# A Structured Approach to Incident Response Management in the Oil and Gas Industry

Presented by Martin Gilje Jaatun

Martin.G.Jaatun@sintef.no

# Background

- The Norwegian petroleum industry is experiencing a paradigm shift with respect to how offshore production installations are operated
- “Integrated Operations” (IO) implies increased reliance on information and communications technology, and increased interconnection of systems and networks
- Furthermore, equipment that is similar or equivalent to the COTS systems found in offices and homes is finding its way into the process control environment (SCADA)
- This brings “familiar” threats with it, and a need for a systematic approach to how computer security incidents are handled

# Empirical Sources

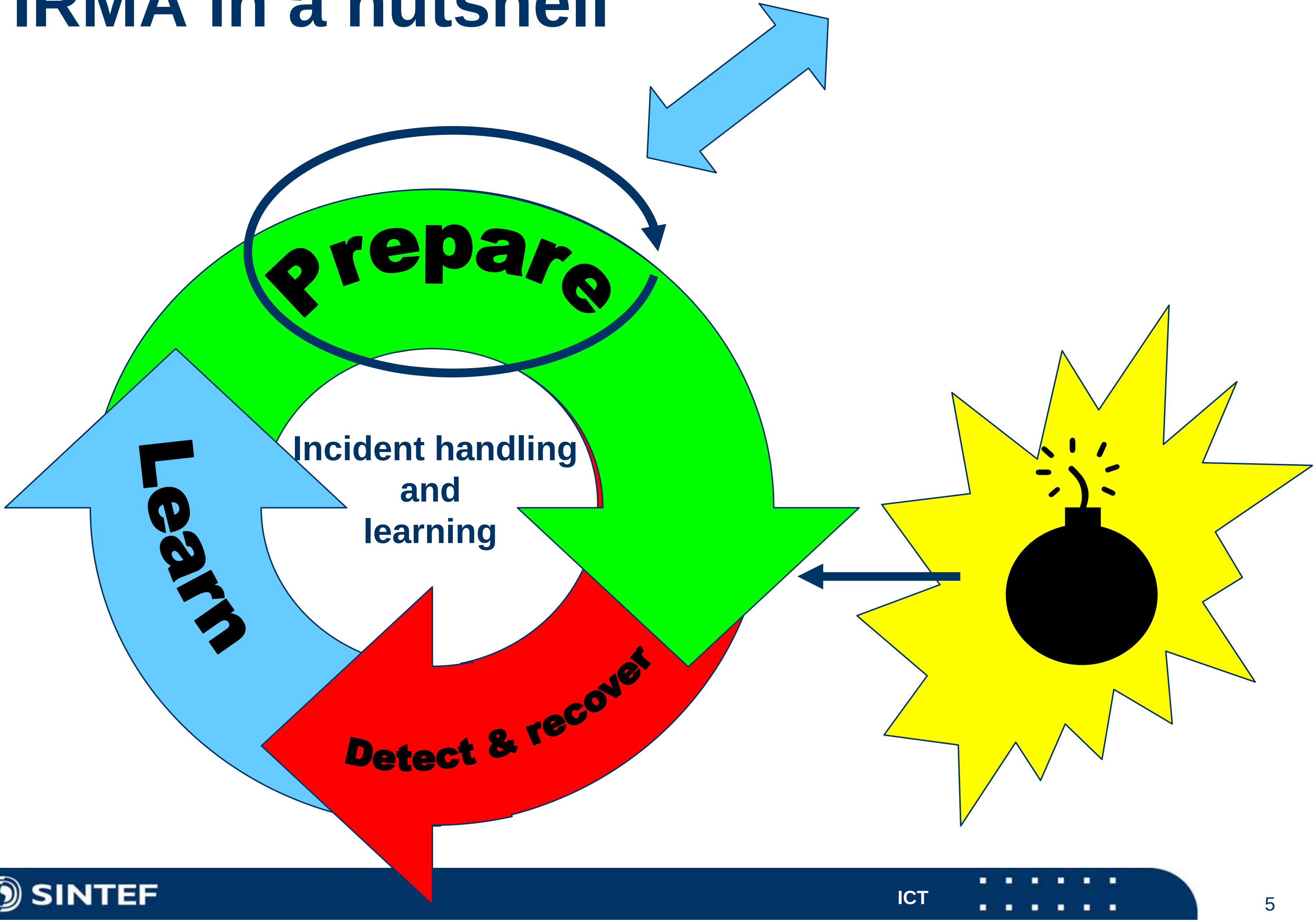
- Interviews with key personnel in the Norwegian oil and gas industry
- A case study of incident response management practice at an oil and gas installation in the North Sea
- A risk and vulnerability assessment of infrastructure and work processes at an offshore installation
- A study of cultural aspects of information security by using a tool for assessing information security culture at a particular installation
- A workshop on information security and integrated operations
- A workshop on the main findings of IRMA
- System Dynamics workshops

# Incident Response Management

- Incident handling is like firefighting
- Incident Response MANAGEMENT implies a perspective that goes beyond the immediate situation
- Make sure that you learn something from every incident!

