



Defending Oil & Gas Critical Infrastructures from Cyber-attacks

Dimitris Gritzalis & George Stergiopoulos

15th International Conference on Critical
Information Infrastructure Security (CRITIS-2020)
Bristol (UK), September 2020

Invited talk

Defending Oil & Gas Critical Infrastructures from Cyber-attacks

Dr. George Stergiopoulos & Prof. Dimitris Gritzalis

INFOSEC Laboratory

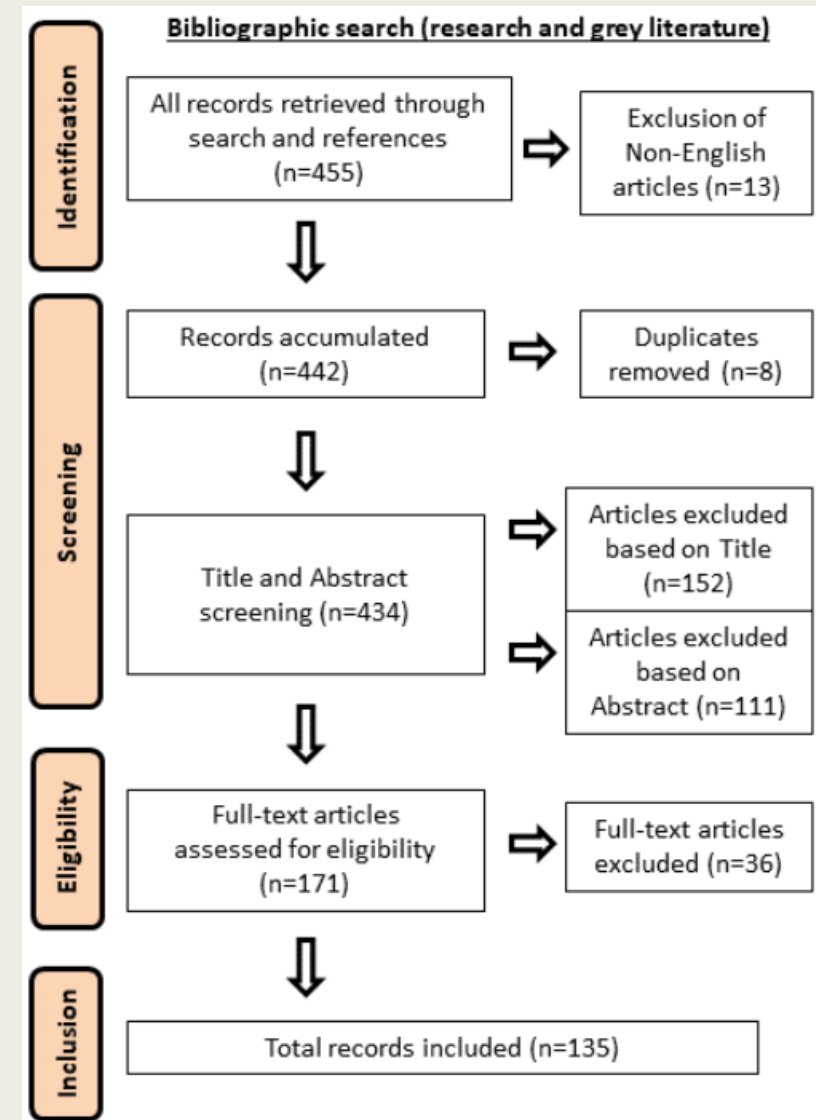
Athens University of Economics & Business (GR)

OUTLINE

- Survey method
 - *MITRE ATT&CK*
 - *MITRE CAPEC*
- Typical O&G architectures
- Taxonomy of potential attacks
- Impact assessment of recorded cyberattacks
- Analysis of recorded cyberattacks
- Mitigation and Security Controls
- Conclusions

SURVEY METHOD

- Four steps:
 - *Survey protocol and scope development,*
 - *Search and identification of selected studies based on scope,*
 - *Screening of literature based on quality,*
 - *Reporting (extraction of information, synthesis and reporting of findings).*
- Detected documents (455 files) both from academia and grey literature (reports, white papers, company publications etc.).



