Break-Out Session 2

Special Topics

Group 4

Please save under a different name, e.g. "Break-out Session 2_Group 4_Presentation"

B. Ageing of instrumentation and other software and hardware

B1. How often has each inspector in the group inspected ageing of IT systems?

Country	Frequency 1 - Very often 2 – Sometimes 3 - Never	Comments
Slovenia	**3**	**there is another authority that is involved in cyber security inspections**
Hungary	**3**	**there is another authority that is involved in cyber security inspections**
Romania	**3**	**there is another authority that is involved in cyber security inspections**
Lithuania	**3**	
Germany	**2**	**They're starting to try implementation of these kind of issue.** **The authorities haven't got he specialist**
Italy	**2**	**during the SMS inspection we start to implement this issue (i.e. interview with CR operator)** **There are specific internl audit for critical equipment on the SIL (check on the hardware and not on the software)**
UK	2	Some plan for the next SMS inspection year with specific specialist

B2. Provide your perspective on how to inspect ageing of instrumentation and other IT software and hardware

- *What sort of systems do you regard to be most relevant for this discussion?*
  - *ESD devices, Maintenance Management System (reliability data, frequency, losses of data during main turnaround), SCADA (process monitoring of parameters), management of documentation (problem with the passage form the paper documents and electronic documents)*
- *What do you regard as the largest threat to the plant integrity regarding ageing of instrumentation and other IT software and hardware?*
  - *Loss of control (data, parameters, documents); if the software is broken, how do you manage the plant (the plant is designed to go to shut-down in a safer way); afraid in the future for the digitalization of all controls (attention on hardware and not software); considering a cyberattack as an external event in the Safety Report*
- *What documentation would you request to see before a visit?*
  - *Operation manual and all operating instructions for the operational control and fitting with hazards evaluation; one or more management systems for safety and security (cybersecurity); tests on all safety loop (test) and the relative results*

B2. Provide your perspective on how to inspect ageing of instrumentation and other IT software and hardware

- *What information/evidence will you look for during a visit?*
  - *Loop test and reliability back-logs, with relative analysis on specific error (procedure for investigation)*
- *How do you expect this to be reflected in*
  - *The safety management system?*
    - *Updating of the documentation*
  - *Consequences of the audit cycle?*
    - *Looking at the PDCA, problems if you don't close the cycle (ACT)*
  - *Incident analysis?*
  - *Maintenance records?*
- *Which requirements can authorities set on the companies with a view of reducing the risk of system failure?*
  - *Recording of failure of the systems; procedure for the management of the cyber threat (i.e. near misses)*
- *What techniques can be used to engage with the operator and achieve action by the operator?*
  - *Recommendations (minor non compliances): the operator didn't treat the issue; the problem is when the issue is non written in the law; involving of the assurance companies in treating the cyber attacks*
- *How can you achieve change within an organisation without enforcement action?*
  - *Seminar with technical experts from CA on cyber attacks*