



DNV

WHEN TRUST MATTERS

Avoid Cyber task overload with use of human factors insights

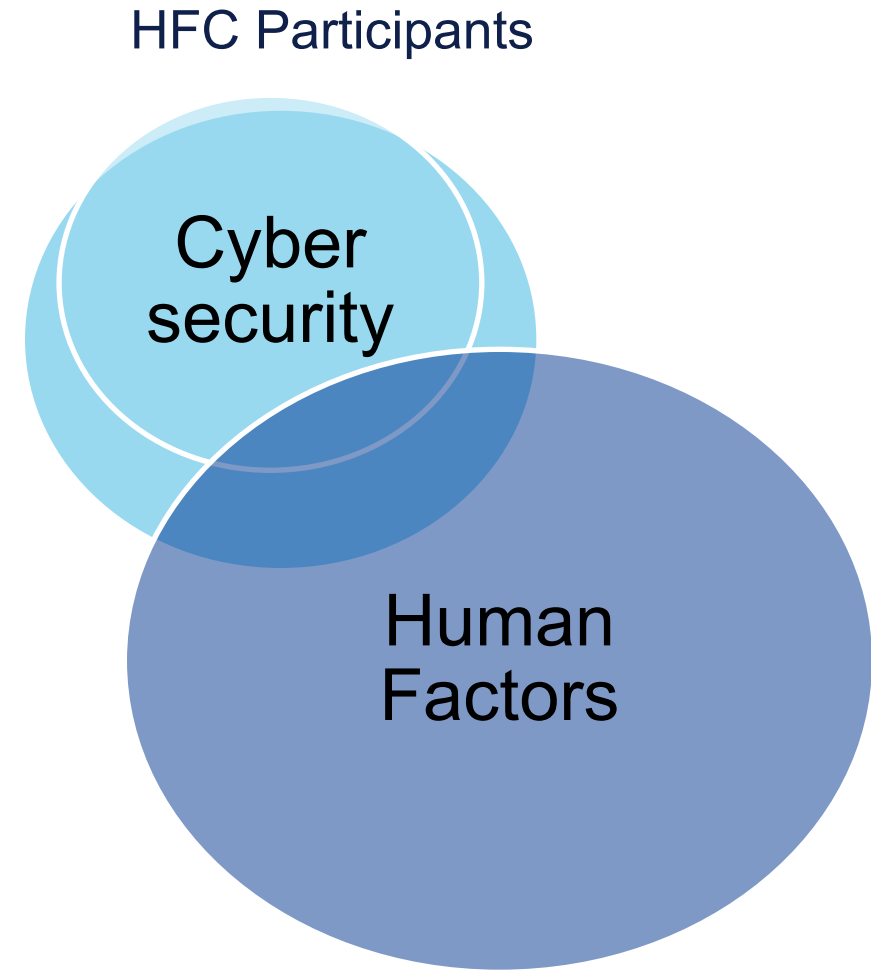
HFS forum-Et systemperspektiv på sikring og beredskap
Tirsdag 17. og onsdag 18. oktober 2023

Anne Wahlstrøm, Senior Principal OT Cyber Security Consultant, DNV



Agenda

- Some definitions and context for OT cyber security
- Human role and performance shaping factors in a cyber security context
- HF methods in Security operations center (SOC) and within Cyber security

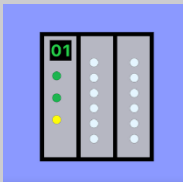


IT and OT



Information Technology (IT) is the tools and system we use in a daily work in an office environment.

