Mitigating Emergent Vulnerabilities in Oil and Gas Assets via Resilience

Stig Johnsen

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

that knowledge is the key concept for handling emergent risks and black-swan-type events.

Since new risks are difficult to anticipate, a key mitigation strategy is to explore and incorporate resilience; in fact, resilience has been used as a framework to handle surprises caused by new environments and changes. Resilience is the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances, so that it can sustain operations even after a major mishap or in the presence of continuous stress [9].

3. Problem Statement

The threat picture in the oil and gas sector is evolving and new risks are emerging. Information and communications technologies are increasingly used in oil and gas production and distribution. Specifically, the information and communications systems are required to operate industrial control systems that manage critical processes. Thus, an undesirable incident – intentional or random – can impact health, safety and the environment. The Stuxnet attack [5] raised awareness of the vulnerabilities in industrial control systems that can be exploited to cause physical harm. In 2008, a cyber attack was launched against an oil pipeline in Turkey; a review of the incident revealed poor knowledge of cyber vulnerabilities and limited follow-up analysis [34]. In 2014, attackers compromised the control network of a German steel mill and caused considerable physical damage by manipulating the controls of a blast furnace [6]. These cyber-physical incidents and others are important and there is a need to learn from them and to share the knowledge in order to address current and future threats.

Empirical analysis of the Industrial Incident Database [2] reveals that the reported incidents are broad and that multiple actions must be considered because incidents typically involve the exploitation of multiple vulnerabilities. The following categories of incidents were reported in the database:

- **Unintentional Incidents (80%):** Software or hardware errors (38.4%), general malware (30.4%) and human error/poor design (11.2%).
- **Intentional Attacks (20%):** External hackers/attackers (9.4%) and insiders (i.e., employees or consultants) (10.6%).

Thus, there is a need to consider unintentional incidents (i.e., safety issues) as well as intentional attacks (i.e., security issues).

In the context of new cyber-physical incidents and the broad risk picture of the Norwegian oil and gas sector that combines both safety and security, it is necessary to study two main questions:

- What are the main areas of emergent risks in the context of safety and security in the oil and gas industry?
- What are the key strategies for mitigating the emergent risks proactively (i.e., during the planning stage) and reactively (i.e., during the operating and incident response phases)?

This research builds on the International Risk Governance Council's framework of contributing factors related to emergent risks [10]. The contributing factors, as specified in the framework, are: (i) scientific unknowns; (ii) loss of safety margins; (iii) positive feedback; (iv) varying susceptibilities to risk; (v) conflicts about interests, values and science; (vi) social dynamics; (vii) technological advances; (viii) temporal complications; (ix) communication; (x) information asymmetries; (xi) perverse incentives; and (xii) malicious motives and acts. This research has added an additional contributing factor: (xiii) increased connectivity and network interactions.

4. Methods

This research focuses on emergent risks and risk mitigation at two levels: (i) proactively, based on national cyber security strategies and plans, and regulations focused on protecting critical assets; and (ii) reactively, based on assessing knowledge of threats/vulnerabilities, risk assessment procedures, documentation/awareness of incidents/events and procedures for handling emergencies. The perspective is based on a "bow-tie" approach that examines: (i) proactive mitigation through systematic planning of proactive barriers; (ii) incident handling; and (iii) reduction of incident consequences through reactive barriers. Proactive mitigation engages systematic sets of barriers and activities that reduce incident probability. Reactive mitigation engages systematic sets of barriers and activities that reduce incident consequences.

The exploration of the proactive aspects was performed via document reviews and workshop participation. Reviews were performed of cyber security strategies in Europe and in the United States, with an emphasis on emergent threats and impact mitigation through resilience. Regulatory progress related to the protection of critical assets was also studied.

The exploration of the reactive aspects involved thorough reviews of government status reports, surveys of knowledge maturation and interviews of key personnel from the Norwegian Ministry of Justice and Public Security, Norwegian National Security Authority (NSM), Norwegian Police Directorate, and oil and gas industry. Publications produced by the Petroleum Safety Authority (PSA) of Norway were also examined.

5. Vulnerabilities and Resilience

This section presents the results of the analysis of the proactive aspects. Specifically, it discusses strategies and regulatory conditions, and how security activities are performed based on observations by safety authorities and industry personnel.

5.1 Asset Protection

The Security Act of Norway [21] mandates measures for asset protection as specified in the regulations for protecting objects [22]. The Ministry of Defense

has administrative responsibility over the Security Act and the National Security Authority. The National Security Authority is the entity responsible for following up on measures for protecting objects.

