Exercise planner

Package 1, exercise 3

'Maintenance and modification'

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

This scenario involves modification work that is being carried out from the equipment contractor's offices.

2.1 Overview of the scenario

Table 1 provides an indication of which roles/departments may be appropriate to include in the various stages of this scenario. Those coordinating the exercises can decide which tasks shall be included.

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

Task	Stage	Personnel responsible for SAS/IACS	Local operations managers	Personnel responsible for systems operation	ICT department
2.2	Initial events – updating of CCTV software	x	x		
2.3	Escalation		x	x	

2.2 Initial events – updating of CCTV software

Software CCTV updates are executed routinely. As CCTV is not classified as safety-critical equipment, the supplier has permanent access to the systems on all of the operator's facilities. The work is performed from the supplier's locations for remote work and shall be regulated through work permits. A control room operator discovers irregularities in the CCTV system.

2.2.1 Advisory questions

Local operations managers

- What has happened?
- What are the potential consequences of this related to the operations of or safety at the facility?
  - How can these consequences be managed?
- Who do we contact?

Personnel responsible for SAS/IACS

- How do we uncover what has happened?
- Who do we involve? Why?

2.2.2 Additional action points (dependent of the outcome of discussions/decisions)

- How do we manage a situation where several CCTV cameras are rendered inoperable?
- What may happen if CCTV images freeze without this being immediately discovered?
- How have we assessed criticality of the CCTV system?
  - in the maintenance system?
  - perceived criticality in a control room and by operations managers?

2.3 Escalation – planned work on the CCTV system on another facility

Through dialogue with the personnel responsible for systems operation, it is uncovered that updates of the CCTV software are being installed on other facilities. However, the updates for the facility in question is not scheduled to start until next week. The cause of the problems described in 2.2 is that there is lacking correspondence between the pre-installed camera configuration and the one the suppliers has used as part of the completed work.

2.3.1 Advisory questions

Operations managers on the facility

- How is the situation managed moving forward?
- What consequences can this have for the operations of or safety on the facility?

Personnel responsible for systems operation

- How do we figure out what has happened?
- How is coordination with the CCTV contractor organised?
- What is being done to restore functionality in the CCTV system?
- Is it possible to reset the system to its status prior to the maintenance work?

2.3.2 Further clarifications

It is uncovered that there is a discrepancy between the installed camera configuration and the one used by the supplier during the completed work.

- How do we address ‘minor modifications’ such as the installation of new matrix functions for the CCTV cameras?
- What are the procedures for ensuring that suppliers use an updated configuration?

3 Additional information for preparation and implementation

It has been possible for some time to monitor and perform work on industrial ICT systems remotely from onshore, both for the operators and system suppliers. This includes both 'read access' (access to view and monitor parameters for troubleshooting) and 'write access' (make software modifications). Some companies have expertise available offshore, while others employ expertise stationed onshore. Others again outsource parts of the support functions either to their own corporate global functions or to suppliers.