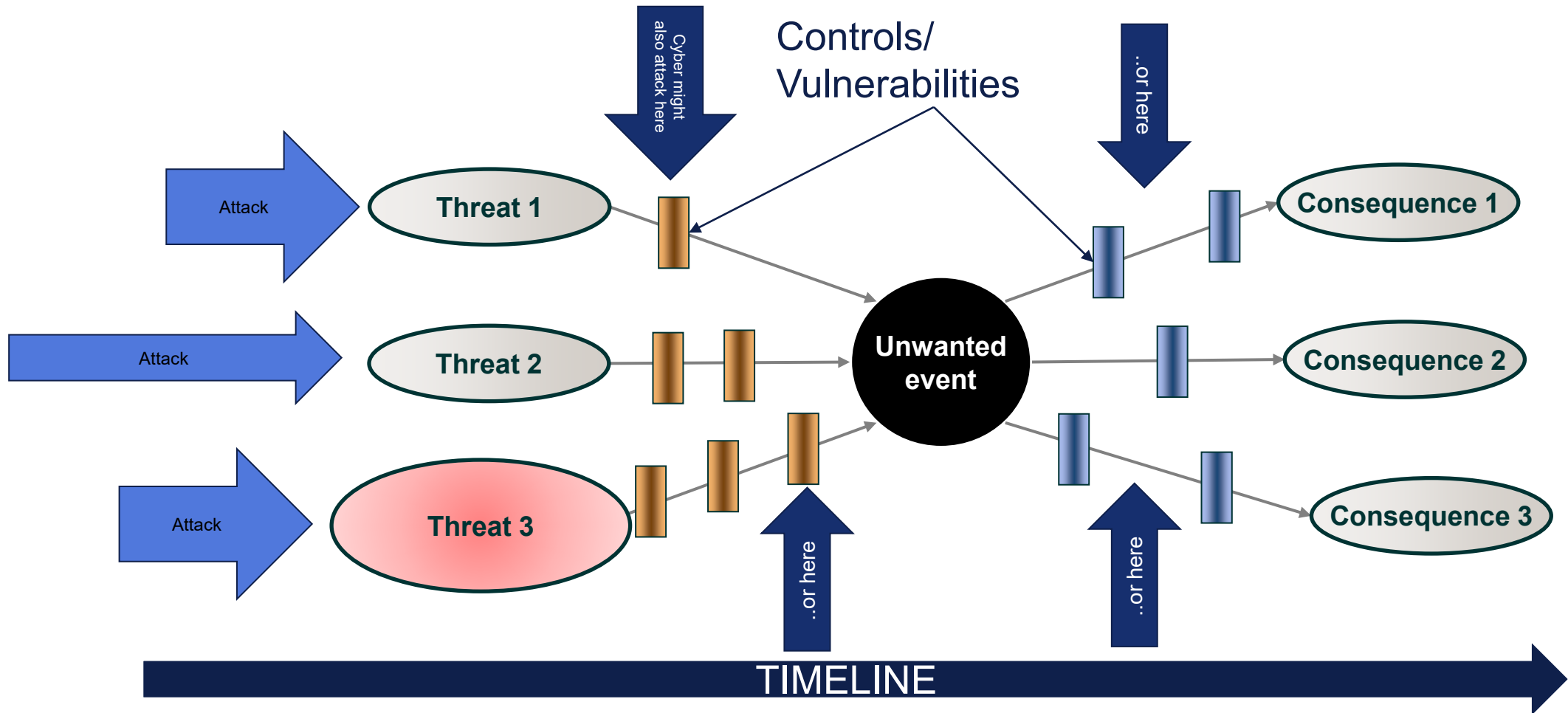
Confidentiality, Availability, Integrity



