



Kaspersky Industrial
Cybersecurity
Conference

Taxonomy of Cyberattacks in the Liquefied Petroleum Gas (LPG) Industry

kaspersky



Sulaiman Alhasawi, PhD



@alhasawi

About me



- Sulaiman Alhasawi
- Kuwait
- Independent Researcher IT/OT cyber security
- ZeronTek company: Founder
- My projects:
<https://github.com/selmux>

ICSrank

PhD thesis [1]
 Taxonomy of LPG attacks
 Risk scoring framework for ICS
 John Moores University - UK

ICSrank: A Security Assessment Framework for Industrial Control Systems (ICS)

Tools

Alhasawi, S (2020) ICSrank: A Security Assessment Framework for Industrial Control Systems (ICS).
 Doctoral thesis, Liverpool John Moores University.



Text
 2020AlhasawiPhD.pdf - Published Version
[Download \(3MB\)](#) | [Preview](#)

Abstract

This thesis joins a lively dialogue in the technological arena on the issue of cybersecurity and specifically, the issue of infrastructure cybersecurity as related to Industrial Control Systems. Infrastructure cybersecurity is concerned with issues on the security of the critical infrastructure that have significant value to the physical infrastructure of a country, and infrastructure that is heavily reliant on IT and the security of such technology. It is an undeniable fact that key infrastructure such as the electricity grid, gas, air and rail transport control, and even water and sewerage services rely heavily on technology. Threats to such infrastructure have never been as serious as they are today. The most sensitive of them is the reliance on infrastructure that requires cybersecurity in the energy sector. The call to smart technology and automation is happening nowadays. The Internet is witnessing an increase number of connected industrial control system (ICS). Many of which don't follow security guidelines. Privacy and sensitive data are also an issue. Sensitive leaked information is being manipulated by adversaries to accomplish certain agendas. Open Source intelligence (OSINT) is adopted by defenders to improve protection and safeguard data. This research presented in thesis, proposes "ICSrank" a novel security risk assessment for ICS devices based on OSINT. ICSrank ranks the risk level of online and offline ICS devices. This framework categorizes, assesses and ranks OSINT data using ICSrank framework. ICSrank provides an additional layer of defence and mitigation in ICS security, by identification of risky OSINT and devices. Security best practices always begin with identification of risk as a first step prior to security implementation. Risk is evaluated using mathematical algorithms to assess the OSINT data. The subsequent results achieved during the assessment and ranking process were informative and realistic. ICSrank framework proved that security and risk levels were more accurate and informative than traditional existing methods.



<http://researchonline.ljmu.ac.uk/id/eprint/13480/>

Key topics

- LPG cylinder
- Safety PLC
- Cyber Incidents
- ICS Kill Chain
- Search Engines
- CVEs
- Hacking tools
- Taxonomy of LPG attacks
- Mitre ATT&CK for ICS
- Threat model
- Top 20 secure PLC
- Mitigations
- Summary

Energy Cybersecurity

5



Large attack surface

[transmission, distribution networks, supply chain , and network data theft and ransom]

Political Motivation

[Rise of Ransomware]

Digital and smart technology

[Benefit and Risk]

Source : [15]

LPG VS LNG ^[6]

LPG

_____ **Liquefied petroleum gas = Propane**

_____ **Heavier than air**

_____ **Stored and distributed as a liquid under pressure in gas bottles, cylinders or tanks**

_____ **Portable , high energy , less expensive**

• LNG

_____ **Liquefied Natural Gas = Methane**

_____ **Lighter than air**

_____ **Stored and distributed in pipes or gas mains**

_____ **Easy delivery , less CO₂**

LPG and Cylinder Specs

7



CYLINDER PROPERTIES:

- Mass of empty cylinder (m_1) = 16 kg
- Mass of gas (m_2) = 12 kg
- Total mass ($m = m_1 + m_2$) = 28 kg
- The volume of the cylinder = 21 m^3
- Filling time for cylinder = 75 seconds

