Hadjistassou Constantinos
University of Nicosia, University of Cyprus, Nicosia, Cyprus

Bratskas Romaios

Koutras Nikolaos

Kyriakides Alexandros
ADITESS Advanced Integrated Technology Solutions & Services, Nicosia, Cyprus

Charalambous Elisavet
ADITESS Advanced Integrated Technology Solutions & Services, Nicosia, Cyprus
University of Cyprus, Nicosia, Cyprus

Hadjiantonis Antonis M.
CyRIC Cyprus Research and Innovation Center Ltd., Nicosia, Cyprus

Safeguarding critical infrastructures from cyber attacks: A case study for offshore natural gas assets

Keywords

critical infrastructure, cyber attacks, energy, natural gas, gas hydrates

Abstract

The majority of operations, as well as the physical and chemical processes, which take place on offshore Natural Gas installations are controlled by computer systems. These computer systems are vulnerable to cyber-attacks. If successful, such attacks can have disastrous and far-reaching consequences, including human casualties, large-scale pollution, and immense financial cost. In this paper we identify one possible way that an attacker can inflict material damage, by altering the parameters of the gas hydrate inhibition system. The formation of gas hydrates can completely halt operations for a prolonged period of time, could damage equipment, and directly endanger human lives. To raise the level of protection we propose the implementation of two lines of defense the second based on machine learning algorithms. Appreciating the sophistication of attacks, the inherent risks and complexity of multi-billion offshore energy assets we highlight the need for further research intended to address safety loopholes.

1. Introduction

Cyber attacks on critical energy infrastructure, such as oil and gas facilities, do not constitute far fetched scientific fantasy scenarios any more. In fact, such an assault can well be part of a ``fire sale[1]" plan. A recent resounding case was the alleged cyber spying on Petrobras-- the Brazilian National Oil Company (NOC) – by the US National Security Agency (NSA), as reported in the press [12].

Petroleum operations are increasingly becoming more dependent on computers. In turn, computers are interconnected allowing the generation, transfer, manipulation and management of vital data. At the same time, these systems are vulnerable to cyber-attacks for several reasons. For instance, attackers may seek financial benefits, commercial secrets, or social or environmental advantages. In this paper, we present the hazards that cyber-attacks can pose to of offshore natural gas extraction.

The Cyprus Cyber Crime Center of Excellence (3CE) will provide short-term, highly focused and specialised training seminars on cybercrime-related issues for public and private sector participants.

[1] The term ‘fire sale’ was coined in the movie “Die Hard 4.0” where hackers target US Government, transportation & energy, and financial networks.

Courses will facilitate the exchange and diffusion of tacit knowledge and expertise and familiarise participants with new technologies and tools, and improve their day-to-day activities related to the Cybercrime area. University courses on Cybercrime developed and delivered to stakeholders will provide better understanding of the legal and technical elements of cybercrime for new generation scientists. Courses will be made available under creative commons licensing terms for LEAs worldwide. 3CE aspires to become an exemplary Centre of Excellence in the area of Cybercrime by conducting research in relevant fields, focusing particularly on areas dealing with forensic analysis, intrusion detection systems of critical information infrastructures, and legal aspects of cybercrime.

2. Industrial control systems: vulnerabilities and threats

The majority of Critical Infrastructure Systems are instrumented by special computerised systems, collectively known as Industrial Control Systems (ICS). ICS are command and control networks and systems designed to support industrial processes. These systems are responsible for monitoring and controlling a variety of processes and operations such as gas and electricity distribution, water treatment, oil refining or railway transportation. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems. According to ENISA [3] in the last few years, ICS have passed through a significant transformation from proprietary, isolated systems to open architectures and standard technologies highly interconnected with other corporate networks and the Internet. Today, ICS are often networked in local or wide area networks (LAN/WAN). In turn, these networks are either interconnected using private leased communication lines, or use secure tunnels (Virtual Private Networks) over the public Internet, create complex network of networks. In special cases, infrastructure networks remain locally isolated and disconnected from the outside world. The latter method, often referred to as \security via obscurity," was considered a sufficient protection strategy for these networks. However, the latest generation of malware, with Stuxnet as its poster child has uncovered the severe vulnerabilities of industrial control systems, even in the case of network isolation.

