Measurement and improvement of Information security and safety culture

S. O. Johnsen, M.B.Line/SINTEF

Y.Nordby, C.W.Hansen/NTNU

At 2005 Asia-Pacific conference on Risk Management and Safety

CheckIT

- Introduction – SINTEF
- Background and context
- Challenges
- Suggested methodology - CheckIT
- References

SINTEF - NTNU and UiO

- **SINTEF, Research foundation with 1,800 employees closely affiliated with :**
  - **The Norwegian University of Science and Technology**, NTNU:
    - 20 000 full-time students, 973 scientific employees
  - **University of Oslo, UiO,** Faculty of Mathematics and natural sciences:
    - 4500 full-time students , 518 scientific employees
- **NTNU and the SINTEF Group Collaboration in R & D**

SINTEF

Technology for a better society

CheckIT

- Introduction – SINTEF
- Background and context
- Challenges
- Suggested methodology - CheckIT
- References

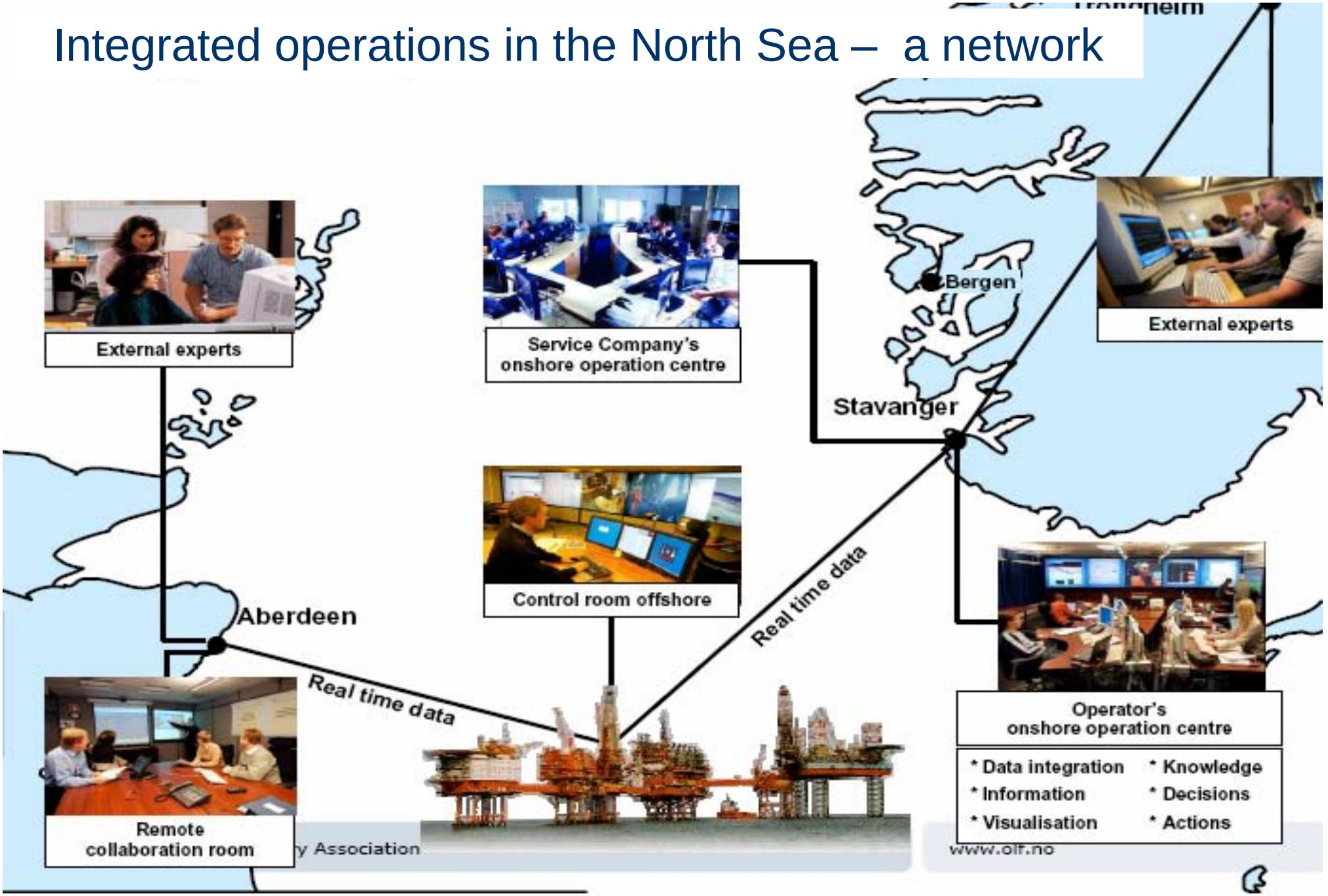
Background

- At present there is a major thrust in the North Sea to improve Oil recovery and reduce the total costs by implementing Information Technology in the value chain (the initiative is called Integrated Operations)

