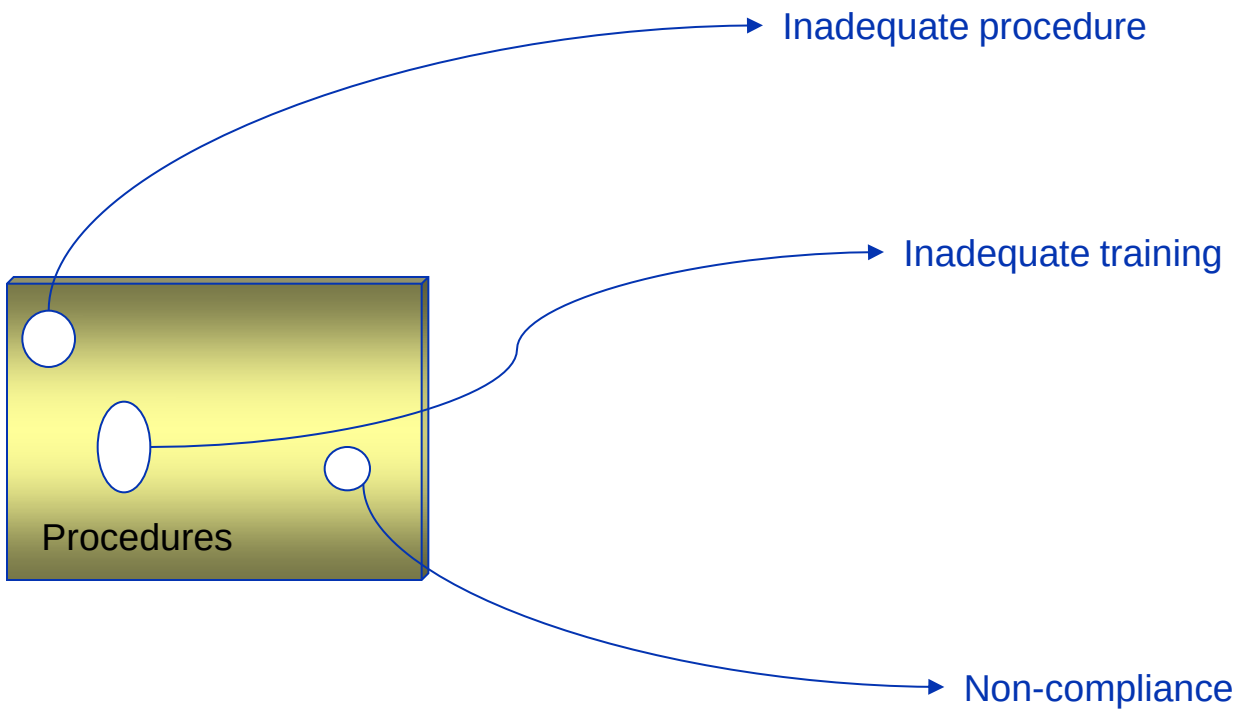
- Barrierer
- Ledelse og storulykkesrisiko
- Risikoutsatte grupper
- Ytre miljø

- Det skal være kjent hvilke barrierer som er etablert og hvilken funksjon de skal ivareta.
- Det skal være kjent hvilke barrierer som er ute av funksjon eller er svekket.
- Den ansvarlige skal sette i verk nødvendige tiltak for å rette opp eller kompensere for manglende eller svekkede barrierer.
- Noen barrierer er IT avhengige.
  - Alarmer
  - Kontrollsystem generelt (SIS)
- Kjennskap til barrierestatus IT avhengig