3. Review of major critical infrastructure cyber security incidents

To provide an insight into the emergence of previously unknown vulnerabilities and threats to critical infrastructures, we analyse recent incidents. Later, in §4 we draw lessons from these examples in order to explain the risk of Cyber Attacks and to suggest possible actions for defense.

Table 1. Summary of Incidents

Incident	Stuxnet	Night Dragon	Flame	Shamoon
Type	Computer Worm	Trojan back-door	Modular malware	Modular virus
Infrastructure Specific	Yes	No	Yes	Partially
Purpose	Industrial system damage	Cyber espionage	Cyber espionage (infrastructure reckoning)	Cyber espionage in the energy sector
Known Impact	Extensive physical damage to Iran's uranium enrichment facilities	Infections reported worldwide	Mapped and monitored Iran's computer networks	Saudi Aramco and RasGas network downtime
Preventable	Unclear	Yes	Yes	Yes

3.1. Stuxnet

The Stuxnet worm attack in 2010 raised the profile of cyber security and ICS vulnerabilities, since for the first time a malicious computer software (malware) had inflicted severe and potentially lethal damage to industrial infrastructures, in particular uranium enrichment facilities. Extensive damage was inflicted on six cascades containing 164 Iranian IR-1 centrifuges used in producing uranium-235 from uranium hexafluoride gas. The delay of Iran's nuclear program is attributed to Stuxnet infection.

Stuxnet primarily targets supervisory control and data acquisition (SCADA) systems which run the Siemens WinCC software, although it can infect all Microsoft Windows® systems. The worm spreads by taking advantage of a multitude of zero-day exploits in Windows, and it can execute itself from an infected removable medium as soon as the drive has been read by the operating system. It is speculated that this was the method used to infiltrate the industrial facilities, where the local area network was not connected on the Internet. Successful exploitation of this vulnerability results in the injection of a backdoor, as well as the installation of two rootkits that will conceal accompanying files [4].

The Stuxnet incident should be examined with caution as its continued examination has revealed that only a state actor could have financed and executed this kind of an attack. An article in Der Spiegel [17] cites a European intelligence agency statement that “it would have taken a programmer at least three years to develop Stuxnet, at a cost in the double-digit millions”. Nonetheless, it highlights the potential impact a determined attacker can inflict. It goes without saying that multi-billion dollar investments in O&G infrastructure are high value targets.

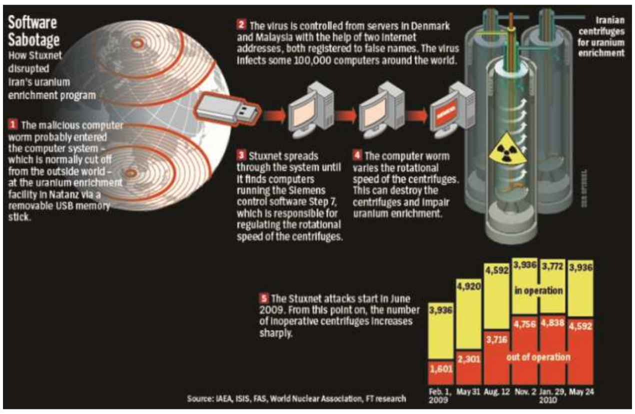
Software Sabotage
How Stuxnet disrupted Iran's uranium enrichment program
1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.
2 The virus is controlled from servers in Denmark and Malaysia with the help of two internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.
3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.
4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.
Iranian centrifuges for uranium enrichment
5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.
3,936
4,920
4,592
3,936
3,772
3,936
in operation
1,601
2,301
3,716
4,756
4,838
4,592
out of operation
Feb. 1, 2009
May 31
Aug. 12
Nov. 2
Jan. 29, 2010
May 24
Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

Figure 1. Stuxnet (Source: IAEA, ISIS, FAS, World Nuclear Association, FT research)

3.2. Flame

Flame malware was discovered in 2012 after the UN's telecoms body ITU asked for help with identifying a virus found stealing data from many PCs in the Middle East and to investigate reports of a virus affecting Iranian Oil Ministry computers. According to the Washington Post [20], citing “Western officials”, Flame collected intelligence in preparation for cyber-sabotage aimed at slowing Iran's ability to develop a nuclear weapon.