# IRMA in a nutshell

External dynamics



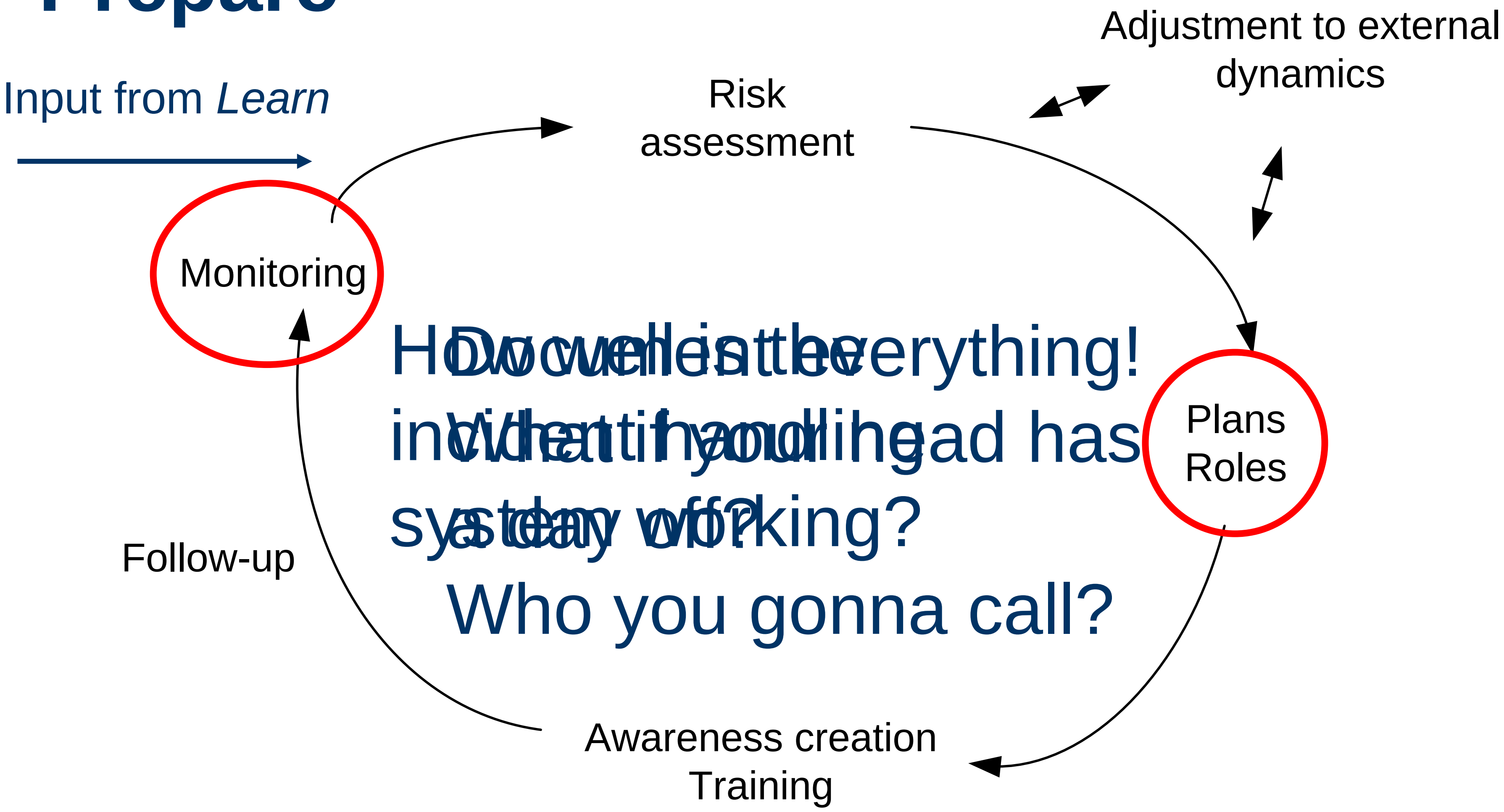
Incident handling and learning

# Deja vu?

- The IRMA wheel is based on well established sources such as ISO/IEC TR 18044 and NIST 800-61
- It is unsurprising that the model also would have been applicable to a ”normal” system
- However: Our empirical studies showed that an “ICT solution” is not necessarily palatable to the process control community – re-packaging is necessary

- Detection? (IDS is out of scope for IRMA)
- Improve? (External dynamics! Also from *Learn*)