Cyber systems are considered to be critical objects and are, therefore, part of the critical infrastructure. The European Council Directive 114/08 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection was released in 2008 [4]. This directive was implemented in Norway in 2012 [25], nearly five years after the European Union implementation, indicating poor proactive efforts.

Additionally, differences exist in how the objects are classified and handled. The European Union considers the Norwegian oil and gas sector to be a part of the European critical infrastructure. A white paper by the Norwegian National Safety Authority [26] specifies the critical infrastructure sectors in Norway as:

- Energy (electricity, oil and gas).
- Transportation and telecommunications.
- Drinking water and infrastructures based on satellites.

On the other hand, the European Council Directive 114/08 lists the sectors as:

- Energy (electricity, oil and natural gas).
- Transportation (roads and highways, railroads, aviation, inland waterways, shipping and ports).

Curiously, as of 2016, the responsible political authority, the Norwegian Ministry of Justice and Public Security, has not designated the Norwegian oil and gas sector as a part of the national critical infrastructure. Thus, the national list of critical objects does not include offshore installations and onshore oil and gas facilities.

In 2009, the Norwegian Police Directorate [28] stated that it is problematic that there is no national list of critical objects outside the scope of the Security Act, such as objects of local character and objects owned by private businesses. This includes offshore installations and onshore oil and gas facilities that are not covered by the Security Act. The same applies to companies in the energy sector such as electric power suppliers.

Norwegian regulations for protecting critical objects [22] were published in 2011. However, discussions of the proposed regulations were extensive, dating back to 1997. In interviews with experts, it was pointed out that the regulations were discussed for more than 13 years before they were finally published. The delay was due to internal discussions – and disagreements – between the various agencies. It was challenging to get the regulations in place; however, they are now used as an important tool to support the work of the Norwegian National Security Authority.

In summary, proactive asset protection efforts in Norway have been poor. It took more than ten years to create regulations for identifying and protecting critical objects.

5.2 Security Guidelines

The process of implementing new rules and regulations was also examined during the interviews. Risk assessment and protection of the oil and gas infrastructure have been considered by industry actors. For example, the safety and security guidelines used by industry were specified in 2004 in the form of checklists and scenarios in methods for verification and validation such as CRIOP [16] and in the OLF 104 best practice technical guidelines [1, 15].

The CRIOP method was developed by key industry participants in collaboration with the Human Factors in Control Network (`www.hfc.sintef.no`).

The OLF 104 best practice guidelines were established in collaboration with the Norwegian Oil and Gas Association (OLF). The guidelines were incorporated in the Petroleum Safety Authority of Norway regulations [31] after ten years. Section 34a of the regulations says that the Norwegian Oil and Gas Guideline No. 104 (OLF 104) should be used as the basis for protecting against information and communications technology hazards. The discussion and acceptance processes were intense and protracted. The slow pace at which the regulations were established demonstrates the poor support given to stakeholders who seek to mitigate emergent vulnerabilities.

Several industrial control system incidents with the potential for harm have occurred in the oil and gas sector, but no major disaster has occurred as of this time (2016). In the surveys and interviews, it was pointed out that there is poor knowledge of security guidelines – only about 50% of the respondents were aware of the guidelines. Additionally, attacks on information and communications technology assets have sometimes not been understood or identified (an offshore server park was unstable for six months before a virus infection was identified and firewall logs are seldom examined and analyzed). Since information and communications system vulnerabilities and incidents are not routinely identified or analyzed, there may be latent vulnerabilities in the infrastructures and poor procedures for handling unexpected incidents if and when they occur. Clearly, the conditions for emergent risks are present.

A key finding related to object protection is that what is prioritized as a part of societal safety does not match what is considered to be a critical infrastructure by all stakeholders. The process of establishing regulations has been slow and cumbersome, and certainly not proactive. Risk assessment is event based (i.e., reactive, not proactive and analytic in nature). Moreover, it took more than ten years to establish regulations, although industry had already prioritized areas of concern with regard to safety and security and had already adopted various rules and best practices.

5.3 Reactive (Not Proactive) Focus

The interviews also focused on how risks were assessed and prioritized. In general, it was observed that the risk assessment process is influenced by undesirable incidents and not driven by a systematic, proactive and analytic approach. Indeed, the process is *ad hoc* and reactive in nature and is driven by

actual incidents. Unfortunately, this may be difficult to change due to limited resources and uncertainties in risk assessments. The 2014 annual report by the Norwegian National Security Authority [27] highlights missing risk assessments, inadequate management and risk governance, and poor proactive implementations of measures for protecting objects. In essence, the interviews and official reports reveal a focus on reactive – as opposed to proactive – protection of objects.