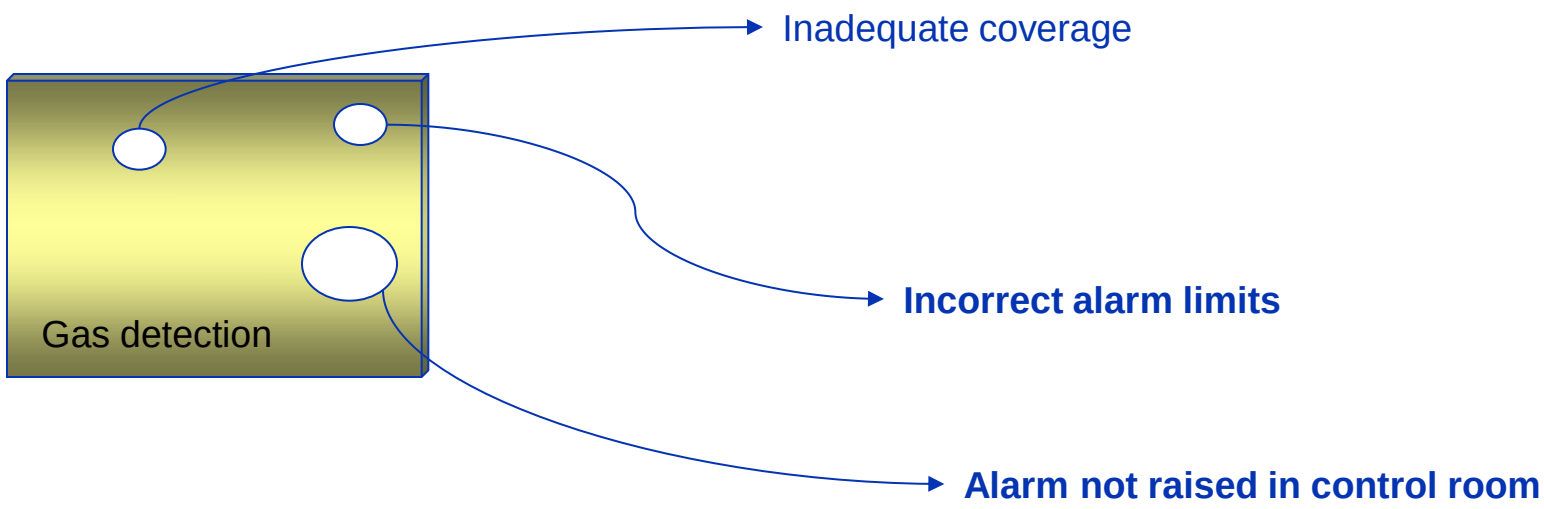
Swiss Cheese Model



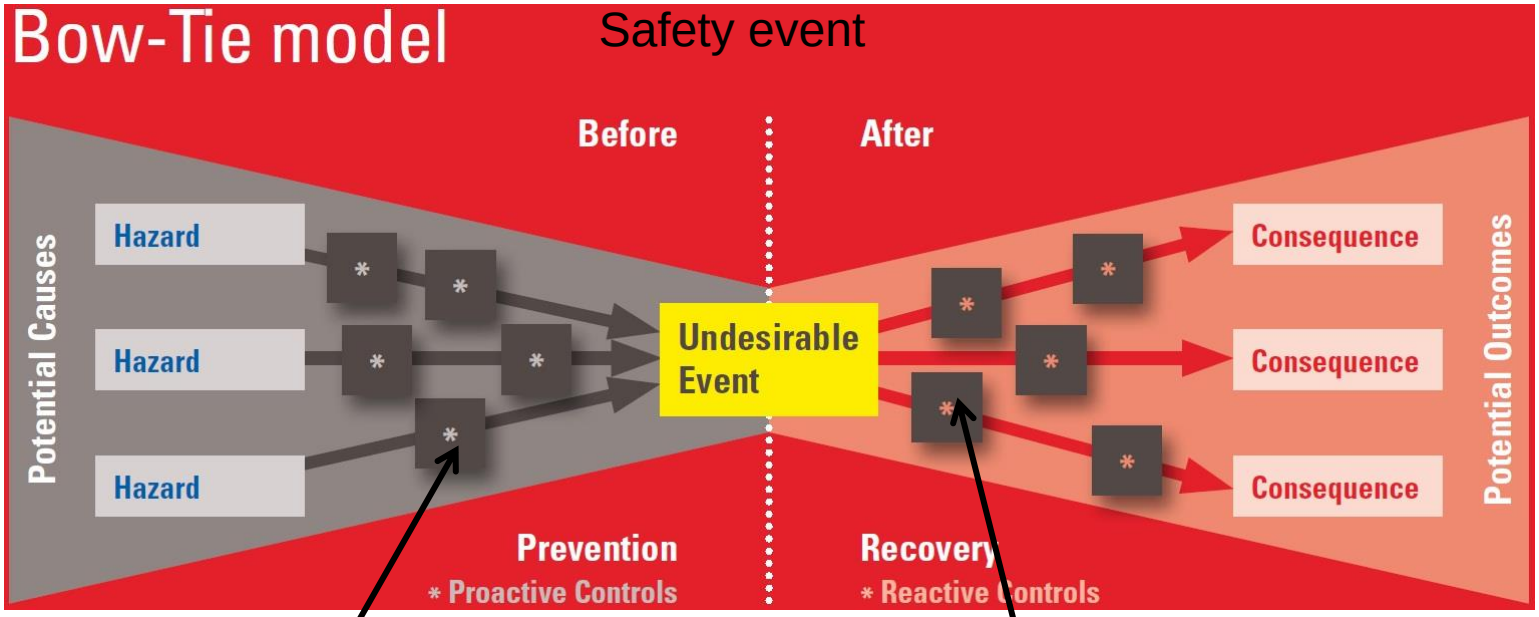
Barrierehull

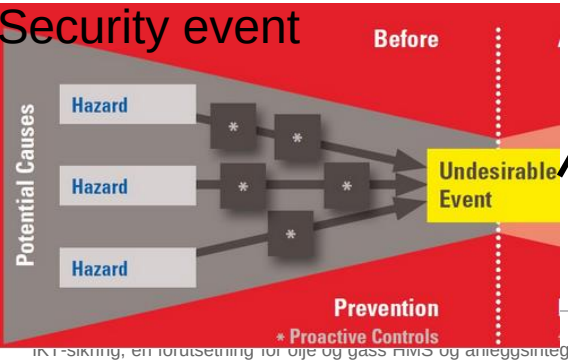


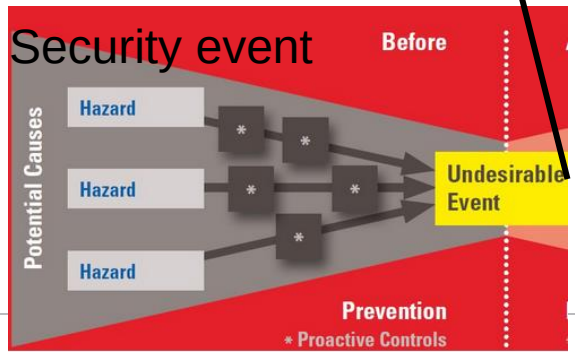
Barrierehull



BowTie –Safety effekt av en Security event



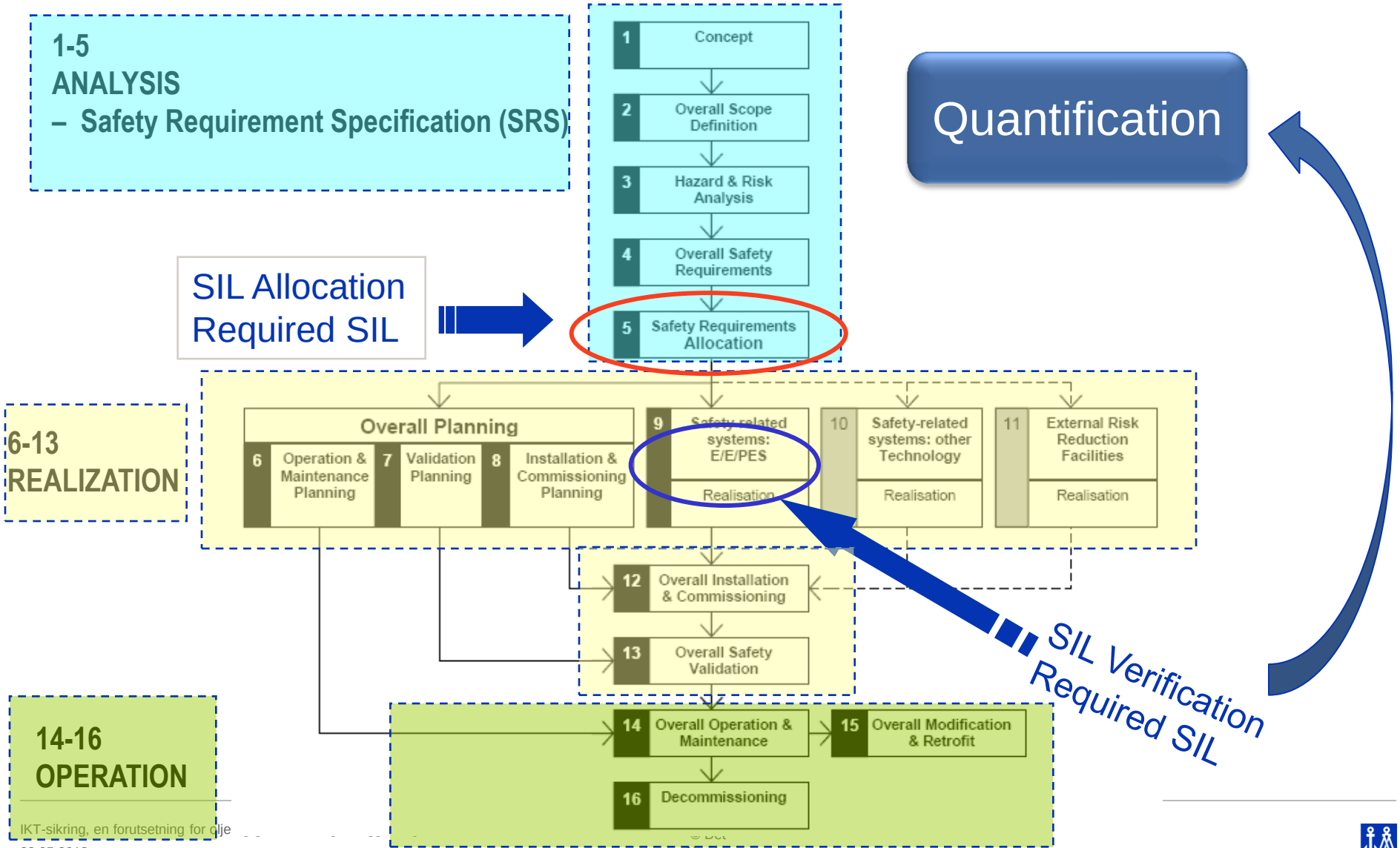