GAS PROPERTIES:

- Flowrate (Q_{in}) = 45 m^3/hr
- Density of the gas (ρ) = 0.564 kg/m^3
- Molecular weight (M.W) = 22.695 $kg/kmol$
- Filling temperature (T) = 273 K



<https://github.com/selmux/ICS-Security/tree/main/Gas%20Model>

Top LPG companies [7]

8



BP Plc



Exxon Mobil
Corporation



Chevron
Corporation



China
Petroleum &
Chemical
Corporation



Bharat
Petroleum
Corporation Limited

Safety PLC



_____A safety programmable logic controller (PLC) is like a standard PLC.

_____ It can be used to control and automate pieces of industrial equipment.

_____A safety PLC supports all the applications that a standard PLC does; however, a safety PLC contains integrated safety functions that allow it to control safety systems as well



source :

<https://huffmaneng.com/what-are-safety-plcs>

LPG Cylinder filling and Safety PLC



_____Safety PLC is used for safety functions [safe torque off , safe stop , safe brake control] [16]

_____Safety PLC monitors pressure, temperature, LPG cylinder and LPG tank integrity

_____Safety PLC reads safety inputs

_____Safety PLC also monitors other parameters : gas flow , time, air pressure, gas mass, air supply, sequence values and order of operation

PLC attack objectives [12]

11



_____ Gain remote access and control

_____ Change controller behaviour

_____ Denial of services

_____ Maintain persistence

Famous Incidents ^[2]

12

Victim	Industry	Country	Year	Attack type	Impact
RasGas	LNG gas producer	Qatar	2012	Shamoon	Shutdown of office computers /website/email servers
Unknown	Natural gas compression facility	USA	2020	Spearfishing / Ransomware	Loss of availability/productivity/revenue
Superior Plus Corp	Gas supplier	Toronto, Canada	2021	ransomware	Shut down some of its operations ^[8]
Bolpegas	Oil/Gas engineering services	Bolivia	2021	ransomware	
Encevo Group (Parent)/ Creos Luxembourg ^[3]	Energy supplier	Luxembourg	2022	ransomware	Data theft

Why only ransomware ?



13

_____ **Don't underestimate it !**

_____ **The issues of ransomware
According to Mitre ATT&CK for ICS**

_____ **Ransomware is used for
initial access/lateral movement
e.g. Exploitation of remote
services (T0866)**

_____ **Loss of availability : T0826.
e.g. Colonial pipeline**

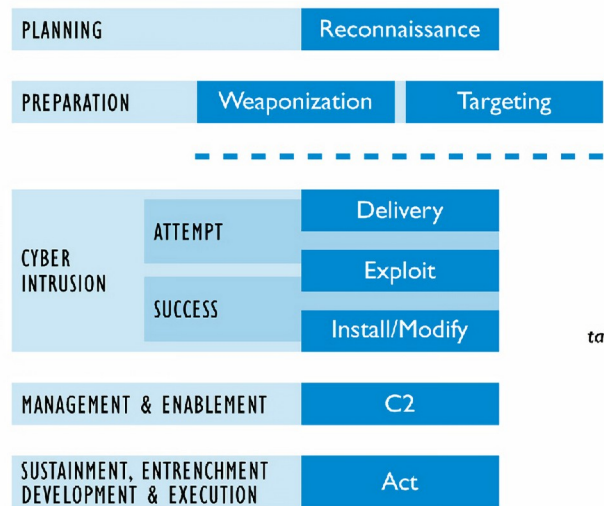
_____ **Loss of Productivity and
Revenue (T0828) e.g. Australian
beverage company , Colonial
Pipeline**

ICS Kill chain [14]

