Monitoring of Incident Response Management Performance

Maria B. Line, SINTEF
Eirik Albrechtsen, SINTEF
Stig Ole Johnsen, SINTEF
Odd Helge Longva, SINTEF
Stefanie A. Hillen, AUC
Norway

Introduction

Monitoring the performance of information security incident response (IR) management is an important part of

- the general information security management
- the risk management
- the total incident response

Agenda

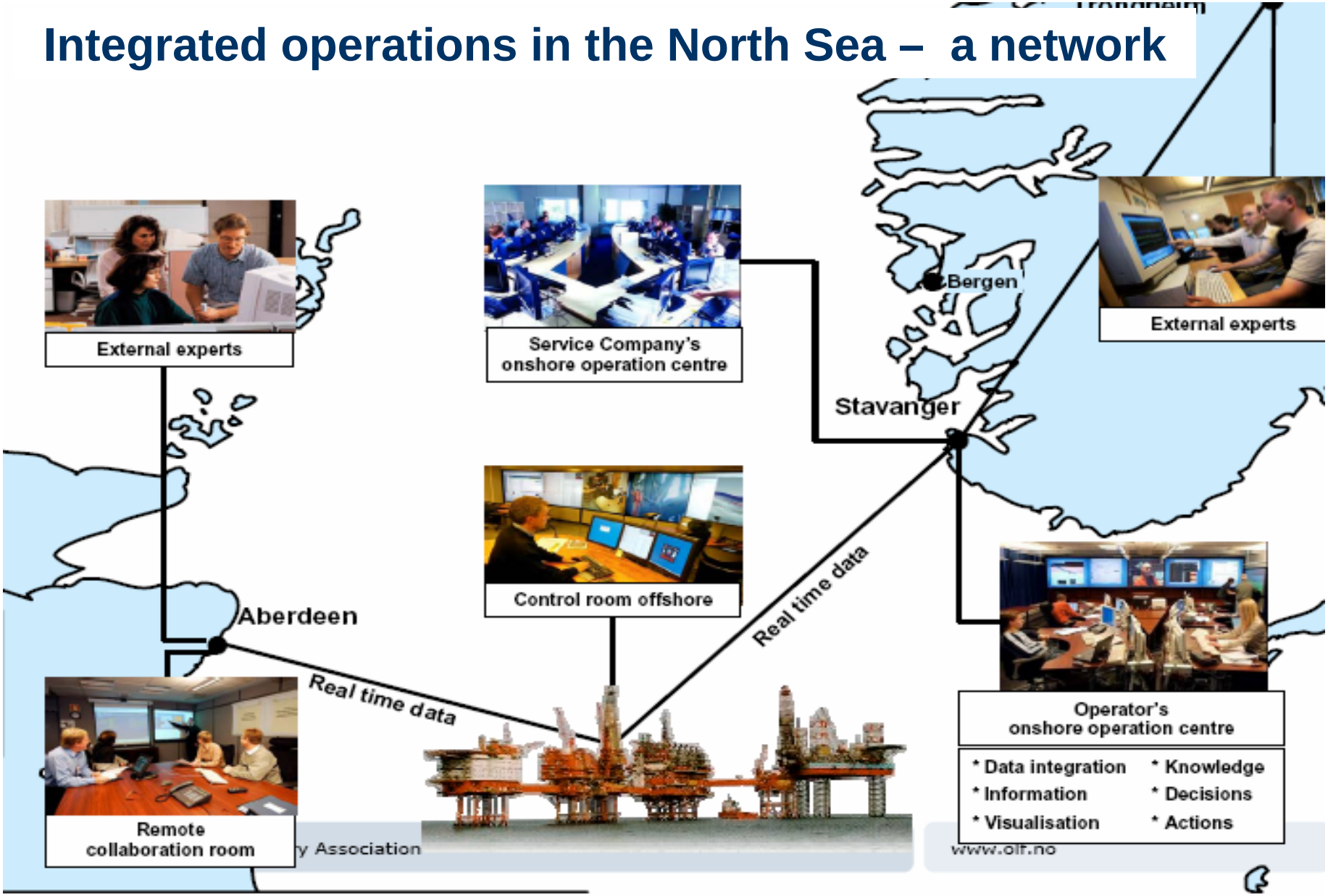
We shall

- Propose and evaluate a set of performance indicators monitoring incident response management
- Show how the indicators might be utilized

