Security Assessment for Offshore Oil and Gas Assets

Prof. Nikitas Nikitakos
Iosif Progoulakis (PhD candidate)
Introduction

Aims:

- Prove the necessity for the implementation of Security Assessment in offshore oil and gas assets.

- Provide an overview of Security Assessment methodologies focusing in the most applicable to offshore oil and gas assets.

- Indicate the inter-disciplinary approach required for the Security Assessment of offshore oil and gas assets.

- Present an example of usage of a Security Assessment tool.
Security and Threats

-> Security Assessment: “...an evaluation of an asset’s characteristics to determine security threats, vulnerabilities and protective/mitigation measures.”

-> Threat: “... an indication, circumstance, or event with the potential to cause loss of or damage to an asset.”

-> Adversaries can be Insider, External or colluded.

-> Threat categories:
  > Terrorists (international or domestic)
  > Activists
  > Disgruntled employees or contractors
  > Criminals (cyber criminals, pirates)
  > Inter-state adversaries
World Security Incidents (1899-2018)

Source: M. Kashubsky, www.start.umd.edu
Information elaborated by authors.
Types of Security Incidents (1899 - 2018)

- Kidnapping: 25
- Armed intrusion: 28
- Armed assault: 11
- IEDs: 11
- Navy attack: 6
- Unauthorised boarding: 10
- Physical attack: 3
- Theft: 3

Source: M. Kashubsky, www.start.umd.edu, Information elaborated by authors.
Effects of Security Incidents

- Injury or death of personnel
- Damage or loss of assets
- Pollution to the environment
- Disruption of oil and gas production operations
- Disruption of oil and gas supply to the market
- Loss of income for companies
- Increase of oil prices
- Effect on global economies and stock exchange
Security Challenges

- Offshore installations are isolated assets.
- Seizure of an offshore platform offers tactical advantages to the intruders due to the difficulties that the security forces would have in mounting an assault.
- IEDs can be planted in various locations maximizing a domino effect if exploded.
- Offshore platforms are complex industrial facilities with the presence of chemical processing equipment and facilities as well as hazardous materials.
- Limited ways of evacuation of platforms via helicopter or ship transfer, depended on weather conditions.
- Attacks on Offshore platforms can cause petroleum and hazardous materials leaks that can lead to environmental catastrophe.
- Offshore installations involve both maritime and chemical processing operations.
- Effects of attacks on Offshore platforms are difficult to contain and can lead to partial or complete destruction of the facilities.
Security Assessment

- Threat
- Vulnerability
- Risk
- Security Assessment

“Macro”-Scale

“Micro”-Scale
Security Assessment Approaches

Maritime Security

SSA/PFSA → ISPS
- MSRAM (Maritime Security Risk Analysis Model) → USCG

Industrial Security

- SRA/SVA → API STD 780, API RP 70, API RP 70I
- VAM-CF
- FVIKOR
- PRAF
- Prototype VAM → DOE, DOJ, SANDIA

CIP
Critical Infrastructure Protection

- RAMCAP → US DHS/ASME ITI LLC
- MBVA /MBRA → NPS
- CIMS
- DECRIS
- CARVER
- CRISRRAM → EC - JRC
- CIPDSS
- CIPMA
- BIRR
- RVA
- NSRAM
- NEMO
- N-ABLE
- MDM
- MIN
- FAIT
- EURACOM
- COUNTERACT
- SSA/PFSA → ISPS
- MSRAM (Maritime Security Risk Analysis Model) → USCG
- SRA/SVA → API STD 780, API RP 70, API RP 70I
- VAM-CF
- FVIKOR
- PRAF
- Prototype VAM → DOE, DOJ, SANDIA
- RAMCAP → US DHS/ASME ITI LLC
- MBVA /MBRA → NPS
- CIMS
- DECRIS
- CARVER
- CRISRRAM → EC - JRC
- CIPDSS
- CIPMA
- BIRR
- RVA
- NSRAM
- NEMO
- N-ABLE
- MDM
- MIN
- FAIT
- EURACOM
- COUNTERACT
Aim: “... to enhance maritime security at sea and at port focusing in the protection against terrorists, pirates & stowaways.”
SSA – PFSA (ISPS Ship- and Port Facility- Security Assessment)

