2008-02-01

Integrated Security Concept for the Oil and Gas Industry by P. Furthner and Friedrich Steinhausler; Strategic Insights, v. 7, issue 1 (February 2008)

Steinhausler, Friedrich; Furthner, P.

Monterey, California. Naval Postgraduate School

Strategic Insights, v.7 issue 1 (February 2008)
https://hdl.handle.net/10945/11176

Integrated Security Concept for the Oil and Gas Industry

Strategic Insights, Volume VII, Issue 1 (February 2008)

by P. Furthner and Friedrich Steinhäusler

Introduction: TAAS Industrial Corporate Security Awareness Programme (ICSAP)

The oil and gas industry is a major component of the national critical infrastructure and as such represents an attractive target for terrorists. Globally terrorists have attacked every segment of the oil and gas fuel cycle, ranging from attacks on exploration and development sites, to maritime shipment, land-based distribution via pipelines, to retail and distribution networks, such as filling stations.[1] In addition to international terrorism, two major oil producing countries have also indicated to resort to the use of force in connection with the oil and gas industry:

> (a) Venezuela is threatening to destroy its installations on its oil fields in case of a military attack by the United States;[2] and
>
> (b) Iran has indicated it aims to *"strike against U.S. interests all over the world"* (note from authors: this includes U.S. oil and gas companies) *"if the United States were to attack to Iran*."[3]

Therefore it will be necessary to engage in a proactive global strengthening of security in the oil and gas industry in order to reduce the risk of significant interruption in the energy production. As part of this effort TAAS has developed the *Industrial Corporate Security Awareness Programme* (ICSAP). In the following ICSAP is discussed in more detail and demonstrated in selected practically applicable examples.

ICSAP Objectives and Modular Structure

ICSAP has three major objectives:

1. Integrated Threat Identification: ICSAP identifies multiple man-made threats for corporation *and* members of the management
2. Comprehensive Risk Assessment: ICSAP enables corporate decision makers to assess the specific risk at the corporate *and* personal level
3. Optimal Risk Management: ICSAP assists in the cost-efficient management of risks from internal *and* external threats.

In order to tailor ICSAP to the specific requirements of the end-user it has a modular structure, with each of the three modules representing a self-contained unit. By implementing ICSAP a coherent Security Policy and Culture within all management levels of the organization will be achieved.

Module 1 addresses *Causation of Corporate Security Risks*. In this module potential attackers representing a security risk to the corporation are identified for each site. In view of the mostly international operations of oil and gas companies it is important to develop a specific risk portfolio for each area, country and region the company operates in. Such a portfolio covers *inter alia* national terrorism, international terrorism, insider threat, organized crime, and cyber hackers.

Furthermore, this module identifies also potential targets in seven asset categories of an oil or gas corporation:

1. Major buildings (process units, on-site control rooms, corporate offices abroad, administration offices;
2. Specific equipment of strategic value (product storage tanks, surge vessels, boilers, turbines, process heaters, sewer systems);
3. Critical support systems (electrical power grid, natural gas supply lines, drinking water and process water supply, waste water treatment facilities);
4. Inter-modal transportation and its interfaces (product loading areas and vehicles, railroad lines and railcars, pipelines supplying the facility, pipelines delivering products to outside of the plant, marine vessels and docking areas, offsite storage sites);
5. Indispensable information technology components (SCADA software platforms for control of pipeline infrastructure, onsite computer networks, devices with remote maintenance ports, PDA, notebooks, and mobile phones of employees);
6. Vital sectors of the retail sector (transport of refined products to petrochemical facilities, gasoline stations, and power stations; point of sale, such as bulk stations, gasoline stations); and
7. Staff (technical experts in the field, top management, key administration officers).

Module 2, which focuses on *Management of Corporate Security Risks,* prioritizes risks with *risk* defined as:

$$R = p1 * p2 * C / E$$

Where:

- R = Risk to a specific oil and gas corporation due to a major terror attack
- P1 = Probability of terrorists to possess all necessary means to carry out a particular terror attack
- P2 = Probability for the successful implementation of a particular attack mode
- C = Primary and secondary consequences of a specific mode of attack
- E = Effectiveness of countermeasures during the emergency response phase.

This module is implemented in five steps:

1. Integrated threat and risk analysis for all seven asset categories identified in *Module 1*, i.e., from *buildings* to *staff;*
2. Ranking of assets in terms of *damage minimization* and *business continuity*;
3. Ranking of specific security vulnerabilities for the most valuable corporate assets;
4. Scaling of risks in accordance with Table 1 below; and,

5. Prioritization of cost-efficient security upgrades by using different security-optimization tools (Annual Loss Expectancy (ALE); Return on Investment (ROI); Control Analysis (CA); Optimized Mitigation Strategy (OMS).