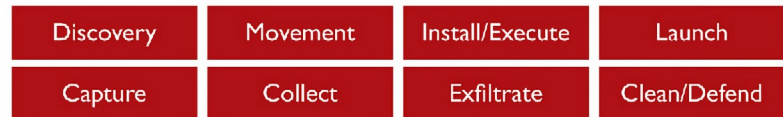
14

Stage 1

Cyber Intrusion Preparation and Execution

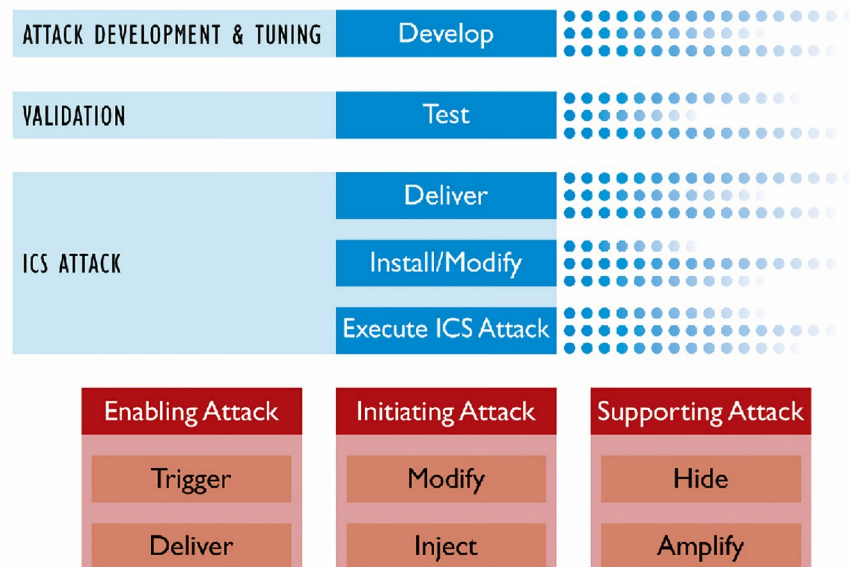


Stage 1 mimics a targeted and structured attack campaign.



Stage 2







ICS Attack Development and Execution



Search Engines

_____OMRON NX1P2 PLC IS
AVAILABLE ON SHODAN , “NX1P2”
ON PORT 44818 TCP/UDP !

_____PORT: 9600 RESPONSE
CODE

	Omron NX1P2 PLC	Compact Machine Controller Built in EtherCAT to simplify the wiring of up to eight servo systems including for single-axis position control.	 BADOMEN
	Omron NX-SL3300	Safety Controller SIL-3 rated safety controller. Integrated safety over EtherCAT.	 BADOMEN
	Omron NJ501-1300 PLC	Machine Automation Controller Native OPC-UA, EtherCAT, Ethernet/IP.	 BADOMEN

[4]

CVEs for Omron PLC NJ/NX ^[10,11]

16

9.8

_____ **CVE-2019-18261**

No Restriction of Authentication Attempts

7.5

_____ **CVE-2022-31205**

Credentials not safe

9.8

_____ **CVE-2022-31207**

Cryptographic Signature issue

7.5

_____ **CVE-2022-31204**

Clear Text information

9.8

_____ **CVE-2022-31206**

Cryptographic Signature issue

Hacking Tools

17



- _____ **Shodan**
- _____ **Censys**
- _____ **Google hacking dorks**
- _____ **Rapture : PLC-Blaster**
- _____ **Nmap (ICS Scripts)**
- _____ **Metasploit**

APT Tool for OMRON [13]

The APT actors' tool for OMRON devices has modules that can interact by:

