IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 28, 2020, accepted July 1, 2020, date of publication July 8, 2020, date of current version July 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007960

Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns

GEORGE STERGIOPOULOS[1], DIMITRIS A. GRITZALIS[1], AND EVANGELOS LIMNAIOS[2]
[1]Department of Informatics, Athens University of Economics and Business (AUEB), 104 34 Athens, Greece
[2]Public Gas Corporation of Greece (DEPA) SA, 141 21 Athens, Greece

Corresponding author: Dimitris A. Gritzalis (dgrit@aueb.gr)

ABSTRACT During the past two decades, oil and gas operational and information technology systems have experienced constant digital growth, closely followed by an increasing number of cyber-attacks on the newly interconnected systems. Adversaries exploit vulnerable accessible device or malware attacks networked services, in an attempt to gain access to critical systems and machinery that are interconnected over networks. Given the importance of the oil and gas sector on the global economy and the diversity of critical systems often being controlled over remote locations, it is highly important to understand and mitigate such attacks. In this paper, we survey cyber-attacks on all three domains of the oil and gas sector (upstream, midstream, downstream) starting from the early 90s up until 2020. For each domain, we document and analyze verified attacks based on real-world reports and published demo attacks on systems. We map and catalogue the attack types used in each case, in order to understand common and subliminal attack paths against oil and gas critical operations. Our aim is threefold, i.e., first, to assess documented attacks using standardized impact assessment techniques and highlight potential consequences of cyber-attacks on this sector, second, to build a vulnerability taxonomy based on technical knowledge gathered by all such incidents and connect each vulnerability with oil and gas systems and respective attack paths, and third, to map the documented knowledge and taxonomies with MITRE's international knowledge base of Adversary Tactics and Techniques, so as to provide a general guide for analyzing and protecting against cyber-attacks at oil and gas infrastructures.

INDEX TERMS Cybersecurity, cyberattack, oil and gas, critical infrastructure, refinery, operational technology, information technology, vulnerability, impact, risk, safety, survey.

I. INTRODUCTION

Oil and Gas (O&G) infrastructures are divided in three broad categories: upstream, midstream and downstream infrastructures. Upstream infrastructures support operations for exploring and drilling operations, midstream is responsible for the transportation of oil and gas and for providing a link between upstream production and downstream dissemination, while downstream focuses on distributing assets to consumers, mainly for crude oil and raw/condensed natural gas.

The O&G sector is one of the most important Critical Infrastructure (CI) sectors for economy, housing and transportation. According to market reports, upstream oil investment reached USD 500B only for 2019, with the global oil demand stabilizing around 1M barrels/day [1], [2]. In Canada, 97% of oil and petroleum products are transported via pipelines. The consumption of natural gas worldwide was recorded to be around 140T cubic feet (Tcf) for 2018 alone [3], and is projected to increase to 203Tcf by 2040 [1]. According to American Petroleum Institute's report of 2019, the US pipeline system (midstream infrastructure) consists of 2.7M miles of pipelines transferring assets between locations [27]. Midstream infrastructure connects to refineries and facilities working to distribute oil and gas to the end-users (downstream infrastructure).

Like all other sectors, the O&G industry has been affected by the constant digital growth. Industrial Control Systems (ICS) used to operate in isolation, without bridging over IT infrastructures. Industry 4.0 enabled the integration of multiple industrial technologies in ICT, with engineers able to remotely maintain Supervisory Control and Data

The associate editor coordinating the review of this manuscript and approving it for publication was Ilsun You.

Acquisition (SCADA) systems [4] and monitor operations in real-time through actuators and smart sensors [5].

This digital evolution exposes Operational Technology (OT) infrastructures to multiple new attack surfaces and vectors. Current estimations state that, by 2020, connected devices may reach 50B globally [6]. Reports from numerous international bodies and organizations state that, even though attacks on interconnected industrial systems can lead to incidents with severe economic and societal impact [7]–[12], still the security readiness and resilience of such infrastructures is considerably low [13]–[19]. Reports from the National Institute of Standards and Technology (NIST) [7], the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [19] and the European Agency for Network and Information Security (ENISA) [20] warn for numerous vulnerabilities in current OT systems in numerous CI. Attacks have occasionally affected power grids [21], smart cities [22], and the health industry [20].

A. MOTIVATION

Numerous publications exist on cyber-physical attacks and defenses, which cover numerous critical infrastructure sectors like the Energy, Health, and Telecommunications sector. MITRE has recently released the ATT&CK framework that covers generic attacks on ICS [23]. ENISA has numerous publications on OT systems [20] and NIST has a specific publication on OT security [7]. Still, to our knowledge, there has been no systematic approach to catalog, map, and classify cybersecurity attacks on the O&G sector. Modern history has already proven that oil and gas OT infrastructure is vulnerable against cyberattacks. A number of reported incidents support this, with the most recent taking place in Q1 2020 when a ransomware attack affected ‘‘the control and communication assets on the OT network of a natural gas compression facility’’ [24].

Reports clearly indicate that attacks on ICS of the O&G sector can have adverse effects to wide geopolitical areas and multiple countries. Even worse, the severity of some security incidents is likely to exacerbate due to cascading failures introduced by dependencies of other CI on the O&G infrastructure [25]. Interesting though, a subset of these attacks did not specifically target O&G OT infrastructures. Instead, some ICS were infected following random spread patterns of ransomware and similar malware.

B. CONTRIBUTION

The first step in creating an overall approach to protect the O&G OT infrastructure is to map, analyze, and understand current attacks and vulnerabilities in this sector. Concerning attacks on the OT infrastructure, we must examine attack vectors and vulnerabilities exploited by documented cases across all layers of an ICS architecture. After mapping attack surfaces, vectors, and common similarities, we must assess the importance and severity of each case, as well as model controls to prevent threats from reoccurring in similar systems.

In this paper, we survey cybersecurity attacks that occurred in all three O&G subsectors from the early ‘90s to Jan. 2020. In each case, we map their attack surfaces, detect the infiltration techniques along with present vulnerabilities and assets affected and classify each incident’s impact and adverse effects according to a standardized impact scale.

We utilize two international cybersecurity information frameworks to (i) support our survey on O&G cyberattacks and (ii) develop an O&G cybersecurity vulnerability taxonomy. The frameworks are (a) MITRE’s ATT&ACK framework [23] and (b) MITRE’s Common Attack Pattern Enumeration and Classification (CAPEC). ATT&CK ‘‘describes operational phases in an adversary’s lifecycle, pre and post-exploit and details techniques used’’ [26]. On the other side, CAPEC enumerates malicious attack patterns.

After gathering white and grey literature on O&G cyberattacks, we utilize these frameworks and our newly established vulnerability taxonomy to classify each attack per layer, per type of system, and per attack technique (i.e. exploit and vulnerability type used). We use CAPEC and ATT&CK complementarily, to aid readers determine which attacks occur most often, map attack types with ATT&CK’s adversary tactics and techniques, and understand which assets are most vulnerable in each type of attack.

We also provide a qualitative impact analysis of each recorded attack based on the adverse effects and type of systems affected. To do this, we use a semi-qualitative impact assessment table, which is assembled by information taken from national bodies, such as NIST, and relevant reports from international companies that analyzed the impact of unavailability of systems in the O&G infrastructure.

We focus on attacks that had extensive or severe impact either to society or to the industry, and targeted infrastructures often supporting other infrastructures that may have consequently been affected. We only map attacks recorded by official bodies or valid organizations and researchers. Lab attacks or simulated attacks (e.g. such as attacks validated in Hardware-In-the-Loop (HIL) testbeds) are not included in this survey. This cumulates to:

(1) A novel vulnerability taxonomy, specifically developed for O&G systems that is directly tied to MITRE’s frameworks,
(2) An extended catalog of real attacks on upstream, mid and downstream O&G systems, along with their impact analysis that utilizes the above-mentioned taxonomy and an O&G -specific impact assessment method to assess real attacks. As a result, the presented approach is directly applicable to any O&G situation by relevant experts.
(3) A systematic catalog, analysis, and classification of attacks on all three O&G systems (upstream, midstream, downstream), as well as a thorough analysis of those that highlights commonalities, most used attack vectors and most common vulnerabilities currently being exploited in the O&G sector, presented per subsector and per vulnerability.

C. STRUCTURE

The following sections are structured as follows: Section II presents related surveys and analysis in the field of industrial cyberattacks, while Section III explains the survey methodology we used to detect, record, and classify cyber-attacks in the O&G sector through various reports, articles, and publications.

Section IV provides a typical model of the OT infrastructure in ICS, specifically for the O&G systems. Here, we map assets of O&G ICS per layer and create a reference connection of each one to ATT&CK's asset type levels.

Section V presents the developed taxonomies used in this paper to classify recorded attacks. First, we present a taxonomy of generic types of attacks on O&G systems. We rely on the Common Attack Pattern Enumeration and Classification (CAPEC) and MITRE ATT&CK taxonomies to introduce basic attack types for O&G systems. We then develop a taxonomy of vulnerabilities per layer, assembled from relevant literature and recorded attacks on O&G systems. We identify, map, and present different types of vulnerabilities that have affected the O&G sector. Last but not least, we introduce an impact assessment methodology for assessing the severity of attacks and briefly analyze its dimensions and evaluation attributes.

In Section VI, we present all identified cyber-attacks on the O&G sector and classify them using the above mentioned taxonomies. We also provide a brief presentation and assessment of the impact of each detected attack.

In Section VII we summarize security controls that can mitigate the impact or lower the threat of the presented attacks.

Finally, Section VIII discusses potential security controls that stem from all classified attacks and can be used for mitigating cyber-attacks in O&G infrastructures, while Section IX discusses identified security gaps and elaborates on potential future work.

II. LITERATURE REVIEW

Numerous publications exist, both in the academic and grey literature, that address diverse aspects of cybersecurity issues in critical infrastructures and operators of essential services. From an academic point of view, most surveys either tackle various threats and vulnerabilities common in multiple ICS types and CI sectors [4], [5], [8], [52], [115], [117] or emphasize on specific sectors, e.g. Energy or Telecommunications [93]. The field is densely published, even with a few meta-surveys that summarize and classify CPS domains, attacks, and research-trends [116].

In this section, we briefly present both types of articles and relevant surveys. We then highlight their differences in scope and goal with our survey.

A. ACADEMIC SURVEYS ON CRITICAL INFRASTRUCTURE SECURITY

Industrial control and SCADA system architectures are similar between infrastructures and usually apply to diverse systems and components. Thus, most surveys target ICS security in general, and group security concerns and mitigation mechanisms with generic SCADA models. These generic surveys combine several domains when addressing CPS security. Such approaches may provide a common overall picture for ICS cybersecurity and allow national bodies [7] and standards [111] to address issues, threats and vulnerabilities that are common to all CI; a useful approach when addressing cybersecurity threats and mitigation mechanisms for diverse operators.

Kim and Kumar [121] published one of the first surveys concerning CPS research efforts, while Krotofil and Gollmann [122] presented a survey on ICS security and discussed protocol-related (Modbus/TCP, DNP3, IEC 61850) and sensor/actuator-related vulnerabilities, along with potential security controls to mitigate their risk.

Kim *et al.* [93] were one of the first to publish an extended survey on CPS and smart grids, highlighting security challenges and approaches in the broad field of CPS security.

McLaughlin *et al.* [8] explore the ICS cybersecurity landscape and address key principles of ICS operation and testing. They provide an overview of ICS security assessment techniques and suggest a process for ICS vulnerability assessment.

Other surveys focus on the Industrial Internet of Things (IIoT), like [123] and [5]. In [5], authors assess the current IIoT landscape by analyzing representative attacks and assessing IoT-enabled cyber-incidents using a risk-like approach. In [123], authors delve into security and privacy concerns for the industrial Internet of things and propose mitigations.

Khan *et al.* [134] published research specifically about reliable IoT-based architectures for the Oil and Gas Industry. They propose alternate architectures for functional and business requirements applicable in both upstream, midstream and downstream oil field services that take into consideration security issues.

In [4], authors present identify vulnerabilities and potential threats in CPS, and describe solutions for mitigating the presented attacks. Sayegh *et al.* [52] present a test-bed for detecting vulnerabilities within SCADA protocols against internal attacks and present a comprehensive list of such vulnerabilities.

In [117] authors survey tools and techniques to detect SCADA system vulnerabilities in CPS common in numerous sectors, while Bhamare *et al.* [115] document major publications both from industry and academia that tackle the applicability of machine learning techniques on ICS cybersecurity.

Our work is close to [118], where authors review industrial systems using real cyber-security incidents against SCADA systems. Authors also classify the attacks based on similar criteria like the attack method and the potential impact of the attack. They too opt to provide a taxonomy that will be used in order to compare current and future SCADA incidents, although their analysis is of limited depth and does not correlate to international frameworks such as MITRE's ATT&CK, and is rather generic, without focusing on a specific sector. Thus, it cannot support the technicalities and consequence idiosyncrasies of the O&G sector.

B. RELATED WORK FROM INDUSTRY AND ORGANIZATIONS

Outside academia, various grey literature publications exist, mainly from industry and national organizations. Such publications usually neither analyze the effects of real-world attacks, nor allow for targeted analysis of events per sector. Rather, they aim to model types of threats and vulnerabilities along with mitigation measures for assets common in numerous ICS architectures. For example, special publication NIST 800-82 [7] examines such a range of security and privacy issues in ICS and addresses industrial IoT issues. Report SP800-82's content is applicable to all domains and CI sectors.

Still, some reports exist that briefly mention or catalog cybersecurity incidents on CI (e.g. [5], [16], [66], [79], [94]), although they mostly utilize events to support other types of analysis, such as statistics or trend analysis. To this end, such publications either do not focus on real-world events or are incomplete in their listings and only refer to real-world attacks for argument's sake, to support their analysis or conclusions on relevant subjects.

Kaspersky Labs frequently publish reports and case studies [11], [47] that identify security issues in ICS on all layers, i.e., from physical and network security to vendor-specific vulnerabilities, SCADA systems and Programmable Logic Controllers (PLC).

FireEye [18] also publishes annual or bi-annual ICS vulnerability surveys, identifying common vulnerabilities and issues present in CPS.

MITRE recently published the ATT&CK framework [23], a knowledge base of adversary tactics and techniques based on real-world observations. ATT&CK has a separate section for ICS security, along with lists of ICS threats and techniques and documented adversary groups from ICS related incidents. Although not O&G-specific, most information therein is relevant to O&G cyberattacks and systems.

Dragos has published a comprehensive time frame of ICS attacks [55], along with numerous cataloguing of potential cyber-attacks on industrial systems. Although analysis is high-level, Dragos also publishes similar reports in a modular way, assessing different sectors and systems.

National bodies and organizations also publish reports that survey aspects of CPS security. Among those, the most important seem to be best practice reports and frameworks published from the United States, as well as some key Directives of the European Union.

The US Dept. of Homeland Security (DHS) has frequently published best practices on identifying common cybersecurity vulnerabilities and mitigation control in industrial control systems [9]. DHS has also published the US National Infrastructure Protection Plan (NIPP) [101] that highlights key concepts concerning threats, attacks and risk on all types of CI. NIST has relevant publications: Special Publication 800-82 [7] provides a thorough guide to industrial control systems (ICS) security, tackling ICS threats and vulnerabilities, recommended practices, and architectures. Other NIST publications that apply to CPS include publications from the Computer Security Division-Computer Security Resource Center [33], as well as Special Publication 800-63-3 [37] on technical requirements for implementing digital identity services, identity proofing and authentication of users in critical systems.

The US Dept. of Energy published a Risk Management Guide specifically for the Energy infrastructure that also covers the O&G sector [105]. The article provides a non-mandatory risk management approach for energy systems and does not correlate directly with cyber-attacks, although most of its procedures are applicable to our concepts.

ISO/IEC publish standardized guidelines for assessing risk and providing guidelines for information security risk management [59]. ISO's international standards support the general concepts specified in ISO/IEC 27001 which are also applicable to CPS and ISO/IEC TR 19791:2010 on the security evaluation of operational systems [119].

From an EU perspective, the European Commission has published numerous Directives that either highlight key cybersecurity issues concerning ICS similar to those in the O&G sector, or lay the groundwork for the publication of reports and best practices like those presented in this chapter. Briefly, the most important appears to be the Directive (EU) 2016/1148 of the European Parliament and of the Council 2016 "concerning measures for a high common level of security of network and information systems across the Union" [99]. Also, the EU published a regulation [100] 2019/881 of the European Parliament and of the Council on information and communications technology cybersecurity certification. Other relevant publications include the 2012/18/EU Directive from the European Parliament (SEVEZO-III) [102] which highlights key concepts of addressing hazards and consequences from various types of scenarios, including cyberattacks on industrial systems.

Modern reports also focus heavily on the digitization of the O&G sector, along with the use of IoT and smart meters to automate monitoring and control. EY [124], Deloitte [126] and PWC [127] all published technical reports recently on the cybersecurity aspects of IoT in the Energy sector, with some reports focusing specifically in O&G [124], [126], [127].

CISCO published a report together with Schneider Electric and AVEVA [128] on how to tackle security in real-time pipeline operations. Fortinet recently (2020) published an extensive independent study [125] on security trends on the digitization of critical infrastructure, and focused specifically to those who utilize IoT to manage and maintain; along with the O&G sector.

C. SURVEYS ON O&G CYBERSECURITY

To our knowledge, very few academic publications survey cybersecurity topics specifically for the O&G sector. Still, some grey publications exist that describe different cybersecurity issues that concern this sector. Companies, security vendors and O&G boards have published some approaches and reports that list potential security threats or highlight common vulnerability types that exist in O&G ICS.

Hacquebord and Pernet from TrendMicro have published a survey on threats that target the O&G Industry [77]. They support their analysis by also providing a list of known hacking groups and their cyberattacks on the O&G sector.

In [66], Dragos published a survey on O&Gas Cyber Threats, where authors assess activity groups affecting the global O&G Industry and provide ''a snapshot of the threat landscape and what is expected to change in the near future''. This publication effectively catalogues hacking groups and state actors that target O&G infrastructures, although they do not provide any analysis on systems or impact factors.

Another publication specifically targeting cyber security attacks for the O&G industry is presented by Radmand *et al.* in [92]. Authors present a taxonomy of wireless sensor network cybersecurity attacks in the O&G industries. They present common wireless network security requirements and tie them to potential attacks on wireless networks implemented in O&G ICS. This is a survey targeted specifically on O&G, although it only focuses on wireless technologies and do not refer to known cyber-incidents to extend their analysis.

Last but not least, authors in [94] published a comprehensive cyber risk technical review specifically for the upstream subsector in O&G sector. They provide an extensive analysis of threats, common attacks, and even catalog an extensive list of upstream cybersecurity incidents. To our knowledge, this is the only existing publication that addresses both threats and vulnerabilities for the O&G sector, while supporting their analysis using real-world documented incidents. However, their approach focuses only on upstream infrastructures and considers only systemic risks [94].