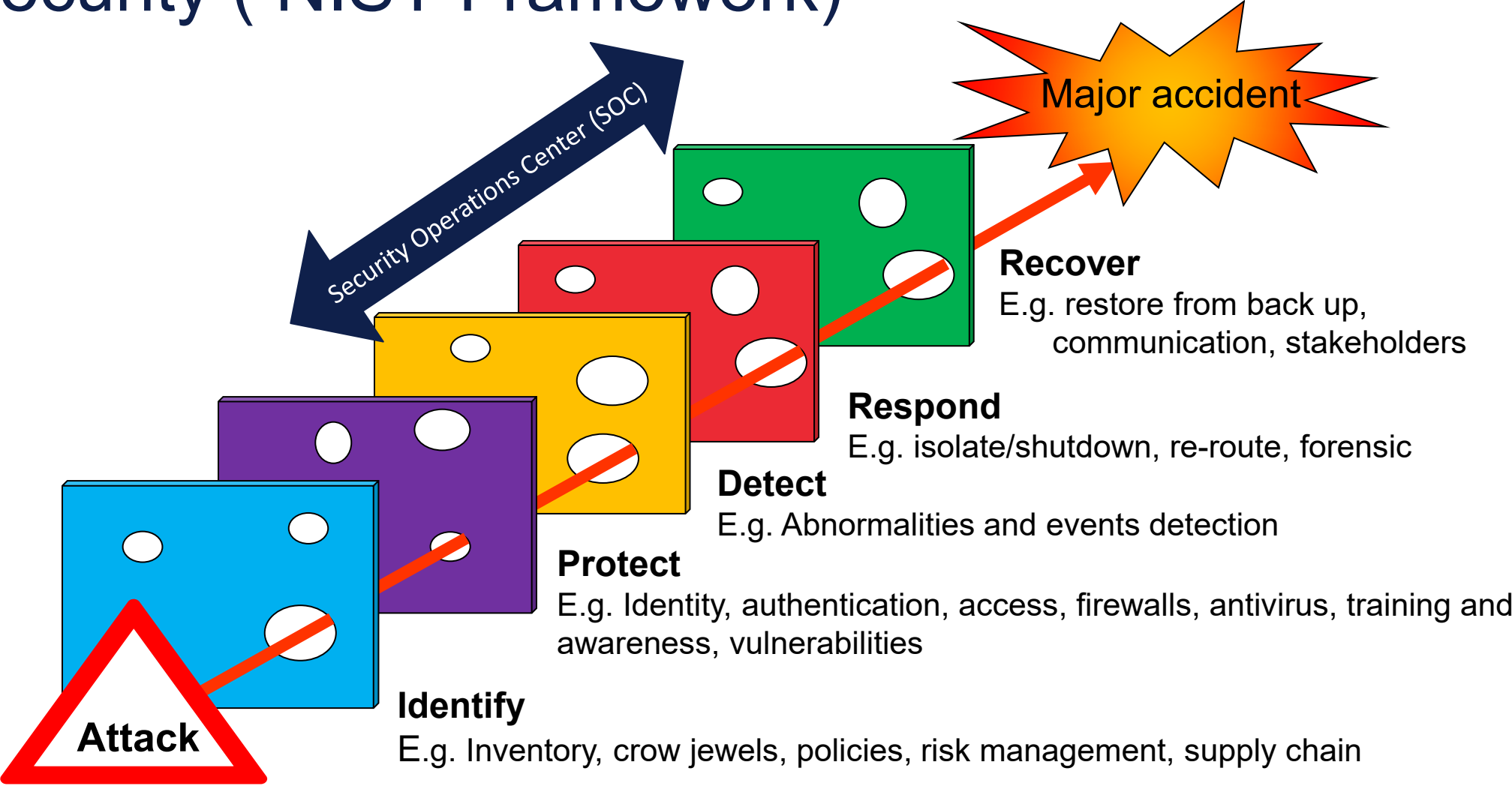
Operational technology (OT) is the systems that controls the production processes and its safety and integrity e.g. ICS, telecom, 3rd party systems.

Confidentiality, Availability, Integrity

Safety + cyber security



Cyber security (NIST Framework)



Some definitions and similarities....

• Occupational risk

- Owned by HSE manager
- Can count
- Management system in place
 - Defined in risk matrix
 - System for reporting incident

• Major accident risk

- Multiple owners
- Impaired barriers
- On NCS O&G barrier management is in place
 - Often not explicitly defined as category in risk matrix
 - System for reporting impaired barriers

• IT cyber security risk

- Owned by IT
- Can count
- Information Security Management system (ISMS)
 - Training is in place
 - Reporting and handling is in place

• OT cyber security risk

- Multiple owners
- Impaired barriers
- Often not include in ISMS
 - Training is not in place
 - Reporting and handling is often unclear

...and different practices ☹️.....


Ignitions source control

- A. Control of all ignition sources onboard
 - Design- zones and classification
 - Maintenance- PFP of hot surfaces
- A. Able to isolate out
- B. Overpressure in critical rooms to prevent gas ingress
- C. If hotwork
 - Use of habitat
- E. Operation
 - Need permission when using temporary equipment or bringing new ignitions sources onboard