 Existing security measures, procedures, operations.
 Critical asset operations
 Threats for critical asset operations
 Incident likelihood
 New security measures
 Vulnerabilities

 Physical Security
 Structural Integrity
 Personnel Protection Systems
 Procedural Policies
 Communication Systems
 Asset infrastructure
 Utilities

“…a subjective risk analysis of all aspects of the operation in a port or ship to determine vulnerabilities and likelihood of a terrorist attack…”
MSRAM (Maritime Security Risk Analysis Model)

“MSRAM was designed to identify and prioritize critical infrastructure, key resources and high consequence scenario’s across sectors using a common risk methodology, taxonomy and metrics to measure security risk from terrorism at the local, regional and national levels.”

<table>
<thead>
<tr>
<th>Mission</th>
<th>MSRAM Assessment Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent terrorist attacks within the United States.</td>
<td>Assess terrorist intent and capability to focus resources to deter and interdict attacks.</td>
</tr>
<tr>
<td>Reduce America’s vulnerability to terrorism.</td>
<td>Assess ability of owner/operator, local law enforcement, and USCG forces to protect targets.</td>
</tr>
<tr>
<td>Minimize the resulting damage if prevention fails.</td>
<td>Assess ability of owner/operator, local first responders, and USCG forces to respond to attacks that do happen.</td>
</tr>
<tr>
<td>Recover from attacks that do occur. Insure economic security.</td>
<td>Estimate the primary and secondary economic impacts of the scenario considering the recoverability and redundancy of the system.</td>
</tr>
</tbody>
</table>
The API has developed standards applicable to the security assessment of offshore oil and gas assets and operations implementing the Security Risk and Vulnerability Assessment (SRA/SVA) methods.
“Security risks should be managed in a risk-based, performance-oriented management process to ensure the security of assets and the protection of the public, the environment, workers, and the continuity of the business.”

1. Analyze assets and criticality.
   Screen Assets on consequence.
   Identify Critical Assets.

2. Analyze threats and asset attractiveness.
   Determine target assets.

3. Conduct scenario analysis.
   Determine act-specific consequences and vulnerability.

4. Assess risk against security criteria.

5. Evaluate security upgrades as required.
   Determine residual risk.
API SVA (API RP 70 and API RP 70I)

“...a secondary evaluation that examines a facility’s characteristics and operations to identify potential threats or vulnerabilities and existing and prospective security measures and procedures designed to protect a facility.”

- **STEP 1: Potential Threat**
  - Company policy that defines security goals and commitments including and control of SSI.

- **STEP 2: Consequence Assessment**
  - Communication protocol with authorities for emergency preparedness, assessment and reporting of security issues.

- **STEP 3: Vulnerability Assessment**
  - Security Plan, Company Security Officer (CSO) and Facility Security Officer (FSO).

- **STEP 4: Mitigation**
  - Integration of HSAS and MARSEC Security Levels rankings into offshore and company operations.

- **STEP 5: Implementation**
Developed to support US-DHS in the definition of a common framework for the assessment of vulnerability from terrorist acts.

Designed to provide comparable results across infrastructure assets and sectors in order to prioritize risk across the critical infrastructure.

Aimed at the identification of an efficient and consistent mechanism of reporting essential risk information to US-DHS, to be applied to both private and governmental sectors.
MBVA (Model-Based Vulnerability Assessment)

Simple → Identify asset network and hubs. Reduce asset complexity and identify criticality.

Standardized → Quantify threats by identifying the faults and likelihoods.

Quantified → Achieve thorough analysis of asset components and fault/failure combinations.

Rational → Develop mitigation strategy. Justify budget expenditure (CAPEX/OPEX).

OUTPUT
- Node Histogram
- Critical nodes (hubs)

OUTPUT
- Fault Tree

OUTPUT
- Threats

OUTPUT
- Budget Allocation
- Strategy

\$
CRISRRAM (CRitical Infrastructures & Systems Risk and Resilience Assessment Methodology)

It adopts a system of systems approach and aims to address issues at asset level, system level and society level.

It follows an all-hazards approach.