D. COMPARISON WITH THIS SURVEY

All mentioned publications, articles and reports cover numerous security concepts that are directly or indirectly relevant to the O&G sector. Even though some of them provide extensive analysis of major ICS security issues and vulnerabilities [8], [18], [21], [40], [47], [71], just a few actually support their impact assessment outcomes besides listing the consequences of attacks. Only three articles provide a thorough systematic analysis of real-world cybersecurity incidents [8], [47], [61], while none focuses specifically on the O&G sector. In addition, most publications that catalog real-world attacks are either incomplete or lack adequate substantial knowledge extraction from them to be used directly by O&G system operators. Some grey literature works [18], [66], [94] manage to catalog a number of O&G cybersecurity events, without providing further analysis of these events to draw useful risk assessment conclusions for O&G systems.

The methodology used in this article is conceptually close to [5] and [118] with relevant aspects also shown in [66] and [94]. The corresponding analysis studies documented attacks (real-world, as well as a few testbed attacks), but focuses specifically on the O&G sector. Thus, it is making our impact assessment and systematic analysis more thorough and useful for O&G operators. Also, our vulnerability taxonomy is created by analyzing the architecture of actual O&G ICS and supports results through the actual documented incidents that happened to them. We do not use generic, simulated or component-based attack assessment. In addition, we define a qualitative impact/consequences assessment method specifically for the O&G sector, taking into consideration relevant particularities of the sector through previous analysis of targeted attacks on O&G ICS infrastructures, network and PLC/RTU systems. Our vulnerability taxonomy is directly tied to MITRE's frameworks and is specifically developed for O&G systems. The presented impact analysis of real-world documented events follows as a proof-of-use of the taxonomy and assessment on real attacks. Thus, it is directly applicable to any O&G situation by relevant experts. Also, contrary to [94], we catalog, analyze and classify all three O&G systems (upstream, midstream, downstream) and detect commonalities and security issues per subsector and per vulnerability.

III. SURVEY METHOD

The method utilized to develop this survey is comprised of 4 steps: (1) Survey protocol and scope development, (2) Search and identification of selected studies based on scope, (3) Screening of literature based on quality, and (4) Reporting (extraction of information, synthesis and reporting of findings).

Figure 1 depicts the overall survey framework and describes the flow of each aforementioned step. Presented steps offer a reproducible algorithm for managing scientific and industrial literature used in this article both for developing the O&G vulnerability taxonomy and for recording and classifying cyber-attacks at the O&G sector. Our approach is based on the survey methodology presented in [98].

First, we gathered all detected documents (455 files) both from academia and grey literature (reports, white papers, company publications etc.). We excluded articles written in languages we could not parse, removed duplicates and moved on to evaluate each detection. Some articles were excluded based on title (152), while other were excluded upon reading their abstract (111) or full text body (36). Most common issue we faced was to detect information that is tightly coupled with O&G, and not to a generic ICS system that applies to any OT infrastructure. Final inclusion addressed 135 articles.

A. OBJECTIVES AND STRATEGY

We first define the aims and scope of the survey. Then, we evaluate available vulnerability taxonomies and cybersecurity controls relevant with O&G infrastructures. These will aid in understanding underlying issues in recorded attacks,

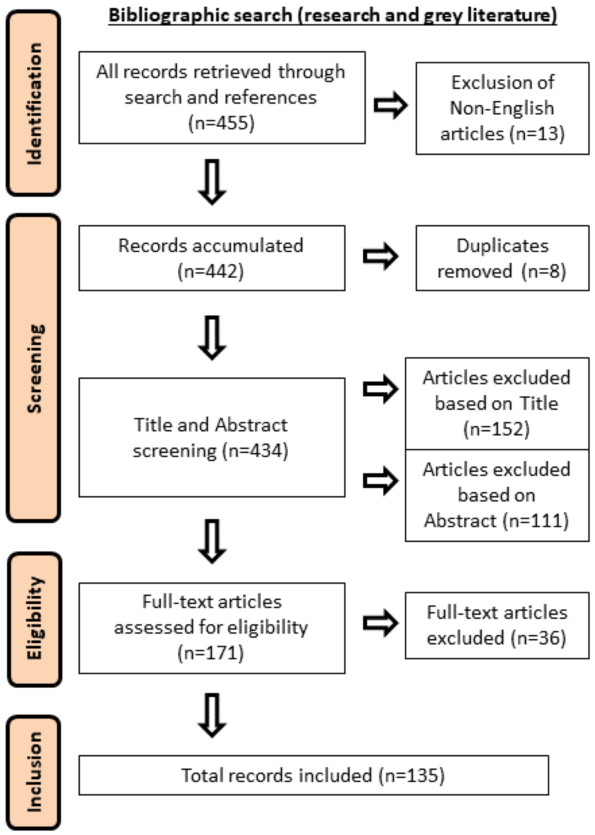
Bibliographic search (research and grey literature)
Identification
Screening
Eligibility
Inclusion
All records retrieved through search and references (n=455)
Exclusion of Non-English articles (n=13)
Records accumulated (n=442)
Duplicates removed (n=8)
Title and Abstract screening (n=434)
Articles excluded based on Title (n=152)
Articles excluded based on Abstract (n=111)
Full-text articles assessed for eligibility (n=171)
Full-text articles excluded (n=36)
Total records included (n=135)

FIGURE 1. **Overview of the survey methodology.**

develop an O&G vulnerability taxonomy, and support the analysis of existing implementation gaps and areas open to improvement in the sector.

The objectives along with their supporting research questions are presented in Table 1. The table depicts our search goal, the relevant question posed to achieve this goal and the related key-word searches used to detect relevant material. Key-word searches were first based on the TITLE of each article, and were further refined by searching the ABSTRACT of each detected publication. To work on set goals and scope, we conducted a systematic literature search from Oct 2019 to Jan 2020.

Preliminary findings were subsequently recorded in Jan. 2020. Search engines utilized were Scopus, IEEE Xplore, Google, and Google Scholar. IEEE Xplore, Google Scholar, and Scopus supported the detection of scientific literature, while Google was used to locate international standards, technical reports, industry best practices, and articles for locating cyber-attacks and relevant incidents at the industry.

Searches used a variety of keywords and their combinations and were subjected to filtering and fine-tuning based on the context of results. Grey literature used and relevant articles were sampled from a total of 400 hits from Google. Additional articles and reports were detected through references of key articles pertaining the above-mentioned hits. Additional citations were also extracted from the google scholar algorithm that proposes relevant bibliography for each search.

B. PUBLICATIONS AND GREY LITERATURE

The search queries resulted in accumulating a plethora of publications and literature. To assess the validity of the content and reduce the total volume of articles and publications, we opted to define some inclusion and exclusion criteria. Exclusion criteria were applied both before, during, and after title and abstract screening; afterwards mostly excluded due to full-text reading.

The selection process for articles and publications met the following inclusion criteria: (a) relevance of title, (b) assessment of abstract and introduction for useful and relevant content, and (c) full-text reading of each article and publication.

Exclusion criteria consisted of: (a) research papers, book chapters, and scientific articles without peer-review processes, (b) non English- or French-written articles or papers, (c) articles missing abstracts and introduction, (d) irrelevant publications, (e) articles and publications from bodies or organizations without a valid national or international status, (f) generic articles without specific descriptions, (g) unreferenced news articles and publications or unknown authors that were not members of relevant scientific or industrial communities.

We considered related surveys if:

(i) they addressed ICS security and had a similar aim and scope, or
(ii) were directly or indirectly related with the cybersecurity of the O&G sector.

Any articles or publications that met one of the exclusion criteria were discarded from data. Full-text reading of some paper and reports also resulted in excluding them and recording their reason of exclusion. Table 2 summarizes the above.

IV. MODELING OF TYPICAL O&G INFRASTRUCTURES

There exist three categories of O&G infrastructures: upstream, midstream, downstream. Upstream refers to exploration and production, midstream refers to the transportation, and downstream refers to refinement and distribution facilities. This article records, classifies, and analyses attacks on all O&G subsectors. Upstream, mid and downstream infrastructures utilize ICS to monitor operational activities, record operations and make decisions; either automatically (i.e. closed loop) or manually. ICS are used to gather information from endpoint devices and monitor the current state of production.

Attacks analyzed in this paper mostly refer to closed-loop control systems also known as feedback control systems. Such systems implement one or more feedback loops between input and output data to support automatic decision making. This means that parts of the output data are fed back to the monitoring and control system as input to form a part of the systems decision making algorithm [28]. Feedback control systems are designed to automatically achieve and

TABLE 1. Survey methodology attributes and characteristics.

Goal	Question	Key-word search	Literature type
Classify common vulnerabilities in O&G ICS equipment	Which vulnerability taxonomies are developed in scientific literature to support impact assessment in industrial control systems?	TITLE ("oil and gas" OR "oil & gas" AND security OR "vulnerability taxonomy" OR "risk assessment" OR "vulnerability assessment" OR "taxonomy" ABSTRACT (impact AND "ICS" AND "upstream OR "midstream" OR "downstream") ABSTRACT (impact AND "SCADA" AND "upstream OR "midstream" OR "downstream")	Research articles Grey literature (best practices, standards, technical reports, national alerts)
Record and analyze cyber -attacks on organizations along with affected systems and attacks concepts	Which O&G threats and cyber-incidents are recorded in scientific literature and technical reports?	TITLE ("oil and gas" OR "oil & gas" AND attacks OR "security events" OR "IoT security" AND "cyber-attack") ABSTRACT (ICS OR "SCADA" AND threats OR incidents OR refinery OR pipeline OR CNG OR "upstream OR "midstream" OR "downstream")	Research articles News Articles Grey literature (technical reports, white papers)
Derive common criteria from standards and best practices to support classification and assessment of impact for O&G cyber -attacks	What common criteria exist in standards and best practices able to classify threats and impact of events in relevant industrial control systems?	TITLE ("cyber security" OR "industrial control systems" OR "IoT" AND standards OR guidelines OR "technical report") ABSTRACT (threats OR "ICS" OR "threat model" OR "threat taxonomy")	Research articles Grey literature (best practices, standards, technical reports, national alerts)
Provide a structured analysis of current issues and gaps and correlate them with existing security controls	What are the most common implementation gaps related to securing devices in O&G ICS?	TITLE ("oil and gas" OR "oil & gas" AND security OR "guidelines" OR guide OR ICS AND controls) ABSTRACT (ICS OR "SCADA" AND "upstream OR "midstream" OR "downstream" OR refinery OR pipeline OR CNG)	Research articles News Articles Grey literature (technical reports, white papers)

TABLE 2. Survey inclusion and exclusion criteria.

Inclusion criteria		• Peer-reviewed papers and publications • Articles and reports written from respected members of the scientific or industrial community • Articles and reports written from recognized bodies and organizations • Articles written in internationally accepted houses and venues.
Exclusion criteria	***Before reading***	• Research papers, book chapters and scientific articles without peer-review processes • Non-English-written or French-written articles • Papers missing abstracts and introduction
	During abstract & introduction reading	• Articles and publications from bodies or organizations without a valid national or international status • Irrelevant publications
	During full-text reading	• Unreferenced news articles and publications • Authors are not members of relevant scientific or industrial community • Generic articles relevant to security or cyberattacks without specific descriptions

maintain desired infrastructure states without manual intervention. Closed-loop SCADA systems imply that a highly configurable set of industrial software applications is used to support the management of processes in production.

In the rest of this chapter we present a typical architecture of a closed-loop industrial system used in O&G infrastructures. It involves common types of assets (e.g. sensors, actuators, relays, SCADA system) and asset-specific installations present in downstream infrastructures. We also present typical layers used to describe the architecture of such systems. Information modeled in this chapter is used as reference for attack analysis and classification in the coming chapters.

A. A MODEL OF O&G SYSTEMS AND ASSETS

Figures 2a and 2b depict typical ICS SCADA and OT architectures for downstream (station dissemination) O&G ICS (Fig. 2a) and a high-level industrial system network for upstream and midstream (Fig. 2b) [5], [8], [23], along with brief examples of attack types that can be realized in each part of the architecture. Downstream O&G infrastructures, such as refueling stations, consist of the following components: Inlet systems, Condensate tanks, Dryer units (gas) or Dehydrators (oil), Compressor systems, Storage units (crude oil tanks, compressed tanks), Dispensers, Recovery systems, and Station control systems.

Downstream infrastructures utilize SCADA systems as a focal point for system input and control of all mentioned components. Either through closed loop architectures or using human intervention, SCADA controls analyze sensor input and send commands to actuators and other types of "edge" devices for dispersion monitoring and control.

Midstream and upstream attack types follow the same general architecture for relevant equipment. Typical midstream architectures are mostly below ground and/or have low ratios of ICS components per pipeline kilometers. Most components are pipeline sensors. In specific predefined locations, midstream infrastructures have Above Ground Installations (AGI) that may have numerous ICS assets installed. Block valve stations, primary and secondary pump, and metering stations, remote distribution stations, and critical distribution points are all considered AGI.

Upstream and midstream architectures (Fig. 2b) depict high-level components and emphasize on networking instead of facility installations, since both follow similar CPS logic with downstream in terms of intelligent devices and communication mediums. In fact, midstream implementations are considered simpler in terms of devices and actuators (same SCADA HMI, protocols, sensors, and actuators, but no tanks or processing machinery). Upstream infrastructures deploy SCADA systems for similar monitoring purposes during well extraction, separation of oil and gas and exporting to pipes. Even though processes are different and safety checks vary in comparison to downstream, still the ICS architecture (e.g. PLC, RTU, relays, etc.), connectivity (protocols, routing devices, communications media) and use-cases (HMI, server types, etc.) largely remains the same for midstream AGIs and upstream facilities.

Such ICS mostly focus on humidity, pressure, temperature, CO2, flow and particle sensors to gather environmental and pipe or tank data for monitoring and decision support. Following the trend of Industry 4.0 systems, modern ICS are IoT-enabled, with smart meters and sensors in modern applications. Smart sensors and devices can be defined as any nonstandard computing device able to gather, analyze and send data over a network for decision support [5],[29]. In O&G, this mostly applies to automated tank gauges, smart sensors and valves used to monitor or influence fuel tank inventory levels and raise alarms [30].

Figures 2a and 2b also depict the most common attacks to inflict such systems. Attacks through IT and digital infrastructure refer to attacks that utilize common IT systems and networks (workstations, LAN, portable devices, PCs etc.). Man-in-the-middle (MITM) attacks refer to attacks on the communication mediums used by devices to exchange commands and data. There are mostly injection attacks that add malicious data or commands in a communication stream, or eavesdropping attacks that aim to steal corporate data. Direct attacks on actuators refer to digital, manual or remote injection attacks that aim to change the working state of a field device in an installation (e.g. close a valve, change temperature thresholds in sensors etc.). These attacks will be thoroughly analyzed in the coming sections.

B. ASSET INVENTORY

A typical ICS is comprised of three levels (plus an extra level for the company's internal IT infrastructure). In the O&G industry, each level includes specific asset types and relevant devices [18], [23] regardless of its subsector, as follows: Level 0: Sensors, Relays, Actuators, Level 1: PLC, RTU, Slaves, and Level 2: SCADA industrial control system (HMI, Historian, servers, etc.). Each level involves specific types of devices:

1) LEVEL 0 - EDGE DEVICES

This level includes ICS devices that work in the field, in remote installations or are directly connected to the engineering infrastructure are usually referred to as Edge devices. Their main purpose is to collect physical environment information or control physical engines with input; either automatically (closed loop) or manually through SCADA commands. Edge devices are usually sensors and actuators:

a. **Sensors**: Most common sensors in O&G systems include: Temperature, Pressure, Humidity, Sound, RFID, Gas, Flow sensors. Smart sensors measure process physical environment signals and process variables to capture the state of components. Typically, O&G sensors are divided into 3 types: EX-IA sensors, ATEX sensors, and Normal sensors.

   O&G sensor equipment for potentially explosive atmospheres (ATEX) is standardized under the EU ATEX Directive 2014/34/EU. The directive covers equipment and protective systems intended for use in potentially explosive atmospheres [31]. O&G sensors are commonly classified as ATEX, EX-IA or normal based on their explosion protection and manufacturing. Similar to ATEX, [32] and other relevant sensor certifications are usually combined with Ex-IA or dual certification for sensor protection. All such sensors are considered Level 0 assets on the MITRE ATT&CK framework; lowest layer assets.

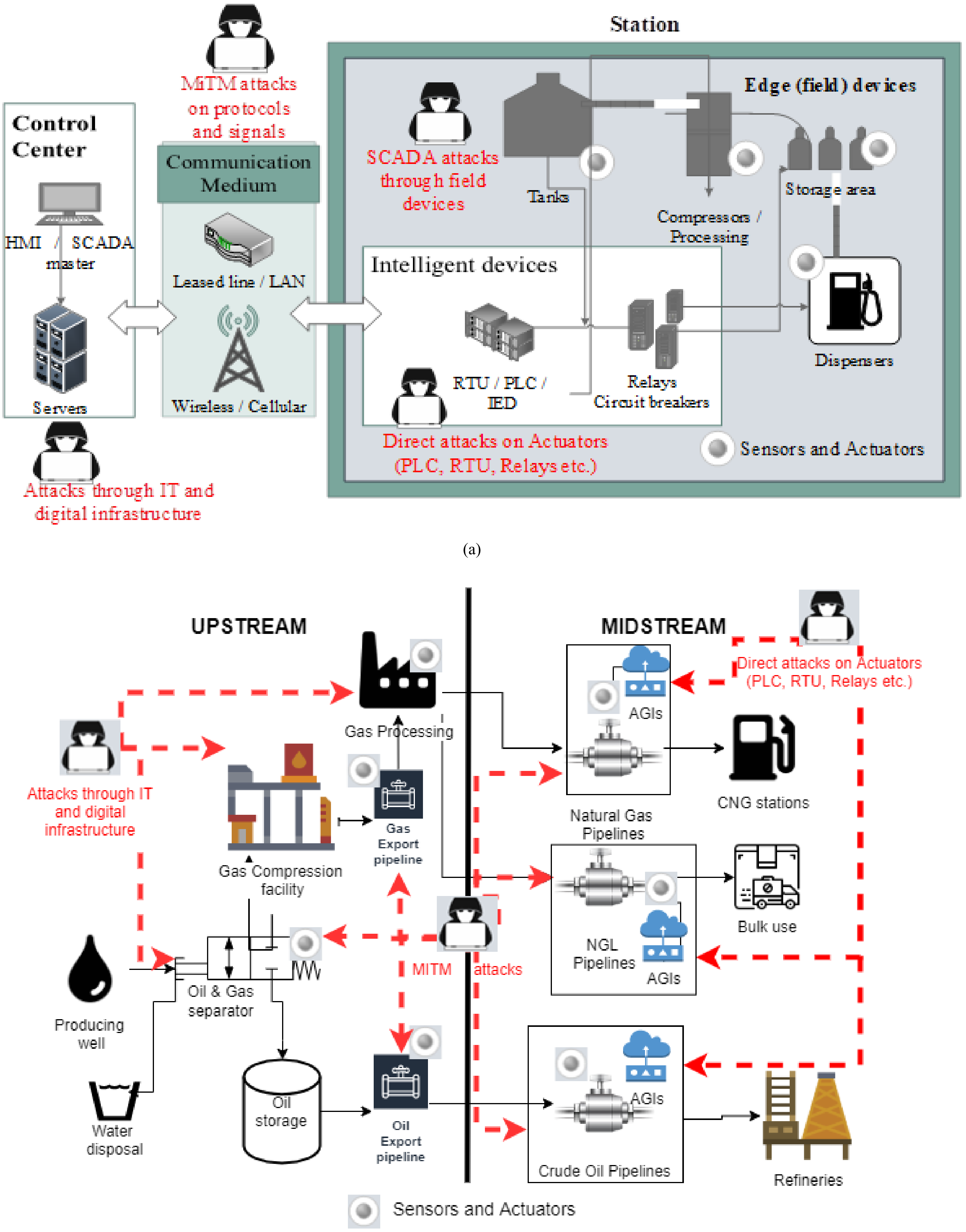

FIGURE 2. a. A typical architecture of an Industrial Control System in O&G downstream stations. b. A high-level architecture of an upstream and Midstream control system in O&G.

b. **Actuators**: NIST defines actuators as "devices for moving or controlling a mechanism or system. An actuator is the mechanism by which a control system acts upon an environment" 33].