During the research, Norwegian National Security Authority officials were asked how audits and controls of the actual use of regulations were performed, including audits of measures for protecting objects. The officials reported that they used the ISO 19011 standard [11] as a framework for performing audits. Starting in 2013, the Norwegian National Security Authority has performed checkbacks of its audits. This checkback process appears to have enhanced the audit process by ensuring that deviations are handled and mitigated.

5.4 Emergent Threats and Resilience

A strategy is a set of actions (or roadmap) to achieve or reach a specific goal or vision. The process of developing a strategy can be as important as the resulting strategy document because it establishes the context, understanding and ownership (responsibility) in the execution of the strategy. A strategy usually has three parts: (i) diagnosis, which defines the challenges; (ii) policy, which deals with the challenges; and (iii) actions, which are designed to carry out the policy. The development of a national strategy is a collaborative effort involving several actors and it is often exceedingly difficult to specify explicit responsibilities. The current Norwegian National Cyber Security Strategy [24] was published in 2012 by the Ministry of Justice and Public Security; Ministry of Government Administration, Reform and Church Affairs; Ministry of Defense; and Ministry of Transport and Communications.

This research also explored the national cyber security strategies of other countries in Europe and of the United States. The national strategies are concerned about new technologies implemented in key areas and the (implicit) possibility of emergent risks. Thus, there are a variety of perspectives with regard to identifying best practices and common goals/strategies between countries. Luiijf et al. [18] have performed a comparison of nineteen national cyber security strategies. However, the comparison does not cover the strategies of Norway and the other Nordic countries. The Nordic countries are mature and advanced users of information and communications technologies at the societal level. Thus, a review of the Nordic experiences could help advance the state of the art.

Johnsen [14] has reviewed the Norwegian National Cyber Security Strategy. Based on this review and the work by Luiijf et al. [18], the following six areas of concern related to the Norwegian National Cyber Security Strategy are identified:

- Limited focus on international collaboration related to the sharing of common strategies and support of good practices.
- Limited support for identifying and specifying critical infrastructure assets.
- Lack of a formal list of critical objects.
- Limited focus and analysis of emergent threats, especially cyber-physical threats.
- Limited focus on resilience as a strategy for mitigating the effects of unexpected events.
- Limited focus on engaging users to ensure the understanding and acceptance of cyber security strategies.

Since there is no formal national list of critical objects (and functions), there may be a varying focus on protection in the value chain that comprises multiple providers. An example is the Norwegian oil and gas facilities, which are not specified as critical objects by Norway; however, they are designated as a part of the European Union critical infrastructure because they supply large amounts of oil and gas to countries in Europe. This missing perception of criticality was seen in the surveys of operators and service providers in the value chain. Specifically, they do not have common perceptions of the criticality of objects and, thus, object protection procedures vary and are limited in their efficacy. Clearly, there is a need for precise definitions of critical objects and functions in a national cyber security strategy.

Infrastructure is often common across national borders and may have the same vulnerabilities across the borders, but the use of terms, standards and best practices varies in the different jurisdictions. Additionally, the same systems are used in different contexts, which results in the manifestation of different vulnerabilities. Thus, the combination of learning experiences across countries enhances the potential for knowledge maturation. Sharing vulnerabilities between companies across countries is also very beneficial. This practice is not common, but it should become the norm. Good practices are of variable quality and are shared based on different policies (i.e., some are shared while some are not). Some countries, such as the United States, invest considerable effort in developing standards and guidelines; where feasible and with appropriate adjustments, they should become the foundations for common standards and guidelines across countries. Moreover, they should be shared in a more proactive manner. Clearly, there is a need to focus on international collaboration, infrastructure responsibility across borders and the development and sharing of standards and guidelines.

The definition of cyber security differs considerably between countries. The Norwegian National Cyber Security Strategy [24] defines information security as the "protection of the confidentiality, integrity and availability of information;" cyber security is defined as the "protection of data and systems connected to the

Internet." The definition of information security matches the common international definition; however, the definition of cyber security does not match an internationally-accepted definition. The Norwegian definition of cyber security should be aligned with international norms. A suitable definition is proposed by Rauscher et al. [33] – cyber security is the ability to resist intentional and unintentional threats and to respond and recover to incidents.