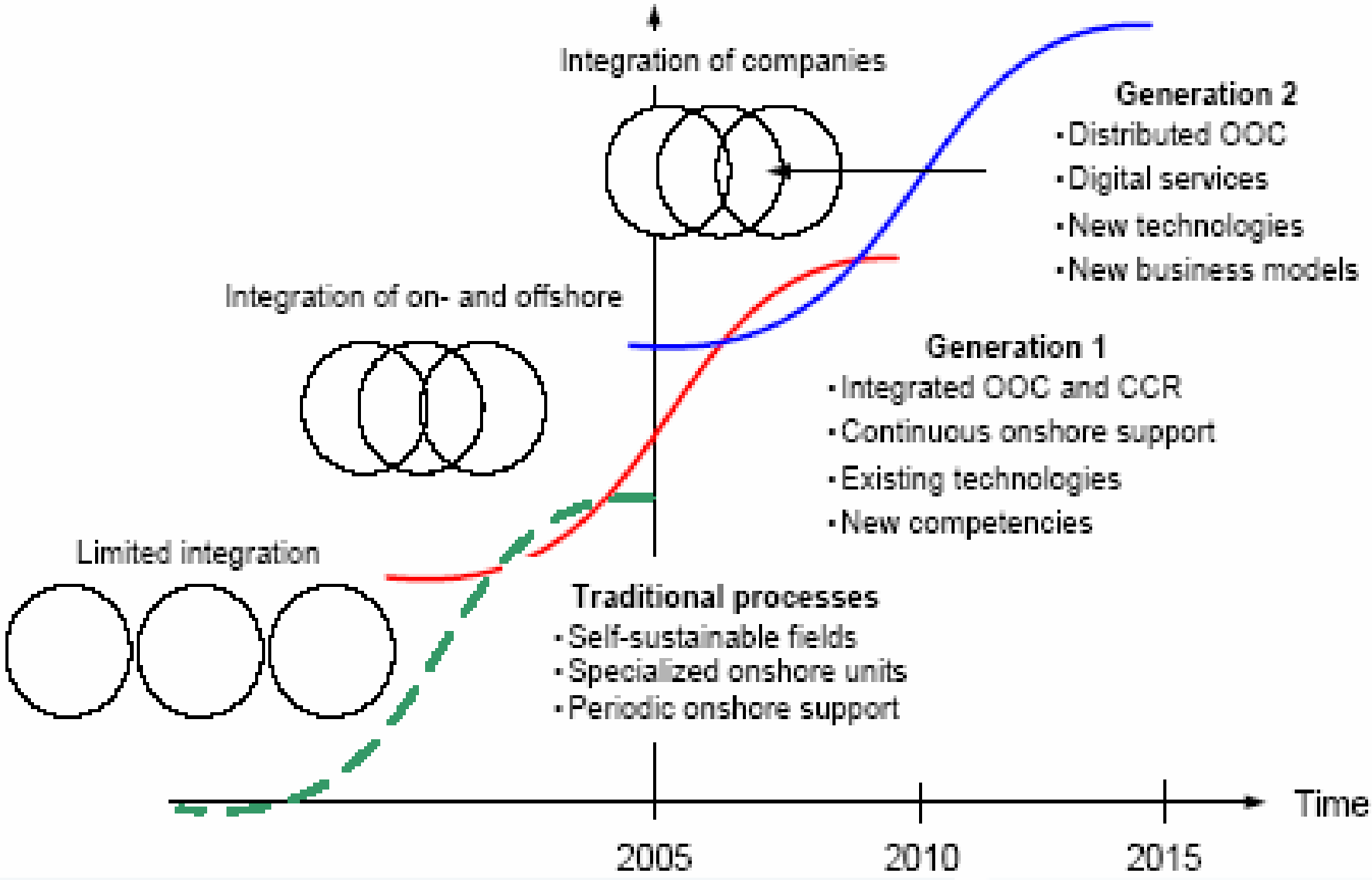
- It is estimated that Integrated Operations can:
  - increase oil recovery by 3-4%
  - accelerate production by 5-10%
  - lower operational costs by 20-30%

- Net present value of “Integrated Operations” in the North Sea are estimated to be 20,000,000 Million $

Integrated operations in the North Sea – a network



Future processes is based on integration between several companies and integration on- and off-shore



Internet Security

G.3.1.1 Connection to external systems via a Data Filtering Function

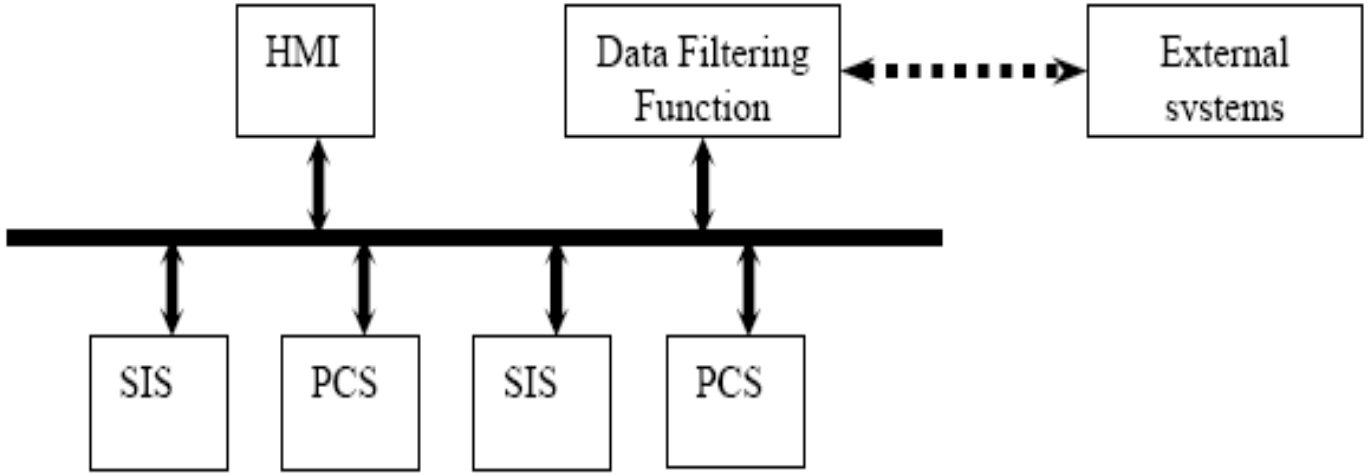


Figure G.3 Connection to external systems via a data filtering function

The Data Filtering Function may e.g. be an integrated Information Management System (IMS) or one or more PCS computers (nodes) and thus be part of the PCS.

