Do provisions to advance chemical facility safety also advance chemical facility security? - An analysis of possible synergies

Hedlund, Frank Huess

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):
Background

The Directive on European Critical Infrastructures (ECI Directive) addresses facility security but does not cover the chemical sector. Some Member States went beyond the minimal requirements of the Seveso II Directive and established additional security-relevant elements or launched special initiatives.

Suggestion that perhaps 80% of the existing safety measures under Seveso-II Directive would also be instrumental in terms of raising security.

The Directive on European Critical Infrastructures (ECI Directive) addresses facility security. This does not cover the chemical sector.

Possible synergies?

- An analysis of chemical facility safety also advance chemical facility security.
- Do provisions to advance chemical industry safety provisions also enhance security of chemical facilities.

Result: The European Commission launched a study on the applicability of existing national initiatives directive and established additional security-relevant elements or launched special initiatives.

Covers the situation in 18 EU Member States.
This presentation

Safety and security

Security Risk = Threat × Vulnerability × Impact

Safety and security

Security relates to acts of malevolence, safeguarding an asset from unauthorized access and crime. For a high-risk chemical facility, many security measures will relate to preventive safety analysis aimed at identifying vulnerabilities in the design and control philosophy. In particular situations in which the failure of a single component could lead to an excursion of the permissible design parameters, the degree of protection against danger, damage, loss, and crime is the degree of protection against malevolence.

Safety Risk = Likelihood of accident × Consequence

The key distinction between safety and security relates to malicious intent.

Examine differences, synergies

Define security, safety

Preliminary analytical findings regarding the extent to which existing provisions have been put into existence to advance safety objectives have not been expected to advance security objectives as well.
### Security Framework – Selected Elements

<table>
<thead>
<tr>
<th>Facility</th>
<th>Facilities with high-risk chemicals present</th>
<th>Facilities with high-risk chemicals that are targets in themselves</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intrusion detection</strong></td>
<td>Intrusion detection system and alarm</td>
<td>Intrusion detection system and alarm</td>
</tr>
<tr>
<td><strong>Security presence</strong></td>
<td>Security personnel</td>
<td>Security personnel</td>
</tr>
<tr>
<td><strong>Personnel vetting</strong></td>
<td>Basic personnel vetting (background check of employees, check of contractors)</td>
<td>Basic personnel vetting (background check of employees, check of contractors)</td>
</tr>
<tr>
<td><strong>Inventory control and response</strong></td>
<td>Procedures that identify, investigate, and resolve shortages</td>
<td>Procedures that identify, investigate, and resolve shortages</td>
</tr>
<tr>
<td><strong>Procedures for preservation of forensic evidence</strong></td>
<td>Procedures for preservation of forensic evidence</td>
<td>Procedures for preservation of forensic evidence</td>
</tr>
<tr>
<td><strong>Security management system (SMS)</strong></td>
<td>Security management system (SMS)</td>
<td>Security management system (SMS)</td>
</tr>
<tr>
<td><strong>Behavioural barriers</strong></td>
<td>Personal, security, and access control</td>
<td>Personal, security, and access control</td>
</tr>
<tr>
<td><strong>Forensics and security</strong></td>
<td>Forensics and security</td>
<td>Forensics and security</td>
</tr>
<tr>
<td><strong>Security plan</strong></td>
<td>Security plan (approved)</td>
<td>Security plan (approved)</td>
</tr>
<tr>
<td><strong>Security management system (SMS)</strong></td>
<td>Security management system (SMS)</td>
<td>Security management system (SMS)</td>
</tr>
<tr>
<td><strong>Intrusion detection system and alarm</strong></td>
<td>Intrusion detection system and alarm</td>
<td>Intrusion detection system and alarm</td>
</tr>
<tr>
<td><strong>Security personnel</strong></td>
<td>Security personnel</td>
<td>Security personnel</td>
</tr>
<tr>
<td><strong>Basic personnel vetting (checklist)</strong></td>
<td>Basic personnel vetting (checklist)</td>
<td>Basic personnel vetting (checklist)</td>
</tr>
<tr>
<td><strong>Procedures that identify, investigate, and resolve shortages</strong></td>
<td>Procedures that identify, investigate, and resolve shortages</td>
<td>Procedures that identify, investigate, and resolve shortages</td>
</tr>
<tr>
<td><strong>Procedures for preservation of forensic evidence</strong></td>
<td>Procedures for preservation of forensic evidence</td>
<td>Procedures for preservation of forensic evidence</td>
</tr>
<tr>
<td><strong>Security management system (SMS)</strong></td>
<td>Security management system (SMS)</td>
<td>Security management system (SMS)</td>
</tr>
<tr>
<td><strong>Behavioural barriers</strong></td>
<td>Personal, security, and access control</td>
<td>Personal, security, and access control</td>
</tr>
<tr>
<td><strong>Forensics and security</strong></td>
<td>Forensics and security</td>
<td>Forensics and security</td>
</tr>
<tr>
<td><strong>Security plan</strong></td>
<td>Security plan (approved)</td>
<td>Security plan (approved)</td>
</tr>
<tr>
<td><strong>Security management system (SMS)</strong></td>
<td>Security management system (SMS)</td>
<td>Security management system (SMS)</td>
</tr>
</tbody>
</table>

(SVA = Security Vulnerability Assessment)
Safety framework (excerpt) – which security elements covered?