# Prepare



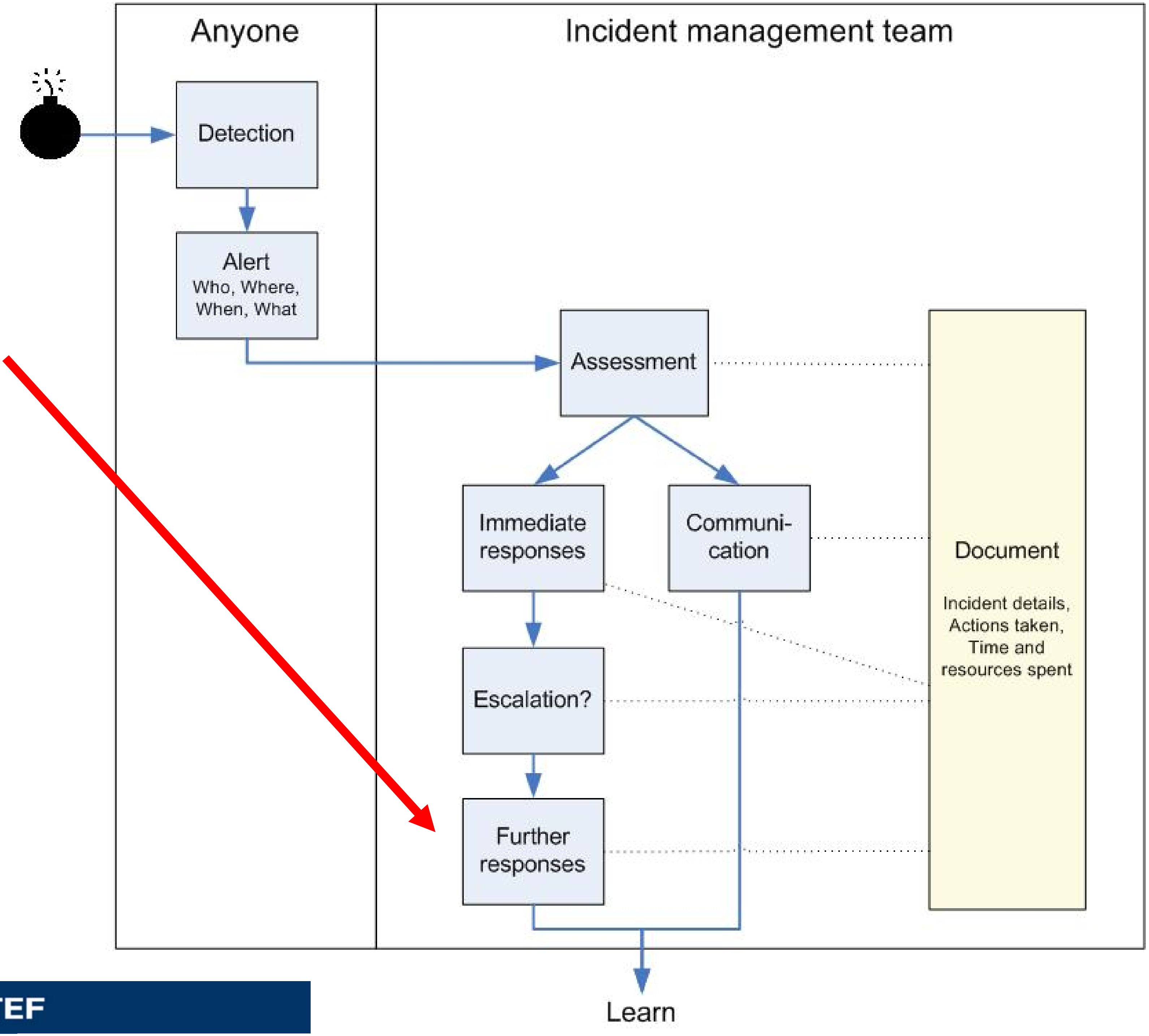
How well is the incident handling system working?

Document everything!

What if your head has a day off?

Who you gonna call?

## Detect & recover



Anyone

Incident management team

Detection

Alert
Who, Where,
When, What

Assessment

Immediate responses

Communication

Escalation?

Further responses

Document

Incident details,
Actions taken,
Time and
resources spent

Learn

# Documenting

- What happened?
- Which systems where affected?
- What damage was sustained?
- How was the incident handled?

- Make it easy!
- Provide tools!