However, the definition of cyber security should also be expanded to include cyber-physical harm and cyber safety. Information and communications systems are used to manage critical processes in the energy sector, especially for controlling electric power generation, transmission and distribution, and oil and gas production and distribution. The information and communications systems are increasingly being connected to industrial control systems that manage critical processes, which increases the likelihood that an undesirable incident (intentional or accidental) can impact health, safety and the environment.

The concept of cyber security does not adequately accommodate the risks of physical harm posed by the interconnections between cyber systems and physical systems. A concept that covers safety – such as "cyber safety" or "cyber-physical safety" – is required. One possibility is to combine the cyber security definition of Rauscher et al. [33] with the definition of safety proposed by the U.S. Department of Defense [36]: cyber safety is the ability to resist undesirable intentional and unintentional incidents, and to respond and recover to avoid death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

As mentioned above, the International Risk Governance Council (IRGC) has specified a framework of contributing factors related to emergent risks [10]. This research has conducted a subjective evaluation of the importance of the factors in the context of safety and security in the oil and gas industry:

- **Information Asymmetries/Communication:** A key issue is to reduce the level of information asymmetries when stakeholders hold back key information about a risk that is not available to others because of a need-to-know policy. Effective, open and honest communication can help build trust and create a learning organization.

- **Scientific Unknowns/Technological Advances:** The development of the Internet of Things and the integration of information and communications technologies in industrial control systems have created an infrastructure with unknown vulnerabilities. Risks often emerge when a technological change is implemented without an in-depth investigation and evaluation of the consequences. The risks can be exacerbated when policy or regulatory frameworks are inadequate.

- **Loss of Safety Margins/Increased Connectivity and Network Interactions:** Tight couplings may lead to the loss of buffering or margins. This has been seen when industrial control systems are integrated with information and communications systems.

- **Interests, Values and Scientific/Social Dynamics:** Public debates about emergent risks seldom show a clear separation between science, values and interests. There are differences in social standing and dynamics between different actors even in the same company (e.g., offshore vs. onshore and suppliers vs. operators). Thus, it is important to support open information sharing and trust between the various actors.

- **Malicious Motives and Acts:** Malicious motives give rise to emergent risks. In a globalized context with interconnected infrastructures and new dependencies across borders, the effects of an undesirable incident can be broader and more intense than in the past.

5.5 Enhancing Risk Assessment and Recovery

The Petroleum Safety Authority of Norway has performed several surveys of the information and communications technology infrastructure used in the oil and gas industry. A 2010 survey [29] covered fixed offshore installations (i.e., operating platforms and production units). One key finding was that operators had performed poor evaluations of the criticality of objects, contributing to poor risk assessments. In addition, no information security policies were in place [13]. Another problem was that the equipment used in critical operations had not gone through systematic testing and certification processes (e.g., as suggested by ISA Secure (`www.isasecure.org`) or Wurdltech/Acilles (`www.wurldtech.com`)). Moreover, industrial control systems were regularly connected to other networks (offshore and/or onshore) – the "air gap" between operational technology and information technology networks was nothing more than a myth.

Poor network segmentation between critical and non-critical systems was common and the systems were not always independent (e.g., control systems and emergency shutdown systems). Too many actors could access critical systems and secure password policies were either not in place or not enforced. Poor awareness and information sharing about incidents between information technology and operational technology professionals were also common. To address this problem, some companies had established local competence groups (e.g., CERTs), but information was generally not shared across the industry and with the Petroleum Safety Authority of Norway.

Examples of poor awareness and poor risk assessments abound. A survey of oil and gas industry suppliers revealed that around 50% of the respondents were unaware of the relevant information and communications technology safety and security standards or rules such as OLF 104 [13]. Additionally, no emergency response plans or limited plans were in place to deal with breakdowns in the critical information and communications infrastructure. Additionally, there was poor attack awareness; for example, logs of firewalls that protected offshore systems were rarely reviewed in a systematic manner.

The Petroleum Safety Authority also conducted a survey of mobile drilling units in Norway in 2012-2013 [30]. The survey was designed to obtain subjec-

tive assessments based on the OLF 104 guidelines. The survey revealed that there was increased integration of information and communications technology and process control systems, which could impact safety. Additionally, new vulnerabilities were identified arising from increased remote support and real-time data transfer between offshore and onshore facilities. A jump in the number of attacks was also observed.

The Petroleum Safety Authority survey identified three primary concerns:

- Poor user education (related to OLF 104, ISBR 5).
- Missing information security policy (related to OLF 104, ISBR 1).
- Poor documentation and testing of disaster recovery plans (related to OLF 104, ISBR 7).