The Flame malware secretly mapped and monitored Iran's computer networks, sending back a steady stream of intelligence to prepare the ground for the actual sabotage that was carried out via the aforementioned Stuxnet worm. However, the discovery of Flame came to light only after Stuxnet had inflicted damage. In addition, Flame's sophistication included a \suicide" command, which was designed to completely remove it from the compromised computer and then overwrite memory locations with gibberish to thwart forensic examination [5].

3.3. Shamoon

The Shamoon computer virus incident was discovered in 2012 [15], reported for attacks on computers running the Microsoft Windows “NT” line of operating systems. The virus is being used for cyber espionage in the energy sector. The virus has been noted as unique for having differing behaviour from other malware cyber espionage attacks, i.e., it is capable of spreading to other computers on the network, through exploitation of shared hard drives.

Once a system is infected, the virus continues to compile a list of files from specific locations on the system, erase and then send information about these files back to the attacker. Finally, the virus will overwrite the master boot record of the system to prevent it from booting. The virus was reposted as hitting companies within the oil and energy sectors, in particular Saudi Aramco, Saudi Arabia's NOC, and Qatari natural gas company RasGas. Shamoon is capable of wiping files and rendering several computers on a network unusable.

3.4. Night dragon

The Night Dragon malware was detected in 2011 and is estimated that it had been around for four years. According to McAfee [11], there was evidence of Night Dragon malware infections in the Americas, Europe, and Asia, as well as countries in the Middle East and North Africa. McAfee has also identified tools, techniques, and network activities utilised during these continuing attacks that point to individuals in China as the primary source.

The Night Dragon attackers had been targeting global oil, energy, and petrochemical companies with the apparent intent of stealing sensitive information such as operational details, exploration research, and financial data. The attacks often focused on the companies' public-facing Web sites, which were attacked using methods such as SQL injection, where hackers try to get backend databases to reply to commands that should be blocked. SQL injection attacks can often return sensitive information or allow for different kinds of attacks.

4. Cyber attacks

Industrial Control Systems rely on a network infrastructure to transmit data. The best possible effort should be made to protect this network. Past incidents have shown, however, that tapping into the networks of Industrial Control Systems is not impossible. This leads to the conclusion that the last line of defense should not be the network itself [14], [18]-[19]. Encryption provides one of the best security measures for protecting data. Even so, some encryption algorithms are vulnerable to attack, and some of them may even contain backdoors. Backdoors can also be present in security protocols and hardware systems which are part of the ICS infrastructure. Is it plausible that such backdoors are introduced by government agencies [13], such as the

NSA [10], so that governments have the ability to attack the critical infrastructures of other countries. When the target is a critical infrastructure, the attacker could therefore be the government of a country, with extensive resources at its disposal. In this section we focus on cyber-attacks regarding Oil & Gas installations. We identify the major points of vulnerability and we make suggestions on possible protection measures.

4.1. SCADA system

The Supervisory Control and Data Acquisition system (SCADA) is used for controlling remote equipment. It is a type of Industrial Control System (ICS). SCADA is used on offshore oil and gas platforms in order to control critical processes [7]. As described earlier in this paper, it is vital that these processes are continually controlled and monitored in order to ensure the proper working of the installation. If the parameters of a process deviate from certain safe limits, the result could be catastrophic. The formation of hydrates, described in detail earlier in this paper, is one such example. The SCADA system is therefore a prime target for attack [21]. For this reason, it is essential that cyber-security measures are taken for critical infrastructure SCADA systems.

4.2. Remote attacks

In order to provide control to remote equipment, the SCADA system can itself be accessed remotely. This presents a gateway for penetration. Various types of defenses can be set up to protect the network which provides access to the SCADA system. Vulnerabilities in network protocols and even in the network infrastructure are common however. An experienced and resourceful attacker, who has physical access to the network infrastructure, can intercept and eavesdrop on communications. Furthermore, the attacker can contaminate the network with malicious packets of information with the intent to disrupt communication or even alter control commands. Although it could be challenging to mount such attacks, it is certainly not impossible.

In the case of offshore oil and gas platforms, the attacker could certainly be a national government, which has more than adequate experience and resources to execute the attack. An attack which disrupts, or even disables, the production of a rival platform could be beneficial to the national interests of the attacker.