Based of incident handling and general information security management in the Norwegian oil and gas industry acquired in the research projects

- **IRMA** – Incident Response Management at SINTEF
- **AMBASEC** – A Model-Based Approach to Security Culture at AUC
- A pilot case at **Hydro**, a Norwegian Oil&Gas Company

Integrated operations in the North Sea – a network

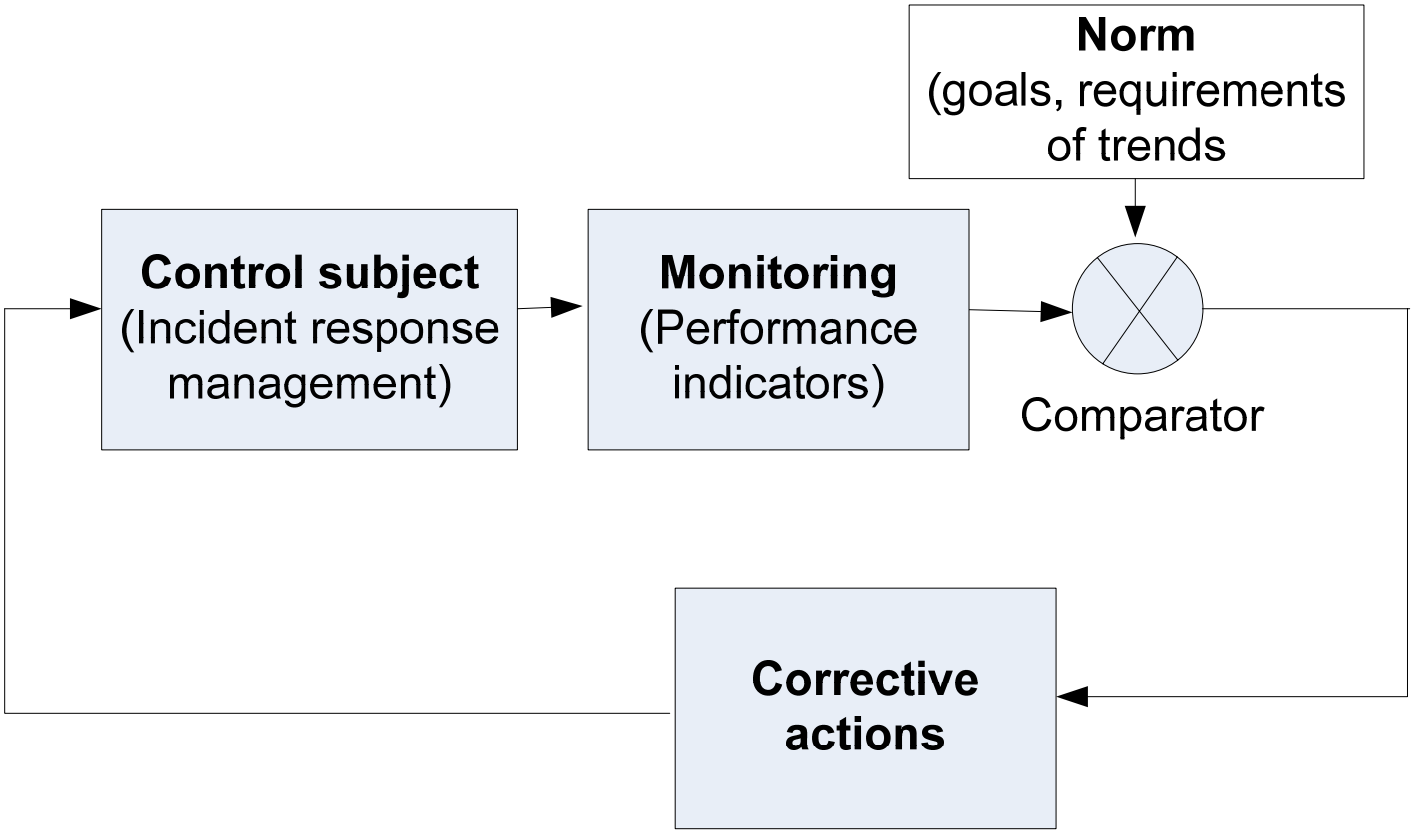


Purpose and Use of Performance Indicators

Performance indicators have been utilized for monitoring a variety of different business processes such as