Developed considering gaps of existing Risk Assessment methods in the industry.

Developed to be applicable nationally and internationally for EU states.
Security Levels

→ Implementation of Security Assessment measures to contain incidents and maintain desired security levels.

→ Security level enables for preemptive planning and proactive implementation of preventive security measures.

<table>
<thead>
<tr>
<th>HSAS (Homeland Security Advisory System)</th>
<th>MARSEC (Maritime Security)</th>
<th>ISPS</th>
<th>API STD 780</th>
<th>API RP 70</th>
<th>API RP70I</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW: Green</td>
<td>LEVEL 1: Maintained at all times</td>
<td>LEVEL 1: Very Low</td>
<td>LOW: Green</td>
<td>LEVEL 1: Minimal risk of threat</td>
<td></td>
</tr>
<tr>
<td>GUARDED: Blue</td>
<td>LEVEL 2: Low</td>
<td>LEVEL 2: Low</td>
<td>GUARDED: Blue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ELEVATED: Yellow</td>
<td>LEVEL 3: Medium</td>
<td>LEVEL 3: Medium</td>
<td>ELEVATED: Yellow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIGH: Orange</td>
<td>LEVEL 2: Maintained for a period of time as a result of heightened risk</td>
<td>LEVEL 4: High</td>
<td>HIGH: Orange</td>
<td>LEVEL 2: Heightened risk of security incident</td>
<td></td>
</tr>
<tr>
<td>SEVERE: Red</td>
<td>LEVEL 3: Maintained for a limited period of time</td>
<td>LEVEL 5: Very High</td>
<td>SEVERE: Red</td>
<td>LEVEL 3: imminent security incident</td>
<td></td>
</tr>
</tbody>
</table>

Source: API with information elaborated by authors.
Quantitative and Qualitative process safety review can define risks, hazards and consequences of security incidents in offshore oil and gas systems, equipments, processes and operations.

Source: ABS with information elaborated by authors.
Assessment Tools: Bow-Tie Analysis

Utilize bow-tie analysis for the identification of security barriers and measures for assets in the micro- and macro- scales.

Source: ABS with information elaborated by authors.
Why Bow-Tie Analysis?

"By linking ‘Hazards’ & ‘Consequences’ to an ‘Event’ it is possible to develop the relationship to include the causes, or ‘Threats’, and the ‘Prevention’ & ‘Recovery Measures’”  (ABS)

→ Simple & pragmatic approach
→ Emphasis on effectiveness of risk reduction measures
→ Effective visualization
→ Allows better communication of hazards
→ Can be applied for all types of hazards
→ Increasingly becoming the preferred techniques by regulatory bodies & leading companies
→ Efficiently aided by user-friendly software
Bow-Tie Example
Bow-Tie Example

**TOP EVENT:** LOSS OF VALVE ASSEMBLY

**Hydrocarbons**

**Threats**
- Armed intrusion
  - + Prevention Barriers
    - Armed guards
    - Intelligence gathering
    - Sensors (EHSS)
- IEDs
  - + Prevention Barriers
    - Proactive security screening
    - Prioritisation of asset locations for security searches
    - IED field detection
    - System sensors

**Consequences**
- Red: Loss of control of valve assembly
  - + Mitigation Barriers
    - Physical barriers
    - Control segmentation
    - Control recover procedures
- Red: Catastrophic failure of valve assembly
  - + Mitigation Barriers
    - Process segmentation
    - Blast proof barriers
    - Fire protection system - Localised
    - Emergency planning
Research - Next Steps

Current status:
→ Selection of security risk analysis method.
→ Compilation of state of the art for security analysis methods in the offshore oil and gas sector.

Next steps:
→ Check implementation issues of selected risk analysis method.
→ Validation of experimental methodology based on selected risk analysis method.

Aims:
→ Study the interaction of components and assets in security breach scenarios and subsequent domino effect propagation.
→ Develop methodologies and tools for assessing and managing the process hazards and vulnerability risks due to security incidents in the offshore oil and gas assets.
Thank you for your attention

Prof. Nikitas Nikitakos: nnik@aegean.gr
Mr. Iosif Progoulakis (PhD Candidate): iprogoulakis@aegean.gr