The three concerns are related. An information security policy usually identifies the criticality and risks that impact the need for user education and the establishment and testing of disaster recovery plans. These areas indicate poor knowledge maturation of threats and risks and, thus, greater likelihood of unanticipated incidents with negative impacts.

5.6 Oil and Gas Sector Vulnerabilities

The Petroleum Safety Authority of Norway and its collaborators have analyzed the digital vulnerabilities in the Norwegian oil and gas industry; a series of reports were published in 2008 [15], 2011 [29] and 2013 [30]. A comprehensive white paper that documented digital vulnerabilities at the societal level was published in 2015 [3]. The white paper identified the following main issues:

- The excellent safety traditions in the oil and gas sector should be transferred to other Norwegian industry sectors.
- The Petroleum Safety Authority should require that barriers be set up to protect against digital vulnerabilities.
- The criticality and vulnerabilities of digital systems in the oil and gas sector should be assessed and documented at the societal level. At this time, there is no national list of critical objects in the offshore and onshore oil and gas industry.
- The ability of the Petroleum Safety Authority to deal with digital vulnerabilities should be strengthened. Specifically, the regulatory framework and knowledge related to protecting oil and gas installations should be enhanced.
- An oil and gas (or energy) computer emergency response team (CERT) should be established.
- Emergency response training related to information and communications system incidents should be enhanced. The reactive barriers in this area are not as sound as the proactive barriers related to digital vulnerabilities.

While the white paper examines resilience related to telecommunications systems, the notion of resilience is not as broad as that described in [9]. What is needed is a strong focus on cyber-physical threats and vulnerabilities, along with a deep consideration of emergent, hidden and dynamic threats.

5.7 Strengths and Resilience

The Norwegian oil and gas industry has certain strengths and resilience characteristics. For several years, the oil and gas industry has been concerned about the vulnerabilities that emerge from increased interconnectivity and real-time monitoring and management of offshore and onshore facilities.

The oil and gas industry has supported the development of methods and regulations to mitigate these weaknesses. Examples are documented in [15], such as the good practice guidelines related to cyber physical threats as described in the CRIOP method [16] and the OLF 104 industry guidelines published by the Oil and Gas Industry Association [1]. These guidelines are effective and should be adapted and used by other Norwegian industries. As a matter of fact, OLF 104 was incorporated in Norwegian regulations in 2014 (however, the process was slow).

The communications infrastructure was created by collaborative efforts between industry and the regulator with a strong focus on safety, security and resilience. For example, the oil and gas industry established a secure, dedicated point-to-point network named SOIL for selected users in the oil and gas community.

Offshore oil and gas equipment employs diverse technical solutions and platforms. The systems are, therefore, difficult to attack at the societal level and it can be argued that they are resilient in some sense [13]. As of 2015, only minor incidents have been reported and no major health, safety or environmental issues have been identified or reported. Some reported incidents [13] could have serious effects in combination with other events. However, systematic vulnerability analyses have not been performed of the entire systems, which means that hidden vulnerabilities may exist.

The criticality of the technical infrastructure has been assessed and documented in a broad survey [13]. Specifically, when a communications infrastructure fails for more than a day, the criticality is assessed to be high and may lead to health, safety or environmental incidents. There has been poor investigation and reporting of cyber-related incidents to the authorities and poor focus on cyber security vulnerabilities in accident analyses (thus, investigations only find what they are seeking [19]). A U.S. National Transportation Safety Board report [20] that scrutinized 13 pipeline mishaps from 1992 to 2004 found key issues in displays, alarm management, training, fatigue and leak detection systems. In ten of these accidents, some aspect of industrial control systems contributed to the severity of the accidents. However, the National Transportation Safety Board did not collect data regarding whether control systems were involved in gas pipeline accidents until 2010. Such information asymmetries can create the foundation for emergent risks.

The Norwegian oil and gas industry has an excellent safety record [32] and has taken proactive steps to develop guidelines and standards. Thus, other Norwegian industries and regulatory agencies (as well as safety authorities) can learn from the industry practices and regulatory principles. At this time, the reporting of information and communications system incidents is not consistent. However, as a result of the report by the Norwegian Committee of Digital Vulnerabilities in Society [3], an excellent opportunity exists to build on the strengths and reduce the weaknesses by reporting industrial control system incidents and successful recovery efforts.