2) LEVEL 1 - INTELLIGENT CONTROL DEVICES (RELAY, PLC, RTU)

Remote Terminal Units (RTU) and **Programmable logic controllers (PLC)** transmit captured data to supervisory systems, control infrastructure components such as O&G actuators (e.g. valves) and reference component status for decision making. These controllers and slaves get data from sensors and can convert output into digital signals. Such devices are considered Level 1 assets on the MITRE ATT&CK framework, connecting Level 0 to Level 2 assets.

3) LEVEL 2- SCADA CONTROL CENTER

Human-Machine

a. **Interface (HMI)**
Human machine interface is a user input system that allows a human operator to control the machinery, monitor systems and issue commands based on processed data. HMI refers to "graphical, textual and auditory information the program presents to the user (operator)" [34].

b. **ICS servers**
Industrial control systems often utilize multiple servers for granular control and resilience. Supervisory systems, MTU and Database servers comprise the backbone infrastructure of the Control Center. Communication servers between the HMI software and field devices, MTU that serve as a supervisory or master system for SCADA command and relevant application servers supporting ICS software, all fall within this category.

4) LEVEL 2- NETWORK INFRASTRUCTURE

Network hardware is typically considered Level 1 assets on the MITRE ATT&CK framework, while communication protocols are Level 2, allowing information distribution on the application layer of an ICS.

a. **Network Hardware**
Communication between a field engine and the control center can be one-way (monitoring only) or two-way (monitor and control). Connected equipment (e.g. PLC and industrial controllers used as middleware between the substation and the control center can connect via leased lines (e.g. fiber cable) or wireless antennas (e.g. cellular/3G).

b. **Communication Protocols**
In O&G infrastructures, devices communicate with servers and actuators to pass critical real time information or commands through numerous protocols (e.g. DNP3, ZigBee, FINS, ModBus, RS-232, etc.)

This asset mapping to ATT&CK type levels [23] is presented in Table 3.

C. IOT AND DIGITIZATION OF O&G SYSTEMS

The digitization of O&G infrastructures mostly involves the use of IoT smart meters (Level 0) that cooperate in closed loops with smart relays (Level 1) and relevant software (Level 2). The use of IoT in O&G offers several benefits. Studies suggest that smart devices can minimize operational risks during drilling, allows for real-time monitoring of infrastructure states [128] (pipelines, platforms etc.) and can improve production up to 8% using data mining and aggregation [124], [135].

Still, implementing smart assets at Levels 0 through 2 unifies control over several systems. Even though smart systems allow for centralized and/or remote control of multiple processes previously left on manual, close-proximity operation, still, this digitization also introduces major overhead in processing, storing and securing incoming data from multiple diverse sources. Such changes involve some significant cyber risks. Operating facilities like offshore rigs, pipelines, stations or refineries through unified, closed loop SCADA systems can pave the way to increased damage from security incidents, lengthier disruptions [94], [95], even result in injuries to employees or civilians and extended environmental hazards triggered from far away [114]. Also, the aggregation of big data from all O&G operations can result in increased privacy risks for business and personnel information [125].

Last but not least, smart meter implementation sometimes bypasses common architectural models in O&G OT systems and allows for indirect communication of devices from different layers (e.g. Layer 0 sensor speaking directly to Level 2 server over 4G without going through Level 1 equipment), or cross-communication of multiple data sources monitoring the same asset (e.g. different smart sensors on a gas tank monitoring the same asset with different data types).

Even though these implementations are mostly operator deployment decisions, still such conveniences make it harder to implement proper security measures across all assets.

V. TOOLS FOR MODELING O&G CYBER ATTACKS

In this section we present all tools that we will use in this paper in order to analyze and classify all detected O&G cyberattacks. We utilized two established cybersecurity information frameworks from MITRE: The Common Attack Pattern Enumeration and Classification (CAPEC) [26] "describes common attributes and techniques employed by adversaries to exploit known weaknesses in cyber-enabled capabilities" [26].

- The ATT&CK framework is a knowledge base of adversary tactics and techniques that "describes the operational phases in an adversary's lifecycle, pre- and post-exploit (e.g., Persistence, Lateral Movement, Exfiltration) and details the specific tactics, techniques, and procedures" [23].

TABLE 3. ICS O&G asset mapping to ATT&CK type levels.

Asset Category	Asset Type	O&G Instances	Level
Edge Devices	Sensors (ATEX, EX-IA, normal)	Temperature, Pressure, Humidity, Sound, RFID, Gas, Flow	0
Intelligent Control Devices	Controllers, Slaves, Relays	PLC	1
		RTU	1
		Automation Controllers (IAC)	1
Network Infrastructure	Hardware	Wireless connectors (cellular, microwave, radio (RF), Wifi)	1
		Switches	1
		Wired (Cable, Fiber, Ethernet)	1
	Communication protocols	DNP3, Modbus, ZigBee, Bluetooth, 6LoWPAN	2
Control Center	Servers	Master Terminal Unit (I/O server)	2
		Application server	2
		Database server	2
	Human-Machine Interface	Graphical User Interfaces (GUI)	2
		Software application	2

- CAPEC's attack patterns are used by techniques described in the ATT&CK framework. We use CAPEC and ATT&CK complementarily, to map attack types with ATT&CK's adversary tactics and techniques and understand which assets are most vulnerable in each case. We build (i) a list of attack types for ICS, (ii) a taxonomy of potential O&G cyber-attacks types, (iii) an ICS layers table applicable to O&G, and (iv) a vulnerability taxonomy of potential O&G vulnerabilities per ICS layer.

A. GENERIC ATTACK TYPES

All attacks in industrial systems can be broadly categorized into two types or a combination of these. Attacks can either target physical security and safety (labeled with 'P') or target a facility's use of cyber space to attack the confidentiality, integrity and/or availability of a computing environment or infrastructure [35] (labeled as 'C'). Attacks can combine the above definitions and create chains of security events. For example, a physical tampering attack on a network device that injects a malware inside the network, able to steal data is a physical-to-cyber ('P-C') attack. On the other hand, malware infiltration able to manipulate a valve and cause gas leakage is an attack that stems from the ICS but has physical consequences (cyber-physical, 'C-P'). All acronyms and potential combinations are presented in Table 4. O&G ICS are cyber-physical systems [36].

TABLE 4. Acronyms of O&G attack types.

Cyber-only attacks	C
Physical-only attacks (Safety)	P
Physical-Cyber	P-C
Cyber-Physical	C-P
Cyber-Cyber	C-C
Cyber-Physical-Cyber	C-P-C
Physical-Cyber-Physical	P-C-P

Physical plant machinery and processes are monitored and controlled by the cyber section to distribute or transfer gas from production to the end-user. Thus, this survey emphasizes on C, C-P, P-C-P and P-C attacks, while considering purely physical attacks (P) out of scope.

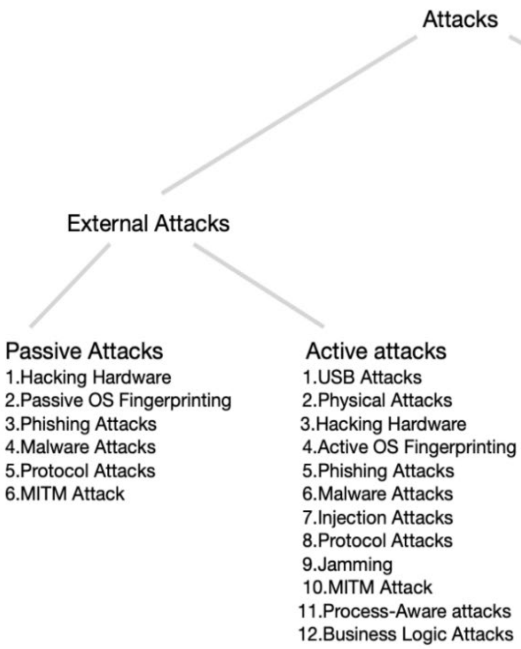

FIGURE 3. A taxonomy of O&G cyberattacks (C-P, C, P-C-P).

B. CYBER-ATTACK TYPES

Attacks can be distinguished based on their starting point. For example, an attack caused by an employee is different than an attack from the outside of a CNG station. Thus, attacks are divided into internal and external. Internal (or insider threat) attacks stem from entities with authorized access to the domain of an information system [33]. These include, but are not limited to, disgruntled employees who may use their privileged access to damage their employers. External attacks try to exploit vulnerabilities in the facility's attack surfaces without prior knowledge or access. Two other commonly used facets when studying cyberattack types are the "active" and "passive" categories. Active attacks alter system or data [35], while passive attacks intercept data traveling along the network but do not alter them (i.e., eavesdropping) [37].

We utilize the Common Attack Pattern Enumeration and Classification (CAPEC) taxonomy to introduce the cyber-attack subtypes for classification. CAPEC [26] "provides a publicly available catalog of attack patterns" and descriptions of common cyberattack approaches employed by adversaries. The tree like structure for categorizing O&G cyberattacks into CAPEC subtypes is shown in Fig. 3.

C. LIST OF CYBER-ATTACK TYPES PER ICS LAYER

All cyber-attacks that are applicable to O&G systems can be assigned to different ICS architecture layers. These layers are commonly used in frameworks and taxonomies to aid classification [7], [8], [23], [38] and will later allow us to effectively present and categorize vulnerabilities in O&G infrastructures. Table 5 summarizes applicable ICS layers and assigns common O&G assets per layer.

TABLE 5. Components of each layer in O&G facilities.

Layers	O&G devices and components
Hardware	Server equipment (RACKs, CPUs etc.), sensors, actuators, RTU's, PLC's, routers, access control hardware (smart cards, RFID etc.), Valves, ATG's, slaves etc.
Firmware	Operating Systems, data and instructions for controlling the hardware, AMI's
Software	HMI's, API's, proprietary software packages, applications
Network	Communication protocols, modems/routers, firewalls
Process	Designed ICS business logic, Control Systems configuration

The hardware layer is comprised of all tangible low-level equipment that connects to the ICS. This includes field devices and sensors, processors, volatile and non-volatile memory, slaves, RTU, PLC, Relays and other relevant components used in machinery. Hardware also includes tangible assets such as underlying network infrastructures such as routers and cables along with digital equipment, such as servers, workstations, laptops and components.

The firmware layer includes software that enables low-level control of devices and hardware. Firmware is typically stored in non-volatile memory and provides an interface between machinery and software. Nearly all modern ICS devices contain in-house or third-party firmware.

The software layer is comprised of all computer software used in an ICS for monitoring and control. This includes any and all programs and applications running on devices and servers that enable user interaction. The network layer contains any assets relevant to the communication medium used in an ICS, namely communication protocols, modems/routers and other network devices, such as firewalls and radio, wireless and similar communication antennas.

The process layer is the abstract layer that describes overall control systems and processes. It contains mappings of business logic, industrial processes and architecture that describes the use of ICS in connection with the business needs of a midstream or downstream infrastructure.

D. TAXONOMY OF COMMON O&G VULNERABILITIES PER LAYER

Expert knowledge, recorded attacks and relevant literature shows that each ICS layer has different security risks and relevant vulnerabilities that an adversary can discover and exploit. This is supported by various technical reports and state publications that define or model attacks on ICSs (e.g. supply chain attacks) [5], [7], [11], [23].

In this section we develop a body-of-knowledge of potential vulnerabilities per ICS layer, and connect them to MITRE's ATT&CK techniques to aid readers detect attack types, adversary tactics and techniques, and pinpoint vulnerable that are most assets. Table 6 assembles a vulnerability taxonomy for O&G ICS, with extensive information collected by filtered from articles, grey literature and government incident reports.

1) HARDWARE LAYER

The hardware layer contains devices and embedded components such as RTU, PLC and relays. This layer is susceptible to tampering attacks and other physical attacks [7], [23] meaning that someone in close proximity can cause alteration or destruction of field devices. Furthermore, hardware is vulnerable to supply chain attacks as hardware trojans can be injected in any stage of the supply chain [8], [39], [40]. In O&G, hardware vulnerabilities considered most critical include the use of legacy/end-of-life or unpatched equipment.

Physical attacks may cause damage to property like infrastructure, equipment, and the surrounding environment, due to the lack of safety mechanisms [7], [60], [111]. For example, physically altering/attacking industrial O&G systems without fail-safe or monitoring mechanisms can lead to extended leakage affecting nearby communities [42], [43]. Frequently there is inadequate protection on engineering workstations connected to the system for device programming and control adjustment. Using third-part devices or services may introduce unknown vulnerabilities, both in mid and downstream infrastructures, e.g. by installing devices with malicious hardware trojans [8].

Last but not least, ICS and especially field devices are rarely updated with modern hardware. Most infrastructures keep using old actuators, PLC and RTU, sometimes even if they contain critical vulnerabilities that cannot be patched. This is even worse in cases of midstream AGI, where the cost of upgrades is considerably higher [7]–[9], [18].

2) FIRMWARE & SOFTWARE LAYER

The firmware layer lies between hardware and software. It consists of the operating system that midstream and downstream controllers, systems and field devices use. This layer is mainly susceptible to malicious firmware injection [8], [44] attacks, in order to disrupt the ICS operation. The software layer consists of all the applications used in an ICS to monitor and control machines and peripheral systems, other software platforms and human machine interfaces. With the coming of Industry 4.0, this layer is susceptible to almost all common IT cyberattacks, including injection, malware attacks, remote code execution, etc. [7], [23], [60].

Unpatched operating systems are a common vulnerability both for ICS and IT systems [12]. Reports consider the lack of OS patching along with software patching as one of the top ICS vulnerabilities since 2016 [18]. This applies to the O&G sector too. Numerous reports consider the use of legacy software and the lack of software patching as one of the top ICS vulnerabilities since 2016 [7], [18], e.g. buffer overflows on ICS software are common [46], [47].

Software lacking proper input validation in its source code is one of the most frequent vulnerabilities at the software ICS layer [7], [9], [18], [48]. SQL injection, XSS and CSRF attacks which are common in Web applications, are also regarded as one of the top ICS software vulnerabilities [47]. Reports consider the use of legacy software and lack of software patching as one of the top ICS vulnerabilities since 2016 [7], [18]. For example, buffer overflows on ICS software have been known to cause serious impact to their processes [46], [47].

DoS attacks on OT equipment is another common attack technique. There are numerous incidents of unavailability attacks using software vulnerabilities found in ICS components [49]. Successful exploitation of vulnerabilities can render O&G systems unavailable which, in turn may cascade to more types of impact to individual organizations than DoS, depending on many factors, although unavailability attacks are common goals in ICS.

Improper access control or authentication processes in software used in ICSs may lead to compromised OT processes, commands and data [8], [18], [47]. Erroneous authentication processes may refer to a variety of errors, including errors in authentication processes, anonymous access to services, weak authentication on remote access to connected processes etc. [9]. This also applies to attack surfaces, i.e., Wi-Fi access points are shipped with a default SSID and passwords.

3) NETWORK LAYER

The network layer consists of the firewalls, modems, routers, remote access points and the underlying protocols used by field devices to communicate data (ZigBee, 6LoWPAN, etc.).

TABLE 6. Taxonomy of potential O&G attacks with ATT&CK Reference ID.

Vulnerability type	ATT&CK Tactic ID	Description
Hardware Layer		
Lack of tamper resistance	T858 - Utilize/Change Operating Mode T848 - Rogue Master Device	Field devices often do not implement hardware security controls that can detect or prevent physical tampering attacks (e.g. key extraction attacks) [81], both in midstream and downstream O&G infrastructures.
Lack of physical security	T825 - Location Identification T801 - Monitor Process State	Physically altering/attacking industrial systems without fail -safe or monitoring mechanisms can lead to leakage affecting nearby communities [41]-[43].
Use of legacy devices & equipment	T858 - Utilize/Change Operating Mode T801 - Monitor Process State T833 - Modify Control Logic	Legacy field devices, PLC and sensors remain active for extended periods, even though they have known vulnerabilities.
Unknown / untrusted Off-The-Shelf devices	T862 - Supply Chain Compromise T811 - Data from Information Repositories	Removable devices are potential attack vectors that can be overlooked by users. COTS components (not custom-made) provide stability, availability and reduce cost but, at the same time, may introduce unknown vulnerabilities, both in mid and downstream ICS.
Firmware Layer		
Outdated OS	T851 – Rootkit T800 - Activate Firmware Update Mode	Unpatched operating systems are a common vulnerability both for ICS and IT systems [12]. Reports consider the lack of OS patching along with software patching as one of the top ICS vulnerabilities since 2016 [18]. This applies to the O&G sector too.
Lack of firmware protection	T839 - Module Firmware T857 - System Firmware T800 - Activate Firmware Update Mode T851 - Rootkit	Facility and ICS are known to lack security measures against firmware modification [45], mostly due to cost cutting this is not happening [7]-[9],[23].
Software Layer		
Improper input validation	T871 - Execution through API T835 - Manipulate I/O Image T833 - Modify Control Logic	Software lacking proper input validation in its source code is one of the most frequent vulnerabilities at the software ICS layer [7],[9],[18],[47]. This includes the HMI along with individual device software [41],[47].
Outdated / Unpatched software	T831 - Manipulation of Control T833 - Modify Control Logic	Numerous reports consider the use of legacy software and the lack of software patching as one of the top ICS vulnerabilities since 2016 [7],[18]. E.g. buffer overflows on ICS software are relatively common [46],[47].
Erroneous configuration / installation	T858 - Utilize/Change Operating Mode T873 - File Infection T836 - Modify Parameter T862 - Supply Chain Compromise (IoT)	Misconfigurations and erroneous installation of devices open up vulnerable attack surfaces [7]-[9]. Sensor misconfigurations may lead to smart meters working against each other on closed loop systems, not cooperating with existing equipment or causing malfunction in real-time decision support systems [124, 125, 128].