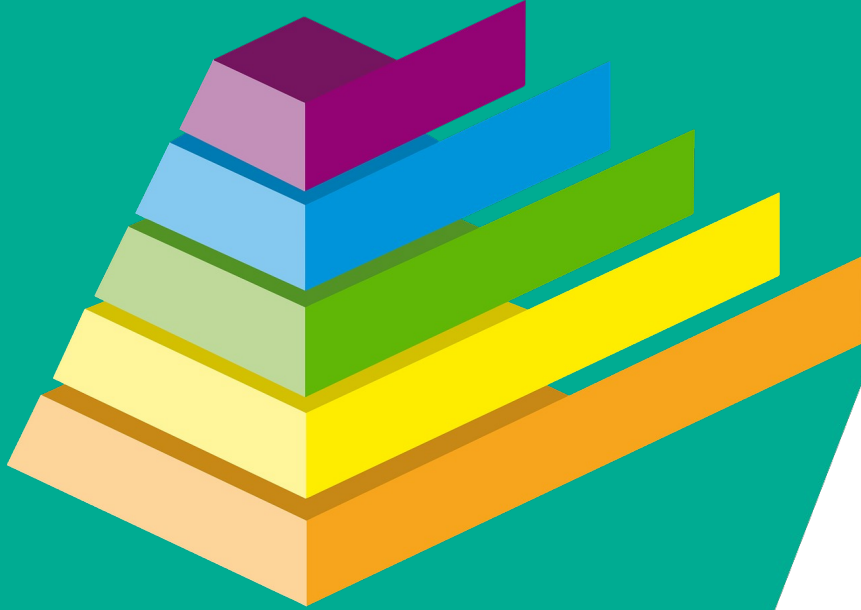
- Scanning for OMRON using Factory Interface Network Service (FINS) protocol;
- Parsing the Hypertext Transfer Protocol (HTTP) response from OMRON devices;
- Retrieving the media access control (MAC) address of the device;
- Polling for specific devices connected to the PLC;
- Backing up/restoring arbitrary files to/from the PLC; and
- Loading a custom malicious agent on OMRON PLCs for additional attacker-directed capability.

Entry point

ACCESS GRANTED

- Internet Accessible Device (T0883) e.g. Bowman dam
- Spear phishing Attachment (T0865)
- Remote Services (T0886) e.g. Oldsmar attack
- Exploit Public-Facing Application (T0819)

Why develop a taxonomy?



_____ Fill the gap between IT and OT departments. IT people can learn about the ICS process and about ICS assets.

_____ Develop technologies that use this kind of information. Many IT security technologies do not support or understand internal ICS network packets.

_____ Ability to perform a risk assessment of ICS system/network and to analyze potential risk/impact.

_____ Understanding ICS system/network operations and security could help prioritize patching and other security procedures.

_____ Development of Threat models of possible scenarios to attack an ICS in the gas industry.

Taxonomy of LPG attacks ^[1]

Action	Action Specific	Physical Property	Action symbol	Impact
Modify Flow	Increase	Flow (Q)	MQ1	Gas cylinder overfill, rupture
	Decrease		MQ2	Gas cylinder half fill
Modify Time	Increase	Time (T)	MT1	Gas cylinder overfill, rupture
	Decrease		MT2	Gas cylinder half fill
Modify Air pressure	Increase	Air Pressure (AP)	MAP1	Destroy air-based devices from high pressure
	Decrease		MAP2	Air-based devices don't operate, due to low pressure
Modify Gas mass	Increase	Gas Mass (GM)	MGM1	Gas cylinder overfill, rupture
	Decrease		MGM2	Gas cylinder half fill
Modify Air supply	Close	Air Pressure (AP)	MAP3	No airflow, operations stop
Modify Sequence Values	Modify	Process Control (PC)	PC1	Affect the entire process. e.g. If the order of operation is affected, the entire filling process fails
Modify Gas tank Level	Increase	Gas Tank Level (GTL)	MGTL1	Overfilled Tanks

Modeling LPG attacks ^[1]

Random variations

This is random changes in a system state. If an attacker happens to make sudden changes in the filling time for instance, to increase the filling time at 1 instance and then suddenly decrease at every filling cycle. A random variable is an easier form of attack and chances of detecting them are easier.

