Exercise planner

Package 2, exercise 2

'Insider'

Version 1.0

1 INTRODUCTION 3
1.1 BACKGROUND AND SCOPE 3
1.2 STRUCTURE OF THIS GUIDE 3
2 SCENARIO 4
2.1 OVERVIEW OF THE SCENARIO 4
2.2 INITIAL EVENTS – EQUIPMENT SHUTDOWN 4
2.2.1 Advisory questions 4
2.3 ESCALATION – UNINTENTIONAL MODIFICATIONS 6
2.3.1 Advisory questions 6
2.4 MODIFICATION - INTENTIONAL MISCONDUCT 6
2.4.1 Advisory questions 6
3 ADDITIONAL INFORMATION FOR PREPARATION AND IMPLEMENTATION 7
3.1 INTRODUCTION TO THE INCIDENT 7
3.2 THE INCIDENT 8
3.3 LESSONS LEARNED 8
3.3.1 Advisory questions 8
3.4 RELEVANT REFERENCE MATERIAL 9

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

The starting point of this scenario is that modifications has been made in the control systems. These modifications have led to a partial shutdown of production. The shutdown cannot be explained by the process conditions or equipment errors.

2.1 Overview of the scenario

If required, the scenario can be split up according to the time available. Table 1 indicates which functions/departments may be appropriate to include in the different stages of the scenario.

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

Task	Stage	Personnel responsible for SAS/IACS	Local operations managers	Personnel responsible for systems operation
2.2	Initial events – Equipment shutdown	x	x	x
2.3	Escalation – unintentional modification	x	x	
2.4	Modification – intentional misconduct		x	

2.2 Initial events – Equipment shutdown

Due to planned switching between equipment units (e.g. duty standby system), the standby system is started. After some time, the system shuts down for unknown reasons, affecting production.

2.2.1 Advisory questions

Personnel responsible for SAS/IACS

- How can we map what has happened?
- Why did it happen?
  - What can be read from the event logs for the control system?
  - How can we figure out what may have caused this?
- Which information can be found in the hand-over from the previous shift?
- How do we proceed to restore the systems?

Local operations managers

- How can we map what has happened?
- Why did it happen?
  - Which systems are affected by the equipment shutdown?

- Was the security of the systems and safety of the employees affected?
- What is the expected downtime or delays?

Personnel responsible for systems operation

- How can we support the personnel responsible for SAS/IACS and local operations managers?

2.3 Escalation – unintentional modifications

It is uncovered that a modification to the logic was made during the previous shift. The modification is reset, and normal production is reinstated.

Jane Smith, who work the previous shift, confirms that she performed a check-up on parts of the control system based on detailed procedures. She explains that the has followed the instructions to the best of her abilities.

2.3.1 Advisory questions

Local operations managers / Personnel responsible for SAS/IACS / Personnel responsible for systems operation

- What are the organisation's procedures for working on the control system?
- Are all personnel aware of who has permission to make modification on the control system?
- Who should be involved when employees have violated the procedures?

2.4 Modification - intentional misconduct

It is uncovered that Jane has not only performed the planned activity, but she has also intentionally executed the modifications that led to the equipment unit shutting down.

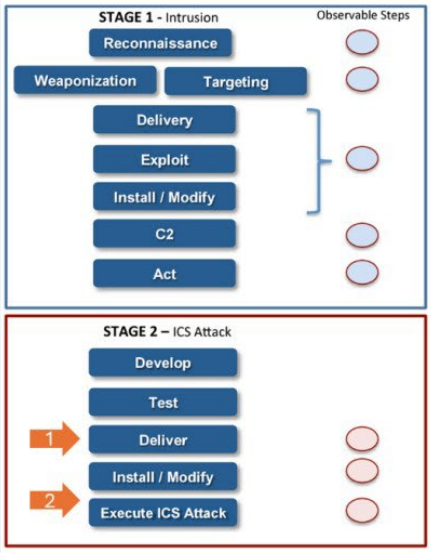
2.4.1 Advisory questions

Local operations managers / Personnel responsible for systems operation

- How do we manage this situation?
- Who should be involved?
- How can we prevent such incidents?