Informasjonssikkerhet – et viktig element i beredskap

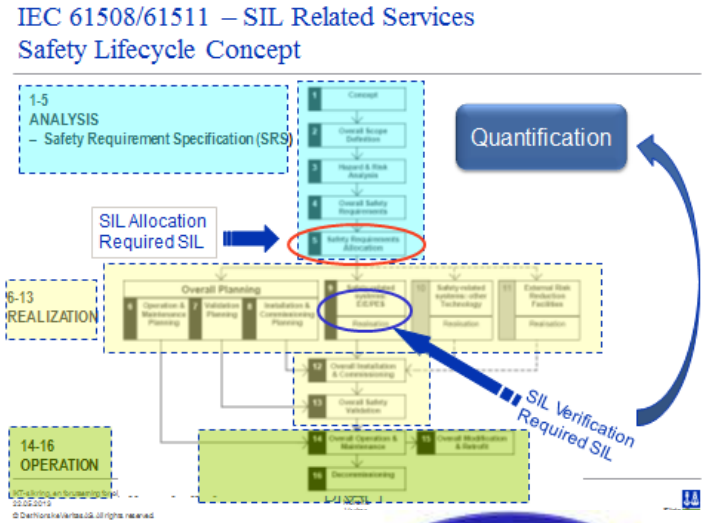
- Beredskap og gjenopprettelse etter hendelser
  - IT er en forutsetning for en velfungerende beredskapsorganisasjon.
  - IT beredskap (redundancy, backup og recovery) må være en del av beredskapsplanleggingen.
  - Gjenopprettelse etter informasjonssikkerhetshendelser, må også øves og testes.
    - ISBR #7: Disaster recovery plans shall be documented and tested for critical process control, safety, and support ICT systems. (Ref PTIL tilsyn 2012)

IEC 61508/61511 – SIL Related Services
Safety Lifecycle Concept



Safety og Security prosesser kan understøtte hverandre.