MITRE ATT&CK

- Knowledge base of adversary tactics and techniques based on real-world observations.
 - *Specific 3-Level section for adversary actions while operating within an ICS network.*
- Used for the development of threat models and methodologies.
- Encodes 81 types of techniques for 11 attack tactics, from initial exploitation and execution to lateral movements and potential impact.

Loss of Availability	Impact	Adversaries may attempt to disrupt essential components or systems to prevent owner and operator from delivering products or services. ^{[6][7][8]} Adversaries may leverage malware to delete or encrypt critical data on HMIs, workstations, or databases.
Loss of Control	Impact	Adversaries may seek to achieve a sustained loss of control or a runaway condition in which operators cannot issue any commands even if the malicious interference has subsided. ^{[6][7][8]}

MITRE CAPEC

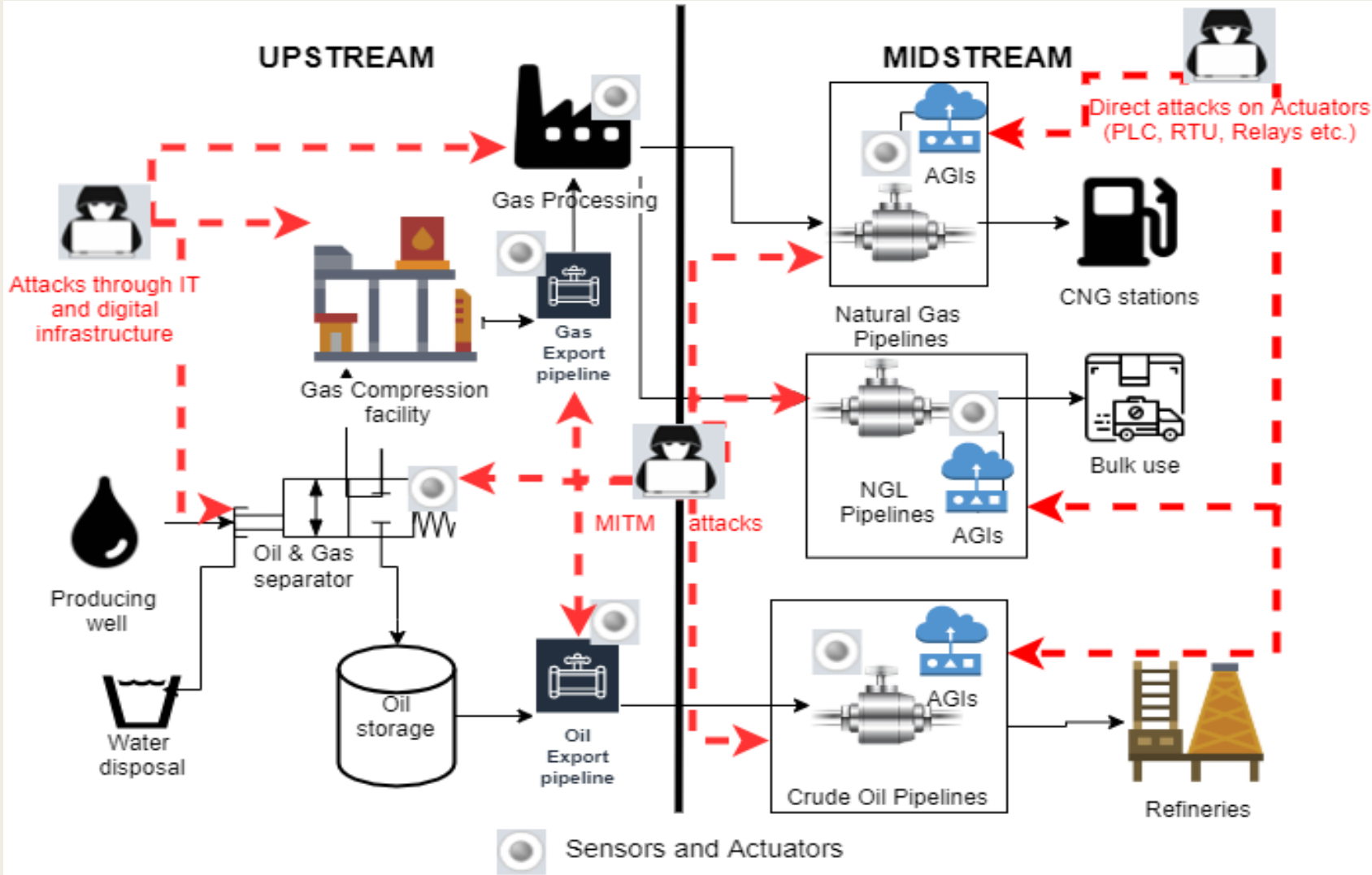
- Common attack pattern enumeration & classification
- Dictionary of known attack patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities.

