Gas Infrastructure Europe (GIE) is an association representing the interests of European natural gas infrastructure operators active in natural gas transmission, storage and LNG regasification. GIE is a trusted partner of European institutions, regulatory bodies and industry stakeholders. It is based in Brussels, the heart of European policymaking. GIE currently represents 68 member companies from 25 countries.

**Introduction**

Gas Infrastructure Europe (GIE) is an association representing the interests of European natural gas infrastructure operators active in natural gas transmission, storage and LNG regasification. GIE is a trusted partner of European institutions, regulatory bodies and industry stakeholders. It is based in Brussels, the heart of European policymaking. GIE currently represents 68 member companies from 25 countries.

**Background**

Natural gas is an essential component of the energy mix of the European Union (EU), constituting one quarter of primary energy supply and contributing mainly to electricity generation, heating, feedstock for industry and fuel for transportation. Gas infrastructure forms a network without national boundaries, which means that a failure of one portion of the network could propagate to other areas, potentially involving several countries.

The European Commission has identified the gas infrastructure as a critical infrastructure and this leads to the need of a common basic security risk level of this network across Europe. To reach this goal, the first step is the definition of a common Security Risk Assessment Methodology.
Gas Infrastructure Security

The GIE benchmark ("Security standards and practices of Gas Infrastructure companies – Benchmark results") shows that most of gas companies adopt a comprehensive approach that covers different security requirements. However, they lack a common methodological framework that can help them to address issues common to the gas operators and that can be used as a reference.

The European Gas Transmission Network

The physical threats - from terrorism to boycotts and strikes, disruptive natural events, earthquakes, floods, very cold periods, big storms - and commercial disputes to which the European network is subject, make it vulnerable and may jeopardise Europe’s secure access to gas.

An illustrative example of the effects of a disruption of the gas network is the Brotherhood pipeline case of 2009. This pipeline, which transports almost 300 million cubic metres of Russian gas every day to Europe, passing through Ukraine, started reducing its flow in early January, leading to a complete shutdown. This disruption had a significant impact on many Member States, in particular those that depend exclusively on this supply route, leaving homes without gas for heating and forcing production stops in some industries. Gas supplies were only fully restored on 21 January 2009. This disruption was the most serious of its kind in Europe in recent history: for an unprecedented period of two weeks, Europe was cut off from 30% of its total gas imports, an equivalent of 20% of its gas supplies on an annual basis.

The need for coordination of risk assessment at European level is therefore clear, and is recognised by Gas Infrastructure Europe (GIE), representing European gas infrastructure operators.

GIE has expressed its support for the EPCIP programme1 and developed in collaboration with KPMG Advisory S.p.A., a common methodology for risk/threat assessment in Europe for gas sector infrastructures, taking an all-hazard approach.

This methodology is in line with the prevention and response coordination implemented in the gas sector under Regulation (EU) Nr 994/2010, in particular the preparation of the national risk assessment and the preventive action and emergency plans to be developed on the basis of the risk assessments.

---


---

Image courtesy of Energinet.dk
GIE has defined, in collaboration with KPMG Advisory S.p.A., a security risk assessment methodology to help European gas infrastructure operators to assess the risks/threats on their assets in order to achieve the delivery of focused and cost-effective risk mitigation measures.

GIE has taken into account the necessity to create standards to ensure a level-playing field for security management. The security risk assessment phase is of central importance to security management, providing the basis on which to determine the type, nature and severity of security risks faced by the owner/operator's gas infrastructure assets and the wider European gas infrastructure network.

The GIE Security Risk Assessment Methodology is a common and integrated approach, amongst the European energy infrastructure operators, to assess the highest threats of failure and highest potential consequences to the safety of the public and industry workers, the environment, and production of gas infrastructure (facilities, systems, and components).

With this methodology a major step to further increase security and resilience of the gas infrastructure network in Europe has been achieved. It is another example of the active participation and contribution of gas infrastructure operators to EPCIP, the European Program for Critical Infrastructure Protection.

The GIE Security Risk Assessment Methodology is accessible to all GIE members, ENTSOG (the European Network of Transmission System Operators for Gas) and all other stakeholders interested in this field. It was presented to representatives of the European Commission and introduced to ENTSO-E, the European Network of Transmission System Operators for Electricity.