TABLE 6. ***(Continued.)*** **Taxonomy of potential O&G attacks with ATT&CK Reference ID.**

Vulnerability type	ATT&CK Tactic ID	Description
Lack of encryption	T801 - Monitor Process State	Cleartext transmission and cleartext storage of sensitive Information rank very high among common software vulnerabilities for ICS in systems similar that those in O&G ICSs [47].
Denial-of-service (DoS) on equipment	T816 - Device Restart/Shutdown T813 - Denial of Control T881 - Service Stop	There are numerous incidents of unavailability attacks using DoS vulnerabilities found in ICS components. Successful exploitation of vulnerabilities can render O&G systems unavailable [49].
Vulnerable third-party services	T822 - External Remote Services	External remote services may act as attack surfaces for the initial access of adversaries to internal network resources from external locations [23].
Lack of proper authentication and access control	T818 - Engineering Workstation Compromise T883 - Internet Accessible Device T810 – Data Historian Compromise T812 – Default Credentials T853 - Scripting T859 - Valid Accounts	Improper access control or authentication processes in ICSs may lead to compromised OT processes, commands and data [8],[18],[47].
Network Layer		
Vulnerable communication protocol	T869 - Standard Application Layer Protocol T802 - Automated Collection T830 - Man in the Middle T831 - Manipulation of Control T804 - Block Reporting Message	Field devices in O&G ICS utilize OT protocols with no authentication or security at any level [51],[52]. Infrastructures usually do not implement any extra security measures to mitigate this. Common network attacks on ICS include blocking or replaying command or reporting messages (DoS).
Lack of encryption and authentication	T830 - Man in the Middle T831 - Manipulation of Control T801 - Monitor Process State T842 - Network Sniffing	ICS devices often implement erroneous or are even completely lacking authentication mechanisms [7],[18],[41]. For example, legacy devices often accept commands without prior authentication. Also, the lack of encryption may lead to accessible OT channels by non-endpoints and allow integrity attacks on OT commands [9].
Erroneous key management	T830 - Man in the Middle T831 - Manipulation of Control T801 - Monitor Process State T842 - Network Sniffing	Frequently, devices of the same model use the same master key for their communications [41]. An adversary who succeed to intercept the key from one device can gain access to all the other devices and attack.
Network design weaknesses	T831 - Manipulation of Control T866 - Exploitation of Remote Services T830 - Man in the Middle T842 - Network Sniffing	Partitioning networks prevent the spread of malicious programs and contain the attacks [7],[18]. Network design weaknesses may allow attackers to reach field devices and make Control-related systems accessible [9].
IoT device connectivity weaknesses	T831 - Manipulation of Control T866 - Exploitation of Remote Services T830 - Man in the Middle T842 - Network Sniffing	Denial of Services can incur from smart devices mostly due to the use of insecure, open source code and implementations (e.g. lack of access control or encryption on IoT device links) [124, 128].
Process Layer		

TABLE 6. ***(Continued.)*** **Taxonomy of potential O&G attacks with ATT&CK Reference ID.**

Vulnerability type	ATT&CK Tactic ID	Description
Business Logic vulnerabilities	T831 - Manipulation of Control T833 – Modify Control Logic	Business logic vulnerabilities allow attackers to modify execution flows of ICSs and make them enter unwanted states [7],[9],[57]. These attacks can have various degrees of impact and may even work within device operational bounds [56],[58]. IoT introduces misconfigurations faults in interconnected systems, smart sensors working against each other because of false, conflicting or blocked device goals (e.g. availability of sensors against integrity checks of ICT equipment) [126]. Also, some vulnerabilities manifest due to the lack of cooperation of smart devices with legacy equipment [124].
Lack of employee training	-	IC often lack proper security policies. Also, industrial engineers and OT employees are usually not trained or under-trained in matters of cybersecurity [9],[11],[60].

This layer is susceptible to unavailability, man-in-the-middle and spoofing attacks [7], [23], [60].

Typical wireless sensors use S-MAC, LMAC or B-MAC protocol and they have little to none protection against jamming. Encrypting the packets may help increasing the security level. Although patterns might be unraveled that the jammer can take advantage even if the packets are encrypted [50].

Field devices in O&G ICS may utilize network protocols with no authentication or security at any level. MODBUS also suffers from lack of secure channel [51]. Most OT network protocols lack embedded security mechanisms. On top of that, many O&G infrastructures do not implement extra security measures to mitigate this issue. Many field devices still utilize the MODBUS protocol to communicate, even though there is no authentication at any level of MODBUS. MODBUS suffers from lack of secure channel [51]. Also, the FINS protocol for PLC does not use any encryption in data exchanges [52]. In general, OT network protocols lack security mechanisms and O&G infrastructures usually do not implement any extra security measures to mitigate this. On top of these, modern ICS utilize IoT smart sensors. IoT-enabled field devices allow misconfigurations and many of these devices do not support any network layer security and they are completely exposed to network attacks [53].

Network design weaknesses is another vulnerability commonly found in O&G ICSs. "Flat LAN" or lack of network partitioning and/or DMZ allows attackers to reach field devices and make Control-related systems accessible [9]. Partitioning networks prevent the spread of malicious programs and contain the attacks [7], [18].

4) PROCESS LAYER

The process layer consists of the designed ICS business process model and operation logic. Every software in an ICS has a different business process, application-specific logic, which can be potentially exploited in an infinite number of combinations. The dynamic behavior of the ICS processes must follow the dynamic characteristics of the designed ICS model [54].

This layer is susceptible to business logic and ICS-centric attacks [55], including attackers leveraging bad configuration or erroneous security processes in handling machinery. Attacks include situations were malicious users operate machinery within acceptable bounds but still manage to deviate production or process from normal operation and cause economic losses or degrade performance [9], [56], [58].

Business logic validation testing verifies that the application does not allow the user to insert invalidated data or cause (series of) software flows to reach unintended states of operation [8], [57]. Data injection in multiple attack surfaces may affect the dynamic behavior of closed-loop systems and make them enter unwanted states. Sometimes, attacks on ICS may well make devices work within acceptable operational bounds but may still cause extended economic impact in an extended time period [58].

ICS operation is also severely affected by the lack of security training in O&G ICS employees. OT engineers and IT security officers frequently do not communicate properly and each has limited knowledge on potential vulnerabilities outside her/his field of expertise.

5) IOT CROSS-LAYER VULNERABILITIES

The industry 4.0 era along with the digitization of O&G infrastructures through the use of IoT may speed up processes but also paves the way to new security incidents. The use of such automation for monitoring and automatic decision support open the way to critical vulnerabilities. The lack of specific security frameworks or relevant standards from regulatory bodies pushes manufacturers to adopt publicly open source code for intra-device communication [124].

Also, contrasting priorities between availability (for field smart sensors and devices) and integrity and confidentiality (for ICT systems) [126], forcing smart sensors to work with legacy equipment and the use of tactical rather than strategic approaches to security from operators [125], [127] all contribute to the multiplication of vulnerabilities in modern IOT-enabled O&G systems.

Contrary to other sectors, O&G IoT systems support real-time monitoring and control of operations across the entire value chain. As such, potential DoS or data integrity incidents will incur exacerbated effects due to the interconnected nature of modern systems and incur the ''biggest impact on the bottom line'' [124] to both the O&G sector and the entire infrastructure ecosystem due to its high dependency on O&G.

Most common vulnerabilities introduced from the use of IoT devices spread across all layers. Most important types of vulnerabilities involve:

- Sensor misconfigurations that may lead to smart meters working against each other on closed loop systems,
- Denial of Services due to malfunctions produced by the cooperation of smart devices with legacy equipment and
- Vulnerabilities introduced at the software and network layer, mostly due to the use of insecure, open source code and implementations (e.g. lack of access control or encryption on IoT device links).

VI. ASSESSING THE IMPACT OF O&G CYBER ATTACKS

In an effort to assess all presented cyber-attacks on O&G ICS, we define a generic impact assessment method to supplement security incident classifications. Our method utilizes typical risk assessment concepts and notions, as defined in numerous standards and reports, e.g. ISO 27005:2005 [59] and NIST 800-53 [60].

According to these standards, risk metrics describe cybersecurity incidents and are modeled as factors of (i) threat, (ii) vulnerability, and (iii) impact. Threat metrics measure ''the potential of events to harm assets such as information, processes and systems and therefore organizations'' [59], while vulnerability metrics quantify the seriousness of flaws and weaknesses in a system. Impact measures the extent of potential damage that will occur, should a threat were to manifest during a security incident [59], [60].

A. ASSESSMENT GOALS AND RESTRICTIONS

In the presented analysis we are interested in the extent of the damage caused, rather on the seriousness of the vulnerability that triggered a security event or the underlying threat that caused the attack in the first place. Threat actors and vulnerabilities vary greatly in significance even between similar O&G infrastructures. This has to do with strategic analysis, geopolitical issues, type of implementation, or simply timing of the event. To this end, and without access to the necessary information, we opt to assess only the impact of each presented attack.

Since we analyze and classify security incidents in the O&G sector that have already taken place, we are more interested to rank the impact of these incidents along with their classification. This is also in line with numerous CI Directives and National plans, which prompt for detailed analysis of consequences of adverse effects in CI before other studies [99]–[102].

We do not attempt to provide a full risk assessment of the recorded attacks. This requires extensive in-house information to develop a proper study; something that should be performed by relevant regulatory bodies or infrastructure owners.

B. GENERIC IMPACT ASSESSMENT METHODOLOGY

Cyber-attacks can have diverse effects on infrastructures and their surrounding area. Identifying and assessing risks of adverse effects (such as attacks) in critical infrastructures is an established concept since the early 2000s. In 2004, the EU first referenced critical infrastructures and their protection against attacks in the ''Solidarity Programme on consequences of Terrorist Threats and Attacks''. The German Federal Office for Civil Protection published (2015) the Baseline protection concept for Critical infrastructures [104]–[108]. The US Dept. of Energy published (2011) the Risk Management Guide for projects in the energy sector risk analysis and management. Since then, nearly all bodies, states and countries have supported risk assessment procedures on CI to identify potential threats and attack scenarios.

Nowadays, all international bodies and organizations recognize economic, societal and environmental damages as parts of attacks on critical infrastructures [99]–[101]; The EU NIS Directive [99], as followed by the EU Cybersecurity Act [100] and the US Dept. of Homeland Security [101], clearly support the use of risk assessment for the characterization and analysis of potential threats and their impact on critical infrastructures. Current standards and best practices such as NIST's publications, ISO and EU directives like SEVESO-III [102] utilize impact scales to understand and model the impact from hazards and adverse effects in critical infrastructures. Such models and scales are implemented in a wide variety of tools for the analysis of risk and impact in operators of essential services and CI [62].

To describe the potential impact of the accumulated cybersecurity attacks, we opted for a semi-qualitative scale with 3 levels (low, medium, high), similar to those used in the above-mentioned literature [16], [61]. Semi-qualitative scales utilize both textual evaluation of scenarios (as used in qualitative risk assessment) along with a numerical ranking scale (used commonly in quantitative assessments) [103].

Each level is described by four (4) dimensions that represent different types of impact: (i) Economical, (ii) Societal, (iii) Environmental, and (iv) Operational. The three values quantify these dimensions. Such scales are in accordance to relevant specifications [59], [60] and are used by commonly accepted risk assessment tools for critical infrastructures, such as CRAMM [10], EAR/PILAR, or EBios [62]. As such,

TABLE 7. Impact assessment scale for O&GP cyberattacks.

IMPACT TYPE	LOW	MEDIUM	HIGH
Economical	• Minimum or no asset cost for company (e.g. loss of time, need to repeat process) • No cost for society	• Limited asset cost to company (e.g. hundreds of thousands of euro). • Minimum cost to society (e.g. limited, short-term increase to prices)	• Extended asset cost to company (e.g. millions of euros) • Significant costs to society (e.g. serious and/or long-term increase in prices)
Societal	• No injuries • Minimum number or no citizens affected (e.g. <30 people)	• Limited num of injuries only to personnel. • Limited number or no citizens affected (e.g. less than 50 houses)	• Extended num of injuries in personnel. • Injuries to citizens. • Loss of life.
Environmental	• No treatment needed for clean up or contamination	• Treatment or clean up needed in limited areas in and around the facility	• Wide area subject to clean up or decontamination treatment
Operational	• Minimal downtime of services or resumed in very short time (e.g. <4h).	• Limited downtime of services or resumed in very short time (e.g. less than 48h).	• Extended downtime of services (>48h).

presented impact levels are deliberately simple, so as to provide a point-of-reference for readers.

Table 7 presents the qualitative scale along with all dimensions of impact, as they scale over the three-level impact scale. To justify the numbers used inside the scale, we opted to review multiple sources of critical infrastructure impact [10], [59], [60], [62] along with the relevant, above mentioned standards and Directives like NIST, ISO and SEVESO-III 102]. This scale is used in the extended Table 10 to qualitatively rank each recorded incident (Table 10 in Appendix presents the analysis of all recorded attacks).

Aligned with international literature, we too follow the common practice of taking into account the worst-case impact scenario for each potential outcome of such events (e.g. each documented attack will get an impact rank according to the worst consequence that occurred during each event).

C. CASCADING FAILURES BETWEEN INTERCONNECTED INFRASTRUCTURES

1) INFRASTRUCTURE DEPENDENCIES

Many security incidents frequently do not have only direct consequences. The interconnected nature of modern O&G infrastructures allows for some failures to affect external systems and facilities and cause indirect adverse effects over the course of time; a common issue when trying to quantify the impact of security incidents. Such disruptions are based on infrastructure interdependencies and are usually classified as cascading, escalating, or common-cause [129]–[131].

Common-cause disruptions refer to incidents where two or more infrastructures are simultaneously but disjointly affected due to the same event. Escalating disruptions refer to events where a failure in one facility "exacerbates an independent disruption of another infrastructure" [130], and cascading failures are defined as failures in one infrastructure (e.g A) that eventually lead to partial or total unavailability of resources and services to a different infrastructure (e.g. B) that is depended on A for providing its own services [129].

Cascading failures in particular are a common and unfortunately recurring issue in the O&G sector. The most common cascading failure in O&G involves the unavailability of a midstream infrastructure for transporting oil or gas (e.g. pipeline), which, if continued for a prolonged amount of time, eventually leads to sectorial cut off of resources in downstream (e.g. gas stations have shortage of fuel), which in turn may affect various other sectors (in our example, the entire transportation sector of an affected region).

Oil & Gas, is widely considered as one of the top critical infrastructures most relied upon by other infrastructures [133]. Consequently, O&G infrastructures may cause major cascading failures, especially to the transportation and housing sector.

2) COMPONENT DEPENDENCIES

Cascading failures also occur between components inside the same infrastructure. For example, IoT and interconnected devices within the same system may allow threats like malware cause malfunctions to equipment, which in turn may affect other components due to erroneous data reports, unavailability of service or injection of malicious code [5].

For internal analysis of interconnected components, proper risk assessment methodologies must take into account

TABLE 8. Statistical analysis of results from all recorded attacks (full analysis table in Appendix).

ANALYSIS ATTRIBUTE	STATISTICS
Most frequent Attack Types	External – malware attack (**9 incidents**) External – phishing attack (**8 incidents**) Internal – Injection attack (**6 incidents**)
O&G sectors affected	Upstream (**15 incidents**) Midstream (**13 incidents**) Downstream (**14 incidents**)
Most frequent Attack Scenarios	C-C (**16 incidents**) C-P (**20 incidents**)
Most frequent MITRE ATT&CK techniques	Internet Accessible Device (T883) (**12 incidents**) User Execution (T863) (**10 incidents**) Spear phishing (T865) (**9 incidents**) Removable Media (T847) (**5 incidents**)
Most frequent MITRE ATT&CK impact types	Modify Control Logic (T833) / state (T875) (**10 incidents**) DoS (T814) / Availability Loss (T826) (**14 incidents**) Damage to Property (T879) (**9 incidents**) Information theft (T882) (**13 incidents**)
% of incidents per Impact rank	High (**51.6%**) Medium (**25.8%**) Low (**22.6%**)

conditional probabilities of threat manifestation and calculate such attack paths using overall metrics.

This is an open issue in research, with many publications proposing various solutions, such as mathematical series over graph-based models of infrastructures [25], system dynamics that use top-down methods to analyze complex adaptive interdependencies (e.g. CIP/DSS [132]) and various other approaches.

Such complex methods require access to information that is not publicly available. Therefore, in this survey's Table 8 of recorded attacks, we do not provide quantitative estimations of the severity of each recorded cascading failure, but instead opt to only catalogue security incidents that involved cascading failures to other systems.

VII. ANALYSIS OF O&G CYBER-ATTACKS

O&G systems follow the typical ICS architecture used in numerous types of critical infrastructures and frequently utilize simpler approaches that others, e.g. smart grids. Thus, most ICS implementations follow common technologies and thus utilize similar security controls and architectures, as documented extensively in the past in reports, standards and numerous official sources [7], [10], [20], [29]. Also, numerous research papers exist that describe potential attacks on SCADA systems, widely used in the O&G sector [4], [8], [39], [41], [52], [56]–[60], [74], [78], [92]. Threat actors include criminals, terrorists, nation states and antagonists, although documented attacks show that most attacks stem from nation states and relevant hacking groups [14], [61], [66], [83], [86], [88], [94]. Consequences of such attacks on O&G systems vary greatly, from theft of data and information to direct manipulation of machinery, even control the angle of entire oil rigs [96] or pressurization of pipelines [13], [80].

Most documented vulnerabilities used in such events involve unpatched systems, legacy equipment, and vulnerabilities in underlying networks. Still, the integration of smart sensors, remote monitoring and control in closed loop systems over thousands of miles introduced novel attack vectors and vulnerabilities previously unknown to the O&G sector.

During the early 2000s, we witnessed attacks on infrastructures that had limited damage due to the fact that back then systems still remain on manual and were not connected to wide networks [94].

O&G upstream infrastructures support operations for exploring and drilling operations, midstream is responsible for the transportation of oil and gas and for providing a link between upstream production and downstream dissemination, while downstream focuses on distributing assets to consumers, mainly for crude oil and raw/condensed natural gas.

All infrastructures are mainly controlled using SCADA systems over actuators and relays. SCADA systems are widely known to focus on increased availability and have limited to no security measures in place [20], [52]. ICS are used to monitor the state of machinery, implement automatic control of processes and provide real-time monitoring of process states. This functionality gave rise to information theft attacks with financial motives [109], [110].

In this survey, we document and classify attacks on all types of O&G infrastructures according to their domain type (upstream, midstream, downstream). We also document their initial input technique and the type of impact they had on the infrastructure using MITRE's ATT&CK framework. Finally, we examine the range of impact from each attack using the semi-qualitative impact assessment scale (Section III.B) using international standards. Attacks can target all types of O&G infrastructures. Still, significant differences occur when examining prior security incidents, with differences mainly focusing on the type of impact from each event.

Table 8 provides a broad overview of statistics from recorded and analyzed real-world cyberattacks and for all types of O&G infrastructures, using the taxonomies and frameworks as presented above (full Table 10 in Appendix with extended classification on all recorded incidents).