Strong encryption can be used to protect communications. Encryption ensures the confidentiality and integrity of the transmitted data. Standard open protocols and algorithms are available for encryption, as well as proprietary ones. Recently however, it has come to public attention that certain encryption standards are not secure. It is speculated that the National Security Agency (NSA) has played an instrumental role in introducing backdoors in some important encryption implementations. Although this is allegedly done in the interests of national security, it is can also be done for economic espionage. The backdoors in the software allow the US government, and others discover the backdoor, to break the encryption. It is not enough therefore to rely on encryption alone.

4.3. Intelligent monitoring

For critical infrastructures it is not enough to rely on standard methods of protection. The network infrastructure is vulnerable and encryption is not always reliable. An attacker who gains access to the SCADA system can modify control parameters. This can be done covertly, making it impossible for a human monitoring the system to detect. A compromised SCADA system can show false sensor outputs which are different from the true sensor readings. Relying solely on a SCADA system could prove disastrous when the system is compromised.

As attacks on critical infrastructures become more prevalent, a second line of defense becomes necessary. A system which is completely independent from the SCADA system is needed. The purpose of this system is for monitoring in order to alert for possible danger. It should act as an early warning system before the actual attack takes place.

More recently, machine learning has been proposed as a tool for protecting critical infrastructures [1]. Machine learning models have the advantage that they can learn and adapt to situations based on data. Intrusion Detection Systems provide a means to detect attacks before they cause any damage. Such systems usually monitor network activity for patterns which are anomalies and are therefore possible indications of attack. We propose that in the case of Oil & Gas installations, the models can be trained on data related directly to the control parameters of the process, in order to detect anomalies in the control commands. If a command with malicious intent is issued by the SCADA system, the machine learning model can be trained to identify it. For example, if a command is issued to deploy an amount of gas hydrate chemical inhibitor (such as MeOH), the machine learning model will be able to asses all the control and sensor parameters at that specific time and determine if the amount of inhibitor is of an acceptable quantity.

5. A case study: gas hydrates

Flow assurance refers to the unobstructed and continuous flow of hydrocarbon fluids, usually oil, natural gas, and gas condensates, in pipelines and flow-lines from the reservoir to processing or gathering facilities. Increasingly larger volumes of oil and natural gas are sourced from deepwater to floating facilities for processing and, subsequently, via submarine pipelines to onshore plants. Gas extraction from offshore gas fields is particularly prone to the formation of gas hydrates. Gas hydrates, also termed as "clathrates"' or inclusion compounds, are crystallised (solid) water molecules (cages) which predominantly trap paraffin molecules, that is, methane, ethane or propane structures.

Occasionally, the formation of gas hydrates has led to the blockage of natural gas flow, damage to Oil & Gas (O&G) equipment, and to the loss of human lives. Often, the formation of gas hydrates is predicated on the presence of water and paraffins, in the fluid pressure range of 0<P<2,500psi (0<P<17.2MPa), and low ambient temperature regime of 30<T<80˚F (-3<T<27˚C) [16]. Due to the almost ubiquitous use of imperial units in the O&G industry we have opted to use these units.

5.1. The perils of gas hydrates

Gas hydrates strike fear in the oil & gas industry mainly because they:

(i) Manifest themselves within minutes without being easily detected;
(ii) Their perplexing thermodynamics, emanating from various interacting chemical components, renders their prediction intractable, and
(iii) Risk of failure to equipment, suppressing hydrates, cannot be completely eliminated.

Formation of gas hydrates in natural gas transfer operations is undesirable for several reasons. Prime of those are:

(i) Increase in conduit pressure;
(ii) Flow rate irregularities attributed to multi-phase flow;
(iii) Environmental hazards due to hydrocarbon leakage;
(iv) Reduced field productivity;
(v) Safety perils to equipment, and
(vi) Risks to human lives.

Owing to the difficulty of access, gas hydrates are of critical concern to offshore O&G extraction. This is particularly acute for deep water [depths] ($\approx 700\text{ft} < H_{H_2O} < 4{,}500ft; 200m < H_{H_2O} < 1{,}500m$) and ultra-deep water $H_{H_2O} > 1{,}500m$; $H_{H_2O} > 5000m$ petroleum developments. High hydrocarbon fluid pressures and low sea-water temperatures are pre-requisites for gas hydrate generation.

