Security at chemical facilities – overview of different regulatory approaches taken in EU Member States

RISK 2017
The Nordic Chapter of the Society for Risk Analysis (SRA) Conference
Aalto University, Espoo, Finland, November 2-3, 2017.

Frank H Hedlund
Risk expert, COWI, Denmark
Ext. associate professor Technical University of Denmark

Background

› It is a European Union policy goal to enhance high-risk chemical facility security. This presentation presents some results of a study carried out for the European Commission, DG Home Affairs.
› The study aimed to provide an overview of existing provisions and measures that help to enhance security at chemical facilities.
› These provisions and measures may for instance have their background in safety legislation or non-regulatory initiatives implemented by industry or in specific legislative provisions targeting security aspects.
Situation

- The Directive on European Critical Infrastructures (ECI Directive) addresses facility security but does not cover the chemical sector.
- Chemical facility safety at EU level is addressed by way of the Seveso-II (III) Directive.
- Suggestion that perhaps 80% of the existing safety measures under Seveso-II would also be instrumental in terms of raising security.
- EU study on the applicability of existing chemical industry safety provisions to enhancing security of chemical facilities.

This presentation

- Key terms - Safety vs security
- Overlaps and synergies – key findings
- Key findings from Member State Survey
Safety and security

- The key distinction between safety and security relates to malicious intent
- Preventive safety analysis aims at identifying vulnerabilities in the design and control philosophy
- Security is the degree of protection against danger, damage, loss, and crime

Result:
Study finds rather limited overlaps and synergies between safety and security

Security – two types of facilities and concerns

<table>
<thead>
<tr>
<th>Security concern</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>Theft</td>
<td>of HRC material, to be used elsewhere for malicious activities</td>
<td>Attack - with destructive force, intentional release of HRC onsite</td>
</tr>
<tr>
<td>Attack</td>
<td>with destructive force, intentional release of HRC onsite</td>
<td></td>
</tr>
<tr>
<td>Number of facilities</td>
<td>Many – small and medium sized enterprises (SMEs), even university laboratories, (transportation chain),</td>
<td>Few - often Seveso installations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

HRC - High Risk Chemicals
High-risk chemicals are in principle those that are expected to be relevant in relation to terrorist activities

Seveso installations – covered by the EU Seveso Directive (safety)
### Security framework – selected elements

<table>
<thead>
<tr>
<th>Facility</th>
<th>Facilities with high-risk chemicals present (theft)</th>
<th>Facilities with high-risk chemicals that are targets in themselves</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concern</td>
<td>Theft of HRC material</td>
<td>Attack with destructive force, intentional release of HRC onsite</td>
</tr>
<tr>
<td>Formalism, documentation</td>
<td>Security plan (prepared)</td>
<td>Security management system (SMS)</td>
</tr>
<tr>
<td>Perimeter</td>
<td>Fencing</td>
<td>Fences and gates, access control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vehicle barriers</td>
</tr>
<tr>
<td>Building</td>
<td>Secured, under lock</td>
<td>Target hardening</td>
</tr>
</tbody>
</table>

HRC - High Risk Chemicals  
SVA = Security Vulnerability Assessment
### Safety framework (excerpt) – with security elements covered

<table>
<thead>
<tr>
<th>Safety provision</th>
<th>Interpretation of typical scope</th>
<th>Assessment of security elements (potentially) covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety policy</td>
<td>Example: To prevent accidents and provide adequate control of risks; to provide adequate training; to engage and consult with employees, etc,</td>
<td>Concerns prevention of accidental (unintentional) events. Security elements not covered</td>
</tr>
<tr>
<td>Safety Strategy and Control Framework</td>
<td>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</td>
<td>Concerns prevention of accidental (unintentional) events. Security elements not covered</td>
</tr>
<tr>
<td>Hazard Identification and Risk Assessment</td>
<td>The result of a hazard identification is a list of potential concerns. Risk assessment employ frequency analysis, assuming random failures of components</td>
<td>A hazard identification step is the starting point for a list of possible targets - security overlap. Approach not applicable for security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Safety provision</th>
<th>Interpretation of typical scope</th>
<th>Assessment of security elements (potentially) covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation management, roles and responsibilities</td>
<td>Safe organisation means having necessary resources, qualified staff, and sound division of roles and responsibilities, e.g. separating the responsibility for the inspection and maintenance unit</td>
<td>Security elements not covered</td>
</tr>
<tr>
<td>Inspections, audits, reviews</td>
<td>Typical inspections deal with workplace tidiness, mechanical integrity, corrosion monitoring</td>
<td>Security elements not covered</td>
</tr>
<tr>
<td></td>
<td>Typical audits relate to adherence to permit to work procedures, if preventive systematic risk reviews have been carried out, if checklists used, procedures before entry into confined space adhered to</td>
<td>Security elements not covered</td>
</tr>
<tr>
<td></td>
<td>Typical technical reviews relate to overpressure protection, liquid hammer, adequate capacity of blow down facilities, passive fire protection</td>
<td>Security elements not covered</td>
</tr>
</tbody>
</table>
# Safety framework (excerpt) – which security elements covered?