6. Key Findings

This section presents the key findings. When exploring digital vulnerabilities it is important to define a scope that covers systems, regulations and infrastructure. Thus, the term "digital ecosystem" of the oil and gas industry is used. Three key issues related to dealing with emergent vulnerabilities in the digital ecosystem are:

- Handling emergent threats and risks proactively based on regulations, strategies and plans.
- Handling actual emergent incidents based on knowledge, organization, procedures, actions and operations impacted by the vulnerabilities.
- Handling emergent unexpected incidents in a reactive manner.

The following are the key issues that hinder the ability to deal with emergent threats:

- Slow pace in establishing formal regulations to protect assets.
- Slow pace in incorporating industry-developed information and communications system security guidelines in regulations.
- Reactive instead of proactive focus.
- Lack of strategic focus on emergent threats and resilience.
- Inadequate knowledge of risks, quality of risk assessments and ability to recover from incidents.
- Several digital vulnerabilities in the oil and gas sector.

The complacency in establishing formal regulations related to the protection of objects and in including guidelines in regulations demonstrate the challenges of being proactive when improving regulations. The reactive focus and lack of consideration of emergent threats underscore the need to improve the proactive focus. The inadequate knowledge of risks and the need to recover from unexpected incidents emphasize improved risk governance involving societal audits of key mitigating actions. As mentioned above, the Norwegian oil and gas sector has some strengths and resilience capabilities, but these have to be nurtured to help address the safety and security challenges posed by emergent threats.

6.1 Proactive Regulations and Guidelines

The maturation of knowledge about risks is dependent on collaboration through a process based on the exploration of weak signals, discussion of occurrences (real-world, simulated or testbed) followed by the establishment of industry practices and regulations, as described by IntegRisk Project [8]. The knowledge maturation process regarding vulnerabilities must have a structure; specifically, subjects (i.e., stakeholders who improve their knowledge) and objects (i.e., objects having vulnerabilities). The maturation process must handle learning and continuous adaptation by the key stakeholders. This is a slow process that may be negatively impacted when there are few actual occurrences and few learning opportunities.

The knowledge maturation process at the societal level must handle maturation in value chains in different areas; thus, there is a need for international collaboration. In order to enhance learning and adaptation, there is a need to collect and learn from incidents at the international level and to explore regulatory actions and guidelines established by other countries that may have broader and deeper experiences. As a result, it is necessary to be more proactive when examining regulatory actions, guidelines and best practices across borders.

Since the maturation process cannot cover all the emergent risks, it is necessary to impart the ability to adapt and handle the unexpected, which supports resilience. Resilience involves analyzing the possibilities in advance of incidents, handling undesirable incidents and surprises, utilizing the lessons learned based on diverse perspectives and supporting graceful extensibility and sustained adaptation [9]. Resilience engineering should be considered proactively as well as reactively during incident handling to enhance the ability to recover.

Regulation establishes a framework and context for mitigating emergent risks and undesirable incidents. The arguments in support of regulations are:

- Regulations raise standards. This is especially important in the case of emergent threats that need more attention.
- Regulations help deal with scenarios where the consequences of failures can be catastrophic.
- Formulating industry best practices as regulations forces laggards to toe the line while enhancing knowledge and awareness.
- Establishing common regulatory rules across a value chain ensures common risk perceptions by the involved actors.

The result of the maturation process is the ability to handle emergent threats by proactive as well as reactive means. Given the numerous emergent vulnerabilities, it is imperative to develop and apply proactive and reactive approaches to reduce risk.

6.2 Emergent Threats and Resilience

Resilience is mentioned in only nine of the 19 cyber strategies examined by Luiijf et al. [18] and it is not explicitly addressed in the Norwegian Cyber Security Strategy [24]. In an environment facing emergent risks and the increased possibility of intentional attacks, it is simply not possible to have a clear understanding of risks and undesirable incidents. Therefore, a key strategy is to focus on resilience in order to endow the ability to handle surprises and adapt to ensure adequate operational capabilities and recovery.

It is important to define the notion of cyber safety to handle interconnections between cyber systems and physical systems and to incorporate cyber safety in cyber strategies. As a consequence, the Norwegian Cyber Security Strategy should specify and mandate standards and methods covering information and communications systems as well as cyber-physical systems. To ensure that technology is resilient and robust, stress testing and certification of key components should be performed. Certification should be performed based on accepted standards such as the IEC 62443 Conformity Assessment Program. In a society with emergent risks, the ability to handle unexpected incidents requires the mobilization and involvement of all levels of society. Thus, a national cyber security strategy should focus on engaging citizenry in cyber security and cyber safety efforts. The adaptation to and handling of undesirable and unexpected events must be underpinned by a framework that enables society to support key societal functions.