21

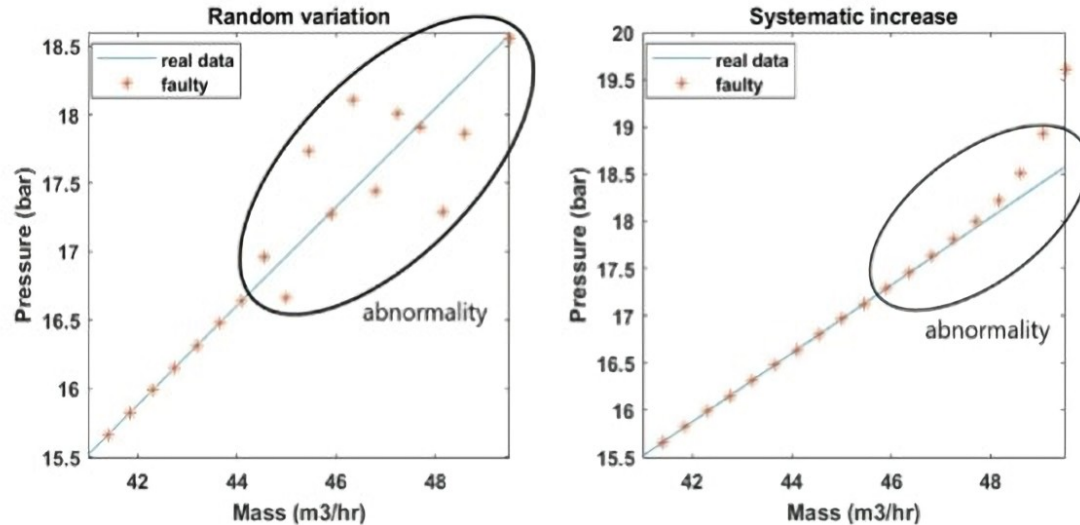
Systematic increase

A systematic increase is when the filling cycle time is changed in a single direction over a larger period of time. This sort of attack is difficult to detect.

Since the gradual increase would often go undetected until the physical effect can be noticed.

Attack 1: CHANGING INFLOW [1]

22

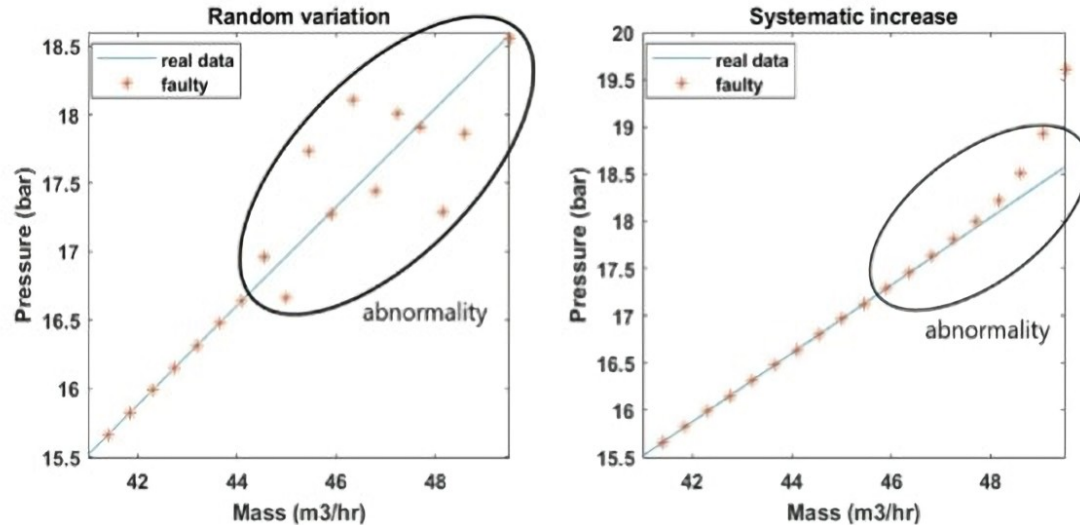


—— Pressure changes/abnormality

Can help us detect attack

Attack 2: CHANGING FILLING TIME [1]

23



Increasing pressure leads to rapture

We observe that time and flow variables share similar pattern ,
as explained in the taxonomy

Mitre ATT&CK for ICS

Why map taxonomy of LPG
attacks to Mitre techniques ?