A. ATTACKS ON UPSTREAM SYSTEMS

Upstream infrastructures are often erroneously considered to be less targeted than downstream ones, in terms of cybersecurity. This was true in the past, due to the remote and disconnected nature of most upstream infrastructures. Also, attack surfaces able to allow unintended access to upstream infrastructures only include telecommunications, either satellite or cellular [66], which at first seems to be an inhibiting factor for attacks on upstream. Still, modern infrastructures are digitized and interconnected in their majority, with companies deploying ICT and OT systems that are frequently used in diverse sectors simultaneously. As depicted by our analysis of recorded attacks, more often than not, we see that attacks may infiltrate from specific systems but eventually affect multiple, sometimes all O&G sectors.

Analysis of recorded attacks shows that modern upstream operations are not safe against cyberattacks. A number of cases have been reported were upstream systems were directly or indirectly compromised by malicious insiders or malware, causing a number of adverse effects on operations and machinery [15], [94]. Even though there exist no known hacking groups that specifically target upstream infrastructures and target exploration and drilling operations [66], eventually we managed to document 24 major cybersecurity attacks and events on upstream systems, especially during the first decade (2000-10).

One of the first documented cybersecurity attacks on upstream infrastructures was a malware attack that hit the Gazprom company in 1999 [94]. Records state an insider executed a malware file on purpose. The attack's consequences included having the entire gas flow control system of the Russian gas supplier under direct control of the attackers for a number of hours. Attack presumably performed with malware brought inside the ICS using the employer's own access control rights granted.

Three years later, in 2002, the Venezuelan oil company PDVSA reported to have several of their computers hacked, which reduced their oil production by 87.6% per day [114]. Assumed attackers were employees participating in a strike at that time.

In 2009, a disgruntled tech employee purposely impaired an industrial system for monitoring pipeline leaks at 3 oil derricks near Southern California [15], [94]. The leak-detection system was "rendered inoperable for a period of time", exposing the entire California area to environmental disasters [94].

In 2010, a rig en route from South Korea to Brazil was infected with computer malware [94], [95]. Infection reached such extent that it took IT stuff 19 days to make resume operations.

In December 2012, a hacking attack shut down an oil rig off the coast of Africa by tilting it [94], [95] 17 degrees. Attack was attributed to manipulation of the ballast control that led to equipment failure [96], probably through PLC-actuator command-and-control. Attack caused injuries to 89 workers involved in building the rig. This is the only documented cyberattack which directly resulted to the physical injury of multiple employees.

During the Gaza Cybergang attacks on O&G industry in 2017, adversaries were discovered inside O&G organization in the MENA region. Attackers extracted data continuously for more than one year using the CVE 2017-0199 vulnerability [88].

In 2016, attackers extracted data continuously for more than a year using the CVE 2017-0199 vulnerability. Dubbed as the OilRig malware attacks, they targeted O&G institutions in Saudi Arabia [17]. Similar scripted malware TwoFace Webshell was also used to break into and infect systems to the Ministry of Oil of a Middle Eastern country [85]. Attacks used credential dumping tools, such as Mimikatz, and stole credentials to accounts. TwoFace used to access the victim's network and establish presence for lateral movement.

In 2019, the LYCEUM hacking Group was known to mainly target Middle East oil and gas facilities [14]. Attacks relied on password spraying and spear phishing. Remote access Trojan used DNS and HTTP-based communication to provide remote access capability for executing arbitrary commands and additional modules and uploading files [14]. Attack compromised email accounts of employees and stole information and credentials.

B. ATTACKS ON MIDSTREAM INFRASTRUCTURE

Midstream ICS processes connect the upstream production with downstream facilities and refining. Midstream facilities mostly include pipelines and storage, along with maritime and rail transportation. Since rail and maritime transportation are parts of different critical infrastructure sectors (namely, the Maritime and Transportation sectors), in this article we will only present attacks on pipelines and intermediary facilities on land.

From O&G infrastructures, midstream demonstrates the smallest number of documented security events, with only the XENOTIME hacking group documented as a threat to midstream [66]. The most probable target in midstream infrastructures is the pipeline network and their AGI installations used to manage and control operation flow and transport. The APT33 hacking group is also known to have targeted, amongst others, the oil supply chain of companies in Europe and Asia. Spear phishing campaigns specifically targeted oil tanker companies, IT specialized in the oil industry, online magazine for news on oil, and several manufacturers of O&G equipment. Attacks targeted the supply chain of facilities [77].

Only seven (7) documented ICS security events exist against midstream pipeline networks. Even though the first cyber-attack took place back in 1982, when an allegedly CIA malware caused a pipeline explosion at the Siberian Oil Pipeline, still the first documented event using actual networks to attack midstream infrastructures was back in 1999, when an unintended series of database queries caused an availability attack on systems and services. This, together with a misconfigured PRV that failed to open resulted in the rupture and explosion of the Olympic Pipeline Company's gasoline pipeline at Washington, USA. 3 people died and 8 were injured. Property damage was estimated at $58.5 million and the legal settlement was $112 million [94].

In 2008, the Japan Oil, Gas and Metals Corporation (JOGMEC) server was compromised by SQL injection (2008) [48]. Computers that accessed the falsified website were redirected to a server set up by the attackers for information theft

Again in 2008, state-sponsored cyber actor successfully compromised servers of the Baku-Tbilisi-Cheycan pipeline. Attack exploited Internet connections or wireless networks for access to camera network. Attack caused temporary disruption in pipeline transfers using overpressurization [13], [80].

In another attack in 2013, malformed commands injected in the network of a gas network operator in southern Germany and also reached the Austrian energy network]. Effect was probably an unintended event when unspecified processing of commands by O&G components caused an endless loop to trigger and disrupt controls in all flow operators [82].

C. DOWNSTREAM AND CROSS-SECTOR ATTACKS

Downstream infrastructures are presumed to be the most common target of cyberattacks, especially refining operations, storage and dissemination facilities. Reports state that this is mostly due the centralization of systems and operations along with technical complexity of multiple machinery and a higher value for attackers [66].

Many documented attacks that affected downstream operations, administration and/or business processes, are also indirectly or directly connected with midstream and upstream systems, like in the case of Chevron back in 1992, when a malicious former employee hacked the warning controls of the management systems and reconfigured them to crash, eventually leading to an environmental pollution around the area of Richmond, California.

The first documented attack with effects purely on downstream operations was back in 2001, when a US-company-owned gas plant suffered an attack from one of its suppliers. The supplier hacked three of the company's computers and caused a gas provision outage to homes and businesses in a European country, in order to create a distraction and cover up an error they had caused [114].

In 2011, several vulnerabilities on Microsoft Windows resulted in the Night Dragon attack on downstream infrastructures of oil, energy and petrochemical companies around the globe, including Exxon Mobil Corp and BP Plc [113]. Data stolen focused on operational O&G field production systems. The attack exploited vulnerabilities in proxy setting in Windows to steal data from operational O&G field production systems [72], [94]. In one of the worst attacks in upstream infrastructures, attackers exfiltrated files of interest for years, including operational O&G field production systems (including ICS) and financial documents related to field exploration and bidding data on O&G assets of many O&G companies (incl. supermajors).

TRITON/TRISIS malware attacked Saudi oil Petro Rabigh in 2017 by the Xenotime hacking group. It modified behavior of Triconex Safety Instrumented System (SIS) from Schneider Electric [83], [84]. SIS are used in 18,000 different plants around the world [86]. Triton ‘‘was designed to sabotage operations and trigger an explosion'' and force controllers to enter fail-safe mode, that automatically shut down processes.

The same attack that affected German midstream infrastructures in 2013 cascaded to downstream operations through the Austrian network [82].

In 2011, the Night Dragon attack exploited vulnerabilities in the proxy settings of Microsoft Windows operating systems. The series of attacks targeted global oil, energy and petrochemical companies including Exxon Mobil Corp and BP Plc [113]. Data stolen focused on operational O&G field production systems [72], [94]. Attackers exfiltrated files of interest for years, including operational O&G field production systems (including ICS) and financial documents related to field exploration and bidding data on O&G assets of many O&G companies (including supermajors).

In April 2012, the Flame malware affected Iran's oil industry [72], [91]. Flame spread itself via either USB, or using Windows Update exploiting Microsoft's erroneous security techniques in updates. Officials stated impact was low due to oil services and exports relying on systems primarily mechanical and not connected to LAN or the Internet [91].

Another attack happened during 2018 at the Energy Services Group (ESG). ESG handled customers' transactions for natural gas pipelines owned by several energy firms [61]. Customers during the ESG attack did not have access to transactions for a substantial amount of time. Attack stemmed probably from collateral damage from the unavailability of ESG systems led to gas outages, since at least five major energy companies had to disable operating processes [89].

HEXANE attacks target O&G telecommunications in Africa, Middle East, and Southwest Asia (2018) [66]. Attack used malicious documents to drop malware [66] and perform information gathering against ICS entities [66].

In 2012, one of the most famous attacks took place. Dubbed as ‘‘Shamoon'' from the CHRYSENE hacking group, the attack targeted national oil companies including Saudi Arabia's Saudi Aramco and Qatar's RasGas. Attackers sent a spear phishing email with a Microsoft Office document as an attachment containing powershell malicious code [90]. The attack affected 35,000 Saudi Aramco workstations, causing the company to spend more than a week restoring their services [77]. It also left computers inoperable. It aimed to disrupt oil and gas production in Saudi Arabia and prevent resource flow to international markets. Attack did not spread to industrial network areas.

During the same period, the Stuxnet worm, although intended to target centrifuges at nuclear facilities in Iran, also seriously affected oil refineries, gas provision systems and power plants and has therefore been included in this list. Stuxnet exploited Microsoft Windows to seek out Siemens Step7 software and cause fast-spinning centrifuges at Iranian nuclear enrichment facilities to over-speed, tearing themselves apart.

Numerous other controlled simulated attacks on low-cost Wireless Sensor Networks (WSN) used in modern oil and gas infrastructures were demonstrated in controlled environments [92]. Researchers Critical investigated WSN security issues in all layers (from hardware to application layer) showing potential issues on such wireless smart sensors [92]. Effects vary according to attack vector and vulnerability, but include numerous events such as exposing sensitive information and data, inject false information to affect actuator state, cause DoS in processes and systems and even cause network devices to crash, shutdown, restart, or even require reprogramming.

The DYMALLOY hacking group has continuously targeted various O&G infrastructures, in Turkey, Europe, and North America [66]. Most attacks were spear phishing attacks and malware attacks on connected systems. Associated Groups are reported to be Dragonfly 2.0 and Berserk Bear10 [66]. Attacks resulted mostly in information theft for ICS operations, credentials and process details.

In 2017, an employee used a USB drive to download and view a movie on a critical infrastructure computer in the Middle East. The user did not realize that this action released a malware later dubbed as Copperfield by Nyotron, the company responsible for detecting it. Copperfield resulted in data leakage, network scanning and remote control of an ICS workstation [65].

In August 2017, Xenotime caused the disruption at an O&G facility in Saudi Arabia by using the TRISIS framework. This malware had a specific target, the Triconex safety controllers [66]. It used backdoor code and caused the industrial systems of the facility to shut down.

Last but not least, a cross-sector spear-phishing attack targeted all O&G sectors by impersonating an Egyptian contractor with experience in relevant projects in oil and gas or a shipment company. Based on Bitdefender [87], attackers abused the contractor's and company's reputation to target facilities in Malaysia, the United States, Iran, South Africa, Oman and Turkey, among others. The attack aimed at dropping the Agent Tesla spyware Trojan.

D. RESEARCH AND TESTBED ATTACKS

Although to date no recorded cyberattacks exist that affected the O&G sector through hardware trojans, still researchers have proven that hardware trojans in integrated circuits of systems commonly used in O&G can undermine security, allow remote access or simply disrupt operations when triggered [8], [39], [40].

The use of selective laser melting known commonly as 3D printing, which is a type of additive manufacturing, is increasing in O&G industry [67]. Some organizations within the industry have incorporated metal 3D printing in their business processes as a cost-efficient way to build machinery parts [68]. A report 3D Printing in O&G by Thematic Research estimates that the 3D printing market will be worth $32bn by 2025 and over $60bn by 2030. Related publications state that 3D printing procedures might be vulnerable to cybersecurity attacks and introduce novel attack surfaces, even though currently no attacks have hit 3D printing operations. Still, judging from other sectors and considering the fact that 3D printing is being used in O&G, adversaries may be able to alter blueprints-code [69] leading to faulty manufactured parts that may trigger serious failures [67], [69].

Injection attacks refer to a broad class of attack vectors that an attacker uses in order to supply untrusted input to a program. One of the types is fault injection. Hardware implemented fault injection uses additional hardware to introduce faults to the target system's hardware. Disruptive signals, such as clock glitches electromagnetic pulses are some techniques the adversary can use to systems reported to be used in O&G infrastructures [70].

According to sources [12], [97], in 2018 and 2019 researchers continuously detected a total of more than 50 vulnerabilities in the Siemens SPPA-T3000 distributed control system, a system also used in O&G infrastructures. As reports state, most vulnerabilities could be exploited for DDoS attacks. From 2018 until March 10 2020, US-CERT has been issuing updates on a technical alert [97] composed by the Dept. of Homeland Security and the Federal Bureau of Investigation that highlighted the above-mentioned issue.

Several publications both from the research community [4], [5], [8], [12], [38], [39], [50], [56], [57] and the industry [112] continuously demonstrate adverse potential effects from attacking commonly used networks and systems, like PLC, RTU and SCADA protocols like MODBUS. Such vulnerable systems and network connections are the most effective attack vector to compromise the O&G sector [11], [16], [61]. Recent publications highlight many security concerns and challenges related to hardware, supply chain, and way of monitoring operations. In [39] and [40], authors demonstrate ways to expose the vulnerability of untrusted computing platforms and avoid detection of hardware trojans; these attacks are also applicable to O&G equipment. In [58] authors present attacks able to cause severe financial damage by affecting the performance of plants while remaining within operational bounds. Although the attack was presented on a desalination plant, its ICS architecture is applicable to O&G facilities.

Applicable smart grid architectures [36], [110], wireless sensors [92] and generally IoT architectures [5], [41] are frequently reported to be vulnerable to various types of attacks.

VIII. MITIGATING CYBER ATTACKS IN O&G INFRASTRUCTURES

Following up on the classification of impact, type of attack, and potential vulnerabilities in O&G ICS, in this chapter we examine potential security controls able to mitigate the risk in most common patterns detected in the above scenarios. However, this is not a full risk management plan, since we only focus on basic gaps commonly detected by real-world cyberattacks. Security controls presented here often mitigate more than one threats or reduce the vulnerability in multiple systems, while at the same time cannot be seen as a full list of necessary security controls by system administrators. For optimal results, security officers are advised to conduct a full

TABLE 9. O&G Security Controls for Attack Mitigation.

SECURITY CONTROLS	CONTROL TYPE	PRIORITY
Tamper resistance controls on field devices	Technical – Preventive	Low (3)
Trusted procurement procedures	Administrative – Preventive	Low (3)
Patching and updating	**Administrative - Preventive**	**High (15)**
Encryption	Technical –Preventive/Deterrent	Low (2)
Authentication and access control procedures	Administrative – Preventive/Detective	Medium (7)
Penetration testing and internal audit	Administrative - Detective	Medium (6)
Employee training and awareness	**Administrative – Preventive/Detective/Deterrent**	**High (18)**
Network segmentation	**Technical – Preventive**	**High (12)**
Use of different device technologies	Administrative – Preventive/Deterrent	Low (2)
Segregation of duties and minimum privileges	Administrative – Preventive	High (11)
Catalogue and reduce system dependencies	Administrative/Technical – Preventive	Medium (6)
Minimize unified closed loop	Technical – Preventive	Medium (6)

* Priority levels: Low (control not properly implemented in 5 or less incidents), Medium (control not properly implemented in 6 to 10 incidents), and High (control not properly implemented in more than 10 incidents) from 31 incidents in Table VIII.

risk assessment based on international standards [59], [60] and develop a security plan tailored to the needs of each CI.

An analysis of the presented attacks shows that, even though impact varies depending on systems affected, still attack surfaces, infiltration techniques, and types of vulnerabilities exploited follow patterns common to all ICS and relevant IT environments. The number of interconnected devices that are internet accessible increases the attack surface, while the lack of basic security controls in most cases exposes systems to a wide range of potential attack paths.

Table 9 depicts all controls presented in this subsection, along with their categorization per type. Security control categorization follows a common pattern, grouping controls into two categories: (a) technical or administrative, and (b) preventive, detective or deterrent. We also introduce a prioritization factor (low, medium, high) for each control. The prioritization factor number is calculated based on the number of recorded incidents of Table 8. Numbers next to each priority level depict the number of recorded incidents in which infrastructures attacked would have benefited in real-world, should this control be in place/working as intended during incident manifestation. (see Table 9, PRIORITY column).

By analysing Table 9, we see that numerous attacks were performed by insiders (disgruntled employees, human error etc.) or third-parties (contractors, service providers) with partial access to systems. This calls for extended segregation of duties and minimum privileges measures to all employees. Also, strong authentication and access control procedures with help minimize the damage from such threats.

Spear phishing attacks were also one of the top techniques used by attackers in O&G incidents. Spear phishing attacks are difficult to mitigate, with employee training and awareness along with strong security procedures and internal audits being the only viable solutions.

The use of legacy equipment and the lack of proper patching procedures is one of the top cybersecurity issues in O&G infrastructures. This issue is recorded in numerous relevant reports [7], [18], [124]–[126] and also emerged during our own analysis of recorded incidents.

O&G infrastructures that aim to digitize their processes need to invest and update old equipment with modern devices that support extended security measures. Also, critical security patches must be installed the moment they are released by official vendors.

Obviously, listed security measures are not exhaustive but rather focuses on the most important and/or most frequently missing security controls, as extracted from the attack vectors used in all documented events and attacks.

A. VULNERABILITY MITIGATION

In this section, we present the most common practices and controls missing from O&G ICS and that are directly related to the most common vulnerabilities, as identified in

Section IV.C. The following measures are usually implemented by system operators and asset owners.

- **Tamper resistance controls on field devices**: Field devices must implement hardware security controls to prevent physical tampering.
- **Trusted procurement procedures**: COTS components (not custom-made) must follow strict procurement procedures that only allow installing certified devices that follow strict security standards.
- **Patching and updating**: Support stuff must install critical updates as soon as they are available, both for operating systems and ICS software.
- **Encryption**: Devices must implement end-to-end encryption and include embedded security in their processes. In some cases, certificate pinning (SSL pinning) must be required to avoid spoofed devices. It includes protection from side channel attacks that can compromise encryption keys (e.g. electromagnetic side channel attacks).
- **Authentication and access control procedures**: Facilities should implement strict authentication and authorization procedures for their employees and for all software entities.
- **Penetration testing and internal audit**: All facilities must implement rigorous vulnerability assessment and penetration testing audits in regular bases, to ensure continuous analysis of operational systems.
- **Employee training and awareness**: All employees working on critical systems must have proper training and/or certifications to support the elevated threat level of their position. Human error and phishing attacks can be most effectively avoided through proper employee awareness, rather through technical means.