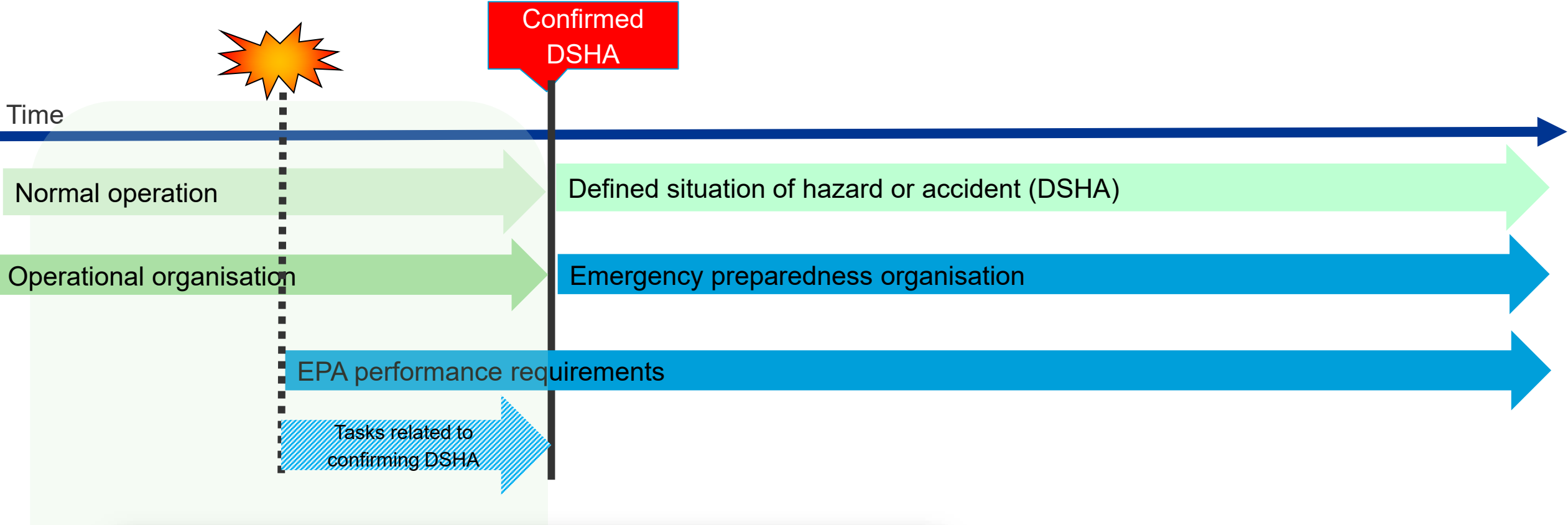
OT cyber security

- A. Control of all data access points onboard
 - Design- segmentation and zones&conduit
 - Maintenance- Antivirus and patching
- A. Able to isolate out= island mode
- B. Closing off critical servers/rooms to prevent access
- C. If file transfer
 - Service laptops= use of staging network
 - USB= deviation and needs to be checked
- E. How to control service laptops and USB used/brought onboard?

...due to lack of clear responsibility and identified competence requirements!

Role	Responsibility	Competence requirements based on Blooms taxonomy			
		Knowledge	Skills	Behaviour	
Instrument	Modification/update	Understand cyb...	<ul style="list-style-type: none"> Ensure file transfer is done ... that has ... and latest ... USB 	"Never use a USB I find"	
CCR operator	OT Cyber s... event	 <p>"Training awareness"</p>		... formal	"First thought should be if we are under attack, secondly that it can be a technical failure"
	Potential incident			... files in OT	... to support our

Emergency preparedness Safety vs Security



Additional findings from the 2021 report include:

- **Time to respond:** The average time to detect and contain a data breach was 287 days (212 to detect, 75 to contain) – which is one week longer than the prior year report.

CCR operator vs SOC analyst

- Control room operators and Security operations center (SOC) analysts have many similar characteristics in their work environment
 - Many different repeating manual tasks
 - Expert level with regards to competence
 - Need to understand multiple different operational modes
 - Key input to operational decision processes
 - HMI
 - High level of stress and pressure
 - Shift work
- OT SOC will also need in-depth knowledge of process and safety controls**

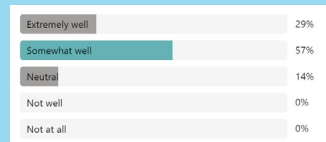


We have robust knowledge about how human factors influence the reliability and performance of operators working in control rooms
(Petro-HRA)

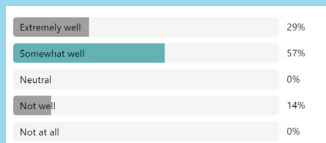


Survey- Factors influencing human performance in SOC

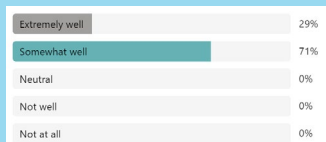
1. How well is your SOC design accounting for ergonomics and working environment needs?