3 Additional information for preparation and implementation

This chapter contains background information about targeted cyber-attacks against industrial ICT systems. Digital attacks often adhere to fixed patterns, often referred to as 'kill chains'. The diagram on the right illustrates the various stages making up this exercise, as well as the exercise items incorporated into the guide.



- Insider
  - The threat actor is already inside the barriers in stage 1
- Attack:
  1) Modifications in program code
  2) Modifications lead to operational disruption
- Exercise points:
  - Uncover sequence of events
  - Uncover and manage motivation

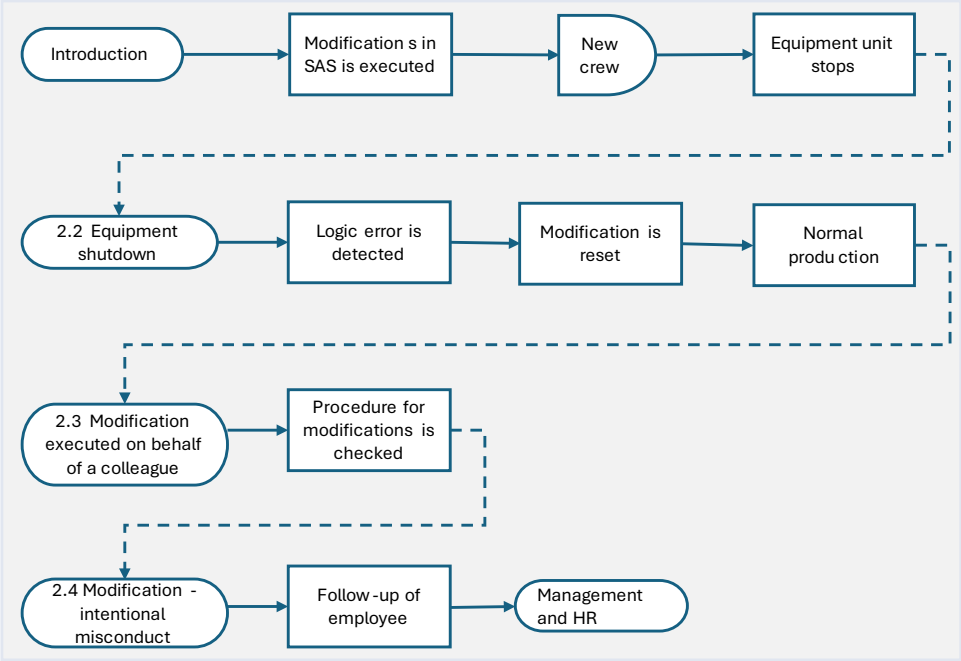
3.1 Introduction to the incident

The sequence of events is based on the premiss that an employee with legitimate access to the control systems makes a modification that, at a later time, leads to operational disruption due to an equipment unit being shut down.

The exercise does not discuss why this employee elects to perform such acts. Such circumstances are discussed in the report referred to in chapter 3.4.

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

- How do the defined procedures support routine checks and modifications on the control systems?
- Which permissions do the employees have to work on the control systems?
- Which measures can be implemented to prevent intentional misconduct to occur?

Local operations managers

- How do we ensure that key personnel are taken care of?
- What are the procedures for managing the incident described in this exercise?

Personnel responsible for systems operation/ICT department

- How do we ensure that key personnel are taken care of?
- What are the procedures for managing the incident described in this exercise?

3.4 Relevant reference material

The use of insiders is an attack technique utilised by various threat actors. Mitre states on their website that *"This technique cannot be easily mitigated with the preventive controls since it is based on behaviours performed outside the scope of enterprise defences and controls. Efforts should focus on minimising the amount and sensitivity of data available to external parties."*

In 2019, the Norwegian Ocean Industry Authority (Havtil) conducted a project to enhance the knowledge about managing insider risk. The report is available on our website.