ENISS letter
on the Safety and Security Glossaries

40th Meeting of the Nuclear Safety Standards Committee (NUSSC)
01. – 03. December 2015, Vienna VIC, C Building

ENISS Reactor Safety Group
Gerd Bassing
Establishment of ENISS

On May 2005, when WENRA was about to publish its first draft of Reference Levels (RLs), European nuclear operators gathered together:

- To establish a common licensee view on these RLs and to present it to WENRA.
- To support an exchange of information about the interaction of license holders with their national regulators, in order to achieve a harmonised set of new regulations
- To cooperate with the European Institutions on regulatory issues

ENISS European Nuclear Installations Safety Standards Initiative under the umbrella of FORATOM was created
ENISS: Interaction with WENRA

Comments on

- Various versions of Reference Levels for operating reactors and waste storage/decommissioning activities
- WENRA safety objectives for new build
- The terms of reference of post Fukushima stress tests
- The guideline on Natural Hazards and Design Extension Conditions
ENISS: Interaction with IAEA

- Observer status representing European licensees in
  - IAEA Safety Standards Committees: NUSSC, WASSC, RASSC, EPReSC
  - IAEA Nuclear Security Guidance Committee: NSGC
- Provides comments on a selection of Safety Requirements, Safety Guides, Security Series documents and TECDOCs
- Participates in drafting groups of relevant Safety Standards and publications
IAEA Nuclear Safety / Nuclear Security Glossaries

• IAEA glossary for Nuclear Safety is under revision (2007)
• New glossary for Nuclear Security is in preparation (05-2014)
• Use of same terms in different context and definitions may lead to complexity and misinterpretation in the daily work
• Does the different definitions impact the use of the Safety Standards and have an adverse affect on Nuclear Safety?
• ENISS Reactor Safety Group carried out a comparative study of respective definitions of technical terms in the related glossaries
IAEA Nuclear Safety / Nuclear Security Glossaries

Results:

• The overall risk of confusion and impact on Nuclear Safety is controllable at the time being.
• No issues identified which might have an adverse effect on Nuclear safety.

Three areas of terms where further action may be needed:

Terms

• where the meaning is completely different depending on context, but definitions are already commonly established (e.g. defence in depth)
• in one glossary which are referred to in the other but with different wording and meaning (e.g. deterministic safety analysis, HCLPF in security glossary, nuclear security in safety glossary)
• Terms not defined in the Safety Glossary (e.g. target, threat, unacceptable radiological consequences), but used in Safety Standards
Detailed results:

- Approx. 26% of terms in the Security Glossary are included in the Safety Glossary
- Most of them has low to middle differences and low to middle impact
- 12 terms have no need for two definitions, one harmonized definition seems reasonable
- A low number of terms have high differences and may cause problems
# Safety/Security Glossary

## Examples

<table>
<thead>
<tr>
<th>Term</th>
<th>Safety Glossary</th>
<th>Security Glossary</th>
<th>Difference</th>
<th>Impact</th>
<th>New definition justifiable</th>
</tr>
</thead>
<tbody>
<tr>
<td>availability</td>
<td>The fraction of time for which a system is capable of fulfilling its intended purpose. Reliability represents essentially the same information, but in a different form.</td>
<td>The property of being accessible and usable upon demand by an authorized entity. [17T – from ISO]</td>
<td>High</td>
<td>Low</td>
<td>No, if system is changed e.g. into device</td>
</tr>
<tr>
<td>Configurati on manageme nt</td>
<td><strong>The process</strong> of identifying and documenting the characteristics of a facility’s structures, systems and components (including computer systems and software), and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation. ‘Configuration’ is used in the sense of the physical, functional and operational characteristics of the structures, systems and components and parts of a facility.</td>
<td>The process of identifying and documenting the characteristics of a facility’s physical protection system — including computer systems and software — and of ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation</td>
<td>Low</td>
<td>Low</td>
<td>No</td>
</tr>
<tr>
<td>Disused source</td>
<td>A radioactive source that is no longer used and is not intended to be used, for the practice for which an authorization has been granted. (From Ref. [11].)</td>
<td>A radioactive source which is no longer used, and is not intended to be used, in facilities and activities for which authorization has been granted [11G, attributed to Safety Glossary]</td>
<td>Low</td>
<td>Low</td>
<td>No: Definition is only slightly different</td>
</tr>
</tbody>
</table>
### Safety/Security Glossary