B. IMPACT MITIGATION

Since the impact in O&G cyberattacks often stems from the manipulation of physical machinery, which in turn results to real-world hazards, the following list of measures emphasizes on the security controls able to increase resilience of critical systems, mostly by disconnecting them from generic networks and services.

- **Network segmentation**: All facilities must deploy proper network segmentation, with DMZ configured and network isolation to protect critical systems. Whenever possible, ICS should be must not share the same network with internet accessible devices.
- **Use of different technologies**: Implemented ICS should use devices and systems from different vendors in an effort to reduce the number of compromised assets per vulnerability. Although this measure introduces management complexity, still it is proven to be a vital control for increasing resilience of critical systems [120].
- **Segregation of duties and minimum privileges**: Staff must have discrete credentials and relevant privileges, according to their job description and needs. The least privileges principle must be implemented in all accounts used in CI.
- **Catalogue and reduce system dependencies**: Critical systems must identify and minimize dependencies on other systems and services (such as third-party processes).
- **Minimize unified closed loop**: Although closed loop systems facilitate monitoring and control and it is true that manual control exacerbates workload, still operators should complement on the idea to minimize the use of automatic controls over critical machinery, or at least implement heavy monitoring and break closed loop systems down to individual procedures.

IX. CONCLUSION

In our survey we presented a systematic cataloguing, analysis and classification of cybersecurity attacks and techniques in oil and gas infrastructures: both for upstream, midstream and downstream systems. We analyzed relevant best practices, industry reports and publications and developed a taxonomy of vulnerabilities specifically for O&G CPS, which we tied directly to MITRE's attack framework. This allows readers to further extend the knowledge gained by the survey, by directly referring to MITRE to better describe post-compromise adversary behavior and potential solutions.

Using this taxonomy and an impact assessment method that we developed using current standards, we presented an analysis and assessment of an extended catalog of cybersecurity incidents in O&G ICS. The analysis extracted attack patterns, techniques, subliminal issues that may have gone unnoticed during the incidents, and connected them with historical consequences, thus creating a web of knowledge for O&G ICS operators. Analysis included both scientific and grey literature to highlight commonalities, trends and technical issues of current cybersecurity practices in O&G implemented systems.

Results from this procedure highlighted a couple of issues that still remain to be solved, mainly an increasing number of dependencies and interconnections of O&G ICS with third-party services and operators. A decade ago, most security weaknesses stemmed from the lack of basic security controls, even in critical systems. Even though CPS in the O&G sector have come a long way and nowadays most infrastructures follow basic cybersecurity concepts, it is still evident that most security weaknesses stem from poor security designs, lack of systematic use of information security management systems, as well as critical dependencies of equipment to third-party components and services, mainly telecoms.

A. GAP ANALYSIS

By analyzing documented attacks using our vulnerability taxonomy, the presented impact assessment method and MITRE's ATT&CK techniques, we identified a number of research and implementation gaps that complement the mitigation measures presented in Section VIII.

Current best practices and common defense strategies go along way towards mitigating cybersecurity attacks. Still, analysis of attacks shows that existing strategies have issues when it comes to protecting facilities from insider threats and spear phishing attacks that exploit the human factor to cause adverse effects. Also, technical incoherencies coupled with internet access to field devices inhibit proper protection from security measures such as firewalls, intrusion detection systems and minimum privileges access controls.

To this end, we identify and present gaps in today's cybersecurity implementations that can serve as a "to-do" list of defense strategies for oil and gas infrastructures, so as to be able to properly resist the cybersecurity attacks currently not fully mitigated.

1) VULNERABILITY ASSESSMENT

Most attack techniques used by threat actors against O&G CPS follow the statistics of regular ICT systems (see Table 8). They can be properly mitigated to a degree through the implementation of controls and standardized procedures documented in relevant best practices and standards. The fact that most infrastructures lack basic security procedures and controls affect the amount of vulnerabilities present and the severity of potential attacks. This is supported by the fact that most worst-case scenario attacks that have happened involved critical systems and procedures that were insecurely interconnected to remote networks through telecom or third-party services.

O&G software vulnerabilities can often directly affect machinery. This an important factor to consider during impact assessment. Spillovers, tilting rigs and pipeline unavailability are only a few of the documented examples of such vulnerabilities. Operators should specifically take into account software vulnerabilities in critical systems and that may be inherited through third-party components.

Also, proper network segregation and isolation of critical machinery and procedures seems to be a very effective way to reduce the number of vulnerabilities and attack paths for adversarial groups. Network monitoring seems ineffective due to the high number of false-positives and the distributed nature of processes in the O&G infrastructure. Instead, monitoring third-party services and isolating critical equipment has literally saved operators times, as documented in Iran and the US.

Employee awareness is one of the top issues in ICS security and seems to be as important for the O&G sector. Email phishing and information spoofing seems to be the most frequent attack technique in this sector, followed closely by insider threats and disgruntled employees. Even though it is common knowledge that such systems must have proper cybersecurity and safety training in place and always strictly follow segregation of duties, still history shows that most O&G infrastructures either lack proper employee training that focuses both on OT and IT systems, or assign too many privileges to staff.

One of the most alarming issues in O&G systems is the extended and regular use of legacy equipment and software in CI. Although operators seem to be in a process of updating systems and services, still many infrastructures deploy old components that have either no support (end-of-life) or limited ratios of patches issued per vulnerabilities detected. Also, some of these components lack basic security measures, such as encryption or access control. This situation introduces numerous vulnerabilities that either cannot be fixed on time, or require complex work-arounds to enable secure use, which sometimes lead to erroneous implementations of controls. Most frequent example is the lack of encryption and segregation of connections in local SCADA systems that still use unencrypted MODBUS/TCP protocols to manipulate equipment.

2) IMPACT ASSESSMENT AND RESILIENCE

Assessing the potential impact from vulnerability exploitation in each instance is based on evidence gathered by the documented attacks on O&G systems and infrastructures. A basic remark here is that impact (and risk) assessment procedures in O&G infrastructures should take into account subliminal and indirect dependencies of their systems on external third-party operators, services, and equipment. History has shown that most attacks were expected in terms of techniques, but operators greatly underestimated the potential impact that the lack of resilience on their systems.

Current impact assessment methods do not adequately represent the evolution of consequences over time, nor do they properly depict estimations of cost during system unavailability. This, coupled with the fact that most resilience analysis in the O&G sector does not take into consideration inherent dependency loops (i.e. situations were unavailability of a service leads to the exacerbation of consequences in another department inside the infrastructure, which in turn does not allow for the first service unavailability to be fixed) further provides an erroneous sense of safety since major consequences are left unnoticed. An example was the cyber-attack on the refinery that lead to loss of access and loss of control on remote components, which in turn did not allow operators to stop the malware from using equipment due to the remote nature of the ICS.

Even though numerous publications exist that tackle cybersecurity issues for industrial systems, current literature seems fragmented and does not focus on the O&G sector, despite its importance.

B. CURRENT ATTACK TRENDS

By summarizing findings, there is a clear indication that current attacks in oil and gas systems follow similar attack trends for common ICT systems. Specifically, most common attack vectors against O&G infrastructures include spear phishing through email, external attack (malware or injection) to exposed devices and user execution of some sort, either intentionally (malicious insiders) or erroneously (e.g. employee opening an email, or wrong command execution).

TABLE 10. Detailed Analysis of Attacks on O&G infrastructures.

ATT&CK technique	Attack type	O&G sector	Incident description and reports	Attack scenario	ATT&CK impact	Impact rank and description
Internet Accessible Device (T883)	External – Malware attack	Upstream	In 2010, a rig en route from South Korea to Brazil was infected with computer malware [94],[95].	C-P	• Denial of Service (T814) • Loss of Availability (T826) • Damage to Property (T879)	Infection reached such extent that it took IT stuff 19 days to make resume operations. **Impact rank: High** **Cascading effects: Internal**
User Execution (T863)	Internal – injection attack Internal - Jamming	Upstream Midstream Downstream	A worker at the Chevron oil company was fired, having hacked the computers in the company's New York and San Jose offices that were responsible for the warnings systems, and reconfiguring them to crash when the system was started up.	C-P	• Change Program State (T875) • Damage to Property (T879) • Modify Control Logic (T833)	Toxic substance was leaked in Richmond, California, and the system failed to generate the corresponding warning, placing thousands of lives at risk for the ten hours that the system was down **Impact rank: High** **Cascading effects: Yes**
User Execution (T863)	Internal – injection attack Internal - Jamming	Downstream	Gas plant run by a US oil company also suffered an attack in 2001. After a 6-month investigation, it was determined that it had been the work of one of the suppliers who, in order to cover up an error they had caused on a computer, had created a distraction by hacking three of the company's computers and causing a service outage to homes and businesses in a European country [114].	C-P	• Denial of Service (T814) • Loss of Availability (T826) • Damage to Property (T879) • Modify Control Logic (T833)	Cyber-attack leads to gas service outage to homes and businesses in a European country [114]. **Impact rank: High** **Cascading effects: Yes (housing)**
User Execution (T863)	External – malware attack	Midstream	First ever cyber-attack was in 1982 and was attributed allegedly to the CIA, when attackers managed to install a Trojan on the SCADA system that controlled the Siberian oil pipeline.	C-P-C	• Damage to Property (T879) • Modify Control Logic (T833)	Malware caused massive explosion. **Impact rank: High** **Cascading effects: No**
Internet Accessible Device (T883) User Execution (T863)	External – Injection attack (assumed)	Upstream	In December 2012, an attack shut down an oil rig off the coast of Africa by tilting it [94], [95] 17 degrees. Attack was attributed to manipulation of the ballast control that led equipment failure [96], probably through PLC-actuator command-and-control.	C-P	• Modify Control Logic (T833) • Change Program State (T875) • Denial of Service (T814) • Damage to Property (T879)	Attack caused injuries to 89 workers involved in building the rig. **Impact rank: High** **Cascading effects: No**

TABLE 10. ***(Continued.)*** **Detailed Analysis of Attacks on O&G infrastructures.**

ATT&CK technique	Attack type	O&G sector	Incident description and reports	Attack scenario	ATT&CK impact	Impact rank and description
Replication Through Removable Media Technique (T847)	Internal - USB attack	N/A	The malware Copperfield (2017) infected critical infrastructures in the Middle East via USB. Script-based malware attack leveraged Windows Script Host [65].	C-C C-P	• Theft of Operational Information (T882)	Attack stole data for reconnaissance purposes **Impact rank: Low Cascading effects: No**
User Execution (T863) Replication Through Removable Media Technique (T847)	Internal – Malware attack	Upstream	In 1999, a malware attack hit the Gazprom company by an insider who opened it deliberately [94]. Affected systems involved the control of flow inside the pipelines.	C-P C-C	• Loss of Control (T827) • Modify Control Logic (T833) • Change Program State (T875)	Entire control system of the Russian gas supplier was under direct control of the attackers for a number of hours. **Impact rank: High Cascading effects: No**
Internet Accessible Device (T883)	External – Malware attack	Upstream Midstream Downstream	TRITON/TRISIS malware attacked Saudi oil giant Petro Rabigh in 2017 by the Xenotime hacking group. It modified behavior of Triconex Safety Instrumented System (SIS) from Schneider Electric [83], [84]. SIS are used in 18,000 different plants around the world [86].	C-C C-P	• Modify Control Logic (T833)	Triton "was designed to sabotage operations and trigger an explosion" [86]. Forced controllers to enter fail-safe mode that automatically shut down processes. **Impact rank: High Cascading effects: No**
User Execution (T863)	Internal – Injection attack (unintended)	Midstream Downstream	Malformed commands injected in the network of a gas network operator in southern Germany and also reached the Austrian energy network and was forwarded to different operators [82].	C-P	• Change Program State (T875) • Denial of Service (T814) • Loss of Control (T827)	Unspecified processing of command by O&G components, an endless loop triggered disruptions to controls in all operators [82]. **Impact rank: Medium Cascading effects: Internal**
User Execution (T863) Modify Control Logic (T833)	Internal – Injection attack	Upstream Midstream Downstream	Test attacks introduced clock glitches and electromagnetic pulses on equipment and machinery used by O&G plants [70].	C-P	• Change Program State (T875) • Denial of Service (T814)	Attacks could lead to disruption of operations and cause numerous collateral issues. **Impact rank: Medium Cascading effects: No**

TABLE 10. ***(Continued.)*** **Detailed Analysis of Attacks on O&G infrastructures.**

ATT&CK technique	Attack type	O&G sector	Incident description and reports	Attack scenario	ATT&CK impact	Impact rank and description
Spear phishing Attachment (T865)	External – phishing attack	Midstream	APT33 attack group targeted, amongst others, the oil supply chain to compromise oil companies in Europe and Asia. Spear phishing campaigns sent targeted oil tanker companies, IT specialized in the oil industry, online magazine for news on oil, and several manufacturers of O&G equipment [87].	C-P	- Supply Chain Compromise (T862)	Attacks targeted the supply chain of facilities [87] **Impact rank: High** **Cascading effects: Yes (procurement)**
Spear phishing Attachment (T865)	External – phishing attack	Downstream	IN 2011, the Night Dragon attack exploited vulnerabilities in proxy setting in Microsoft Windows. The series of attacks targeted global oil, energy and petrochemical companies including Exxon Mobil Corp and BP Plc [113]. Data stolen focused on operational oil and gas field production systems [72], [94].	C-P	- Theft of Operational Information (T882)	Attackers exfiltrated files of interest for years, including operational oil and gas field production systems (includeing ICS) and financial documents related to field exploration and bidding data on oil and gas assets of many oil and gas companies (including supermajors). **Impact rank: Medium** **Cascading effects: No**
Spear phishing Attachment (T865)	External – phishing attack	Upstream	Gaza Cybergang attacks on Oil and Gas Industry (2017), the adversaries were discovered inside oil and gas organization in the MENA region. Attackers extracted data continuously for more than a year using the CVE 2017-0199 vulnerability [88].	C-C	- Theft of Operational Information (T882)	Attackers extracted data continuously for >1year using the CVE 2017-0199 vulnerability **Impact rank: Low** **Cascading effects: No**
Internet Accessible Device (T883)	External – Malware attack (assumed)	N/A	Wiper malware attack hit Iran's oil industry and the Oil Ministry in spring 2012.	C-P-C C-P	- Damage to Property (T879)	Wiper aggressively stole and destroyed data on purpose. Wiper caused no permanent damage due to backups of essential and non-essential data. **Impact rank: Medium** **Cascading effects: No**

TABLE 10. *(Continued.)* **Detailed Analysis of Attacks on O&G infrastructures.**

ATT&CK technique	Attack type	O&G sector	Incident description and reports	Attack scenario	ATT&CK impact	Impact rank and description
User Execution (T863)	Internal – injection attack	Upstream	(2002) the Venezuelan oil company PDVSA had several of their computers hacked [114]. Assumed attackers were employees participating in a strike at that time.	C-P	• Damage to Property (T879)	Reduced their oil production by 87.6% per day [114]. **Impact rank: High** **Cascading effects: Yes (transport)**
Internet Accessible Device (T883)	External – Injection attack	Downstream	Energy Services Group - ESG attack (2018), handled customers transactions for natural gas pipelines owned by several energy firms [61].	C-C	• Loss of Availability (T826) • Loss of Productivity and Revenue (T828)	Customers during the ESG attack did not have access to transactions for a substantial amount of time. Collateral damage led to Gas outages [89]. **Impact rank: High** **Cascading effects: Yes (financial, transport)**
Internet Accessible Device (T883) Man in the Middle (T830)	External – Malware attack	Upstream	OilRig malware attacks targeted oil and gas institutions in Saudi Arabia (2016) [17]. Similar scripted malware TwoFace Webshell used to break into and infect systems to the Ministry of Oil of a Middle Eastern country [85].	C-C	• Theft of Operational Information (T882)	Attack used credential dumping tools, such as Mimikatz, and stole credentials to accounts. TwoFace used to access the victim's network and establish presence for lateral movement. **Impact rank: Medium** **Cascading effects: No**
Internet Accessible Device (T883) Replication Through Removable Media Technique (T847)	External – Malware attack Internal – USB attack	Downstream	Flame attack affected Iran’s oil industry [72],[91]. Flame spread itself via either USB, or using Windows Update exploiting Microsoft’s erroneous security techniques in updates.	C-C	• Theft of Operational Information (T882)	Officials stated impact was low due to oil production or exports relying on systems primarily mechanical and not connected to LAN or the Internet [91]. **Impact rank: Low** **Cascading effects: No**
Spear phishing Attachment (T865)	External – Phishing attack External – Malware attack	Upstream	LYCEUM Group attacks mainly targeting Middle East oil and gas facilities (2019) [14]. Attack relied on password spraying and spear phishing. Remote access trojan used DNS and HTTP-based communication to provide remote access capability for executing arbitrary commands and additional modules and uploading files [14].	C-C	• Theft of Operational Information (T882)	Attack compromised email accounts of employees and stole information and credentials. **Impact rank: Low** **Cascading effects: No**

TABLE 10. ***(Continued.)*** **Detailed Analysis of Attacks on O&G infrastructures.**

ATT&CK technique	Attack type	O&G sector	Incident description and reports	Attack scenario	ATT&CK impact	Impact rank and description
Internet Accessible Device (T883)	External – Injection attack	Midstream	Japan Oil, Gas and Metals Corporation (JOG-MEC) server was compromised by SQL injection (2008) [48].	C-C	- Theft of Operational Information (T882)	Computers that accessed the falsified website were redirected to a server set up by the attackers for information theft **Impact rank: Medium** **Cascading effects: No**
Spear phishing Attachment (T865)	External – Phishing attack (assumed)	Midstream Downstream	HEXANE attacks target oil and gas telecoms in Africa, Middle East and Southwest Asia (2018) [66]. Attack used malicious documents to drop malware [66].	C-C	- Theft of Operational Information (T882) - (assumed)	Information gathering against ICS entities [66]. **Impact rank: Low** **Cascading effects: No**
Spear phishing Attachment (T865)	External – Phishing attack (assumed)	Upstream Midstream	In 2013, MAGNALLIUM attack targeted petrochemical manufacturers including energy firms in Saudi Arabia, Europe and North America [66]. Malware did not have an ICS-specific capability, instead focused on IT systems. Attack tied to APT 33 and Elfin5 groups [66].	C-C	- Theft of Operational Information (T882)	Information gathering against ICS entities [66]. **Impact rank: Low** **Cascading effects: No**
Spear phishing Attachment (T865)	External – phishing attack	Midstream Downstream	Shamoon (2012) / Disstrack attack to oil producers. The malware was used against national oil companies including Saudi Arabia's Saudi Aramco and Qatar's RasGas. Attackers sent a spear phishing email with a Microsoft Office document as an attachment containing powershell malicious code [90]. Attributed group: CHRYSENE	C-C C-P	- Denial of Control (T813) - Denial of View (T815) - Loss of Availability (T826) - Loss of Control (T827) - Loss of Productivity and Revenue (T828) - Loss of View (T829)	Attack affected 35,000 Saudi Aramco workstations, causing the company to spend >1 week restoring their services [77]. It also left computers not operable. It aimed to disrupt oil and gas production in Saudi Arabia and prevent resource flow to international markets. Attack did not spread to industrial network areas. **Impact rank: High** **Cascading effects: Yes (financial)**