Definitions

- **Safety:**
  - Not exposed to danger, freedom from danger or risks
- **Security:**
  - Safe against attack, freedom from (intentional) dangers or risks

- Information System Security:
  - The protection of information systems against unauthorized access or modification of information. Protection against the denial of service to authorized users [US National Information Systems Security Glossary]
- **Important aspects of Information Security:**
  - **Confidentiality**
  - **Integrity**
  - **Availability**

CheckIT

- Introduction – SINTEF
- Background and context
- Challenges
- Suggested methodology - CheckIT
- References

Unwanted incidents has been increasing

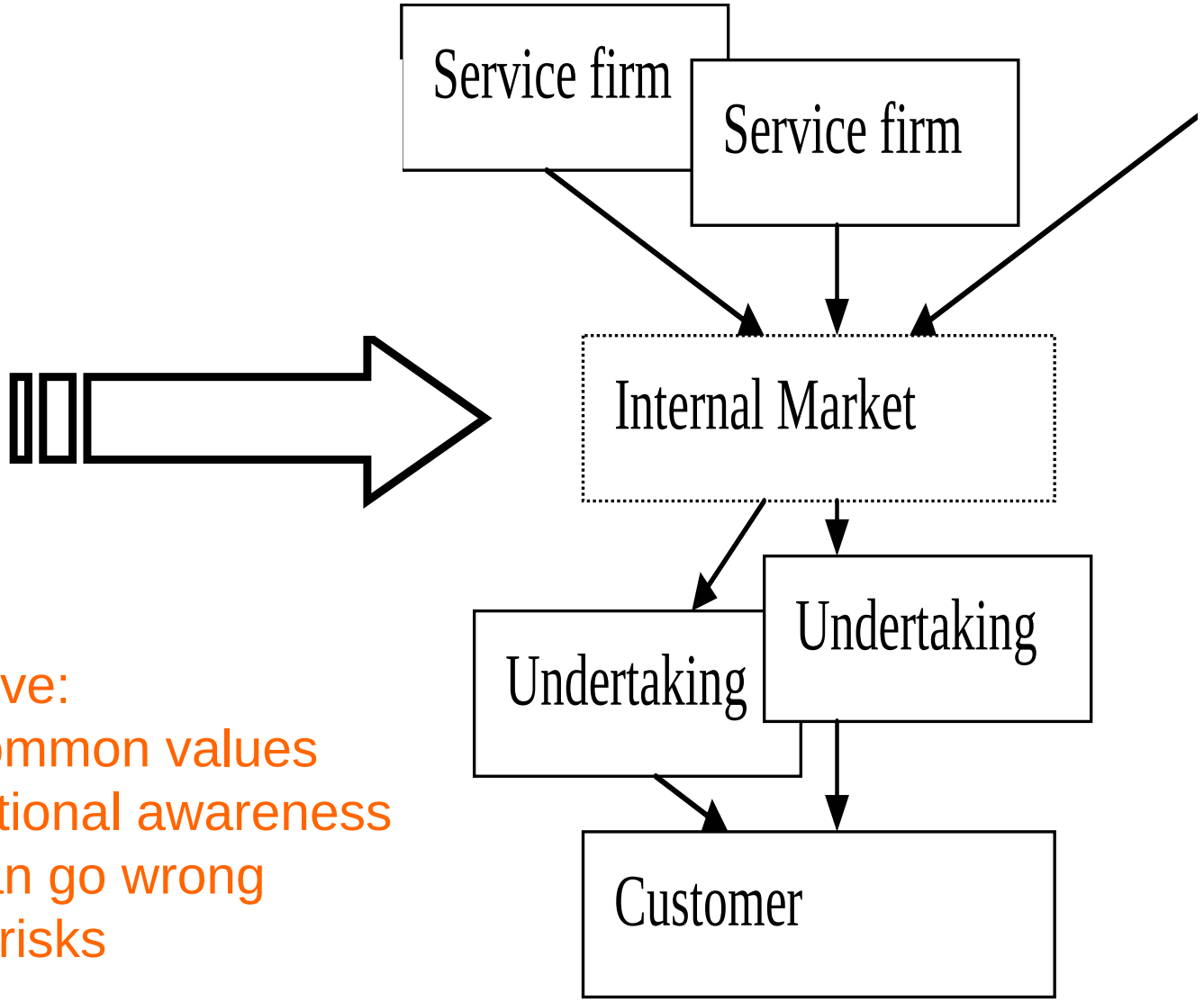
- Missing situational awareness
  - A supplier onshore closed a production valve off-shore (believing that the valve vas part of a test set up)
  - The gas explosion at the Longford plant: The operators did not understand the situation, part of the process was undercooled leading to leakage and explosion
- Stop of production because of (Denial of Service- DoS) attack or incidents
  - SCADA systems in the Oil & Gas industry had to be shut down because of jamming
  - Web sites performing “betting”
- Stop of production (or large cost is incurred) because of Virus attack
  - Several incidents each month leading to irregularities, because of virus on portable PC’s attached to production equipment
  - Virus can make a Emergency Shutdown system inoperable

Challenges

- Safety and security in a geographically dispersed network related to:
  - Understanding and communication among participants from different organisations and cultures
  - In an emergency - Creating common situational awareness in the network - doing the “right ting”?
  - Use of Internet as a (robust?) communication channel in the network
  - Establishing robust systems even if Windows is being used in the SCADA systems .(Windows has a high vulnerability to virus attack)
  - Blackmail? - If the SCADA systems are stopped – the daily cost is around 3 Mill $ and serious accidents can happen.

