Exercise planner

Package 2, exercise 3

'Loss of communication'

Version 1.0

Table of contents

1 Introduction

1.1 Background and scope

Facilities and installations in the petroleum sector are required to have preparedness plans in place for managing serious incidents. The industry is subject to various scenarios involving ICT incidents, but the Norwegian Ocean Industry Authority (Havtil) has, through audits, noted that little or no training is carried out related ICT security in the industrial control and security systems. Considering this, Havtil has commissioned a set of training and exercise scenarios. These exercises have been prepared by Proactima together with Netsecurity and was adapted by Havtil.

The Activity regulation § 23 stipulates that: «necessary training and necessary drills are conducted, to ensure that the personnel are always able to handle operational disturbances, hazard, and accident situations in an effective manner». The Technical and Operational regulation stipulates the same in § 52. This means that the requirements for training and exercise are the same for onshore and offshore facilities.

Training enhances personal skills and knowledge, while exercises test collaboration and response capabilities during an emergency. In addition, exercises can reveal organisational and structural strengths and weaknesses and prepare management for dealing with various crises.

1.2 Structure of this guide

The exercise planner contains several scenarios. Each scenario includes suggestions on which functions are relevant to the exercise. The scenarios can be used for training, tabletop exercises, or incident response simulation exercises.

Part 3 of the guide contains additional information to aid in preparation and implementation. This includes:

- a possible sequence of events prior to exercise start-up
- a sequential incident flow chart
- relevant technical material

2 Scenario

2.1 Overview of the scenario

There are various scenarios that can lead to the loss of communication. The tasks in this guide does not discuss the cause of the incident but focuses on how the arising situation must be managed.

Table 1. Summary of roles/functions that can be trained using the various modules.

Task	Stage	Personnel responsible for SAS/IACS/telecom	Local operations managers	Personnel responsible for systems operation	ICT department
2.2	Initial events – Loss of external IP-communication	x	x	?	?
2.3	Identify alternative communication solutions	x	x		?
2.4	Operational consequences	x	x	?	

2.2 Initial events – Loss of external IP-communication

The redundant communication solution between the offshore installation and the onshore facilities is lost, meaning that the offshore installation loses all external IP-communication. This affects voice communication, administrative IT-systems, and access to the internet. In addition, the communication solutions from the industrial ICT-systems are affected. The incident is related to external factors and cannot be mitigated through local initiatives.

2.2.1 Advisory questions

Personnel responsible for SAS/IACS/telecom

- What immediate consequences can this have for the industrial ICT-systems?
- How can we support the local operations managers in this situation?

Local operations managers

- How do we establish contact with the outside world when all external IP-communication is down?
- Who should we notify?
- What immediate consequences can the loss of communication have for the work in progress?
- What immediate consequences may the loss of communication have for the production, integrity of the pipelines, and reporting of production data?

Personnel responsible for systems operation / ICT department

- How will personnel responsible for system operation onshore become aware of this incident?
- How can we support the offshore organisation during such an incident?
- Who do we contact to re-establish communication lines?

2.3 Identify alternative communication solutions

Many of the communication solution can be integrated with common control panels in the control room and are dependent on network-based communication.

2.3.1 Advisory questions

Personnel responsible for SAS/IACS/telecom

- What alternative communication solutions exist?
  - Which ones can be used independently from network-based communication?
- To what extent does our organisation have knowledge and training in establishing alternative communication solution offshore? (Who does what with what equipment)

Local operations managers

- What alternative communication solutions exist?
  - Which ones can be used independently from network-based communication?
- To what extent does the control room operators and crisis management have knowledge and training in the use of equipment for alternative communication solutions?
- If the loss of communication becomes prolonged, how will this be managed?
- How to manage the situation if (another) DHA occurs simultaneously?

ICT department

  - How can we support the offshore organisation during this incident?

2.4 Identify operational consequences

Both the operational routines and the technical systems utilises communication with the central data systems.

2.4.1 Advisory questions

Personnel responsible for SAS/IACS/telecom

- Are there functions in the control system that depend on communication with onshore or cloud-based data systems?
  - What are the short-, medium-, and long-term consequences of a loss of communication?

Local operations managers

- Which operational procedures depend on communication with onshore or cloud-based data systems?
  - What are the short-, medium-, and long-term consequences of a loss of communication?
- Which conditions for normal operations are affected by the lack of communication, in the short, medium, and long term?
- What consequences will a loss of communication have for staffing, including the potential evaluation of downsizing?

Personnel responsible for systems operation

- How can we support the offshore organisation during this incident?

3 Additional information for preparation and implementation

Not all incidents in the industrial ICT-systems are the result of cyberattacks. This exercise is related to an incident in the communication systems.