TABLE 10. ***(Continued.)*** **Detailed Analysis of Attacks on O&G infrastructures.**

ATT&CK technique	Attack type	O&G sector	Incident description and reports	Attack scenario	ATT&CK impact	Impact rank and description
Internet Accessible Device (T883) Wireless Compromise (T860)	External – Injection attack	Midstream	During 2008, state-sponsored cyber actor successfully compromised servers of the Baku-Tbilisi-Cheycan pipeline [13], [80]. Attack exploited Internet connections or wireless networks for access to camera network [13].	C-P	• Denial of Control (T813) • Denial of View (T815) • Loss of Availability (T826) • Loss of Control (T827) • Loss of Productivity and Revenue (T828) • Damage to Property (T879)	Attack caused temporary disruption in pipeline transfers using over-pressurization [13], [80]. **Impact rank: High** **Cascading effects: Yes (distribution)**
Internet Accessible Device (T883) Man in the Middle (T830) User Execution (T863) Modify Control Logic (T833)	Internal – Injection attack External – Malware Internal – Protocol attacks Internal – MITM attacks Internal - Jamming	Upstream Midstream Downstream	Extensive testbed attacks are documented against ICS technologies used extensively in the oil and gas sector. Those include relevant ICS protocols used in all critical infrastructures, including oil, and gas infrastructures, that lack adequate security controls (e.g. MODBUS). [8],[52],[93]. Also, hardware trojan attacks are proven to be possible in oil and gas components, although real-world attacks are to date not recorded in O&G [8].	C-C C-P P-C-P C-P-C	• Denial of Control (T813) • Denial of View (T815) • Loss of Availability (T826) • Loss of Control (T827) • Loss of Productivity and Revenue (T828) • Loss of View (T829) • Theft of Operational Information (T882) • Modify Control Logic (T833) • Change Program State (T875) • Denial of Service (T814)	MITM attacks on unencrypted SCADA packets can lead to information theft. Injected malware can reprogram industrial control systems, or launch DoS attacks on machinery. Even process attacks are possible by sending fake data that push equipment to enter unwanted states of operation [56], [58]. **Impact rank: High** **Cascading effects: No**
Wireless Compromise (T860) Man in the Middle (T830)	External – Injection attack Internal - hacking hardware, - Protocol attacks, - MITM attacks, - Physical attacks, - Jamming	Upstream Midstream Downstream	Controlled simulated attacks on low-cost Wireless Sensor Networks (WSN) used in modern oil and gas infrastructures were demonstrated in [92]. Critical WSN security issues were investigated in all layers (from hardware to application layer) showing potential issues on such wireless smart sensors and IoT devices [92].	C-C C-P C-P-C	• Denial of Control (T813) • Denial of View (T815) • Loss of Availability (T826) • Loss of Control (T827) • Loss of Productivity and Revenue (T828) • Loss of View (T829) • Theft of Operational Information (T882) • Modify Control Logic (T833) • Change Program State (T875) • Denial of Service (T814)	Effects vary according to attack vector and vulnerability, but include numerous events such as exposing sensitive information and data, inject false information to affect actuator state, cause DoS in processes and systems and even cause network devices to crash, shutdown, restart or even require reprogramming. **Impact rank: High** **Cascading effects: No**

TABLE 10. ***(Continued.)*** **Detailed Analysis of Attacks on O&G infrastructures.**

ATT&CK technique	Attack type	O&G sector	Incident description and reports	Attack scenario	ATT&CK impact	Impact rank and description
User Execution (T863) Modify Control Logic (T833)	Internal – Injection attack	Upstream	A disgruntled tech employee purposely impaired an industrial system using a hacking attack for monitoring pipeline leaks at a Southern California detection system (2009) [15],[94].	C-P	- Denial of Service (T814) - Loss of Availability (T826) - Loss of Control (T827)	Attack a number of adverse effects on operations and machinery [15]. **Impact rank: Medium** **Cascading effects: Internal**
Spear phishing Attachment (T865) Internet Accessible Device (T883)	External – phishing attack External – Malware attack	Upstream Midstream Downstream	DYMALLOY hacking group targeted various infrastructures, including oil and gas in Turkey, Europe, and North America [66]. Most attacks were spear phising attacks and malware attacks on connected systems. Associated Groups are Dragonfly 2.0, Berserk Bear10 [66].	C-C	- Theft of Operational Information (T882)	Information theft, mainly ICS operations, credentials and process details **Impact rank: Low** **Cascading effects: No**
User Execution (T863)	Internal – Injection attack (unintended)	Midstream	During 1999, an unintended series of database queries together with a misconfigured PRV that failed to open resulted in the rupture and explosion of the Olympic Pipeline Company's gasoline pipeline at Washington, USA [94].	C-P	- Denial of Service (T814) - Loss of Availability (T826) - Loss of Control (T827) - Damage to Property (T879)	3 people died and 8 were injured. Property damage was estimated at $58.5 million and the legal settlement was $112 million [94]. **Impact rank: High** **Cascading effects: Yes (financial, societal)**
Replication Through Removable Media Technique (T847) Internet Accessible Device (T883)	Internal – Injection attack External – Malware attack	Midstream Downstream	The Stuxnet worm, although intended to target centrifuges at nuclear facilities in Iran, it also seriously affected oil refineries, gas pipelines and power plants and has therefore been included in this list.	C-P	- Denial of Service (T814) - Loss of Availability (T826) - Loss of Control (T827) - Damage to Property (T879)	Stuxnet exploited Microsoft Windows to seek out Siemens Step7 software and cause fast-spinning centrifuges at Iranian nuclear enrichment facilities to over-speed, tearing themselves apart. **Impact rank: High** **Cascading effects: Yes (societal, financial)**
Spear phishing Attachment (T865) Internet Accessible Device (T883)	External – phishing attack External – Malware attack	Upstream Downstream	Cross-sector spear-phishing attack impersonated an Egyptian contractor or shipment company to drop the Tesla malware [87].	C-C	- Theft of Operational Information (T882)	Information theft, mainly ICS operations, credentials and process details **Impact rank: Low** **Cascading effects: No**

Most attacks involve information theft and/or industrial espionage (42% of recorded cases). A total of around 32% of current attacks aim to take control of OT infrastructures, while about 45.1% aim to cause some sort of Denial of Service or unavailability of systems. Both types of recorded cases almost always aim to incur economic losses to companies or regions. This indicates that O&G attackers do not aim to create direct profit, but rather seems to want to create issues to competitors and/or competitive countries.

C. LIMITATIONS

Our survey follows a systematic approach to catalog incidents, extract knowledge and present its analysis, but, still, some limitations exist that may have prevented this article from reaching full potential. For example, during the search process we opted to study articles written in English, French and German languages only. Other articles were not included.

Also, search strings used to identify relevant work may be restricted and not capture the entire present body of knowledge in the area. Some bias on publications may also be present. Any article review process is prone to the reader's bias and, as such, may lead to erroneous inclusion and/or exclusion of relevant articles.

To cope with this, we opted to discuss multiple articles in group meetings so as to avoid one-sided views of content. This, coupled with our effort to only include articles from peer-reviewed publishing houses and companies aims to reduce such issues to a minimum.

D. FUTURE DIRECTIONS

If we follow the trends of all recorded incidents, we can safely conclude that the ongoing digitization of O&G systems will further increase the likelihood of cyberattacks, although it seems that attacks nowadays have smaller environmental and societal impart than 10 years ago. This is intuitively true. The upcoming digitization and decentralization of O&G systems in Industry 4.0 increases the amount of attack surfaces (i.e. increases the likelihood of threat manifestation), but on the other hand, companies and states are starting to issue strict rules, certification and guidelines for cybersecurity. Up until early 2000s, most certifications and technical guides aimed at protecting against safety hazards. This is the reason why major attacks that occurred in previous decades caused extensive damages, while very few aimed at information theft; a trend that seems to be reversing.

APPENDIX

Table 10 presents the detailed analysis of all recorded attacks on O&G sectors, together with a mapping of each attack to MITRE's ATT&CK techniques, types of impact and impact rankings along with potential cascading indicators.

REFERENCES

[1] Analysis & Projections—US Energy Information Administration. *Analysis & Projections—US Energy Information Administration*. Accessed: Dec. 21, 2019. [Online]. Available: https://www.eia.gov/outlooks/

[2] International Energy Agency (IEA). (Mar. 2019). *Market Report Series: Oil 2019—Analysis*. Accessed: Dec. 5, 2019. [Online]. Available: https://www.iea.org/reports/oil-2019

[3] M. Garside. (Aug. 9, 2019). Global Natural Gas Consumption 2018. Statista. Accessed: Dec. 21, 2019. [Online]. Available: https://www.statista.com/statistics/282717/global-natural-gas-consumption/

[4] C. Alcaraz and S. Zeadally, "Critical control system protection in the 21st century," *Computer*, vol. 46, no. 10, pp. 74–83, Oct. 2013.

[5] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 2018.

[6] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 2015.

[7] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, *Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations Such as Programmable Logic Controllers (PLC)*, document NIST SP 800-82 Rev. 2, U.S. Department of Commerce, NIST, 2015.

[8] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proc. IEEE*, vol. 104, no. 5, pp. 1039–1057, May 2016.

[9] T. Nelson and M. Chaffin, *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, document, U.S. Department of Homeland Security (DHS), National Cyber Security Division's Control Systems Security Program, 2011.

[10] *CCTA Risk Analysis and Management Method: User Manual (CRAMM), Ver. 3.0*, UK Central Computer & Telecommunications Agency, London, U.K., 1996.

[11] Kaspersky.Com. *Kaspersky ICS Security Assessment: Identification and Remediation of Security Flaws in ICS Infrastructures*. Accessed: Mar. 11, 2020. [Online]. Available: https://www.kaspersky.com/enterprise-security/ics-security

[12] E. Kovacs. (Dec. 13, 2019). Hackers Can Exploit Siemens Control System Flaws in Attacks on Power Plants. SecurityWeek. Accessed: Dec. 22, 2019. [Online]. Available: https://www.securityweek.com/hackers-can-exploit-siemens-control-system-flaws-attacks-power-plants

[13] R. Lee, M. Assante, and T. Conway, *Media Report of the Baku-Tbilisi-Ceyhan Pipeline Cyber Attack*. Bethesda, MD, USA: SANS, 2014.

[14] K. Yedakula. (Aug. 28, 2019). Lyceum/Hexane Threat Actor Group Targets Oil and Gas Organizations in Middle East: Cyware Hacker News. Cyware. Accessed: Dec. 23, 2019. [Online]. Available: https://cyware.com/news/lyceumhexane-threat-actor-group-targets-oil-and-gas-organizations-in-middle-east-c6c75bcc

[15] D. Kravets. (Mar. 18, 2009). Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System. Wired. Accessed: Dec. 23, 2019. [Online]. Available: https://www.wired.com/2009/03/feds-hacker-dis/

[16] K. Bissell and L. Ponemon, *The Cost of Cybercrime*. Dublin, Ireland: Accenture, 2019.

[17] R. Falcone and B. Lee. (May 26, 2016). The OilRig Campaign: Attacks on saudi Arabian Organizations Deliver Helminth Backdoor. Palo Alto Networks: Unit42. Accessed: Dec. 23, 2019. [Online]. Available: https://unit42.paloaltonetworks.com/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor/

[18] S. McBride, J. Ashcraft, and N. Belk. (Aug. 3, 2016). Overload: Critical Lessons From 15 Years of ICS Vulnerabilities. FireEye. Accessed: Mar. 3, 2020. [Online]. Available: https://www.fireeye.com/blog/threat-research/2016/08/overload-critical-lessons-from-15-years-of-ics-vulnerabilities.html

[19] ICS-CERT. *The Industrial Control Systems Cyber Emergency Response Team*. Accessed: Feb. 3, 2020. [Online]. Available: https://www.us-cert.gov/ics

[20] R. Mattioli and K. Moulinos, "Analysis of ICS-SCADA Cyber Security maturity levels in critical sectors," ENISA, Heraklion, Greece, Tech. Rep., 2015.

[21] A. Keliris, C. Konstantinou, and M. Maniatakos, *GE Multilink SR Protective Relays Passcode Vulnerability*. New York, NY, USA: BlackHat, 2017.

[22] S. Cobb. (Oct. 24, 2016). 10 Things to Know About the October 21 IoT DDoS Attacks. ESET: WeLiveSecurity. Accessed: Dec. 26, 2019. [Online]. Available: https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/

[23] B. Strom, A. Applebaum, D. Miller, K. Nickels, A. Pennington, and C. Thomas, ''MITRE ATT&CK: Design and philosophy,'' MITRE, McLean, VA, USA, Tech. Rep. 01ADM105, 2018.

[24] Alert (AA20-049A). (Feb. 18, 2020). *Ransomware Impacting Pipeline Operations | CISA*. Accessed: Mar. 20, 2020. [Online]. Available: https://www.us-cert.gov/ncas/alerts/aa20-049a

[25] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou, and D. Gritzalis, ''Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures,'' *Int. J. Crit. Infrastruct. Protection*, vol. 12, pp. 46–60, Mar. 2016.

[26] MITRE. (2013). *Common Attack Pattern Enumeration and Classification (CA-PEC)*. Accessed: Jan. 3, 2020. [Online]. Available: https://capec.mitre.org/

[27] American Petroleum Institute. (2019). *America's Generation Energy: State of American Energy 2019*. Accessed: Jan. 3, 2020. [Online]. Available: https://www.api.org/~/media/Files/Policy/SOAE-2019/SOAE2019_Report.pdf

[28] Y. Brun, G. Di Marzo Serugendo, C. Gacek, H. Giese, H. Kienle, M. Litoiu, H. Müller, M. Pezzè, and M. Shaw, ''Engineering self-adaptive systems through feedback loops,'' in *Software Engineering for Self-Adaptive Systems*. Berlin, Germany: Springer, 2009, pp. 48–70.

[29] R. Irons-Mclean, K. Rittie, J. Greengrass, J. van Dijk, R. Albach, J. Pienado, and F. Ahmed, *Oil and Gas Pipeline: Industrial Security Reference Design*. San Jose, CA, USA: CISCO, 2019.

[30] (2017). *The Engineer's Guide to Tank Gauging, Emerson*. Accessed: Mar. 10, 2020. [Online]. Available: https://www.emerson.com/documents/automation/-engineer-s-guide-to-tank-gauging-en-175314.pdf

[31] ATEX Directive 2014/34/EU. (Feb. 2014). *Directive 2014/34/EU on the Harmonization of the Laws of the Member States Relating to Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres*. Accessed: Jan. 3, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0034

[32] *International Electrotechnical Commission System for Certification to Standards Relating to Equipment for Use in Explosive Atmospheres (IECEx System)*. Accessed: Mar. 10, 2020. [Online]. Available: https://www.iecex.com/

[33] National Institute of Standards and Technology (NIST). (2014). *Computer Security Resource Center (CSRC)*. Accessed: Mar. 10, 2020. [Online]. Available: https://csrc.nist.gov/

[34] Department of Homeland Security: Cybersecurity and Infrastructure Security Agency. *Control System HMI Computers*. Accessed: Mar. 9, 2020. [Online]. Available: https://www.us-cert.gov/ics/Control_System_HMI_Computers-Definition.html

[35] C. Dukes, ''Committee on national security systems glossary,'' Committee Nat. Secur. Syst., Rockville, MD, USA, Tech. Rep. CNSSI 4009, 2015.

[36] C. Neuman and K. Tan, ''Mediating cyber and physical threat propagation in secure smart grid architectures,'' in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Oct. 2011, pp. 238–243.

[37] P. Grassi, M. Garcia, J. Fenton, *Digital Identity Guidelines (Rev. 3)*, document NIST Special Publication 800-63-3, United States Department of Commerce, NIST, 2017.

[38] A. Keliris, C. Konstantinou, N. G. Tsoutsos, R. Baiad, and M. Maniatakos, ''Enabling multi-layer cyber-security assessment of industrial control systems through Hardware-In-The-Loop testbeds,'' in *Proc. 21st Asia South Pacific Design Autom. Conf. (ASP-DAC)*, Jan. 2016, pp. 511–518.

[39] N. G. Tsoutsos, C. Konstantinou, and M. Maniatakos, ''Advanced techniques for designing stealthy hardware trojans,'' in *Proc. 51st Annu. Design Autom. Conf. Design Autom. Conf. (DAC)*, 2014, pp. 1–4.

[40] Y. Jin, M. Maniatakos, and Y. Makris, ''Exposing vulnerabilities of untrusted computing platforms,'' in *Proc. IEEE 30th Int. Conf. Comput. Design (ICCD)*, Sep. 2012, pp. 131–134.

[41] E. Ronen, A. Shamir, A.-O. Weingarten, and C. OFlynn, ''IoT goes nuclear: Creating a ZigBee chain reaction,'' in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2017, pp. 54–62.

[42] B. M. S. Arifin, Z. Li, S. L. Shah, G. A. Meyer, and A. Colin, ''A novel data-driven leak detection and localization algorithm using the kantorovich distance,'' *Comput. Chem. Eng.*, vol. 108, pp. 300–313, Jan. 2018.

[43] S. Mokhatab and W. Poe, *Handbook of Natural Gas Transmission and Processing: Raw Gas Transmission*. Noida, India: Gulf Professional, 2012.

[44] W. Gao, T. Morris, B. Reaves, and D. Richey, ''On SCADA control system command and response injection and intrusion detection,'' in *Proc. eCrime Researchers Summit*, Oct. 2010, pp. 1–9.

[45] H. Yoo and I. Ahmed, ''Control logic injection attacks on industrial control systems,'' in *Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection*. Cham, Switzerland: Springer, Jun. 2019, pp. 33–48.

[46] D. Deresford. (2010). *The Sauce of Utter Pwnage*. Accessed: Feb. 6, 2020. [Online]. Available: http://thesauceofutterpwnage.blogspot.com/

[47] O. Andreeva, S. Gordeychik, G. Gritsai, O. Kochetova, E. Potseluevskaya, S. Sidorov, and A. Timorin, *Industrial Control Systems Vulnerabilities Statistics*. Moscow, Russia: Kaspersky Lab, 2016.

[48] H. Kobayashi, K. Watanabe, T. Watanabe, and Y. Nagayasu, ''Development of information security-focused incident prevention measures for critical information infrastructure in Japan,'' in *Critical Information Infrastructures Security* (Lecture Notes in Computer Science). 2010, pp. 22–33.

[49] Department of Homeland Security: Cybersecurity and Infrastru-cture Security Agency. (Feb. 6, 2012). *ING. Punzenberger COPA-DATA GMBH DoS Vulnerabilities*. Accessed: Mar. 11, 2020. [Online]. Available: https://www.us-cert.gov/ics/advisories/ICSA-12-013-01

[50] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, ''Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols,'' *ACM Trans. Sensor Netw.*, vol. 5, no. 1, pp. 1–38, Feb. 2009.