How can we improve safety and security in a network?

Single operator



We would like to improve:

- Understanding and common values
- Perceptions and situational awareness
- Knowledge of what can go wrong
- Behaviour to mitigate risks

CheckIT

- Introduction – SINTEF
- Background and context
- Challenges
- Suggested methodology - CheckIT
- References

Culture as useful framework

- **Safety Culture – common definition:**
  - *'The safety culture of an organisation is the product of **individual and group values**, **attitudes**, **perceptions, competencies** and patterns of **behaviour** that determine commitment to, and the style and proficiency of, an organisation's health and safety management*'. [From Advisory Committee for Safety on Nuclear Installations (HSC, 1993, p. 23)]

- Culture from the functionalistic tradition [E.Schein 1992]
  - Culture can be measured, managed and manipulated
  - We see Climate as a part of culture
  - The change of culture needs broad participation, focus from management and long duration

High “Safety Culture” reduces Accidents/Incidents :

- ESREL (2005) in S.Silva &M.Lima “Safety as an organisational value” documents a clear correlation between high “Safety Culture” and high “Safety”.

Andersen & Itoh (2003) : Train operators’

- **High safety culture as indicated by motivation and morale** were found to be key factors for railway safety based on correlations between their levels and **accident/incident rates**. ..
  - These factors were found to be related to other attitude factors:
    - **Training, Procedures, manuals, checklists (**Advice: critically review manuals and checklists in order to enhance operators’ morale and motivation.)
    - **Work schedule**
    - **Management style and organisational rules.**

A need to move from bureaucratic to cultural management

Bureaucratic control

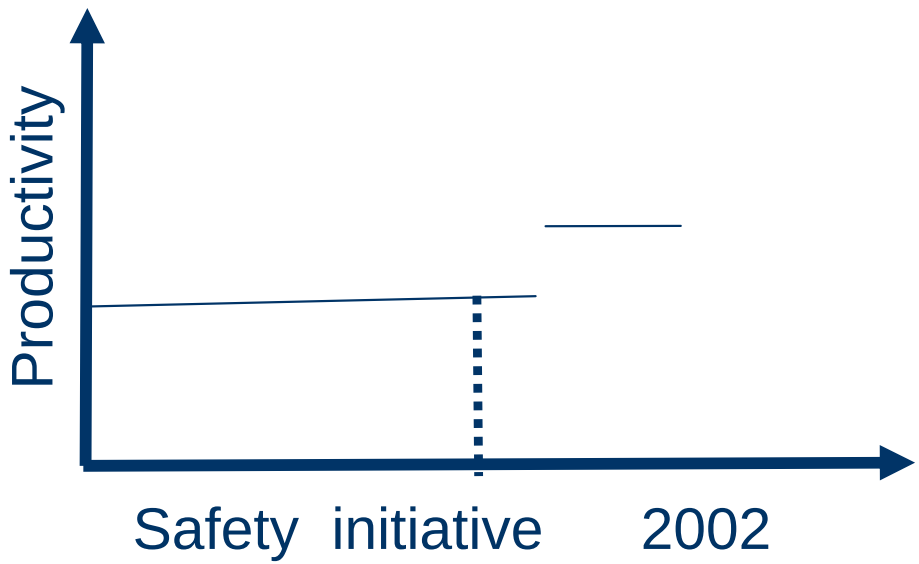
- Detailed rules and procedures
- Time consuming and not flexible