Nature	Type	ID	Name
MemberOf	V	3000	<u>Domains of Attack</u>
HasMember	M	22	<u>Exploiting Trust in Client</u>
HasMember	M	94	<u>Man in the Middle Attack</u>
HasMember	M	117	<u>Interception</u>
HasMember	M	125	<u>Flooding</u>
HasMember	M	130	<u>Excessive Allocation</u>
HasMember	M	148	<u>Content Spoofing</u>
HasMember	M	151	<u>Identity Spoofing</u>

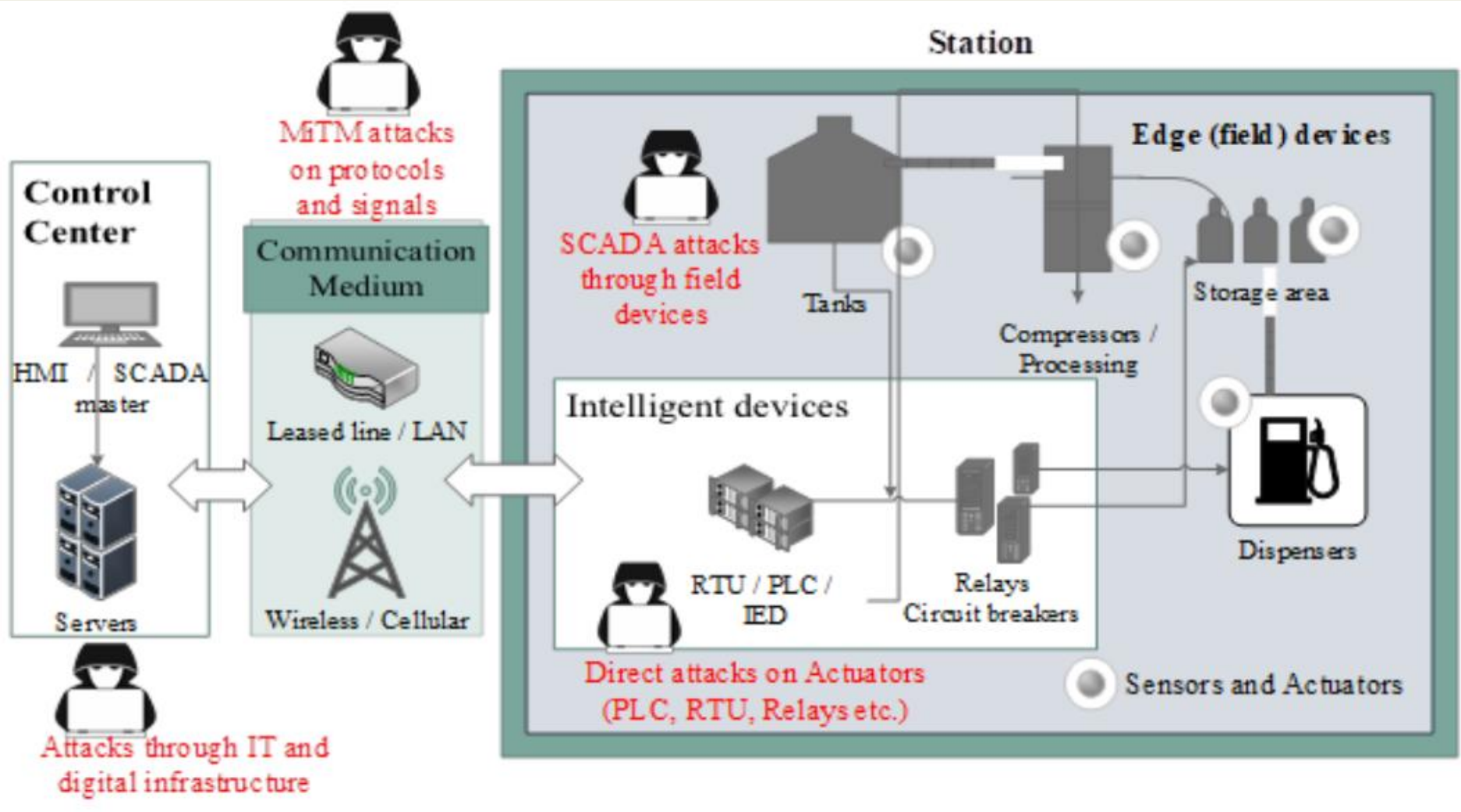
TYPICAL O&G ARCHITECTURES

- Downstream, midstream and upstream follow the same general ICS architecture, even though complexity and assets differentiate.
- Upstream and midstream infrastructures deploy SCADA systems for similar monitoring purposes.
 - *Upstream mostly focuses on well extraction, separation of oil and gas and exporting to pipes.*
 - *Processes differ and safety checks vary but 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.*

TYPICAL O&G ARCHITECTURES



TYPICAL O&G ARCHITECTURES



MITRE ATT&CK MAPPING

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

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

TAXONOMY OF POTENTIAL ATTACKS

- CAPEC and ATT&CK used complementarily
 - *CAPEC's attack patterns used by techniques described in ATT&CK.*
- Mapped most popular attacks and attack types with ATT&CK's adversary tactics and techniques
- Novel taxonomy helps identify most vulnerable assets per type of attack.

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].

CYBERATTACK IMPACT ASSESSMENT

- Generic impact assessment method to supplement security incident classifications.
- Utilizes typical risk assessment concepts and notions, as defined in numerous standards and reports, e.g. ISO 27005:2005 and NIST 800-53.
- Mostly interested in extent of damage caused, not on vulnerability that triggered a security event or the underlying threat that caused the attack.