[9]

- _____ **Apply taxonomy to a common vocabulary for ICS industry**
- _____ **Find related tactics/techniques / tools and adversary groups that apply them**
- _____ **Map defensive controls**
- _____ **Threat Hunting**
- _____ **Process variable anomaly detection**
- _____ **Red team / Penetration testing**
- _____ **Not just depend on CVEs (IT mentality)**

Program m Mode

_____Execution, Evasion

_____Change Operating Mode
(T0858)

_____Example: Triton

Modification Attacks



Tactic: Impair Process Control

Modify Parameter (T0836)

Example: Stuxnet , Maroochy , Oldsmar water treatment

- _____1- Gas flow
- _____2- Time
- _____3- Air pressure
- _____4- Gas mass
- _____5- Air supply
- _____6- Sequence values and order of operation
- _____7- Gas tank level

Impact



27

Disable safety and protection

Target:

PLC
Air Pressure (AP)
Process Control (PC)

Loss of Safety (T0880)

Example: Triton

Loss of Protection (T0837)

Example: Industroyer

Rapture [Flow (Q) ,Time (T), Gas Mass (GM)]

Target : Gas Cylinder

Damage to Property (T0879)

Example: Stuxnet , Maroochy Attack , German steel mill , Lodz city tram system in Poland

Loss of Protection (T0837)

Example: Industroyer

Manipulation of Control (T0831)

Example: Industroyer , Stuxnet

Impact

28

Destroy devices [Air Pressure (AP)]

Target: Devices

Damage to Property (T0879)

Example: Stuxnet , Maroochy Attack , German steel mill , Lodz city tram system in Poland

Loss of Productivity and Revenue (T0828)

Example: Australian beverage company , Colonial Pipeline

Manipulation of Control (T0831)

Example: Lodz city tram system in Poland

Loss of Control (T0827)

Example: Industroyer , Norsk Hydro

Loss of Availability (T0826)

Example: Colonial Pipeline , **Conficker**



Impact

29

Airflow stop [Air Pressure (AP)]

Loss of Productivity and Revenue (T0828)

Example: Australian beverage company ,
Colonial Pipeline

Loss of Availability (T0826)

Example: Colonial Pipeline , Conficker

Sequence values (PC)

Target: PLC

Manipulation of Control (T0831)

Example: Lodz city tram system in Poland



Gas tank (MGTL1)

Target: Gas tank

Loss of Productivity and Revenue
(T0828)

Example: Australian beverage
company , Colonial Pipeline

Threat model/event

____ Threat source : State actor/insider/malware

____ Attack : Internet Accessible Device (T0883)

____ Threat vector: Web Server

____ Vulnerability: **CVE-2019-18261**

____ Target: Omron PLC NJ

____ Attack Objective: Modify Parameter (T0836)

____ Impact: Manipulation of Control (T0831)

9.8

**Vulnerability
Severity**

3.0

**Asset
Criticality**

2.5

**Attack
Likelihood**

3.0

Impact

6.7

**Risk
Score**

$$\text{Risk} = \frac{\text{Severity} + [(\text{Criticality} \times 2) + (\text{Likelihood} \times 2) + (\text{Impact} \times 2)]}{4}$$

Top 20 Secure PLC Coding Practices ^[5]



**Change Operating Mode
(T0858)**

Track operating modes

Modification Attack :

Modify Parameter (T0836)

- Validate HMI input variables at the PLC level, not only at HMI (HMI is a possible attack scenario from insiders and outsiders)
- Validate inputs based on physical plausibility
- Disable unneeded / unused communication ports and protocols
- Restrict third-party data interfaces
- Define a safe process state in case of a PLC restart

Trap false negatives and false positives for critical alerts

Trap false negatives and false positives for critical alerts

- ____ Security Objective : Monitoring
- ____ Web server (common in Shodan) // attacker can modify settings if access rights misconfigured
- ____ Example: Triton

Define a safe process state in case of a PLC restart

- ____ Security Objective : Resilience
- ____ What if operation mode was changed , and attacker restarted the plc !