6.3 Risk Governance and Societal Audits

The Norwegian Cyber Security Strategy [24] describes several gaps. For example, security measures are often unsystematic and fragmented, and information security efforts do not have enough support from management and are not well integrated into business management. These gaps match some of the findings in [3].

According to the Norwegian Cyber Security Strategy, it is also important to audit strategies and the results of the strategies in order to close the gaps and reduce complacency (i.e., lack of management support and poor integration with business management). The audits should be based on a recognized standard such as ISO 19011 [11] that is used by other regulatory authorities, including the Norwegian National Security Authority.

At the societal level, it is necessary to be more proactive by implementing mitigation actions [17] and performing audits and checks that can be reported to the legislative branch. A suitable entity for implementing this could be Norway's Office of the Auditor General (Riksrevisjonen). The office could audit strategies to address complacency, poor prioritization, difficult cross-sectoral challenges and limited collaboration. This may be especially effective because the Office of the Auditor General is the national government auditor and is directly subordinate to the Norwegian Parliament.

7. Conclusions

As with other infrastructure sectors, the Norwegian oil and gas sector faces many emergent digital vulnerabilities. The sector is considered to be a part of the European Union's critical infrastructure because it supplies approximately 10% of the European Union's oil and 30% of its gas. However, Norway itself does not categorize its oil and gas assets and the associated information and communications systems as a part of its national critical infrastructure, creating different perceptions of protection in the value chain. As a result, there is significant variability in safety and security policies, procedures and implementations. Given the scope and magnitude of the emergent threats, there is an urgent need to be more proactive with regard to regulations, knowledge, risk communication and technology, and to establish strategies for dealing with unexpected incidents. Resilience engineering is an important component of any strategy for adapting to and recovering from incidents in a graceful manner.

It is also important to focus on testing and certification of critical cyber-physical equipment whose disruption or destruction can cause negative health, safety and environmental effects. Risk governance should be enhanced through improved incident investigations, audits throughout the value chain and frequent reviews of mitigation strategies and actions. Knowledge sharing should be enhanced through research, collaboration between safety and security experts and the creation of industry-specific computer emergency response teams. Finally, European Union countries, other European nations and the United States should expand and strengthen their cross-border efforts to ensure that the globally-connected critical infrastructure is both secure and resilient.

Acknowledgements

This research was conducted under the New Strains Project supported by the Norwegian Research Council. The research was also supported by the Norwegian University of Science and Technology (NTNU).

References

[1] R. Ask, R. Roisli, S. Johnsen, M. Line, A. Ueland, B. Hovland, L. Groteide, B. Birkeland, A. Steinbakk, E. Hagelsteen, C. Rong and T. Losnedahl, Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems, Norwegian Oil and Gas Association, Stavanger, Norway, 2006.

[2] E. Byres, Using ANSI/ISA-99 Standards to Improve Control System Security (plus White Paper), Tofino Security, Lantzville, Canada, 2012.

[3] Committee of Digital Vulnerabilities in Society, Digital Vulnerability – Secure Society: Protecting People and Society in a Digitalized World (in Norwegian), Official Norwegian Report (NOU 2015:13) to the Ministry of Justice and Public Security, Oslo, Norway, 2015.

[4] European Council, Council Directive 2008/114/EC on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, Brussels, Belgium, 2008.

[5] N. Falliere, L. O'Murchu and E. Chien, W32.Stuxnet Dossier, Symantec, Mountain View, California, 2011.

[6] Federal Office for Information Security, The IT Security Situation in Germany in 2014, Bonn, Germany, 2014.

[7] R. Flage and T. Aven, Emerging risk – Conceptual definition and a relation to black swan type of events, *Reliability Engineering and System Safety*, vol. 144, pp. 61–67, 2015.

[8] German Institute for Standardization (DIN), Standard DIN CWA 16649, Managing Emerging Technology-Related Risks, Berlin, Germany, 2013.

[9] E. Hollnagel, D. Woods and N. Leveson (Eds.), *Resilience Engineering: Concepts and Precepts*, CRC Press, Boca Raton, Florida, 2006.

[10] International Risk Governance Council, Guidelines for Emerging Risk Governance, Lausanne, Switzerland, 2015.

[11] International Standards Organization, ISO 19011:2011, Guidelines for Auditing Management Systems, Geneva, Switzerland, 2011.

[12] S. Jansen, A. Finkelstein and S. Brinkkemper, A sense of community: A research agenda for software ecosystems, *Proceedings of the Thirty-First International Conference on Software Engineering*, Companion Volume, pp. 187–190, 2009.