# Recovering

- The work is not done once the fire is out
- Safe state – particularly important offshore!
- Patching, configuration
- Re-installation?
- Restore from backup?
- Integrity checks!
- Reconnection to external networks

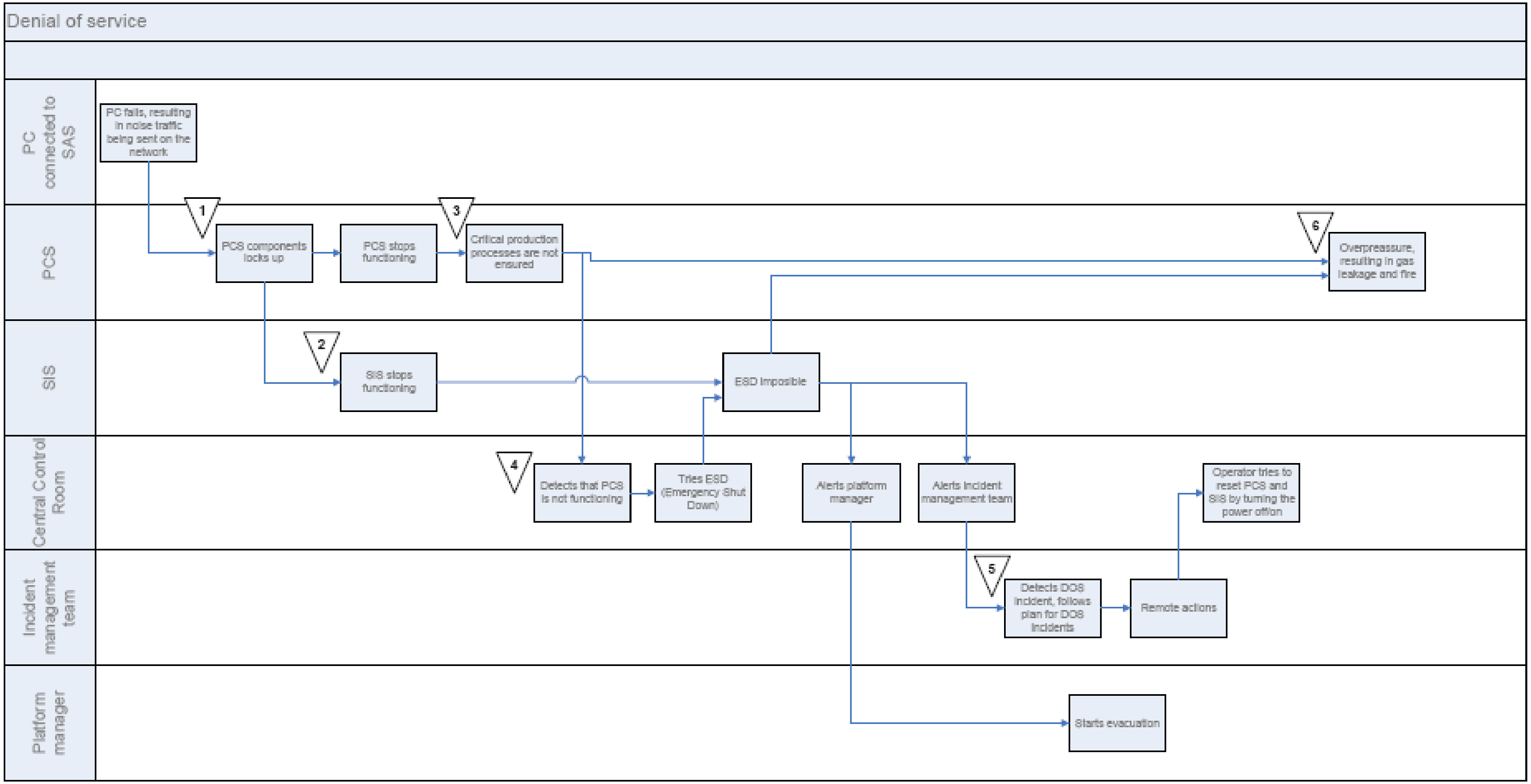
# Learn

- **Commitment**
  and resources
- **What occurred**
  Identify sequences of events with STEP
- **Why**
  Identify root causes and barriers
- Identify security recommendations

- Evaluate the incident handling process

- Identify incident response recommendations

# STEP Diagram for DoS Incident



Denial of service

PC connected to SAS

PCS

SIS

Central Control Room

Incident management team

Platform manager

PC fails, resulting in noise traffic being sent on the network

1

PCS components locks up

PCS stops functioning

3

Critical production processes are not ensured

6

Overpreassure, resulting in gas leakage and fire

2

SIS stops functioning

ESD impossible

4

Detects that PCS is not functioning

Tries ESD (Emergency Shut Down)

Alerts platform manager

Alerts incident management team

Operator tries to reset PCS and SIS by turning the power off/on

5

Detects DOS incident, follows plan for DOS incidents

Remote actions

Starts evacuation

# Learning from Incidents

- Incidents are unwanted occurrences
- ... but represent opportunities to learn
- Reactive: After each incident
- Proactive: Between incidents
- Obstacles: Embarrassment and Threats

# Further information

- More information on IRMA (including the full report) is available at http://www.sintef.no/irma

Questions?

Martin.G.Jaatun@sintef.no