[51] É. Ádámkó, G. Jakabóczki, and P. Szemes, ''Proposal of a secure Modbus RTU communication with Adi Shamir's secret sharing method,'' *Int. J. Electron. Telecommun.*, vol. 64, no. 2, pp. 107–114, 2018.

[52] N. Sayegh, A. Chehab, I. H. Elhajj, and A. Kayssi, ''Internal security attacks on SCADA systems,'' in *Proc. 3rd Int. Conf. Commun. Inf. Technol. (ICCIT)*, Jun. 2013, pp. 22–27.

[53] C. Valasek and C. Miller, ''Adventures in automotive networks and control units,'' IOActive, Seattle, WA, USA, Tech. Rep., 2014.

[54] T. Macaulay, B. Singer, *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*. Boca Raton, FL, USA: CRC Press, 2012.

[55] J. Slowik, *Evolution of ICS Attacks and the Prospects for Future Disruptive Events*. Hanover, MD, USA: Dragos Inc., 2019.

[56] F. Khorrami, P. Krishnamurthy, and R. Karri, ''Cybersecurity for control systems: A process-aware perspective,'' *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 33, no. 5, pp. 75–83, Oct. 2016.

[57] G. Stergiopoulos, M. Theocharidou, and D. Gritzalis, ''Using logical error detection in software controlling remote-terminal units to predict critical information infrastructures failures,'' in *Human Aspects of Information Security, Privacy, and Trust*. 2015, pp. 672–683.

[58] P. H. N. Rajput, P. Rajput, M. Sazos, and M. Maniatakos, ''Process-aware cyberattacks for thermal desalination plants,'' in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Jul. 2019, pp. 441–452.

[59] *Information Technology—Security Techniques—Information Security Risk Management*, Standard ISO/IEC 27005, 2011.

[60] *Security and Privacy Controls for Federal Information Systems and Organizations*, document NIST Special Publication 800-53 Rev. 4, U.S. Department of Commerce, NIST, 2013.

[61] Accenture. (2018). *Cyber Threatscape Report 2018*. Accessed: Feb. 10, 2020. [Online]. Available: https://www.accenture.com/_acnmedia/pdf-83/accenture-cyber-threatscape-report-2018.pdf

[62] ENISA. (Jan. 20, 2016). *Inventory of Risk Management/Risk Assessment Tools*. Accessed: Feb. 10, 2020. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools

[63] S. Egelman and E. Peer, ''Scaling the security wall: Developing a security behavior intentions scale (SeBIS),'' in *Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst. (CHI)*, 2015, pp. 2873–2882.

[64] P. Sinha, A. Boukhtouta, V. H. Belarde, and M. Debbabi, ''Insights from the analysis of the mariposa botnet,'' in *Proc. 5th Int. Conf. Risks Secur. Internet Syst. (CRiSIS)*, Oct. 2010, pp. 1–9.

[65] *Operation Copperfield*, Nyotron, Santa Clara, CA, USA, 2019.

[66] *Global Oil and Gas Cyber Threat Perspective*, Dragos Inc., Hanover, MD, USA, 2019.

[67] Stratasys. *3D Printing in Energy, Oil and Gas Industry: Stratasys Direct Manufacturing*. Accessed: Feb. 10, 2020. [Online]. Available: https://www.stratasysdirect.com/industries/energy/energy-oil-gas

[68] M. Burns and C. Wangenheim, ''Metal 3D printing applications in the oil & gas industry,'' in *Proc. SPE Middle East Oil Gas Show Conf.*, 2019.

[69] M. Yampolskiy, A. Skjellum, M. Kretzschmar, R. A. Overfelt, K. R. Sloan, and A. Yasinsac, ''Using 3D printers as weapons,'' *Int. J. Crit. Infrastruct. Protection*, vol. 14, pp. 58–71, Sep. 2016.

[70] C. Bozzato, R. Focardi, and F. Palmarini, ''Shaping the Glitch: Optimizing Voltage Fault Injection Attacks,'' *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2019, no. 2, pp. 199–224, 2019.

[71] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, and Y. Yarom, ''Meltdown: Reading kernel memory from user space,'' in *Proc. 27th USENIX Secur. Symp. (USENIX Secur.)*, 2018, pp. 973–990.

[72] K. Hemsley and R. Fisher, ''History of industrial control system cyber incidents,'' Idaho Nat. Lab., Idaho Falls, ID, USA, Tech. Rep. INL/CON-18-44411-Revision-2, 2018.

[73] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, ''The cousins of stuxnet: Duqu, flame, and gauss,'' *Future Internet*, vol. 4, no. 4, pp. 971–1003, Nov. 2012.

[74] X. Chen, Y. Zhou, H. Zhou, C. Wan, Q. Zhu, W. Li, and S. Hu, ''Analysis of production data manipulation attacks in petroleum cyber-physical systems,'' in *Proc. 35th Int. Conf. Comput.-Aided Design*, Nov. 2016, pp. 1–7.

[75] R. Thiyab, M. Ali, and F. Basil, ''The impact of SQL injection attacks on the security of databases,'' *Proc. 6th Int. Conf. Comput. Informat.*, vol. 80, 2017, pp. 323–331.

[76] R. Sloan and R. Warner, *Unauthorized Access: The Crisis in Online Privacy and Security*. Boca Raton, FL, USA: CRC Press, 2013.

[77] F. Hacquebord and C. Pernet, ''Drilling deep: A look at cyber-attacks on the oil and gas industry,'' Trend Micro, Tokyo, Japan, Tech. Rep., 2019.

[78] Z. Zorz. Oct. 2015. *WiFi Jamming Attacks More Simple and Cheaper Than Ever Help Net Security*. Accessed: Feb. 15, 2020. [Online]. Available: https://www.helpnetsecurity.com/2015/10/13/wifi-jamming-attacks-more-simple-and-cheaper-than-ever/

[79] Dragos INC. *Chrysene*. Accessed: Feb. 12, 2020. [Online]. Available: https://dragos.com/resource/chrysene/

[80] J. Robertson and M. Riley. (Dec. 2014). *Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar*. Bloomberg.com. Accessed: Mar. 15, 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

[81] D. Genkin, L. Pachmanov, I. Pipman, A. Shamir, and E. Tromer, ''Physical key extraction attacks on PCs,'' *Commun. ACM*, vol. 59, no. 6, pp. 70–79, May 2016.

[82] T. de Maizière, *Die Lage der IT-Sicherheit in Deutschland 2014*. London, U.K.: BSI, 2014.

[83] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, and C. Glyer. (Dec. 2017). Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure. FireEye. Accessed: Mar. 16, 2020. [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

[84] Symantec. (Dec. 2017). *Triton: Malware That Aims to Attack Industrial Safety Systems*. Accessed: Mar. 15, 2020. [Online]. Available: https://symantec-blogs.broadcom.com/blogs/threat-intelligence/triton-malware-ics

[85] R. Falcone and B. Lee. (Jul. 2017). TwoFace Webshell: Persistent Access Point for Lateral Movement. Palo Alto Networks: Unit42. Accessed: Mar. 18, 2020. [Online]. Available: https://unit42.paloaltonetworks.com/unit42-twoface-webshell-persistent-access-point-lateral-movement/

[86] K. O'Flaherty. (Oct. 2018). How the Russian Government Created the Most Advanced Industrial Malware Ever Seen. Forbes. Accessed: Mar. 18, 2020. [Online]. Available: https://www.forbes.com/sites/kateoflahertyuk/2018/10/23/how-the-russian-government-created-the-most-advanced-industrial-malware-ever-seen/

[87] Liviu Arsene. *Oil & Gas Spearphishing Campaigns Drop Agent Tesla Spyware in Advance of Historic OPEC+Deal, BitDefender*. Accessed: Apr. 18, 2020. [Online]. Available: https://labs.bitdefender.com/2020/04/oil-gas-spearphishing-campaigns-drop-agent-tesla-spyware-in-advance-of-historic-opec-deal/

[88] M. Hasbini and G. Saad. (Oct. 2017). *Gaza Cybergang—Updated Activity in 2017*. Securelist. Accessed: Mar. 21, 2020. [Online]. Available: https://securelist.com/gaza-cybergang-updated-2017-activity/82765/

[89] B. Sobczak. (Apr. 2018). SECURITY: Attack on Natural Gas Network Shows Rising Cyberthreat. E&E News. Accessed: Apr. 18, 2020. [Online]. Available: https://www.eenews.net/stories/1060078327

[90] K. Albano and L. Kessem. (Feb. 2017). The Full Shamoon: How the Devastating Malware was Inserted Into Networks. Security Intelligence. Accessed: Mar. 19, 2020. [Online]. Available: https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

[91] The Times of Israel. (May 2012). *Iran Admits That Flame Virus Hit its Oil Industry*. Accessed: Mar. 30, 2020. [Online]. Available: https://www.timesofisrael.com/iran-oil-industry-hit-by-flame/

[92] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, ''Taxonomy of wireless sensor network cyber security attacks in the oil and gas industries,'' in *Proc. 24th IEEE Int. Conf. Adv. Inf. Netw. Appl.*, 2010, pp. 949–957.

[93] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, ''Cyber–physical security of a smart grid infrastructure,'' *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[94] F. Lobo, ''Upstream oil & gas cyber risk: Insurance technical review,'' Lloyd's Market Assoc., London, U.K., 2018.

[95] J. Wagstaff. (Apr. 2014). All at Sea: Global Shipping Fleet Exposed to Hacking Threat. Reuters. Accessed: Mar. 19, 2020. [Online]. Available: https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140424

[96] Space Rogue. (Sep. 2016). *Tilting it Sideways*. Accessed: Apr. 1, 2020. [Online]. Available: https://www.spacerogue.net/wordpress/?p=625

[97] Department of Homeland Security: Cybersecurity and Infrastructure Security Agency. (Mar. 2020). *ICS Advisory (ICSA-19-351-02): Siemens SPPA-T3000 (Update A)*. Accessed: Apr. 5, 2020. [Online]. Available: https://www.us-cert.gov/ics/advisories/icsa-19-351-02

[98] D. Denyer and D. Tranfield, ''Producing a systematic review,'' in *The Sage Handbook of Organizational Research Methods*. Newbury Park, CA, USA: Sage, 2011, pp. 671–689.

[99] (Jul. 2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*. Accessed: Jan. 3, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[100] (Jul. 2019). *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013, (Cybersecurity Act)*. Accessed: Jan. 3, 2020. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[101] *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, United States Dept. Homeland Secur., Washington, DC, USA, 2013.

[102] (Jul. 2012). *Directive 2012/18/EU of the European Parliament (SEVEZO-III)*. Accessed: Jan. 3, 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0018

[103] *NIST SP 800-30 Rev 1 Guide for Conducting Risk Assessments*. Gaithersburg, MD, USA: United States Department of Commerce, NIST, 2012.

[104] *Deliverable D2.1: Common Areas of Risk Assessment Methodologies*, EURACOM, Stanmore, U.K.

[105] *DOE G 413.3-7A Chg 1 (Admin Chg), Risk Management Guide*, U.S. Secretary Energy, Washington, DC, USA, 2011.

[106] G. Giannopoulos, R. Filippini, and M. Schimmer, ''Risk assessment methodologies for critical infrastructure protection. Part I: A state of the art,'' Publications Office Eur. Union, Brussels, Belgium, Tech. Rep., 2012.

[107] *Protection of Critical Infrastructures—Baseline Protection Concept: Recommendation for Companies*, BSI, London, U.K., 2006.

[108] D. Henze, *IT Baseline Protection Manual: Standard Security Measures*. London, U.K.: BSI, 2000.

[109] A. Tajer, ''False data injection attacks in electricity markets by limited adversaries: Stochastic robustness,'' *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 128–138, Jan. 2019.

[110] J. Giraldo, A. Cardenas, and N. Quijano, ''Integrity attacks on real-time pricing in smart grids: Impact and countermeasures,'' *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2249–2257, Sep. 2017.

[111] *Information Technology—Security Techniques—Information Security Management Guidelines Based on ISO/IEC 27002 for Process Control Systems Specific to the Energy Utility Industry*, Standard ISO/IEC TR 27019, 2013.

[112] K. Wilhoit, "The SCADA that didn't cry WolfWho's really attacking your ICS equipment? (Part 2)," Trend Micro, Tokyo, Japan, Tech. Rep., 2013.

[113] G. Tognini. (Jun. 2017). Hacking on the Rise, as 75% of Energy Companies Hit Last Year: Report. Financial Post. Accessed: Mar. 20, 2020. [Online]. Available: https://business.financialpost.com/commodities/energy/hacking-on-the-rise-as-75-of-energy-companies-hit-last-year-report

[114] *Critical Infrastructure: Cyber-Attacks on the Backbone of Today's Economy*, Panda Secur., Bilbao, Spain, 2018.

[115] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *Comput. Secur.*, vol. 89, Feb. 2020, Art. no. 101677.

[116] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Des. Test. IEEE Des. Test. Comput.*, vol. 34, no. 4, pp. 7–17, Aug. 2017.

[117] S. Nazir, S. Patel, and D. Patel, "Assessing and augmenting SCADA cyber security: A survey of techniques," *Comput. Secur.*, vol. 70, pp. 436–454, Sep. 2017.

[118] B. Miller and D. Rowe, "A survey SCADA of and critical infrastructure incidents," in *Proc. 1st Annu. Conf. Res. Inf. Technol. (RIIT)*, 2012, pp. 51–56.

[119] *Information Technology—Security Techniques—Security Assessment of Operational Systems*, Standard ISO/IEC TR 19791, 2010.

[120] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[121] K.-D. Kim and P. R. Kumar, "Cyber–physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, no. 100, pp. 1287–1308, May 2012.

[122] M. Krotofil and D. Gollmann, "Industrial control systems security: What is happening?" in *Proc. 11th IEEE Int. Conf. Ind. Informat. (INDIN)*, Jul. 2013, pp. 670–675.

[123] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2015, pp. 1–6.

[124] (2017). *Ernest and Young, Digitization and cyber Disruption in Oil and Gas*. [Online]. Available: https://www.ey.com/Publication/vwLUAssets/ey-wpc-digitization-and-cyber/$FILE/ey-wpc-digitization-and-cyber.pdf

[125] (2020). *Fortinet, Independent Study Finds That Security Risks are Slowing IT-OT Convergence*. [Online]. Available: https://www.fortinet.com/lat/solutions/industries/oil-gas.html

[126] (2017). *Deloitte, Protecting the Connected Barrels Cybersecurity for Upstream oil and Gas*. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/energy-resources/gx-er-protecting-connected-barrels.pdf

[127] 2016. *PWC, Turnaround and Transformation in Cybersecurity: Oil and Gas Key Findings From the Global State of Information Security Survey 2016*. [Online]. Available: https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2016-oil%20and%20gas.pdf

[128] (2018). *Enable Secure Real-Time Oil and Gas Pipeline Operations Through Digital Solutions, CISCO and Affiliates*. [Online]. Available: https://download.schneider-electric.com/files?p_enDocType=Brochure&p_File_Name=Cisco+Schneider+Aveva+Smart+Connected+Pipeline+SO_R2-10272018AR0_EN.pdf&p_Doc_Ref=SO_R2-10272018AR0_EN

[129] S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Syst. Mag.*, vol. 21, no. 6, pp. 11–25, Dec. 2001.

[130] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," *Rel. Eng. Syst. Saf.*, vol. 121, pp. 43–60, Jan. 2014.

[131] P. Kotzanikolaou, M. Theoharidou, and D. Gritzalis, "Interdependencies between critical infrastructures: Analyzing the risk of cascading effects," in *Proc. Int. Workshop Crit. Inf. Infrastruct. Secur.* Berlin, Germany: Springer, Sep. 2011, pp. 104–115.

[132] B. Bush, L. Dauelsberg, R. LeClaire, D. Powell, S. DeLand, M. Samsa, *Critical Infrastructure Protection Decision Support System Project Overview*. Boston, MA, USA, 2005.

[133] C. L. Chai, X. Liu, W. J. Zhang, and Z. Baber, "Application of social network theory to prioritizing oil & gas industries protection in a networked critical infrastructure system," *J. Loss Prevention Process Industries*, vol. 24, no. 5, pp. 688–694, 2011.

[134] W. Z. Khan, M. Y. Aalsalem, M. K. Khan, M. S. Hossain, and M. Atiquzzaman, "A reliable Internet of Things based architecture for oil and gas industry," in *Proc. 19th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2017, pp. 705–710.

[135] Forbes. (2019). *Refining the Oil and Gas Industry With IoT*. [Online]. Available: https://www.forbes.com/sites/cognitiveworld/2019/09/17/refining-the-oil-and-gas-industry-with-iot/#4254af8579f9

GEORGE STERGIOPOULOS received the B.Sc. degree in informatics from the University of Piraeus, Greece, and the M.Sc. degree in information systems and the Ph.D. degree in critical infrastructure protection at software and information interdependency levels from the Athens University of Economics and Business, Greece. He is currently an Adjunct Lecturer and a Postdoctoral Researcher with the Department of Informatics, Athens University of Economics and Business (AUEB). He has published over 30 articles in peer-reviewed journals and international conferences. He was a Principal Investigator in multiple funded research projects in the areas of critical infrastructure protection, computer security, and network security. He is an Expert in ISO 27001 and EU General Data Protection Regulation consulting.

DIMITRIS A. GRITZALIS received the B.Sc. degree in mathematics from the University of Patras, the M.Sc. degree in computer science from the City University of New York, USA, and the Ph.D. degree in information systems security from the University of the Aegean. He is currently a Professor of cybersecurity with the Department of Informatics, Athens University of Economics and Business (AUEB), Greece. He also serves as the Director of the M.Sc. Programme in Information Systems Development and Security, and the Director of the INFOSEC Research Group. He has chaired several international conferences (ACM, IEEE, and IFIP). He has served as an Associate Rector for Research and the Financial Planning and Development and the President of the Life-long Education Center of AUEB. He has also served as the President of the Greek Computer Society and as an Associate Data Protection Commissioner of Greece. For more than 30 years, he has provided consulting services and has published extensively (more than 200 articles) in peer-reviewed journals and conferences. His current research interests include risk assessment, critical infrastructure protection (ICT, energy, and transportation), malware, smart-phone security, and data protection. He serves as an Academic Editor for *Computers & Security* (Elsevier) and as a Scientific Editor for the *International Journal of Critical Infrastructure Protection* (Elsevier).

EVANGELOS LIMNAIOS received the Dipl.Eng. degree in chemical engineering from the University of Patras, and an Executive M.B.A. degree from the Athens University of Economics and Business. He is currently the Associate IT Head of Public Gas Corporation (DEPA) SA, Greece. He also serves as the NISD Network and Information Systems Security Officer of the company. In his long-lasting professional career, he has held decision-making positions in private organizations, such as the Head of the IT & Document Control Center of construction project management teams working for natural gas transmission and distribution networks. His current interests include inter alia, oil & gas infrastructure protection, security management, and risk assessment.