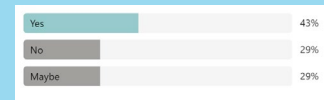
2. Are the dashboards/displays designed in such a way that they support the analysts' tasks?



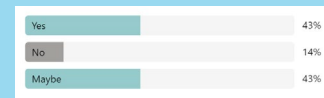
3. Are key alarms (a selection of high priority alarms) identified and presented in a manner that supports rapid detection under all alarm conditions?



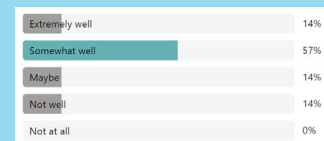
4. Are periods of high and low mental workload within acceptable limits?



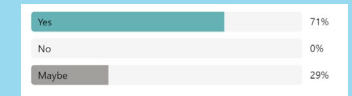
5. Does procedures and work description/instructions support handling of abnormal situations?



6. Are analysts trained in all conditions including abnormal situations?



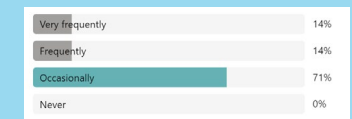
7. Are experience and information from incidents used in the re-training of analysts?



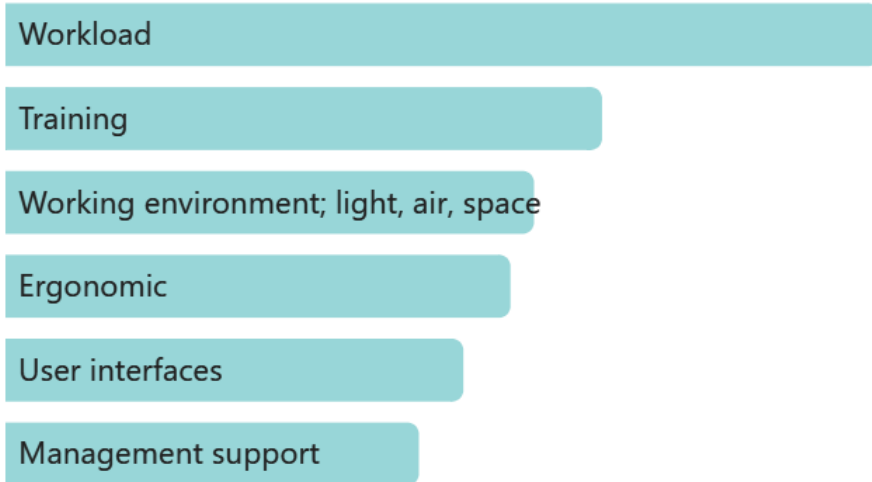
8. Is there an attitude of non-penalization and organizational learning if an analyst makes an error?



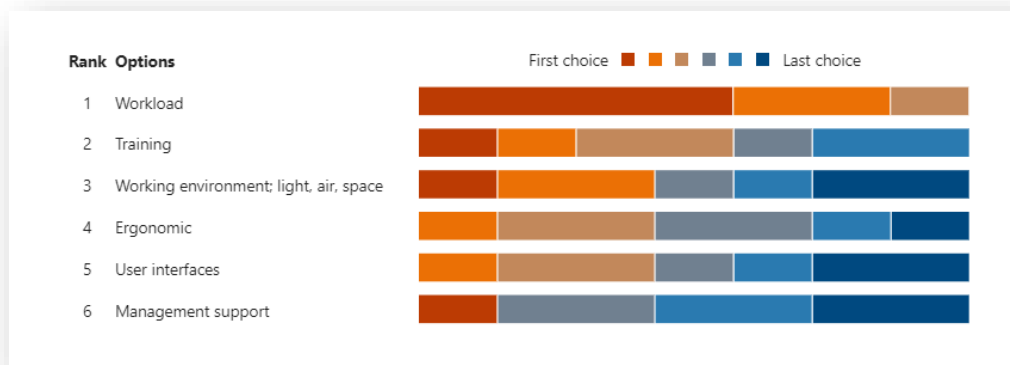
9. To what degree is a lack of contextual information inhibiting fast triage?