- Not a full risk assessment of the recorded attacks.
- Proposed qualitative levels described by four (4) dimensions
 - *Represent different types of impact: (i) Economical, (ii) Societal, (iii) Environmental, and (iv) Operational.*
 - *The three values quantify these dimensions, based on standards and Directives like NIST, ISO and SEVESO-III.*

IMPACT ASSESSMENT OF RECORDED CYBERATTACKS

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

IMPACT TYPE	LOW	MEDIUM	HIGH
Economical	<ul style="list-style-type: none"> • Minimum or no asset cost for company (e.g. loss of time, need to repeat process) • No cost for society 	<ul style="list-style-type: none"> • Limited asset cost to company (e.g. hundreds of thousands of euro). • Minimum cost to society (e.g. limited, short-term increase to prices) 	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • No injuries • Minimum number or no citizens affected (e.g. <30 people) 	<ul style="list-style-type: none"> • Limited num of injuries only to personnel. • Limited number or no citizens affected (e.g. less than 50 houses) 	<ul style="list-style-type: none"> • Extended num of injuries in personnel. • Injuries to citizens. • Loss of life.
Environmental	<ul style="list-style-type: none"> • No treatment needed for clean up or contamination 	<ul style="list-style-type: none"> • Treatment or clean up needed in limited areas in and around the facility 	<ul style="list-style-type: none"> • Wide area subject to clean up or decontamination treatment
Operational	<ul style="list-style-type: none"> • Minimal downtime of services or resumed in very short time (e.g. <4h). 	<ul style="list-style-type: none"> • Limited downtime of services or resumed in very short time (e.g. less than 48h). 	<ul style="list-style-type: none"> • Extended downtime of services (>48h).