Cultural control,

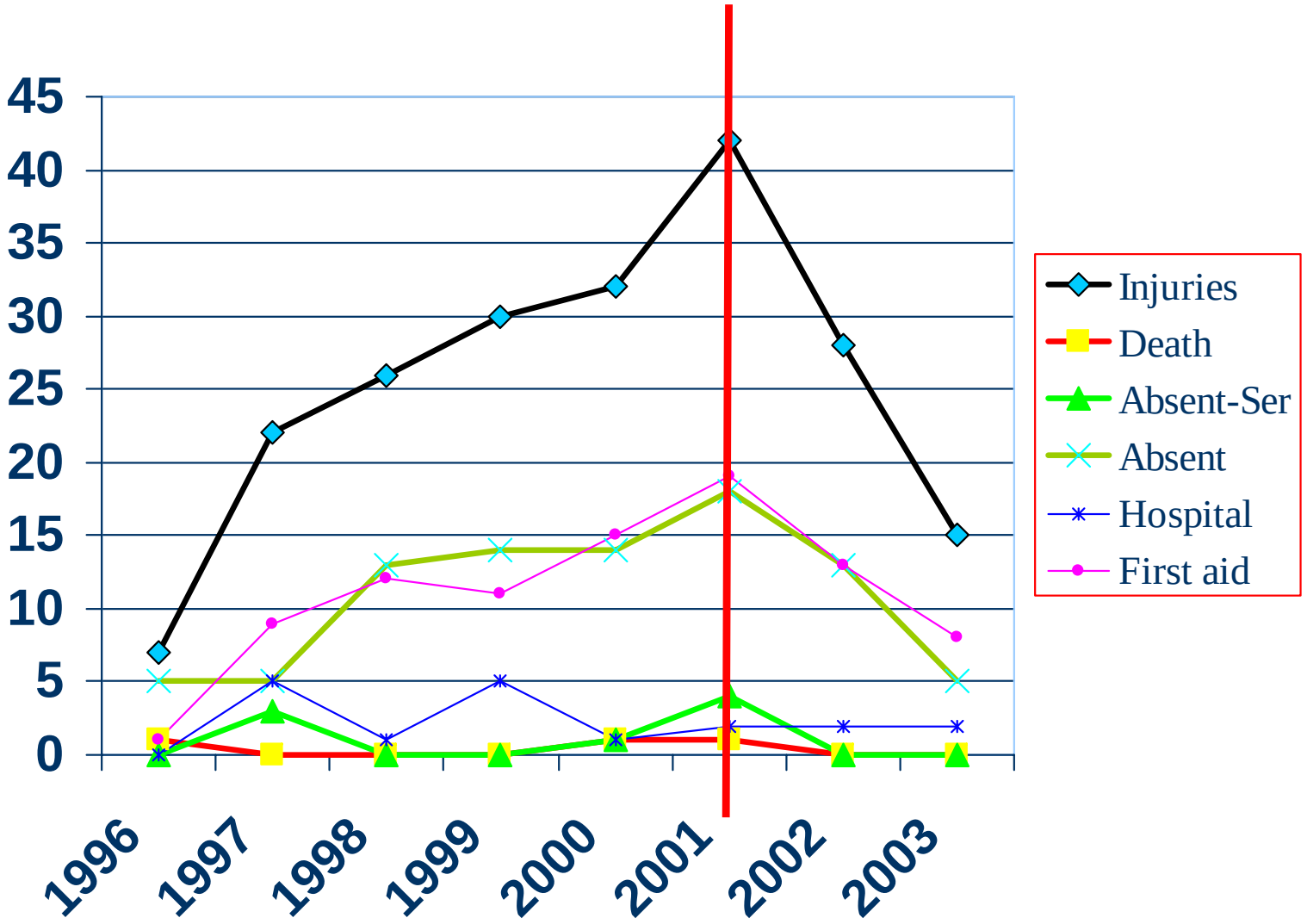
- establishing common values and goals
- choice based on knowledge
- correct actions without detailed management
- flexibility
- good match to the networked organisations

Experiences at building safety in networks – Case -Oil&Gas drilling

- Cooperation between different companies (from different countries), Between drilling crew and operations
- Safety culture changed via Action research, focus on Organisational learning (Esrel 2004, Alteren :"Successful Action Research")
- Result: Increased productivity and reduction of accidents



Incidents and accidents



Results

A methodology – CheckIT has been developed

- The methodology has been based on (safety and security) culture ie **individual and group values, attitudes, perceptions, competencies and patterns of behaviour**

- **CheckIT has been developed to assess and improve individual and group**
  - **values,**
  - **attitudes, perceptions,**
  - **competencies and**
  - **patterns of behaviour**