The use of such tools allows a cost-benefit consideration which leads to an increase of asset values for the whole organization. This increase in value can be communicated and considered for operational, marketing and financial use. Thereby this module contributes to mitigating casualties, minimizing damages to the corporate infrastructure, and restoring service to customers at the earliest time possible after a security-related incident.

Module 3 identifies *Corporate Responsibilities,* addressing:

1. Leadership, i.e., **c**ompliance with the legal environment (e.g., homeland security, data protection), implementing *Corporate Security Culture and Security Policy* (e.g., improving the human factor and its input in effective security and selecting technical and operational security measures to meet risk based performance standards);
2. Crisis management*,* i.e., financial loss (damaged corporate assets; claims by third parties; legal fines for neglecting risks; increased insurance premium); reputational damage (customers, authorities, share holders); loss of market share (national, international); loss of key personnel and know-how; loss of trust by public;
3. Business continuity, i.e. availability of key personnel (number, capability, motivation), access to operational redundancies (raw material supplies, buildings, production, transport, energy, water, communication), availability and support of First Responders (training, exercise, communication, and regular updates).

Security Issues for a LNG Terminal

In the following example selected parts of the ICSAP approach are demonstrated. It is assumed that the terrorist threat is a suicide boat attack on an LNG Terminal. A LNG Terminal represents an attractive target for terrorism due to the high energy density, large operational area, high degree of mobility (persons, traffic), and high media interest.

The basis for the threat assumption are:

1. In 2004 altogether 330 incidents were reported globally involving piracy and armed robbery against ships, of which over 110 happened against oil, gas, and petrochemical transport vessels;
2. The existence of several chokepoints for maritime oil and gas transport, such as the *Straits of Malacca,* where 50,000 vessels pass through annually, carrying 66 percent of the global LNG to China, Japan, and South Korea.

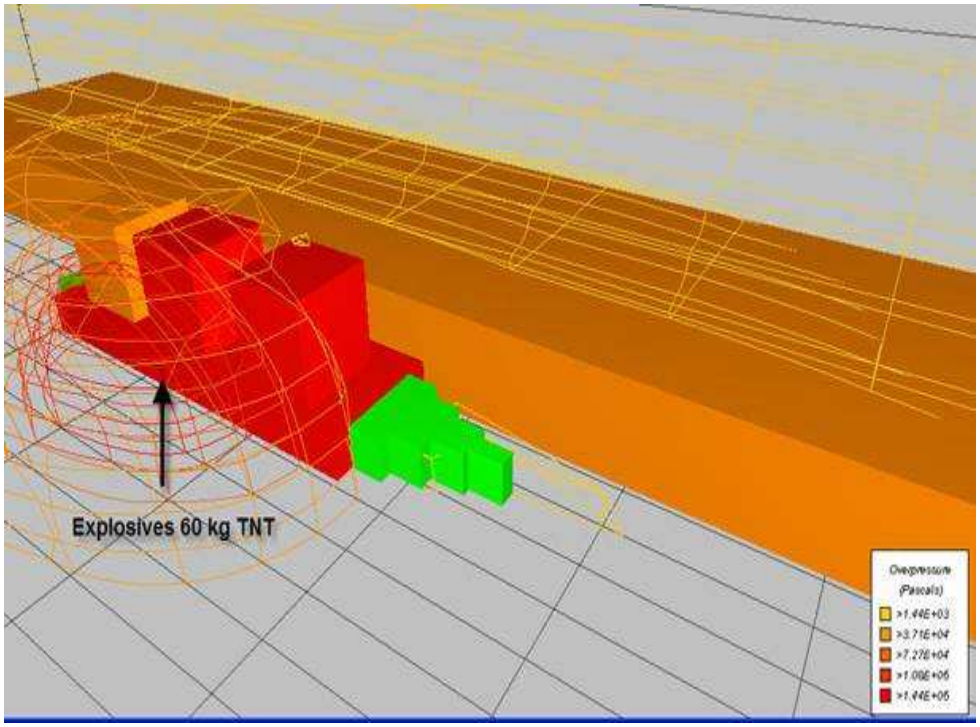
It is assumed that three high-speed boats, loaded with explosives (2000 kg TNT), ram the LNG tanker. Simultaneously additional terrorists attack the emergency response units approaching the scene of attack. During the attack the boats are driven against the vital parts of an LNG Terminal whilst LNG vessels are unloading their cargo. The attacking group consists of six terrorists motivated and trained as suicide attackers, receiving also insider support. The anticipated damage to be considered consists of primary damage (destruction of the LNG terminal, infrastructure and vessels present in the LNG terminal) and secondary damage (e.g., interruption of the supply chain, tightening of regulations, shut down of terminals by the government after massive media campaigns).