Physically, gas hydrates appear is several locations in O&G subsea and floating installations under certain circumstances. Depending on the water depth (and temperature) as well as the fluid pressure, hydrates may form in wellheads, Christmas trees, submarine manifolds, low points of flowlines, jumpers, marine risers and flexible flowlines [6].

5.2. Predicting gas hydrate formation

During the life-cycle of a gas field, the risk of gas hydrate disruption may vary depending on the composition of recovered fluids – especially the water cut (content). Hence, the need to protect petroleum assets, safeguard human lives and preserve the marine environment becomes even more pressing. Driven by the preceding factors, several flow assurance strategies have been devised by the industry and research communities. During the past decade the emphasis has shifted from hydrate inhibition to hydrate risk management [16]

Predicting the precise conditions, for a particular gas stream, at which gas hydrates will precipitate is not an exact science. Even though statistical mechanics offers a powerful tool for narrowing uncertainty, still the complex kinetics of crystal growth remain far from clarified. Throughout the past 50 years various statistical and empirical techniques have been conceived for the prediction of gas hydrates.

Prevailing flow assurance strategies fall into four distinct categories, namely:

(i) Utilisation of hydrate inhibitors;
(ii) Gas stream dehydration;
(iii) Mechanical techniques, such as pipeline depressurisation, and
(iv) Thermal management methods, such as pipeline insulation and active conduit heating.

Notwithstanding the uncertainty, analytical models for chemical inhibitor introduction remain the most popular method for hydrate management.

Hydrate prediction curves for natural gas, as a function of temperature versus hydrate formation pressure, can be used to assess the risk of gas hydrate formation. Likewise, these lines can be digitised into simplified equations offering thus an analytical way for determining the operational boundary outside of which hydrates cease to pose a risk. Below 1,000psi, the gas hydrate threshold is given by:

$$T_g = -16.5 - \frac{6.83}{SG^2} + 13.8\ln(P) \qquad (1)$$

where temperature (T_g) is in ˚F and the specific gravity (SG) of the gas of interest is calculated at 60˚F & 14.7psia (pounds per square inch absolute). In the sequel, we outline the methodology for calculating the dosage of a chemical inhibitor destined to suppress gas hydrates from an offshore natural gas field. As it will become more evident from §5.3 the introduction of a smaller quantity of hydrate inhibitor than the calculated mass can lead to the formation of gas hydrates. Therefore, by all means the operator is obliged to retain control on the hydrate inhibitor injection system. Due to its critical role and computer mediated control, the hydrate suppression unit can fall victim of a malicious cyber intrusion.

5.3. Dosage of gas hydrate inhibition

Natural gas, saturated with water, at a specific gravity (SG) of 0.75, a temperature of 110˚F and a pressure of 800psia, is pumped from an offshore platform to the shore. By the time the gas stream reaches the shore it undergoes a temperature and pressure drop to 40 ˚F and 500psia, respectively. Calculations presented herein assume no hydrocarbon condensates are collected in the export line. Methanol (MeOH) was selected as a suitable gas hydrate chemical inhibitor. We need calculate the mass of methanol per million standard cubic feet of gas (MeOH/MMscf) necessary to potentially avoid hydrate formation between the rig and the coast.

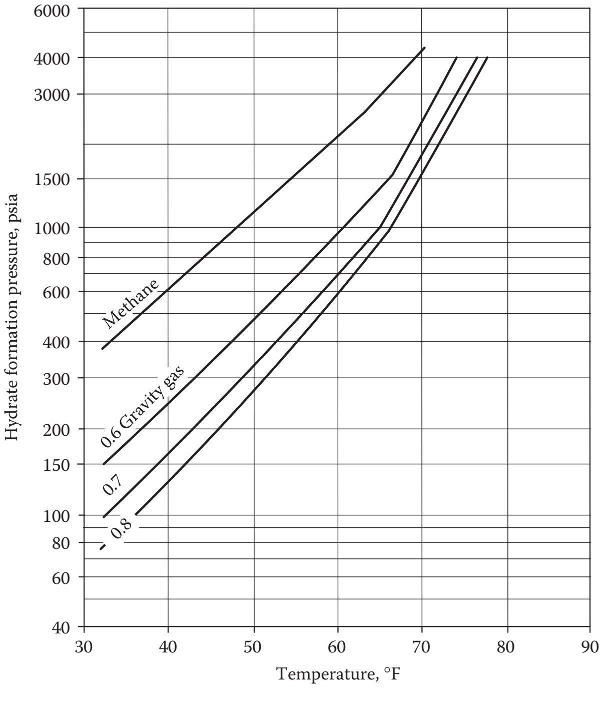

Figure 2. Methane gas pressure-temperature lines for the prediction of gas hydrate formation [2]