IMPACT ASSESSMENT RESULTS

- Upstream often erroneously considered to be less targeted than downstream.
 - *True in the past, due to remote and disconnected nature.*
 - *Modern upstream not safe.*

- E.g. attack allegedly shut down an oil rig off the coast of Africa by tilting it 17 degrees.
 - *Attributed to manipulation of ballast control through PLC-actuator command-and-control.*

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%)

IMPACT ASSESSMENT OF RECORDED CYBERATTACKS

- Only seven (7) documented ICS security events exist against midstream pipeline networks. AGI's primarily targeted.
 - *Baku-Tbilisi attack caused temporary disruption in pipeline transfers using over-pressurization, allegedly through the camera network.*
 - *Some unintended events from unprocessed commands caused an endless loop to trigger and disrupt controls in all flow operators*
- Downstream presumed to be the most common target.
 - *SHAMOON targeted national oil companies including Saudi Arabia's Saudi Aramco and Qatar's RasGas through spear phishing.*
 - *HEXANE attacks target O&G telecommunications in Africa, Middle East, and Southwest Asia (2018)*
 - *Night Dragon attack caused data theft and affected downstream infrastructures of oil, energy and petrochemical companies around the globe.*

MITIGATION AND SECURITY CONTROLS

- Patterns exist common to all ICS
 - *Some attack types are far more common than others.*
 - *Security controls able to mitigate risk in common patterns.*
- Top issues along with relevant mitigation controls are:
 1. *Numerous attacks by insiders with partial access to systems.*
 - Need for extended segregation of duties and minimum privileges measures to employees.
 - Strong authentication and access control procedures with help minimize the damage from such threats.
 2. *Spear phishing attacks one of the top techniques used.*
 - Employee training and awareness along with strong security procedures and internal audits.
 3. *Use of legacy equipment and the lack of proper patching procedures a top cybersecurity issue.*

MITIGATION AND SECURITY CONTROLS

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.

CONCLUSIONS

- Clear indication that current attacks in oil and gas systems follow similar attack trends for common ICT systems.
- Most common attack vectors include:
 - *spear phishing through email*
 - *external attack (malware or injection) to exposed devices*
 - *user execution, either intentionally (malicious insiders) or erroneously*
- Tables referred to herein are partial depiction of an analysis of attacks presented in: Stergiopoulos, G., Gritzalis, D. Limnaios, E., “Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns”, *IEEE Access*, 8, 1284-475, 2020.

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	<ul style="list-style-type: none"> • Denial of Service (T814) • Loss of Availability (T826) • Damage to Property (T879) 	<p>Infection reached such extent that it took IT staff 19 days to make resume operations.</p> <p>Impact rank: High</p> <p>Cascading effects: Internal</p>
User Execution (T863)	<p>Internal – injection attack</p> <p>Internal - Jamming</p>	<p>Upstream</p> <p>Midstream</p> <p>Downstream</p>	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	<ul style="list-style-type: none"> • Change Program State (T875) • Damage to Property (T879) • Modify Control Logic (T833) 	<p>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</p> <p>Impact rank: High</p> <p>Cascading effects: Yes</p>

<p>Internet Accessible Device (T883)</p>	<p>External – Malware attack</p>	<p>Upstream Midstream Downstream</p>	<p>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].</p>	<p>C-C C-P</p>	<ul style="list-style-type: none"> • Modify Control Logic (T833) 	<p>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</p>
<p>User Execution (T863)</p>	<p>Internal – Injection attack (unintended)</p>	<p>Midstream Downstream</p>	<p>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].</p>	<p>C-P</p>	<ul style="list-style-type: none"> • Change Program State (T875) • Denial of Service (T814) • Loss of Control (T827) 	<p>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</p>