The telecom-systems are complex, and different actors can be responsible for different part of the systems. This makes it challenging to view these systems in a holistic perspective. The systems are often built with a high degree of redundancy, and errors resulting in loss of communication seldom occurs. Considering this, there will be limited experience in managing such scenarios.

The operation of the installations is dependent on trustworthy communication systems. This is true for both the administrative operations, as well as for the industrial ICT-systems. For the parts of the communication systems that are operated by telecom operators, the maintenance and check-ups will most often be executed in the telecom operator's systems.

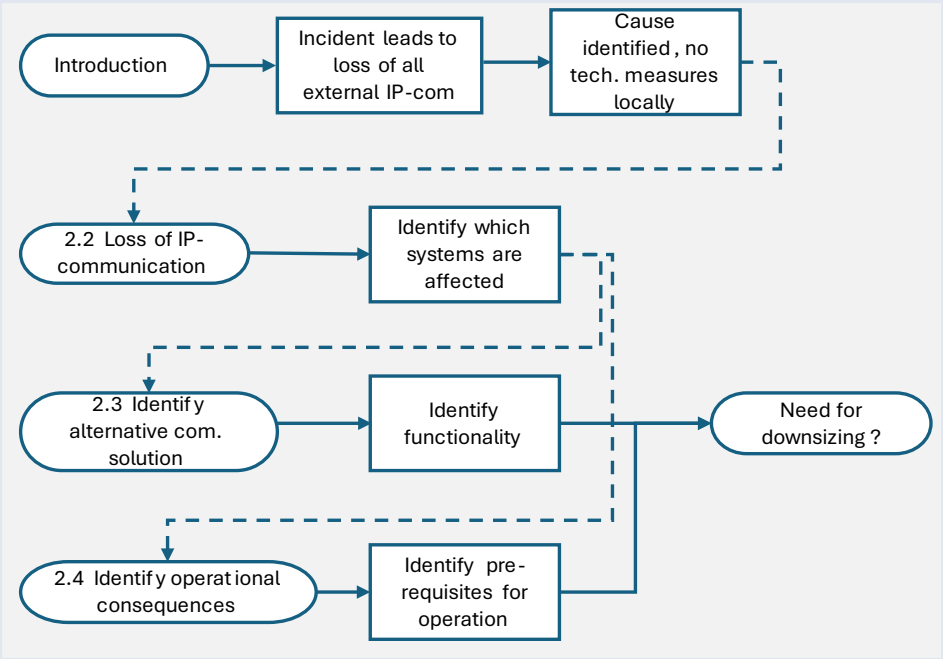
The laws and regulations set requirements for the communication solutions. One of these is that there must be two independent notification paths onshore (The Facilities Regulation §18). NORSOK T101:2019 prescribes that critical alarms from the communication systems must be notified in central control room.

3.1 Introduction to the incident

There are different incidents that may lead to the loss of communication. Loss of communication due to an external occurrence has no local technical measures that can support the re-establishment of communication. This guide discusses how a situation that occurs due to external factors on the communication solutions must be managed.

3.2 The incident

Our preparation of the exercise package has been based on the sequence of events illustrated in the diagram below.



3.3 Lessons learned

Review of procedures, improvement of systems to prevent new attacks, etc.

3.3.1 Advisory questions

Discussion leader

- How are the participants involved to provide feedback to the final report from the exercise?

Personnel responsible for SAS/IACS/telecom

- Are roles and areas of responsibility adequately described?
- Did the existing procedures support this type of incident?
- Were the procedures adhered to? What modifications should be implemented?
- How do we ensure learning across all shifts?

Local operations managers

- How did the existing procedures support this type of incident?
- Were the procedures adhered to? What modifications should be implemented?
- How do we ensure learning across all shifts?

Personnel responsible for systems operation

- Is the involvement of this role relevant?
- How do we ensure that lessons learned from this incident is applied for the future?

ICT department

- Is the involvement of this role relevant?
- How do we ensure that lessons learned from this incident is applied for the future?

3.4 Relevant reference material

The Norwegian Ocean Industry Authority (Havtil) has commissioned a project related to the ICT security for the industrial ICT-systems. The reports *"Communication Systems for External Emergency Communication"*[1] and *"Telecommunication and Protocols"*[2] are part of this work.

The report on emergency communication aims to increase the understanding of the role and vulnerability of communication networks, with emphasis on preparedness situations when a defined hazard and accident situation (DHA) has occurred. The report focuses on external communication between onshore and offshore during a crisis.

The report on telecommunication and protocols addresses changes resulting from the digitalisation of the telecommunication. Information systems and telecom solutions are becoming increasingly integrated. There are a wide variety in the functional areas of the 23 system categories defined as telecommunication systems in the sector. Requirements for the integrity and protection of confidentiality vary for the different systems.

[1] id7-kommunikasjonssystemer-for-ekstern-nodkommunikasjon.pdf
[2] dnv-gl---telekommunikasjon-og-protokoller.pdf