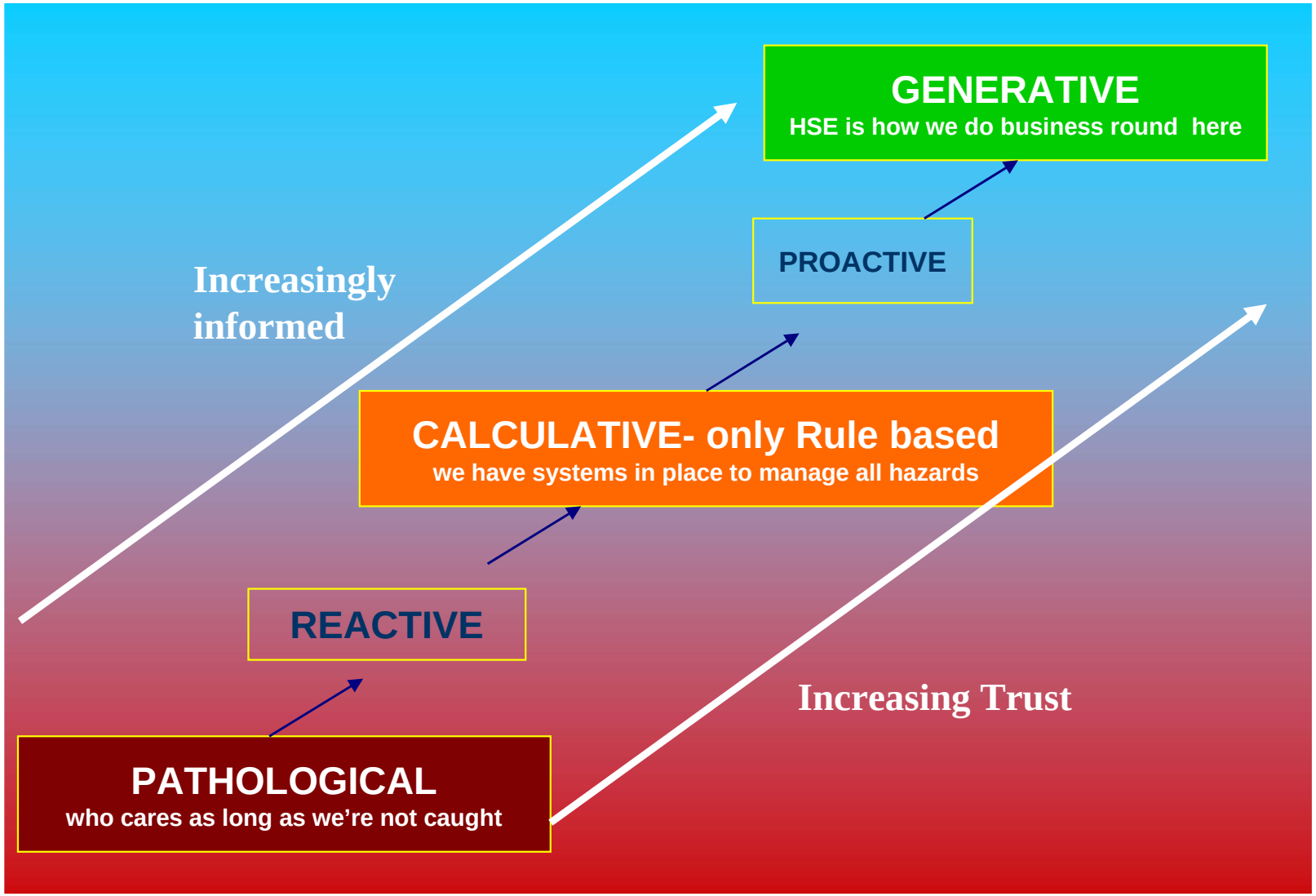
Selection of issues in CheckIT

We have tried to identify around 30 key issues related to measurement and improvement of Information security and safety culture. The issues has been identified based on:

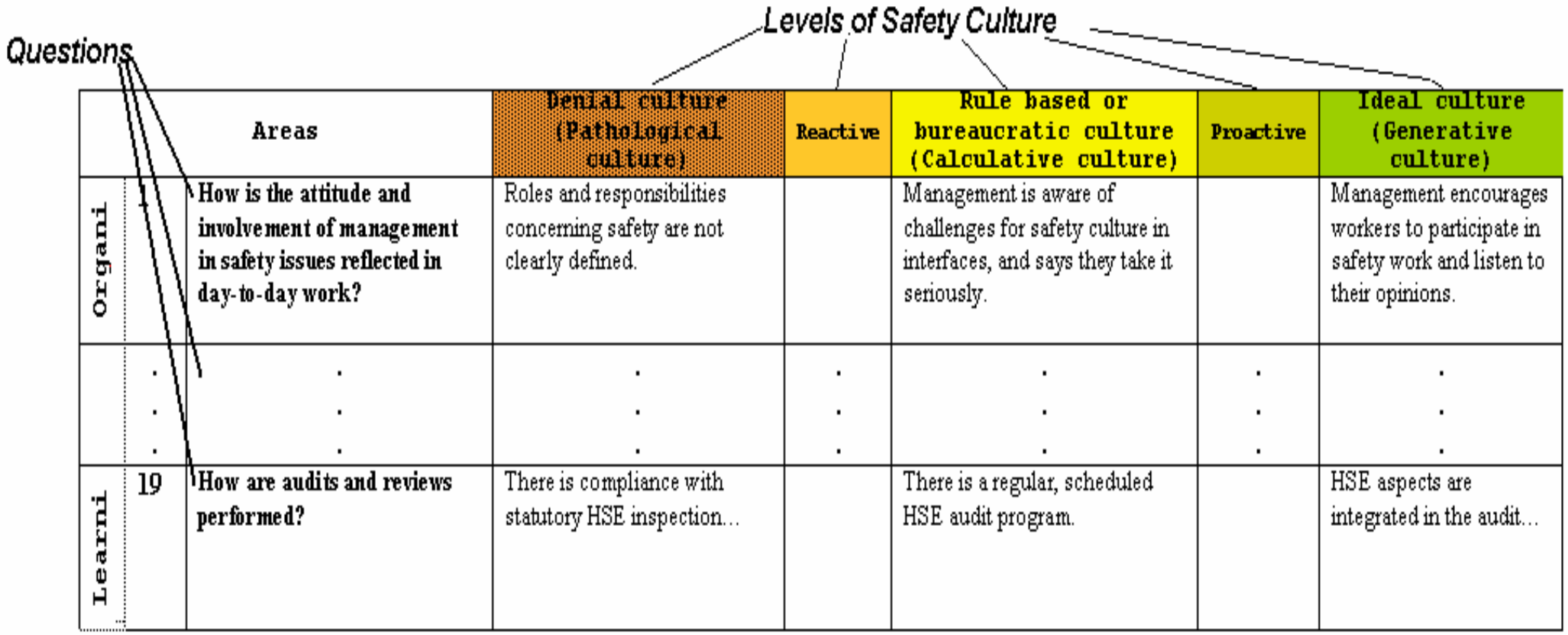
- Trough theoretical study of key issues related to Information security and safety culture, from HRO and other areas :
  - Hale (2000), Reason (1997), LaPorte (1991), Hudson (2002), IS 17799, and 20-40 issues identified as some ”best practice”/”key issues”
- Analysis of actual incidents and accidents – to identify root causes

- The tool CheckIT has been established, and developed trough:
  - Several workshops performed together with the Oil and Gas industry, and we have performed pilot testing in several different companies
- A validation of CheckITis being performed 2005/2006…
  - Comparing the actual level of safety and security culture against the actual level of incidents and accidents

Taxonomy of Safety Culture – (From Westrum)



Example of structure



		Areas	Denial culture (Pathological culture)	Reactive	Rule based or bureaucratic culture (Calculative culture)	Proactive	Ideal culture (Generative culture)
Organi	1	**How is the attitude and involvement of management in safety issues reflected in day-to-day work?**	Roles and responsibilities concerning safety are not clearly defined.		Management is aware of challenges for safety culture in interfaces, and says they take it seriously.		Management encourages workers to participate in safety work and listen to their opinions.
	.	.	.	.	.	.	.
	.	.	.	.	.	.	.
	.	.	.	.	.	.	.
Learni	19	**How are audits and reviews performed?**	There is compliance with statutory HSE inspection…		There is a regular, scheduled HSE audit program.		HSE aspects are integrated in the audit…