5.3.1. Risk of gas hydrate formation

Utilising equation (1), from §5.2, it is possible to determine whether the gas stream (in §5.3) is liable to gas hydrate formation. The gas hydrate formation temperature (T_g), at 800psia, was determined to be 63.6˚F.

The sub-cooling temperature drop is then: $T_{Sub} = 63.6 - 40 = 23.6˚F$. As indicated by *Figure 2*, a temperature drop of 23.6˚F into the gas hydrate zone is sufficient to promote gas hydrates unless remedial action is taken such as the introduction of a hydrate inhibitor, like methanol (MeOH).

5.3.2. Volume of gas hydrate inhibitor

To quantify the mass of methanol needed to suppress gas hydrates it is necessary to determine:

(i) The quantity of liquid water available in the gas pipeline;
(ii) The amount of MeOH in the water-phase, and
(iii) The mass of MeOH in the gas-phase.

Moving from the gas hydrate free region into the hydrate prone regime, as shown in *Figure 2*, raises the risk of either pipe blockage and/or damage to equipment probably at the expense of undue costs. If hackers assume control of the gas hydrate inhibition system, the risk of hydrate blockages becomes a real possibility.

5.3.3. Gas stream water cut

The water content (cut) of the extracted natural gas can be determined from *Figure 3*. Entering the latter figure, at a temperature (T_1) of 110˚F and pressure (P_1) 800psia, the gas is found to hold about 90lb(H_2O)/MMscf. Before being delivered at its destination the gas stream, at T_2 of 40˚F and P_2 of 500psia, contains 15lb (H_2O)/MMscf. Therefore, the water content of the gas stream available for gas hydrates is:

$$\Delta H_2O = 90 - 15 = 75 lb(H_2O)/MMscf$$

5.3.4. Quantity of methanol in aqueous phase

To obtain the quantity of MeOH needed to inhibit gas hydrates in the *aqueous phase*, the empirical equation of Nielsen &Bucklin was used:

$$\Delta T(˚F) = -129.6 \ln(x_w) \qquad (2)$$

where x_w is the mole fraction of water in the aqueous phase.

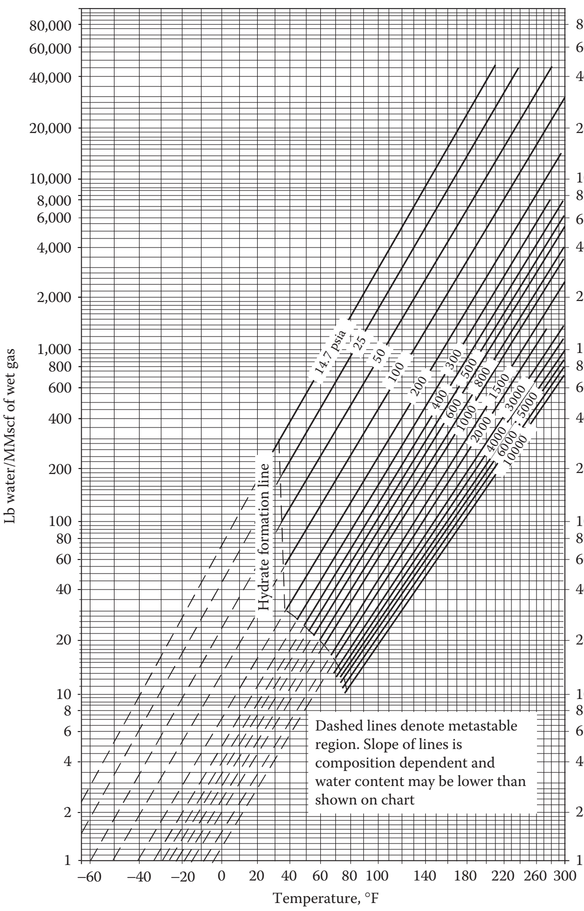

Figure 3. Water content of hydrocarbon gases as a variation of pressure and temperature [8]