- **Safety provision**
  - Interpretation of typical scope
  - Assessment of security elements
  - (potentially) covered

**Safety provision**

- **Safety strategy and control framework**
  - Interpretation of typical scope
  - Assessment of security elements
  - (potentially) covered

**Safety strategy and control framework**

- **Typical control elements**: management of change (MOC) not to introduce errors into the design; a permit to work (PtW) system to coordinate tasks and manage staff; a mechanical integrity program (including corrosion monitoring); etc.
- **Concerns**: prevention of accidental (unintentional) events.

**Security elements not covered**

- **Hazard identification and risk assessment**
  - The result of a hazard identification is a list of potential concerns.
  - A hazard identification step is the starting point for a risk assessment. Employed frequency analysis, assuming random failure of components.
  - Approach not applicable for security.

**Security elements not covered**

- **Inspections, audits, reviews**
  - Typical inspections deal with workplace tidiness, mechanical integrity, corrosion monitoring.
  - Security elements not covered.

- **Typical audits**
  - Relate to adherence to permit to work procedures, if preventive systematic risk reviews have been carried out, if checklists used, if procedures before entry into confined space adhered to.
  - Security elements not covered.

- **Typical technical reviews**
  - Relate to overpressure protection, liquid hammer, adequate capacity of blow down facilities, passive fire protection.
  - Security elements not covered.
Safety provision Interpretation of typical scope Assessment of security elements (potentially) covered

Land-use Planning Good land use planning keeps communities away from hazardous installations
Very clear overlap with security

Emergency preparedness, response and planning
Emergency preparedness aims to mitigate the effects of a release, regardless if it is intentional or accidental
Overlap with security (depends on scenario)

Communication with and information to the public
General knowledge, enables citizens to take adequate protective measures in case of a toxic release
Very clear overlap with security, beneficial both for accidental and intentional releases of toxic chemicals.

Germany has developed a security concept and methodology known as the Basisschutzkonzept (Baseline Protection Concept) which aims to provide guidelines for infrastructure operators to develop protection measures.
Recommendations focus both on the methodology for adopting protection measures and on minimum protection requirements.
A sample checklist is provided to assist private sector operators in completing their infrastructure protection plans in practice.

Baseline Protection Concept

Which security elements covered? - Safety framework (excerpt)
Synergy, safety, security 8 November 2012 Analytical framework

Security framework (baseline protection concept) – any safety elements covered?

Basic barrier diagram

- any safety elements covered? Security framework (baseline protection concept)
8 NOVEMBER 2012 SYNERGY, SAFETY, SECURITY

Mapping overlaps

POLICY LEVEL
PREVENTION measures
MITIGATION measures
Strategic measures

Safety
- (safety) risk analysis
- redundancy: technical, organizational
defs-in-depth
- mechanical integrity programme
- permit-to-work system
- management of change
- onsite emergency response (limit release)

Chemical safety:
- public aware of danger and countermeasures
- Eliminate, substitute
- offsite emergency response, evacuation (limit exposure)
to less toxic chemical

Process safety:
- inherently safer design
- attenuate process conditions, reduce inventories

Security
- vulnerability analysis
- land use planning (security)
- prevention (SVA)
- emergency physical protection, access restrictions
- workplace inspections, (security risk assessment)
audits, technical reviews
- vetting of employee, contractor
- community right-to-know
- cyber
- keep under lock

Malicious intent

Toxic release
- loss of containment (LOC)
- consequences
- equipment malfunction, human error
- malicious

Consequences
- evacuation
- isolation
- containment
- emergency response
- cleanup

Equipment

Prevention measures
- safety policy, plan
- safety control framework (MOC, PTW)
- management of change (MOC)
- contractor management (evaluation, training, control)
- Emergency physical protection, access restrictions
- workplace inspections, (security risk assessment)
audits, technical reviews
- vetting of employee, contractor
- community right-to-know
- cyber
- keep under lock

MOC - management of change
LUP - land use planning

7

Strategic measures

Prevention measures

Administration of the information security management system
- report, act on, mitigate
- limit exposure
- control, prevent
- achieve objectives
- risk management, target setting
- prevention, detection, response

Worker Health, Safety, Security
- vulnerability
- emergency planning
- training (infection control)
- infection control
- health management
- air sampling
- surveillance
- disposal
- education
- health surveillance
- health
- control
- emergency response
- insurance
- training
- infection control
- worker
- employee
- doctor
- patient
- nurse
- emergency
- administration
- risk management
- targets
- prevention
- response
- follow-up

Chemical facility security legislation
- intentional malevolence
- scope: unintentional events

Chemical workplace safety legislation
- worker protection
- scope: unintentional events

Safety policy, plan
- safety control framework (MOC, PTW)
Thank you for your attention!