Since 29 July 2014 the GIE Security Risk Assessment Methodology is published on the GIE website for further spread and knowledge exchange:

www.gie.eu/index.php/publications/gie

The documentation consists of a detailed description, a Risk Assessment Tool and a summary of the Methodology in the form of a presentation.
The GIE Security Risk Assessment Methodology follows an “asset approach” focusing on the identification, analysis, evaluation of the risks that have impact on the assets and on their components.

The GIE Security Risk Assessment Methodology is applicable\(^2\) to the assets described in the picture below.

\(^2\) Even though the pipelines are originally out of scope, the methodology could also be applicable to that kind of assets.
The GIE Security Risk Assessment Methodology, developing the management processes defined in the ISO 31000 Risk Management, represents a tool for the risk management framework and considers the heterogeneity of the European gas companies (in terms of size, distribution on the network, etc.), the common objectives in complying the EC directives and the protection requirements of the gas infrastructure assets.

This methodology does not fix the extent and type of risks that are tolerable, and how unacceptable risks have to be considered, but addresses:

- methods and techniques to be used for risk assessment;
- their contribution to the risk management process;
- the steps that a company has to follow in order to define its risk criteria to be comparable with other GIE members.

### Security Risk Assessment - Framework Overview

![Diagram of the GIE Security Risk Assessment Methodology](image-url)

- **Establishing the context**
- **Risk Identification**
  - **Asset Classification**
    - Asset Type
    - Asset Criticality
    - Asset environment to drive threat applicability
  - **Threat Analysis**
    - Potential threat sources
    - Threat Catalogue
    - Asset vs Threat matrix map
- **Risk Analysis**
  - Evaluation of the likelihood of risk scenario
  - Definition of the risk matrix
  - Evaluation of the Impact & consequences of risk scenario
  - Object Classification
- **Risk Evaluation**
  - Comparing the risk findings with risk criteria
  - Preliminary Analysis
- **Risk Treatment**
  - Selection of the strategy for managing risk
  - Risk Treatment plan
  - Evaluation the effectiveness of the AS-IS security measures & Gap Analysis
  - Identification of countermeasures
  - Security guidelines
  - Evaluation of the residual risk
  - Vulnerability analysis
  - Supplementary measures
The methodology introduces a **“Security Risk Assessment tool (SRA Tool)”** for supporting companies to properly collect and analyze information and data, following the defined methodology, in order to define the global security risk level for each asset considered.

### Asset/Component Classification
- **Type**
- **Criticality**
- **Environment**

### Threat Catalogue
- **Type**
- **Source**
- **Class**

### “Potential” Risk Analysis
- Threat applicability
- Qualitative Likelihood Estimation
- Qualitative Impact Estimation

### Risk Evaluation
- Preliminary Analysis
  (e.g., exclude minor risk scenarios)

### Risk Treatment
- Risk management Strategy
- Effectiveness of AS-IS security measures & Gap Analysis
- Evaluation of the residual risk
- Vulnerability Analysis

### Organization Risk Criteria

### Security Guidelines

### AS-IS Security Measures

### Object Classification
- High Risk Object
- Medium Risk Obj.
- Low Risk Obj.

### Asset vs. Threat applicability matrix

<table>
<thead>
<tr>
<th>Asset XYZ Characteristics (from Asset Classification)</th>
<th>Surrounding environment</th>
<th>Geographical characteristic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat source type</td>
<td>Threat source</td>
<td>Threat class</td>
</tr>
<tr>
<td>Natural threat</td>
<td>Earth</td>
<td></td>
</tr>
<tr>
<td>Threats related to Earthquake (shock waves, earth cracks, etc.)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Likelihood Estimation Scale
- 1. Very low probability
- 2. Low probability
- 3. Medium probability
- 4. High probability
- 5. Very high probability

For **High Risk Objects**, Vulnerability Analysis and the Supplementary measures are mandatory.

### Risk treatment plan (Supplementary measures)

### Risk scenarios likelihood

- 1. Very low probability: It is extremely unlikely that the incident will occur; no experience in the gas sector.
- 2. Low probability: It is unlikely to occur: very limited experience in the gas sector: occurs approximately once over 10 years.
- 3. Medium probability: It is a likely event: similar accidents have been reported in the gas sector and occur approximately once every 5 years.
- 4. High probability: It is very likely to occur: it has been experienced in most systems in the gas sector and occurs once per year.
- 5. Very high probability: It will happen in the close future: occurs twice per year or more.