[13] S. Johnsen, An Investigation of Resilience in Complex Socio-Technical Systems to Improve Safety and Continuity in Integrated Operations, Ph.D. Dissertation, Department of Computer and Information Science, Norwegian University of Science and Technology, Trondheim, Norway, 2012.

[14] S. Johnsen, A comparative study of the Norwegian cyber security strategy vs. strategies in the EU and U.S. – Emerging cybersafety ignored, in *Safety and Reliability of Complex Engineered Systems*, L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio and W. Kroger (Eds.), CRC Press/Balkema, Leiden, The Netherlands, pp. 3485–3492, 2015.

[15] S. Johnsen, R. Ask and R. Roisli, Reducing risk in oil and gas production operations, in *Critical Infrastructure Protection*, E. Goetz and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 83–95, 2008.

[16] S. Johnsen, C. Bjorkli, T. Steiro, H. Fartum, H. Haukenes, J. Ramberg and J. Skriver, CRIOP: A Scenario Method for Crisis Intervention and Operability Analysis, SINTEF, Trondheim, Norway, 2011.

[17] S. Johnsen and A. Oren, Ten years from risk assessment to regulatory action – Is complacency creating a reactive and brittle regulatory regime in Norway? in *Safety and Reliability of Complex Engineered Systems*, L. Podofillini, B. Sudret, B. Stojadinovic, E. Zio and W. Kroger (Eds.), CRC Press/Balkema, Leiden, The Netherlands, pp. 3333–3339, 2015.

[18] E. Luiijf, K. Basseling and P. de Graaf, Nineteen national cyber security strategies, *International Journal of Critical Infrastructures*, vol. 9(1-2), pp. 3–31, 2013.

[19] J. Lundberg, C. Rollenhagen and E. Hollnagel, What-you-look-for-is-what-you-find: The consequences of underlying accident models in eight accident investigation manuals, *Safety Science*, vol. 47(10), pp. 1297–1311, 2009.

[20] National Transportation Safety Board, Supervisory Control and Data Acquisition (SCADA) in Liquid Pipelines, Safety Study NTSB/SS-05/02, PB2005-917005, Notation 7505A, Washington, DC, 2005.

[21] Norwegian Ministry of Defense, The Security Act (in Norwegian), Oslo, Norway, 1998.

[22] Norwegian Ministry of Defense, Measures for Protecting Objects (in Norwegian), Oslo, Norway, 2011.

[23] Norwegian Ministry of Justice and Public Security, Statement on Safety and Security, Report 17 (2001–2002), Oslo, Norway, 2002.

[24] Norwegian Ministry of Justice and Public Security, National Cyber Security Strategy for Norway, Oslo, Norway, 2012.

[25] Norwegian Ministry of Justice and Public Security, The Implementation of the EPCIP Directive, Oslo, Norway, 2012.

[26] Norwegian National Security Authority, Guideline for Protecting Objects, Oslo, Norway, 2014.

[27] Norwegian National Security Authority, Safety Report 2014, Oslo, Norway, 2014.

[28] Norwegian Police Directorate, Response on Measures for Protecting Objects, Oslo, Norway, 2009.

[29] Petroleum Safety Authority of Norway, Safety System Independence in Focus, Stavanger, Norway, 2010.

[30] Petroleum Safety Authority of Norway, Review of ICT – Security in Drilling, Process Control, Safety and Support Systems within the Oil and Gas Sector (in Norwegian), Stavanger, Norway, 2013.

[31] Petroleum Safety Authority of Norway, Regulations Relating to Design and Outfitting of Facilities, etc. in the Petroleum Activities (The Facilities Regulations), Stavanger, Norway, 2015.

[32] Petroleum Safety Authority of Norway, Trends in Risk Level, Stavanger, Norway, 2015.

[33] K. Rauscher and V. Yaschenko (Eds.), Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations, Issue 1, EastWest Institute, New York and Information Security Institute, Moscow State University, Moscow, Russia, 2011.

[34] J. Robertson and M. Riley, Mysterious '08 Turkey pipeline blast opened new cyberwar, *Bloomberg*, December 10, 2014.

[35] V. Subrahmanian, M. Ovelgonne, T. Dumitras and B. Prakash, *The Global Cyber-Vulnerability Report*, Springer International Publishing, Cham, Switzerland, 2015.

[36] U.S. Department of Defense, Department of Defense Standard Practice: System Safety, MIL-STD-882E, Washington, DC, 2012.