Restrict third-party data interfaces

- ____ Security Objective : Hardening
- ____ Restrict read/write to PLC



Disable unneeded / unused communication ports and protocols

- Security Objective : Hardening
- Example: embedded web server are common for maintenance and troubleshooting. Easy to find in Shodan



SHODAN

Validate inputs based on physical plausibility

- Security Objective : Integrity of I/O values
- Example: Oldsmar Florida. No limit was set !



Validate HMI input variables at the PLC level, not only at HMI

- Security Objective : Integrity of PLC variables
- Example: Many are found online in Shodan !



Mitigations

34

Modification Attack Modify Parameter (T0836)

- Authorization Enforcement (M0800)
- Audit (M0947)

Change Operating Mode (T0858)

- Authorization Enforcement (M0800)
- Human User Authentication (M0804)
- Communication Authenticity (M0802)
- Network Allow lists (M0807)
- Access Management (M0801)
- Software Process and Device Authentication (M0813)
- Network Segmentation (M0930)



Summary

- ___ LPG process is secured when ICS equipments are secured
- ___ Understand LPG cylinder filling process and normal operations
- ___ Map LPG attacks to “Mitre ATT&CK for ICS”
- ___ Map LPG attacks to “secure PLC practices (Top 20)”
- ___ Map Safety PLC to “secure PLC practices (Top20)”
- ___ Develop a threat model/event
- ___ Calculate risk score of Safety PLC

Get in Touch



www.zerontek.com



alhasawi@zerontek.com

info@zerontek.com



<https://www.linkedin.com/in/alhasawi>



Sulaiman Alhasawi

**Researcher ICS/OT/IT
cybersecurity**



@alhasawi

References

37

- 1) <https://researchonline.ljmu.ac.uk/id/eprint/13480/1/2020AlhasawiPhD.pdf>
- 2) <https://icsstrive.com/>
- 3) <https://www.spiceworks.com/it-security/security-general/news/blackcat-ransomware-attack-creos-energy-sector/>
- 4) <https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/>
- 5) <https://plc-security.com>
- 6) <https://www.elgas.com.au/blog/486-comparison-lpg-natural-gas-propane-butane-methane-lng-cng/>
- 7) <https://www.expertmarketresearch.com/articles/top-5-companies-in-the-global-lpg-market>
- 8) <https://www.bitdefender.com/blog/hotforsecurity/north-american-gas-supplier-superior-plus-hit-with-ransomware/>

References

- 9) <https://www.anomali.com/resources/what-mitre-attck-is-and-how-it-is-useful>
- 10) <https://www.cisa.gov/uscert/ics/advisories/icsa-22-179-02>
- 11) <https://www.cisa.gov/uscert/ics/advisories/icsa-19-346-03>
- 12) <https://www.mheducation.com.sg/hacking-exposed-industrial-control-systems-ics-and-scada-security-secrets-solutions-9781259589713-asia>
- 13) <https://www.cisa.gov/uscert/ncas/alerts/aa22-103a>
- 14) <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>
- 15) <https://www.ge.com/gas-power/resources/articles/2021/energy-cyber-attack>
- 16) <https://new.abb.com/plc/plc-technology/ac500-plc-applications/safer-greener-and-more-productive-with-ac500-s-safety-plc>

Thank you!



Sulaiman Alhasawi, PhD

**Researcher ICS/OT/IT
cybersecurity**

 **@alhasawi**

kaspersky