This mode of attack has multiple consequences:

1. Upon impact simultaneous rupture of two adjacent cargo tanks result in a spill (assumption: 200.000 m^3 in max 1 min partially vaporized);
2. At the pier vaporization and the existence of primary ignition sources leads to immediate ignition of vapour plume (temperature: > 1,600 C). This results in fatal thermal radiation (lower limit: 60 MJ/m^2, h)[4] within a radius of fatalities due to thermal radiation up to 300 m, respectively due to fatalities (blast energy) up to 3,000 m.

Figure 1 shows the impact (overpressure iso-curves) of a suicide attack on an LNG tanker docked at a terminal.

Figure 1: Structural damage (overpressure iso-curves) to an LNG tanker unloading at a terminal due to a terrorist attack using 60 kg of explosives



According to the latest Sandia report, based upon the worst credible intentional or accidental event release of 200,000 m^3 from two tanks of LNG, it was determined that a wind speed of 2 m/s resulted in the 'worst case' in which the flammable vapour cloud extended about 11.7 km downwind from the proposed offshore LNG Floating Storage and Regasification Unit.[5] The report determined 70,000 casualties could result from an offshore LNG tanker accident but none of the risk assessments even considered acts of sabotage or terrorism. A Lloyd's of London Insurance executive compared an LNG attack with a nuclear explosion.[6]

Risk reduction measures are comprised of a wide spectrum of countermeasures such as (examples only):

1. Lowering the probability of a suicide boat attack by adaptation of the threat assessment for an LNG port facility to include terror attacks and insider support, as well as application of the *Onion Skin Principle*, i.e., increasing layered security measures upon approach of the LNG tanker;

2. Improving emergency response capabilities of first responders by providing armed protection for emergency crews in order to enable them to carry out their response action also in the presence of terrorist on land;
3. Reducing *Insider threat* with a modular *Security Culture Training Course* for LNG-terminal staff members;
4. Improving port security through strengthening of the International Ship and Port Facility Security Code ISPS with realistic, practically applicable protocols.

Table 1: Scaling of security risks

Risk Factor	Scale
Volition	Voluntary-involuntary
Severity	Ordinary-catastrophic
Origin	Natural-man made
Effect manifestation	Immediate-delayed
Exposure pattern	Continuous-discrete
Controllability	Controllable-uncontrollable
Familiarity	Common-new hazard

Conclusions

It is impossible to protect *every* component of the oil and gas fuel cycle against *any* potential security threat in a cost-efficient manner. The ICSAP approach offers a possibility to assess the various components of corporate risk, enable management to prioritize risk and identify corporate responsibilities. This provides the basis for a rational decision-making process, leading to a cost-effective upgrading of currently available physical protection combined with strengthening of corporate security. Also ICSAP assists the oil and gas industry to communicate and demonstrate Security Culture and Policy in order to gain internal and public acceptance and respect for their safe and secure business and operation.

About the Author

P. Furthner is with TAAS Inc., Bad Voslau (Austria) and F. Steinhäusler is with the Division of Physics and Biophysics, University of Salzburg (Austria).

For more insights into contemporary international security issues, see our *Strategic Insights* home page. To have new issues of *Strategic Insights* delivered to your Inbox, please email ccc@nps.edu with subject line "Subscribe." There is no charge, and your address will be used for no other purpose.

References

1. See: F. Steinhäusler, P. Furthner, W. Heidegger, S. Rydell, L. Zaitseva, "Security Risks to the Oil and Gas Industry: Terrorist Capabilities," *Strategic Insights* VII, no. 1 (February 2008)

2. Statement by President Hugo Chavez as cited by Roger Howard, "Oil Price Warfare," *The National Interest*, September 2006, 85.

3. Statement by Ayatollah Ali Khameni as cited by *CNN International*, February 8, 2007.

4. 1 MJ = 948 British thermal units (BTU)

5. See Tim Riley, "LNG Vapor Cloud Danger To Our Communities," on *TimRileyLaw.com*; and "Liquefied Natural Gas (LNG)" on the website of the Federal Energy Regulatory Commission at *FERC.gov.*

6. This assertion, which is contested by industry experts, was made in a speech delivered by chairman Peter Levene to business leaders in Houston: "Gas carriers too, whether at sea or in ports, make obvious targets," said Levene. "Specialists reckon that a terrorist attack on an LNG tanker would have the force of a small nuclear explosion." (Mark Reynolds, "Lloyd's Executive Likens LNG Attack to Nuclear Explosion," *The Providence Journal,* September 20, 2004, archived online at *EnergyBulletin.net*.)