Break-Out Session 2

Special Topics

Group 3

Please save under a different name, e.g. "Break-out Session 2_Group 3_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
Germany	**3**	**We ask if they take care of the IT-systems focusing on cyber security, not on the ageing aspects.**
Bulgaria	**3**	**Normally they have a checklistr, do what is on the checklist. If point of IT is put on list it will be done in future.**
Italy	**3**	**We never inspect IT. It is a matter of priority (older inspectors). Focus on physical detoriation of pipes, vessels, etc. Aging, also question of obsolescence, standard is not supporte, but not deteriorated.**
France	**2**	**In Seveso. We are not specialist, we are looking at safety barriers. Look at documentation of the IT-systems and top see that industry are developing recommendations. We are not into black box. Sensors have to be tested according to certain frequency.**
Finland	**3**	**The security part could be in the future. Now it doesn't happen.**
Ukraine	**3**	**Could be subject by IT-checks if Sevesosite considered to be critical infrastructure. Other services might do check ups.**
Sweden	3	Are planning to start asking about cyber security. How many cyber incidents have you hade since the last inspection? We need to start to ask questions about system compability, of ICS, etc.

B3. What requirements and strategies can authorities expect on sites to reduce the risk of IT system failure?

- *What kind of programmatic elements would you expect for a proactive approach to reduce risk from ageing of IT sites? From accidents? From cyber attacks?*

- *How can a site deal with the procurement challenges to reduce the risk of getting stuck with a patchwork of parts that have varying degrees of compatibility, creating a safety and security risk?*

- *How can authorities get a better picture of the challenges the companies are facing with the industrial control systems?*

- *How far can inspectors go in examining security concerns with ageing IT systems, especially in view of the interconnections across the entire industrial information and control systems?*

B3. What requirements and strategies can authorities expect on sites to reduce the risk of IT system failure?

- *What kind of programmatic elements would you expect for a proactive approach to reduce risk from ageing of IT sites? From accidents? From cyber attacks?*

- *Answer:*
- *We need to have power back-up for electricity if we lose that.*
- *Back up for data should cover several years since the bug could be there. If you have a longer interval for backup storage is that it might be easier to reproduce data. Maybe you can re-generate the IT.*
- *Pick up foreseen data.*
- *Up to dated software.*

B3. What requirements and strategies can authorities expect on sites to reduce the risk of IT system failure?

- *How can a site deal with the procurement challenges to reduce the risk of getting stuck with a patchwork of parts that have varying degrees of compatibility, creating a safety and security risk?*

- Answer:
- It is a question of attitude, the management must understand tha aspect of process safety / safety culture.
- You need to have a long time planning for keeping software and hardware updated.
- Intercompability
- Long term contracts with suppliers with communication about needs. The company must be able to define long time goals, have a strategic idea. Plan ahead before the spare parts run out.
- Audits for software, hardware, etc. Periodic test.

B3. What requirements and strategies can authorities expect on sites to reduce the risk of IT system failure?

- *How can authorities get a better picture of the challenges the companies are facing with the industrial control systems?*
-
- *Answer:*
- *Ask questions. What systems do you have? What needs do you have? Dialogue public-authority. Have a discussion about struggles, advantages of systems.*

B3. What requirements and strategies can authorities expect on sites to reduce the risk of IT system failure?

- *How far can inspectors go in examining security concerns with ageing IT systems, especially in view of the interconnections across the entire industrial information and control systems?*

- *Answer:*
- *At the moment not so far, since we need more knowledge. Scratch at the surface and wait and see how they react, then read their reactions. Use some checklist… point at what you think is most important.*

B3. What requirements and strategies can authorities expect on sites to reduce the risk of IT system failure?

- *What training and competency should inspectors have to address ageing of IT systems?*
  Answer: Many inspectors are chemical or mechanical engineers, etc, not so many system/computer engineers in this field.
- *Ask general questions, scratch on the surface. Take with us some expert. Co-operate with other authorities.*

- *What could your organisation do to raise awareness of these issues?*
- *Answer: Maybe organize some meetings and discuss the questions with the industry or put in a point in one of your regular meetings regarding IT-issuers regarding aging and cyber security.*

B4. In what circumstances, would the following inspection approach be useful:

a. ***Use of standards to determine the level of ageing risk, e.g., gap analysis against a standard?***
   - *For what sort of equipment? What standards could be used?*
   - *What gaps are acceptable and what would require action?*

b. ***Following a checklist (produced from this workshop)?***
   - *When would this be useful?*
   - *List some suggestions of questions on the checklist.*

c. ***Asking open questions?***
   - *When would this be useful?*
   - *List some questions that would be useful.*

d. ***Other?***

Joint Research Centre

B4. In what circumstances, would the following inspection approach be useful:

a. ***Use of standards to determine the level of ageing risk, e.g., gap analysis against a standard?***
   - *For what sort of equipment? What standards could be used?*
   - *What gaps are acceptable and what would require action?*

Answer:

The company must do regular risk analysis of their IT-systems regarding to ageing and cyber security.

B4. In what circumstances, would the following inspection approach be useful:

b. Following a checklist (produced from this workshop)?

- *When would this be useful?*
- *List some suggestions of questions on the checklist.*

Answer:

- *It could be useful for us to get started with the questions.*
- *Open questions from checklists. Look at what is previously written in the field, see example MSB…*
- *We need to follow up these questions in the following inspections. What has changed? Better/worse?*

MSB – Guide to increased security in industrial information and control systems. *This is an example*

1 Secure management's commitment and responsibility for security in industrial information and control systems.

2 Clarify roles and responsibilities for security in industrial information and control systems.

3 Maintain processes for system surveys and risk management in industrial information and control systems.

4 Ensure systematic change management in industrial information and control systems.

5 Ensure systematic contingency planning and incident management in industrial information and control systems.

MSB – Guide to increased security in industrial information and control systems

6 Introduce security requirements in industrial information and control systems right
from the start in all planning and procurement.

7 Create a good security culture and heighten awareness of the need for security in
industrial information and control systems.

8 Work with a security architecture in the industrial information and control systems.

9 Continuously monitor connections and systems in order to detect intrusion attempts
in industrial information and control systems.

10 Conduct regular risk analyses of industrial information and control systems.

MSB – Guide to increased security in industrial information and control systems

11 Conduct periodic technical security audits of industrial information and
control systems.
12 Continually evaluate the physical security of industrial information and
control systems.
13 Regularly ensure that any and all connections to industrial information and
control systems are secure and relevant.
14 Harden and upgrade industrial information and control systems in collaboration
with system vendors.

MSB – Guide to increased security in industrial information and control systems

15 Conduct training and practice regarding IT incidents in industrial information and
control systems.
16 Follow up incidents in industrial information and control systems and monitor
external security problems.
17 Participate in user associations, standardisation bodies and other networks for
security in industrial information and control systems.

B4. In what circumstances, would the following inspection approach be useful:

c. Asking open questions?

- *When would this be useful?*
- *List some questions that would be useful.*

Answer:

- To scratch on surface and see how they react so you know if you need to dig further.

B4. In what circumstances, would the following inspection approach be useful:

d. Other?

Answer: