Chapter 3

MITIGATING EMERGENT VULNERABILITIES IN OIL AND GAS ASSETS VIA RESILIENCE

Stig Johnsen

Abstract This chapter discusses digital vulnerabilities and resilience in the Norwegian oil and gas infrastructure. The Norwegian oil and gas sector is a part of the European Union’s critical infrastructure because Norway supplies approximately 10% of the European Union’s oil and 30% of its gas. Hidden, dynamic and emergent risks are considered and resilience engineering is suggested as a framework for handling, recovering from and adapting to unexpected incidents.

Keywords: Oil and gas assets, emergent vulnerabilities, safety, security, resilience

1. Introduction

Analyzing digital vulnerabilities and enhancing resilience in the Norwegian oil and gas infrastructure are essential to handle the hidden, dynamic and emergent risks that are introduced as new technologies and solutions are incorporated in the infrastructure. The digital infrastructure comprises information and communications systems integrated with supervisory control and data acquisition (SCADA) systems that manage oil and gas production and distribution to customers in the European Union and other countries.

The oil and gas sector is a significant part of Norway’s national industry – it represented more than 19% of the total value creation and contributed 27% of the total state revenue in 2015. Norway is a significant supplier of oil (10%) and gas (30%) to the European Union, which has previously faced energy supply problems that resulted in blackouts and gas shortages.

The term “societal safety” is used in Norway when discussing vulnerabilities at the societal level, such as those in the energy and transportation sectors. The Norwegian Ministry of Justice and Public Security [23] defines it as the ability of society to maintain important societal functions and safeguard citizens’ lives, health and basic needs during different forms of stress. Since oil and gas are
required for transportation, power generation and heating, their uninterrupted supply helps maintain important societal functions. The oil and gas sector can, therefore, be considered a part of the critical infrastructure that supports societal safety. In fact, the Norwegian energy sector is specifically designated by the European Union as a part of its critical infrastructure [4].

The oil and gas industry can be perceived as a “digital ecosystem.” A software ecosystem is defined as a set of businesses functioning as a unit and interacting with a shared market of software and services, along with the relationships among them. The relationships are frequently underpinned by a common technological platform or market and operate via the exchange of information, resources and artifacts [12]. A digital ecosystem is a metaphor inspired by natural ecosystems that describes a distributed, adaptive and open socio-technical system comprising a legal and organizational framework, applications (with components) and their data and digital content, supported by a set of infrastructure services. The concept is useful when exploring digital vulnerabilities and resilience in the oil and gas sector because they depend on how the entire ecosystem is working, developed and improved.

Norway is considered to be one of the most “digitalized” countries in the world [3]. This status offers many major benefits, but challenges abound because the vulnerabilities and risks have progressed significantly. The Norwegian status and experience can be of value to other countries that do not yet have such a high degree of digitalization. Based on a systematic analysis of Symantec incident reports, Subrahmanian et al. [35] have suggested that the Nordic countries (i.e., Norway, Denmark and Finland) are among the safest countries in terms of reported cyber incidents and attacks.

This chapter discusses digital vulnerabilities and resilience in the Norwegian oil and gas infrastructure. Hidden, dynamic and emergent risks are considered and resilience engineering is suggested as a framework for handling, recovering from and adapting to unexpected incidents.

2. Terminology

The goal is to protect critical assets (i.e., objects and processes) of value to stakeholders. The assets are a part of the infrastructure that is of critical importance to society, namely the critical infrastructure.

A vulnerability is a weakness in an asset or process or a gap in the protection efforts. A threat is something that has the potential to cause harm by exploiting a vulnerability. Risk is the combination of the likelihood of occurrence of harm and the potential severity.

The European Union IntegRisk Project [8] defines emergent risk as a risk that is new and/or increasing. The International Risk Governance Council (IRGC) [10] defines emergent risks as new risks or familiar risks that become apparent in new or unfamiliar conditions. Since emergent risks are described as new to an actor or environment, the concepts of knowledge and knowledge maturation are important when examining these risks and the surrounding environment and actors. This is in line with Flage and Aven [7], who emphasize