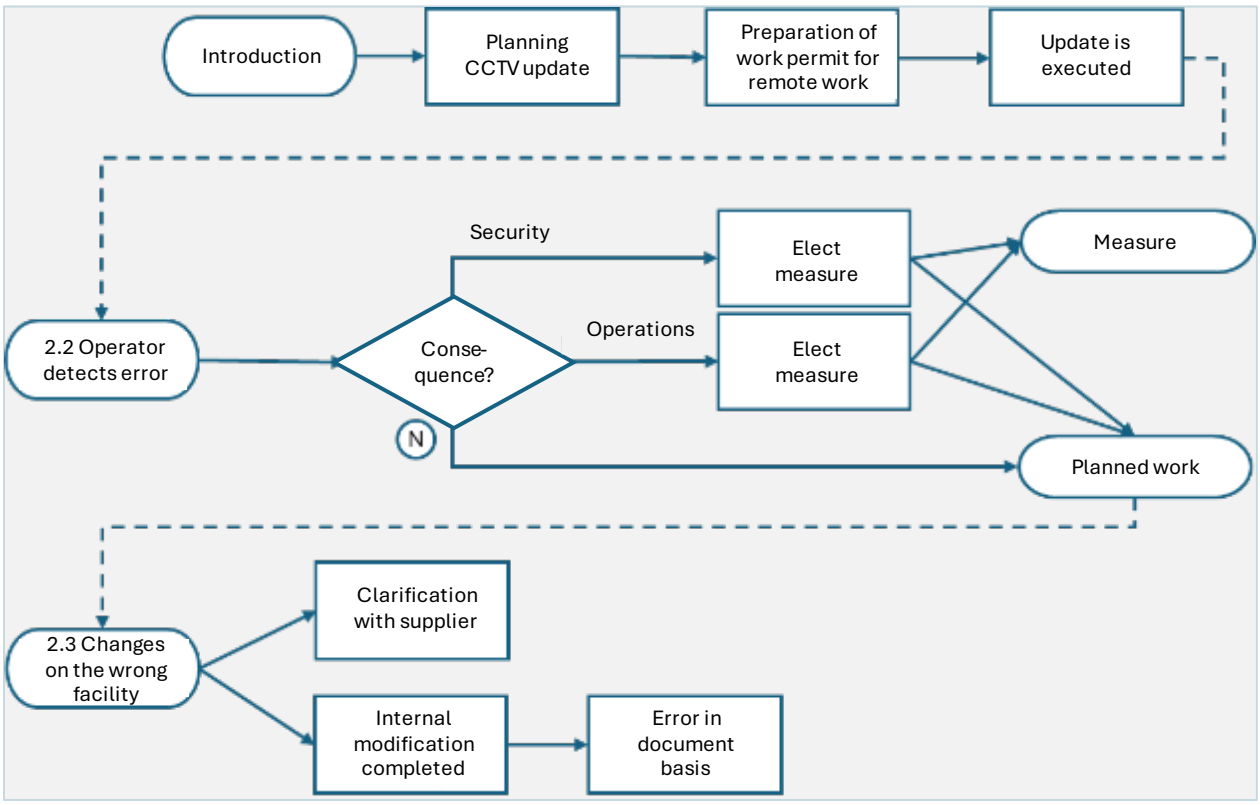
Control systems and other computer systems are updated remotely at regular intervals. Some planned maintenance tasks and modifications must be carried out as part of turnarounds, but many are performed during normal operations.

3.1 Introduction to the incident

CCTV software is updated on a regular basis. As CCTV is not classified as safety-critical equipment, the supplier is granted permanent access to CCTV systems on all of the operator's facilities. The work is performed remotely from the supplier's offices and shall be regulated by work permits.

3.2 The incident

This scenario has been based on the following sequence of events:



3.3 Lessons learned

Review of procedures, clarification of areas of responsibility and systems improvements.

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

Personnel responsible for systems operation

- Are roles and areas of responsibility adequately described?
- How do existing procedures support incident management?
- Were the procedures adhered to? What modifications should be made?

Personnel responsible for SAS/IACS

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

Local operations managers

- How do existing procedures support incident management?
- How do we ensure learning across all shifts?

3.4 Relevant reference material

Havtil has completed a major project addressing ICT security in industrial ICT systems. The SINTEF report '*IKT-sikkerhet – Fjernarbeid og HMS*'»[1] (ICT security – remote working and HSE, in Norwegian) gives an account of part of this work. The report is based on 14 group interviews carried out in late 2018/early 2019 with representatives from operator and drilling companies, as well as system contractors. It also contains a review of relevant documents supplied by operator and drilling companies and integrates SINTEF's general expertise and experience in the elds of HSE and ICT security.

[1] '*IKT-sikkerhet – Fjernarbeid og HMS*', published on 5 April 2019.https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/sluttrapport-ptil-ikt-sikkerhet---fjernarbeid-og-hms-med-underskrift-og-vedlegg.pdf