- financial results
- production efficiency
- market reputation
- quality management
- HSE (health, safety and environment) management

System controlled through negative feedback



(adapted from Kjellén 2000)

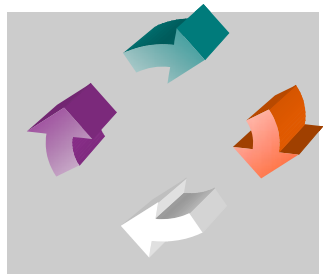
Purpose and Use of Performance Indicators

The principles for establishing norms for different indicators may vary

- a fixed goal established for a specific period of time
- an indicator must show continuous improvement from one period to the next
- evaluate whether a process is stable, by using control charts for several periods of time

Framework for Indicators
(Phases)

Phase: Plan and prepare

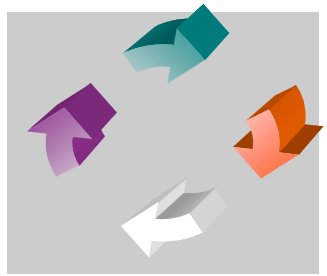


Performance indicators

1. Rating system for the quality of the IR management system

2. Assessment of information security culture with respect to IR

Phase: Use

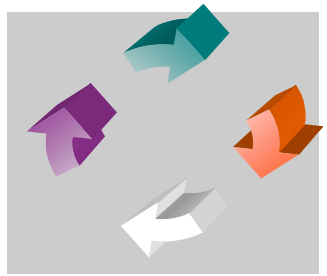


Performance indicators

3. Number of incidents responded to during a period

4. Average time spent on responding per incidents during a period

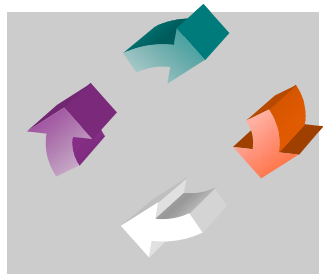
Phase: Review



Performance indicators:

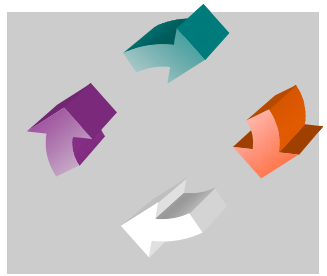
5. Total consequences of incidents during a period

Matrix for evaluating the consequences of incidents



	Direct financial loss	Injury to people	Damage to the environment	Loss or damage of assets	Immaterial loss
Catastrophic					
Critical					
Serious					
Marginal					
Negligible	< € 10.000	First aid			

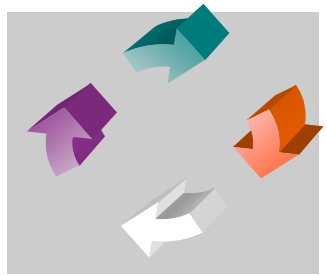
Phase: Review



Performance indicators:

5. Total consequences of incidents during a period
6. Number of Incidents of high loss during a period
7. Downtime of SCADA Systems due to incidents during a period
8. Total costs related to incident response during a period

Phase: Improve



Performance indicators

9. Average Order of Feedback during a Period

(adapted from Van Court Hare 1967)

Combining Indicators

Combining two or more indicators will produce better support for decision-making

- Examples
  - The ratio of number of incidents with high loss to total number of incidents
  - Comparing the consequences of incidents and the costs of incident response management
  - Average loss per incident of high loss can be created by the ratio of the consequences of high loss incidents to the number of incidents with high loss

Evaluation of the Performance Indicators

A performance indicator should satisfy the following requirements:

- observable and quantifiable
- valid
- sensitive to change
- compatible with other indicators
- easily understood

Completeness of the Performance Indicators

Performance indicators can be categorised as leading or lagging indicators

- Leading indicators focus on
  - removal or reduction of root causes
  - establishing and strengthening barrier
  - improving the organisation before an incident occurs

- Lagging indicators focus on
  - reducing the consequences of incidents

Conclusions and future tasks

- **Monitoring** incident response management is important support for decision-making aiming at improved incident response
- **Performance indicators** are well suited for this purpose as they in a comprehensible way **make it possible to measure** processes, **communicate** results, and **make decisions**
- We have **proposed** and **evaluated** a set of performance indicators
- We shall **test empirically** the proposed performance indicators