- Safety syklus (IEC 61508/61511)
  - Analyse
  - Realisering
  - Operasjon
- Security syklus (IEC 62443-2-1)
  - Asess (Risikovurdering),
  - Develop (CSMS)
  - Implement and maintain
- Kombinert safety og security risikovurdering:
  - Inkluder *security* i risiko identifisering
    - (HAZID/HAZOP, CHAZOP, FMEA)
  - Inkluder *security* avvik og feilmodi. (nettverksstorm, DoS, etc.)
  - Identifiser evt. common mode failures.
  - Estimer sannsynlighet og konsekvens – prioritet på safety.
- Layer of Protection analysis (LOPA), kompatibelt med Defence in Depth



Trenger vi ICS-security når vi har et SIS?

- Safety Instrumented systems (SIS) en del av ICS, "kronjuvelen" i samlingen.
  - SIS består av kompenserende kontroller for å unngå farlige situasjoner (ESD, PSD, F&G)
- SIS og Safety fokuserer på beskyttelse mot ikke-intendert hardware feil
- security har et bredere fokus: - brukerhandlinger, intenderte trusler, nettverksfeil, applikasjonsvakheter
- SIS og ICS avhengigheter
  - SIS resten av ICS deler gjerne teknologisk plattform. ICS sårbarheter kan medføre kompromittering av SIS.
  - SIS må kommunisere mot resten av ICS for å kunne utløse safety funksjoner – kan ikke være frakoblet, segregering (isolasjon) blir viktig.
  - SIS blir i økende grad integrert opp mot IP baserte nettverk – øker eksponeringsflaten.
- Et ICS/SIS som er kompromittert er ikke lenger sikkert!
  - forsåLoss/Manipulation of View/Control, Wrong control signals, MitM
- Uønsket nedstengning av anlegg uten safety konsekvens,har likevel store økonomiske konsekvenser. .

Safety og security - koblinger

- ICT-security nært knyttet til HMS - forankret i myndighetskrav og forskrifter
- Barrierestyring og storulykke - IKT sikkerhet er et viktig element
  - Noen barrierer er IKT avhengige, eller sårbare gjennom å være koblet opp.
  - Fungerende IKT er en forutsetning for at man kan ha kontroll med barrierenes status
  - SIS (Safety Instrumented Systems) er kritiske og trenger beskyttelse. Uavhengighet/isolasjon.
- Beredskapsplaner
  - IKT sikkerhet både som forutsetning og del av planene.
- Prosesser for safety (IEC 61508/11) og security (IEC 61234) kan med fordel integreres, støtte og berike hverandre
  - Risikoanalyse er basis for arbeid både med safety og med med informasjonsikkerhet. En integrert tilnærming kan være verdifull.
- Oppfyllelse av en del av sikkerhetskravene (i NOG 104) kan implementeres gjennom eksisterende safety regime på sokkelen.
  - Sikker jobb analyse og arbeidstillatelser for oppkobling av utstyr
    - Ta høyde for IKT sikkerhetssrisiko i analysen
  - Tilgang til systemer.

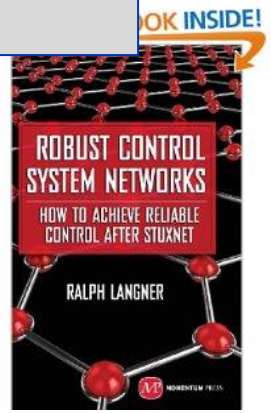
En alternativ tilnærming: *cyber robustness*.

- Risikoevaluering (security) avhengig av forutsigelser om fremtidige hendelser.
  - Ikke kvantifisert og basert på reliability data som for safety analyse.
  - Vanskelig å forutse trusler basert på mulig adferd fra en angriper (ikke engineering)
- Hvordan ta høyde for det uforutsette og svært usannsylige (Stuxnet, 9/11, etc) Paradigmeskifte:
  - Risk ➔ Fragility
  - Security ➔ Robustification

Robusthet er evnen til å fortsette normal operasjon til tross for uforutsette omstendigheter, evnen til å motstå endring i prosedyre eller omstendigheter, og evnen til å håndtere variasjon i (de operasjonelle) omgivelsene, med minimal eller liten skade, endring eller tap av funksjonalitet.