#### Examples

<table>
<thead>
<tr>
<th>Term</th>
<th>Safety Glossary</th>
<th>Security Glossary</th>
<th>Difference</th>
<th>Impact</th>
<th>New definition justifiable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deterministic safety assessment</td>
<td><strong>deterministic analysis</strong>&lt;br&gt;Analysis using, for key parameters, single numerical values (taken to have a probability of 1), leading to a single value for the result.&lt;br&gt;Typically used with either ‘best estimate’ or ‘conservative’ values, based on expert judgement and knowledge of the phenomena being modelled.&lt;br&gt;Contrasting terms: probabilistic analysis or stochastic analysis. See probabilistic analysis.</td>
<td>A comprehensive, structured analysis that assesses the performance of the facility against a broad range of operating conditions, postulated initiating events, and other circumstances, demonstrating that normal operation can be carried out safely, in such a way that facility parameters do not exceed operating limits.</td>
<td>High</td>
<td>High: See yellow marked sentence</td>
<td>No: The security definition tries to redefine the an existin g definiti on</td>
</tr>
</tbody>
</table>
### Safety/Security Glossary

**Examples**

<table>
<thead>
<tr>
<th>Term</th>
<th>Safety Glossary</th>
<th>Security Glossary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defence in depth</td>
<td>1. A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions. The objectives of defence in depth are: (a) To compensate for potential human and component failures; (b) To maintain the effectiveness of the barriers by averting damage to the facility and to the barriers themselves; (c) To protect workers, members of the public and the environment from harm in accident conditions in the event that these barriers are not fully effective. INSAG defines five levels of defence in depth: (a) Level 1: Prevention of abnormal operation and failures. (b) Level 2: Control of abnormal operation and detection of failures. (c) Level 3: Control of accidents within the design basis. (d) Level 4: Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents.</td>
<td>The combination of successive layers of systems and measures for the protection of targets from nuclear security threats. [20F, 17F] 2. The combination of multiple layers of systems and measures that have to be overcome or circumvented before nuclear security is compromised. [13R*, 14R] 3. The combination of multiple layers of systems and measures for the protection of targets from nuclear security threats. [15R] 4. Implementing several layers of defence, including both administrative aspects (procedures, instructions, sanctions, access control rules, confidentiality rules) and technical aspects (multiple layers of protection together with measures for detection and delay) that adversaries would have to overcome or circumvent to achieve their objectives. [9G f/n] The term “defence in depth” is widely used in safety standards. While the general concept is similar, the safety definition of “defence in depth” is too complex and specific to be directly adapted for security.</td>
</tr>
<tr>
<td></td>
<td><strong>Difference</strong></td>
<td><strong>Impact</strong></td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Middle</td>
</tr>
<tr>
<td></td>
<td>Middle</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

IAEA 40th NUSSC

01. – 03. December 2015

ENISS
IAEA Nuclear Safety / Nuclear Security Glossaries

Proposal

- To reduce the existing risk in the process and facilitate the work on Safety Standards and Nuclear Security Series Publications ENISS proposes
  - To initiate a development for a common IAEA Glossary, which includes terms and definitions both used by Nuclear Safety and Nuclear Security at the same position
  - To check in this frame both glossaries on completeness related to their use
- One common document reduces the administrative effort when revision become necessary
THANK YOU FOR YOUR ATTENTION