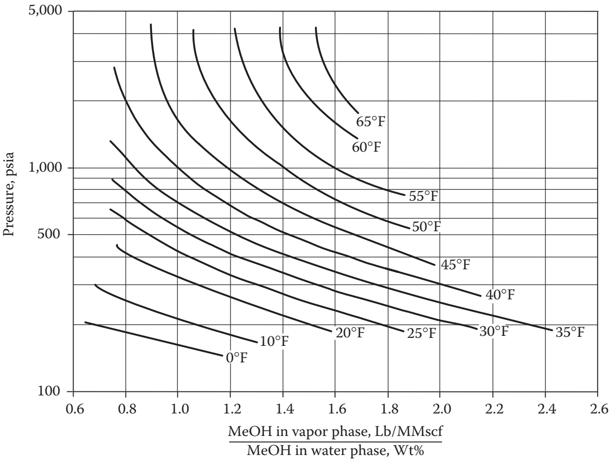

Figure 4. Methanol in vapour to gas phase as a function of pressure [2]

Once x_w is found, the % by weight (wt%) of ethanol can be obtained from:

$$wt\% = \frac{x_{MeOH}{*}MM_{MeOH}}{x_{MeOH}{*}MM_{MeOH}+x_w{*}MM_w} \quad (3)$$

where MM_i is the molar mass of the chemical compound of interest. To convert wt% of methanol into mass one can use wt%/(wt%-1). Hence, the mass of methanol needed to suppress gas hydrates is wt%× ΔH_2O. Substituting, the mole fractions of H_2O and MeOH into equation (3) the weight of MeOH was found to be 26.1wt%. Hence, the mass ratio of MeOH needed to suppress gas hydrates is 0.353lb (MeOH)/lb(H_2O).

Finally, the quantity of methanol for hydrate inhibition is 0.353×75=26.5lb (MeOH)/MMscf.

5.3.5. Quantity of methanol in vapour phase

Considering the volatile nature of methanol some of the alcohol will evaporate in the vapour state. This quantity can be determined from *Figure 4*. At 40˚F & 500psia the ratio of MeOH in vapour to MeOH in water phase is estimated to be 1.43. Thus, 37.9 lb(MeOH)/MMscf will be needed. In aggregate, the total amount of methanol needed to combat gas hydrates in the vapour state is: 37.9+26.5=64.4lb (MeOH)/MMscf.

5.4. Risks inherent to the malicious control of methanol injection

Assuming no endogenous factors, such as variations in gas composition and water cut, act to invalidate the calculations presented in §5.3, the introduction of 26.5lb(MeOH)/MMscf will suffice to inhibit gas hydrate formation. A smaller MeOH dosage endangers natural gas extraction by permitting gas hydrates to develop.

Still an excess quantity of MeOH can result in undue operational costs incurred from the cost of methanol. The introduction of a surplus quantity of MeOH at the subsea wellhead promotes multi-phase flow and could lead to a drop in the flowline gas stream pressure.

Methanol can cost $1.6/gal [9]. Apparently, the use of an unnecessary amount of MeOH can prematurely deplete methanol reserves and could pose serious logistics issues in terms of replenishment especially offshore. Running out of MeOH could prove hazardous to natural gas extraction as gas hydrates may develop. Therefore, if hackers assume control of the MeOH inhibitor system the risks from gas hydrate formation are real and could prove catastrophic. Consequently, retaining control of the MeOH inhibitor system is of vital importance.

6. Conclusion

According to the aforementioned ENISA report, the biggest challenges in ICS security are identified and it is worth noting two of them in the context of this paper. The 1st Challenge is the lack of specific initiatives on ICS security: “At the EU level, there are policy areas addressing Critical Infrastructure Protection and Critical Information Infrastructure Protection (CIIP). However, none of them are addressing ICS specifically. A European Commission Communication [COM(2011) 163] recognizes that new threats have emerged, mentioning Stuxnet explicitly.