<table>
<thead>
<tr>
<th>Safety provision</th>
<th>Interpretation of typical scope</th>
<th>Assessment of security elements (potentially) covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Land-use Planning</td>
<td>Good land use planning keeps communities away from hazardous installations</td>
<td>Very clear overlap with security</td>
</tr>
<tr>
<td>Emergency preparedness, response and planning</td>
<td>Emergency preparedness aims to mitigate the effects of a release, regardless if it is intentional or accidental</td>
<td>Overlap with security (depends on scenario)</td>
</tr>
<tr>
<td>Communication with and information to the Public</td>
<td>General knowledge, enables citizens to take adequate protective measures in case of a toxic release</td>
<td>Very clear overlap with security, beneficial both for accidental and intentional releases of toxic chemicals.</td>
</tr>
</tbody>
</table>

## Overview of overlaps and synergies

- **Major accident hazard legislation** (scope: unintentional events)
  - Safety policy, plan
  - Safety control framework (MOC, PTW)
  - Safety risk assessment
  - Contractor management (evaluation, training, control)
  - Workplace assessments, audits, technical reviews
  - Community right-to-know

- **Chemical facility security legislation** (scope: intentional malevolence)
  - Security policy, plan
  - Resolve inventory shortages
  - Reporting of theft
  - Physical protection, access restrictions
  - Security vulnerability analysis (SVA)
  - Security risk assessment
  - Vetting of employees, contractor
  - Keep under lock

- **Chemical workplace safety legislation** (scope: worker protection)
  - Workplace assessment
  - Employee training, instruction, knowledge
  - Personal protective equipment
  - Employee consultations

- **Major accident hazard legislation**
  - Gates, guards, guns
  - Deter, detect, delay, deny

- **Chemical facility security legislation**
  - Management of change (MOC)
  - Permit to work (PTW)
  - Land use planning (LUP)

- **Chemical workplace safety legislation**
  - Hazard identification
  - Emergency plans
  - Plan, workplace inspections, audits, technical reviews
  - Cyber security

- **Employee consultations**
  - Community right-to-know
Key findings from Member State Survey

Germany, Latvia (and Denmark in 2016) – folding security into Seveso Safety Report

- Germany has implemented a broadened version of the Seveso II Directive
- Federal Act defines an incident (Störfall) as a hazardous event that could arise from either 1) technological breakdowns or other accidental causes, 2) from natural causes like earthquakes, or 3) from intentional acts.
- Yet, the questionnaire reply from Germany indicates that specific security provisions are mostly absent. No provisions for fencing, vulnerability analysis, etc. Connects to the Seveso concept of taking "necessary precautions".
- Latvia’s extended interpretation of Seveso II Directive: causes of accidents "being external to the establishment" (earthquakes, domino from neighbour company) – includes intentional acts. In the Safety Report the company shall therefore demonstrate that appropriate security counter measures have been taken.
Austria – folding HRC Seveso sites into Critical Infrastructure Protection

› We identified no explicit requirement in the Austrian Programme for Critical Infrastructure Protection (APCIP) that would cover Seveso II sites with inventories of toxic chemicals.

› In practice however, most sites appear to be subject to APCIP.

› This implies that physical protection measures, Operator Security Plans, as defined in Critical Infrastructure Protection legislation are implemented for these enterprises. Although the main focus of the APCIP list is on "loss of service" meaning that the main concern is that these enterprises cannot supply their customers with their respective products or services, public safety is indirectly covered.

Poland - chemical facility security addressed in existing national security provisions

› In Poland, extensive security legislation in place with broad provisions. Security Act on the protection of people and property covers a wide range of activities, including, facilities which are essential for the functioning of urban areas or whose destruction or damage may pose a threat to human life and health and the environment.

› The Act permits enterprises to set up or hire armed private internal security service, which in principle could exercise lethal force.

› Only partial picture of practical implementation. Authorities at the provincial level (Voivodship) carry out a risk assessment procedure and apparently the result is processed as an administrative decision. Details are confidential.

› We conclude that a legal basis to demand extensive security precautions exists at the same time providing a measure of implementation flexibility allowing local provinces to interpret and determine what facilities the Act should cover.
United Kingdom (The Netherlands) – partnership with industry associations

- Minimal security provisions in place for establishments which are not classified as critical national infrastructure.
- Instead, industry associations are extensively involved in the preparation of guidelines and best practices which the industry association then recommends their members to follow.
- Very important for a company to maintain membership of industry associations, to maintain its reputation as a responsible company.
- To support implementation, extensive advice and support provided at the local level, network of specialist police advisers known as Counter Terrorism Security Advisers.
- Penetration difficult to assess - because agreements are voluntary and self-imposed, and because the enforcement mechanism is unclear.

CEFIC - Responsible Care Security Code

- Many Member States identified the chemical industry’s global initiative, the Responsible Care Programme, and specifically its Security Code Addendum as a relevant voluntary practice.
- CEFIC’s role is to advance Responsible Care in Europe promoting and ensuring consistency of implementation by national member federations. At the national level, each CEFIC member federation is responsible for developing and running its own national Responsible Care programme with its member companies, and for overseeing implementation by those companies.
- It has not been possible to further examine the penetration of the Responsible Care Programme, and specifically its Security Code Addendum in industry.
Identified security gaps for high-risk chemical facilities considered most important

<table>
<thead>
<tr>
<th>Facilities with small amounts of high-risk chemicals present (thief)</th>
<th>Facilities with high-risk chemicals present that are targets in themselves</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appointing security responsible, primarily to address basic facility theft protection and inventory management</td>
<td>Appointing security responsible to address issues listed below</td>
</tr>
<tr>
<td>Reporting inventory shortages</td>
<td>Reporting inventory shortages</td>
</tr>
<tr>
<td></td>
<td>Carrying out vulnerability assessment and addressing identified vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>Cyber security (currently unaddressed)</td>
</tr>
</tbody>
</table>

Additional information

› on synergies

› on inclusion of security in Danish Seveso III legislation