Example of questions

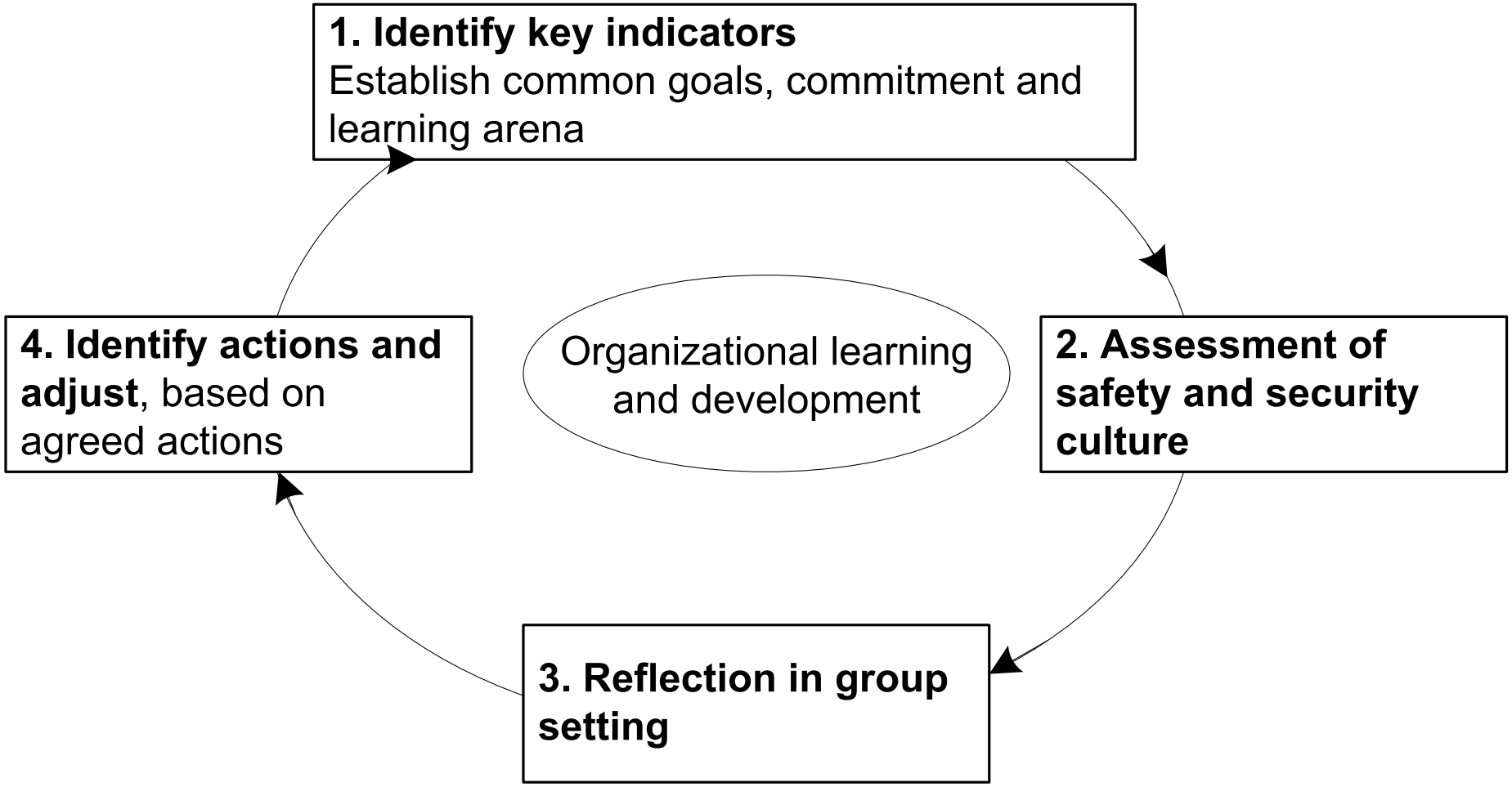
- *To what extent are unwanted incidents analysed and used as a learning experience?*
  - Example of generative/Learning culture: Unwanted incidents are shared in the industry. The incidents are used as cases during training and during emergency practices

- *To what extent are individuals blamed if an accident or unwanted incidents occurs?*