  - Et robust kontrollsystem er i stand til å håndtere
    - "naturlige/tilfeldige" variasjoner og feil.
    - variasjon som følger av security hendelser, angrep eller forsøk på angrep.
  - Tese: Et robust system ville kunne motstå et Stuxnet lignende angrep
    Standard information security kontroller kunne det ikke.

Robust Control System Networks – How to achieve reliable control after Stuxnet. Ralph Langner

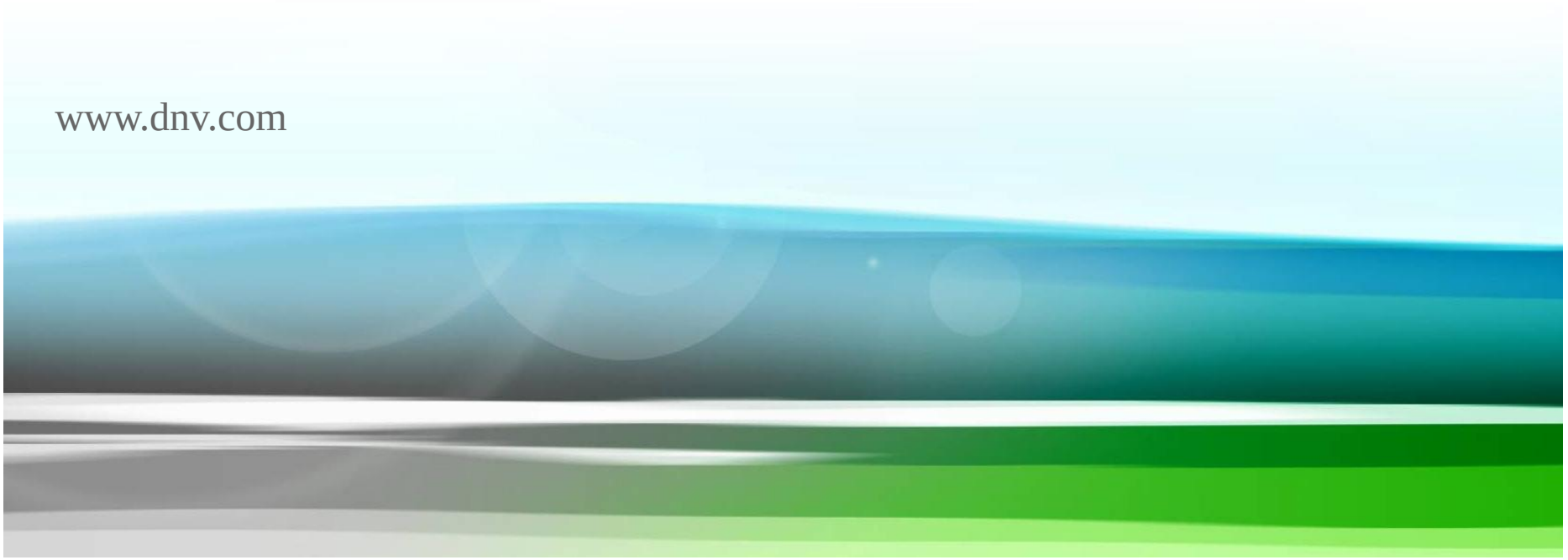


Oppsummering

- "Er det mulig se safety og security som to viktige elementer i en større sammenheng?"
- Det er mange berøringspunkter og muligheter for gjensidig berikelse mellom Safety og Security
- Et primært siktemål for security arbeidet er å ivareta safety
- En utfordring er å ikke snakke forbi hverandre, viktig å være klar over ulikhetene mellom disiplinene.
- Det må være en balansert tilnærming: I enkelte tilfeller kan det være motstridende interesser mellom IKT-sikkerhet og safety. F.eks: nødprosedyrer må ikke forsinkes gjennom komplekse systemer eller rutiner for adgangskontroll.
- Vi lever i en verden. I en verden med et økende trusselnivå er det viktigere enn noen gang med samarbeid på tvers av disipliner for å oppnå sikre systemer og unngå hendelser enten årsaken er feil på utstyr/ulykke, eller ondsinnete trusler.