How would you rate the importance of the following factors influencing human performance?

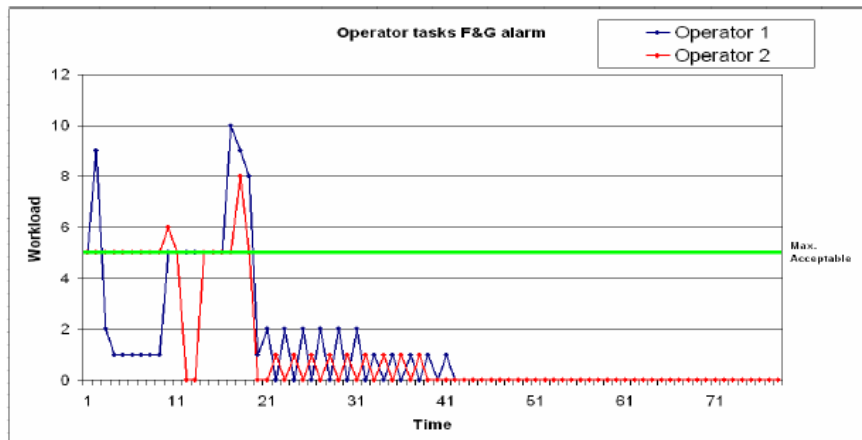


- Consequences of not accounting for PSF's
 - Burnout
 - Longer remediation times
 - Wrong decisions
 - Worsening of consequences
 - In an OT setting potential escalation to a major accident scenario



Workload analysis

- Description:
 - A systematic analysis of physical and/or cognitive demands imposed on operator or team of operators
- Goal:
 - Ensure that operator mental workload is optimized (avoiding underload and overload)
- Result:
 - Overview of expected mental workload during shift
 - Provides insight into requirements for operators, manning levels and distribution of tasks



Scenario 7 – ICT and SAS systems breakdown and loss of communication

Scenario Description

The ICT system and main part of the SAS system have a common failure.

The common failure could be loss of power, loss of communication or stop of several critical systems.

The failure could be due to someone connecting faulty or misconfigured ICT equipment to the network or equipment infected with a virus. The faulty equipment could be a PC with an error flooding the network with unanticipated traffic.

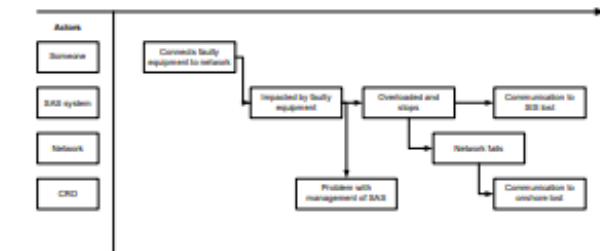
The result could be network overload (denial of service) or virus being spread from the infected equipment, impacting several systems and/or infrastructure such as the communication network. The scenario could impact and stop the safety and automation system (SAS) or impact safety instrumented systems (SIS). Communication based on high speed data network between onshore and offshore could be lost, influencing ICT systems, video communication and telephony.

The CRO may lose control of part of the process, and some part of the system may degrade to an unsafe condition. The breakdown could influence common situational awareness among the different actors involved and lead to serious errors.

Main Steps of the Scenario

1. Someone connecting faulty equipment (e.g. PC) into the network
2. SAS system is impacted and parts of the system stops
3. CRO has problems with management of the SAS system
4. SAS system stops, problem with communication to SIS
5. Network fails and high speed data network between onshore and offshore is closed down
6. Communication onshore (ICT, Video, telephony) lost

STEP



HF Methods we can use

Security operations center

- SOC design by use of CRIOP
- Human Machine Interface and large screen
- Alarm prioritization and management

Individual/organisation

- Competence requirements
- Competence building
- Emergency training
- Mental workload assessment

Task

- Functional analysis and allocation
- Security critical task analysis
- Workload analysis
- Human Reliability Analysis
- Human tasks in a barrier context

Environment

- UX design
- Security Cultural assessment

Questions?

Anne.Wahlstrom@dnv.com

+47 913 75 502

www.dnv.com