However, new activities proposed by this Communication on CIIP do not include any specific to ICS. In this context, ENISA has already stated that after Stuxnet, currently prevailing practices on CIIP will have to be reconsidered.” Another challenge identified in ENISA's report is the difference in the ruling security paradigms between classic ICT and ICS environments. The ruling security paradigm in Classic ICT systems' security is based on the CIA model (Confidentiality, Integrity, Availability), but in the ICS environment the SRA model (Safety, Reliability, Availability) is predominant, often referred to as AIC (the inverse of CIA) to emphasise the priority given to Availability. In closing, using the gas hydrate inhibitor system as an example we have highlighted some of the cyber vulnerabilities of offshore O\&G installations. It is evident that further research is necessary for bulletproofing the secritical infrastructure systems.

Acknowledgments

The paper describes research results of the Cyprus Cyber Crime Center of Excellence (3CE) for Training, Research and Education (a project co-funded by the Prevention of and Fight against Crime Programme of the European Union) in the field of Critical Infrastructure and cyber-attacks. C.H. acknowledges financial support from the University of Cyprus.

References

[1] Cazorla, L., Alcaraz, C., & Lopez, J. (2013). Towards automatic critical infrastructure protection through machine learning. *In 8th International Conference on Critical Information Infrastructures Security*, 8328:197-203, Amsterdam, The Netherlands, Springer.

[2] *Engineering Data Book*. (2004). 12th ed., Dehydration, Gas Processors Supply Association, Tulsa OK, USA.

[3] ENISA, Protecting Industrial Control Systems - Recommendations for Europe and Member States," (2011).

[4] *Exploring Stuxnet's PLC Infection Process*, http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process; Posted on Sep 22, 2010

[5] *Flame malware makers send suicide code*, http://www.bbc.com/news/technology-18365844; Posted June 8, 2012

[6] Hadjistassou, C., Efthymiou, M. & Papanastasiou, P. (2014). *Well and Subsea Completions and Production Facilities (PET522)*; Lecture Notes, University of Cyprus, Faculty of Engineering.

[7] Hadjistassou, C., Hadjiantonis, A. (2012). *Risk Assessment of Offshore Oil & Gas Installations Under Cyber Threats*. In: EASTWEST 2012, International Congress, European Office Cyprus, Cyprus, 95-101.

[8] Kidnay, A.J. & Parrish, W.R. (2006). *Fundamentals of Natural Gas Processing*. CRC Press, Boca Raton, Fla.

[9] Methanex, Methanol Price: www.methanex.com/

[10] *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

[11] *Night Dragon*, http://www.mcafee.com/us/about/night-dragon.aspx?cid=WBB009

[12] *NSA Documents Show United States Spied Brazilian Oil Giant*, Globo.com. (2013). Posted Sept., 9, 2013.
products/methanolprice.html; Posted on May 23, 2014.

[13] *Revealed: how US and UK spy agencies defeat internet privacy and security*, www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[14] *Risks and Dangers of Fiber Optic Cables*, http://infoguard.ch/pdf/publikationen/wp_fiber_optic_communication-e.pdf

[15] *Shamoon virus targets energy sector infrastructure*, http://www.bbc.com/news/technology-19293797; Posted Aug 17, 2012

[16] Sloan, E. D., Koh, C. & Sum A.K. (2011). *Natural Gas Hydrates in Flow Assurance*. Gulf Professional Pub.Elsevier, Oxford.

[17] Stark, H. (2011). *Stuxnet Virus Opens New Era of Cyber War*. Der Spiegel Online: www.spiegel.de/international/world/mossad-s-miracle-weapon-stuxnet-virus-opens-new-era-of-cyber-war-a-778912.html; Aug 08, 2011, Lecture Notes in Computer Science 13

[18] *Tapping Fibre Channel connections is much easier than commonly believed!*, White paper. http://infoguard.ch/pdf/publikationen/wp_infoguard_fibrechannel_e.pdf

[19] *The 7 Security Myths Surrounding Fibre Optic Networks*, White paper. http://infoguard.ch/pdf/publikationen/wp_infoguard_securitymythen_e_v10.pdf

[20] U.S., Israel developed Flame computer virus to slow Iranian nuclear e_orts, o_cials say:

http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html; Posted June 19, 2012

[21] Zhu, B., Joseph, A. & Sastry, S. (2011). *A taxonomy of cyber attacks on scada systems. In Internet of Things (iThings/CPSCom)*, 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, 380-388. IEEE.