Safeguarding life, property and the environment

www.dnv.com



MANAGING RISK

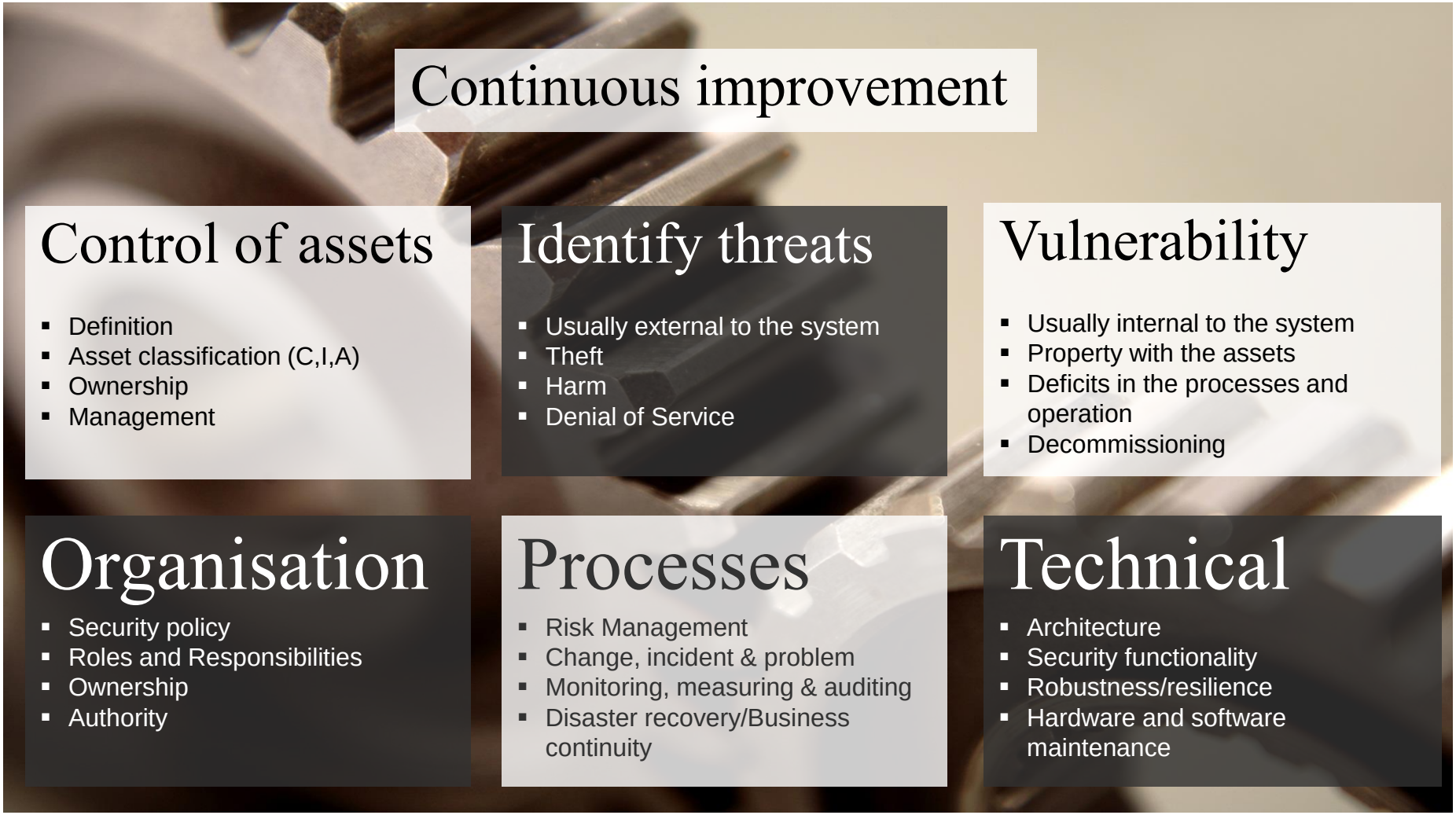
Cyber security – definitions

Cyber security (Wikipedia)