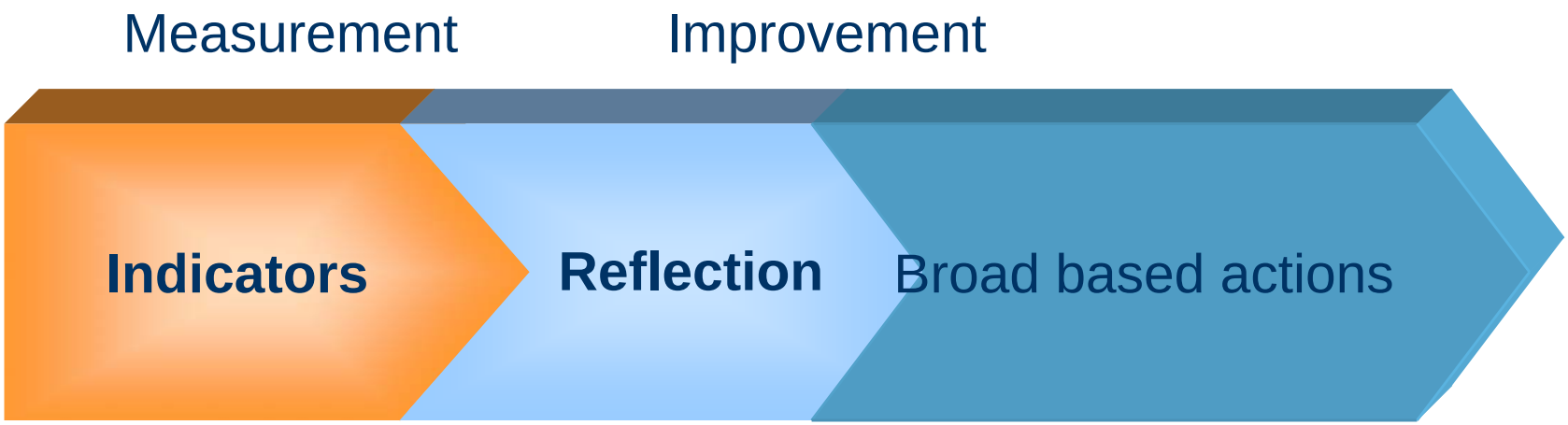
Effort to use CheckIT

½ day	Preparation and Organisation – Identify key indicators. Identify people to attend the workshop, fill out CheckIT in advance.
½ day Workshop performed	Based on CheckIT - assessment and reflection of how to improve information security and safety culture. Identify key actions – as agreed in team-work
½ day	Follow up of agreed actions and key indicators, to insure that action is taking place by the proper responsible person. Measure development relative to key indicators.

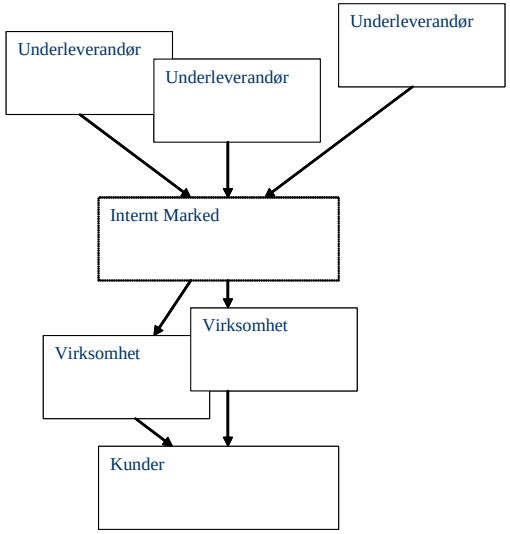
The learning loop of CheckIT



Focusing on key indicators, culture and broad participation in group processes

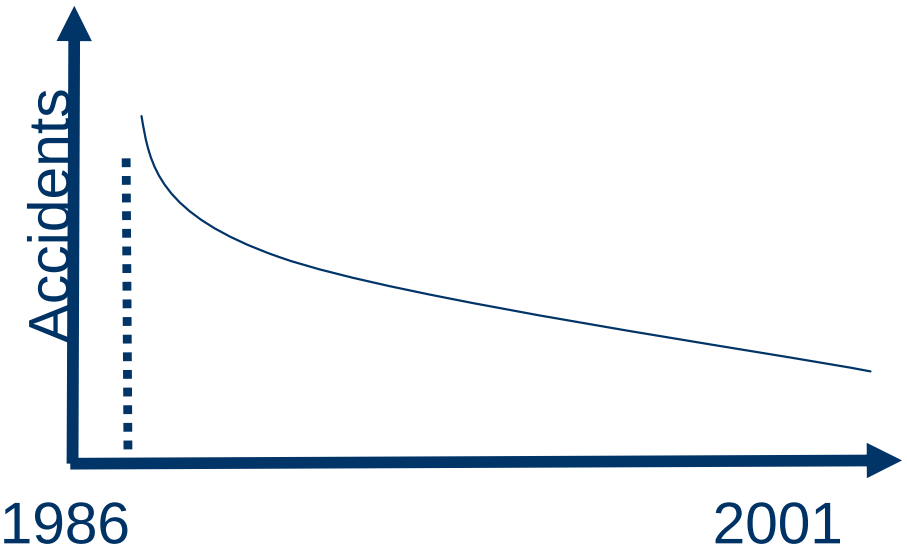


Key stakeholders involved in the process



Experience from 15 years of “Hearts and Minds” has inspired SafeCulture

- The “Hearts and Minds” has been used by Shell International
- Safety culture changed via “similar” Questionnaire - focus on employee participation and Organisational learning (SPE 2002, van Graaf et al :”Hearts and Mind”: The status after 15 years Research”)
- Result: Reduction of accidents



Some References

- Integrated Operations in Norway
  - www.olf.no/english and “Future work processes on the Norwegian Continental Shelf”
- Reliability, Safety and Security Studies http://www.ntnu.no/ross/
  - at the Norwegian University of Science and Technology (NTNU)
  - Safety and security at SINTEF www.sintef.no, http://www.risikoforsk.no/
- CheckIT http://www.CheckIT.sintef.no/
  - Draft English version of CheckIT
- Code of Practice for Information Security Management (IS 17799)
- E.H. Schein, “*Organizational Culture and Leadership*”, Jossey-Bass, 1992, San Francisco.

Tools to improve safety culture

- Johnsen S. & al (2003)“The track to Safety Culture” report to the UIC, ISBN 82-14-02731-4, see http://www.sintef.no/upload/Teknologi_og_samfunn/Sikkerhet%20og%20p%C3%A5litelighet/Rapporter/STF38%20A04414.pdf

- Tools from RSSB in UK – see http://www.rssb.co.uk/pdf/research_misc/T143/Research%20Brief%20Version%204.pdf

- Johnsen S., Vatn J., Rosness R. (2005)“Cross border railway operations: Building safety at cultural interfaces” First European Conference on Rail Human Factors published by Ashgate in 2005 and appearing in special issue of the journal Cognition Technology and Work .