<p>Internet Accessible Device (T883)</p> <p>Replication Through Removable Media Technique (T847)</p>	<p>External – Malware attack</p> <p>Internal – USB attack</p>	<p>Downstream</p>	<p>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.</p>	<p>C-C</p>	<ul style="list-style-type: none"> • Theft of Operational Information (T882) 	<p>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].</p> <p>Impact rank: Low</p> <p>Cascading effects: No</p>
<p>Spear phishing Attachment (T865)</p>	<p>External – Phishing attack</p> <p>External – Malware attack</p>	<p>Upstream</p>	<p>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].</p>	<p>C-C</p>	<ul style="list-style-type: none"> • Theft of Operational Information (T882) 	<p>Attack compromised email accounts of employees and stole information and credentials.</p> <p>Impact rank: Low</p> <p>Cascading effects: No</p>

References

- Faily S., Stergiopoulos G., Katos V., Gritzalis D., "Water, water, everywhere: Nuances for a Water Industry Critical Infrastructure specification exemplar", in *Proc. of the 10th International Conference on Critical Infrastructures Security (CRITIS-2015)*, pp. 243-246, Springer (LNCS 9578), Germany, October 2015.
- Gritzalis D., Theocharidou M., Stergiopoulos G. (Eds.), *Critical Infrastructure Security and Resilience - Theories, Methods, Tools & Technologies*, Advanced Sciences & Technologies for Security Applications Series, Springer, 2019.
- Kotzanikolaou P., Theocharidou M., Gritzalis D., "Assessing n-order dependencies between critical infrastructures", *International Journal of Critical Infrastructure Protection*, Vol. 9, Nos. 1-2, pp. 93-110, 2013.
- Lykou G., Moustakas D., Gritzalis D., "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensors technologies", *Sensors*, Vol. 20, No. 3537, June 2020.
- Lykou G., Anagnostopoulou A., Gritzalis D., "Smart Airports Cybersecurity: Threat Mitigation and Cyber Resilience", *Sensors*, Vol. 19, No. 19, pp. 1-27, January 2019.
- Stergiopoulos G., Valvis E., Mitrodimas D., Lekkas D., Gritzalis D., "Analyzing congestion interdependencies of ports and container ship routes in the maritime network infrastructure", *IEEE Access*, Vol. 6, pp. 63823-832, December 2018.
- Stergiopoulos G., Kouktzoglou V., Theocharidou M., Gritzalis D., "A process-based dependency risk analysis methodology for critical infrastructures", *International Journal of Critical Infrastructures*, Vol. 13, Nos. 2/3, pp. 184-205, 2017.
- Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D., "Time-base critical infrastructure dependency analysis for large-scale and cross-sectoral failures", *International Journal of Critical Infrastructure Protection*, Vol. 12, pp. 46-60, March 2016.
- Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Gritzalis D., "Risk mitigation strategies for Critical Infrastructures based on graph centrality analysis", *International Journal of Critical Infrastructure Protection*, Vol. 10, pp. 34-44, September 2015.
- Stergiopoulos G., Vasilellis S., Lykou G., Kotzanikolaou P., Gritzalis D., "Critical Infrastructure Protection tools: Classification and comparison", in *Proc. of the 10th International Conference on Critical Infrastructure Protection (CIP-2016)*, USA, March 2016.
- Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Gritzalis D., "Using centrality metrics in CI dependency risk graphs for efficient risk mitigation", in *Proc. of the 9th IFIP International Conference on Critical Infrastructure Protection (CIP-2015)*, Springer, USA, March 2015.
- Stergiopoulos G., Gritzalis D., Limnaios E., "Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns", *IEEE Access*, Vol. 8, pp. 128440-475, 2020.
- Theocharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent Critical Infrastructures", *International Journal of Risk Assessment and Management (Special Issue on Risk Analysis of Critical Infrastructures)*, Vol. 15, Nos. 2/3, pp. 128-148, 2011.
- Theocharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in *Proc. of the 7th IEEE International Conference in Global Security, Safety & Sustainability (ICGS3-2011)*, pp. 171-178, Springer (LNICST 99), Greece, 2012.