- Computer security is a branch of computer technology known as information security as applied to computers and networks.
- The objective of cyber security includes protection of people*, environment*, information and property theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.
- The term “cyber security” often used in military context and related to systems* that used to be separated from Internet

*Process control and SCADA systems

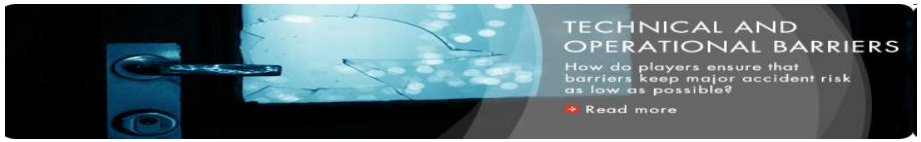
Information Security Management System (ISMS - ISO/IEC 27001)
Cyber Security Management System (CSMS - IEC 62443)



Is it safe to do it here? I really really have to…

Oh! What a relief!
By the way, is this place properly secured?

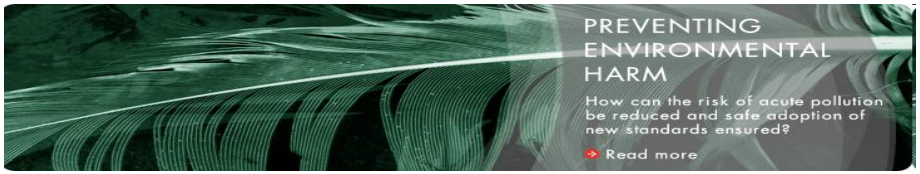
PSAs prioritised areas



- **Barriers**
  Safety barriers must be maintained in an integrated and consistent manner in order to minimise the risk of a major accident.

- Management and major accident risk
  Management at all levels in the industry must work to reduce the risk of major accidents, and ensure that such efforts are made in an integrated manner.

- Groups exposed to risk
  Reduce the risk of injury and ill health for particularly vulnerable categories of petroleum industry employees to the lowest possible level.



- Natural environment
  The industry must work purposefully to prevent accidents which can cause acute discharges.The players must also work to reduce greenhouse gas emissions from the Norwegian petroleum industry.

Defs

- **Safety/Security**(Merriam Webster)
  - Safety : the condition of being safe from undergoing or causing hurt, injury, or loss
  - Security:
    1. the quality or state of being free from danger
    2. measures taken to guard against espionage or sabotage, crime, attack, or escape
- A **Safety Instrumented System (SIS)** consists of an engineered set of hardware and software controls which are especially used on critical process systems. (Wikipaedia)

Typer av angrep og mulige konsekvenser

- DOS eller network storm => SIS systemer fail to safe state => downtime
- Hijacking malware (Botnet) => lack of responsiveness, erratic behavior.
- MitM attack => manipluation of view/control => possibly severe consequences.

- "Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.)."

Texas City Refinery explosion

- Eksplosjon ved BP raffineri i Texas City (2005)
- En del av årsaken var feil og mangler ved alarmer og nivå indikatorer som medførte overoppfylling.
- Hydrokarbonsky ble antent og eksploderte.

Innhold – detaljert

1. Introduksjon
2. (Disposisjon)
3. Safety & (information) security
   1. Safety & Security
   2. Informasjonssikkerhet i prossessanlegg (ICS)
   3. Safety vs. security, hovedforskjeller
   4. IT og ICS standarder.
4. Trusselbilde, myndighetenes fokus, regelverk og forventninger
   1. Internasjonalt
   2. APT
   3. Defence in depth
   4. Norske myndigheter og PTIL
   5. Regleverk og forventninger
5. Hvordan jobber DNV med informasjonssikkerhet
   1. Risikostyring for informasjonsikkerhet
   2. Nettverk og topologi – design og implementasjon (teknologi)
   3. Rammeverk og forankring (personell og operasjon)