Lessons learnt from I&C modernisation regarding Cyber Security

Obvious things in actual context – or how newbie learnt the hard way the cyber security is not rocket science but still organisations do not get it.

Representatives

Pekka Nuutinen, Teollisuuden Voima Oyj

- Chief Engineer – Olkiluoto 1 and 2, Automation Engineering
- DIMA-project: responsible for quality management, systems engineering and cyber security
- 20 years of experience in nuclear engineering (thermal hydraulics, neutron/reactor dynamics, safety engineering, systems engineering)
- 2 years of experience in Cyber Security (newbie learning the hard way – every day)

Background of DIMA project

- TVO investigated different options on the strategy of maintaining the lifetime of the I&C systems / functions
- One option was to replace all main automation systems with digital I&C:
  - CCF / diversity issue
  - Qualification of Cat. A software
  - Was seemed too risky and costly..
- Led to a hybrid-strategy:
  - Cat. A functions to be realised by hardwired technology
  - Other functions may utilise digital technology

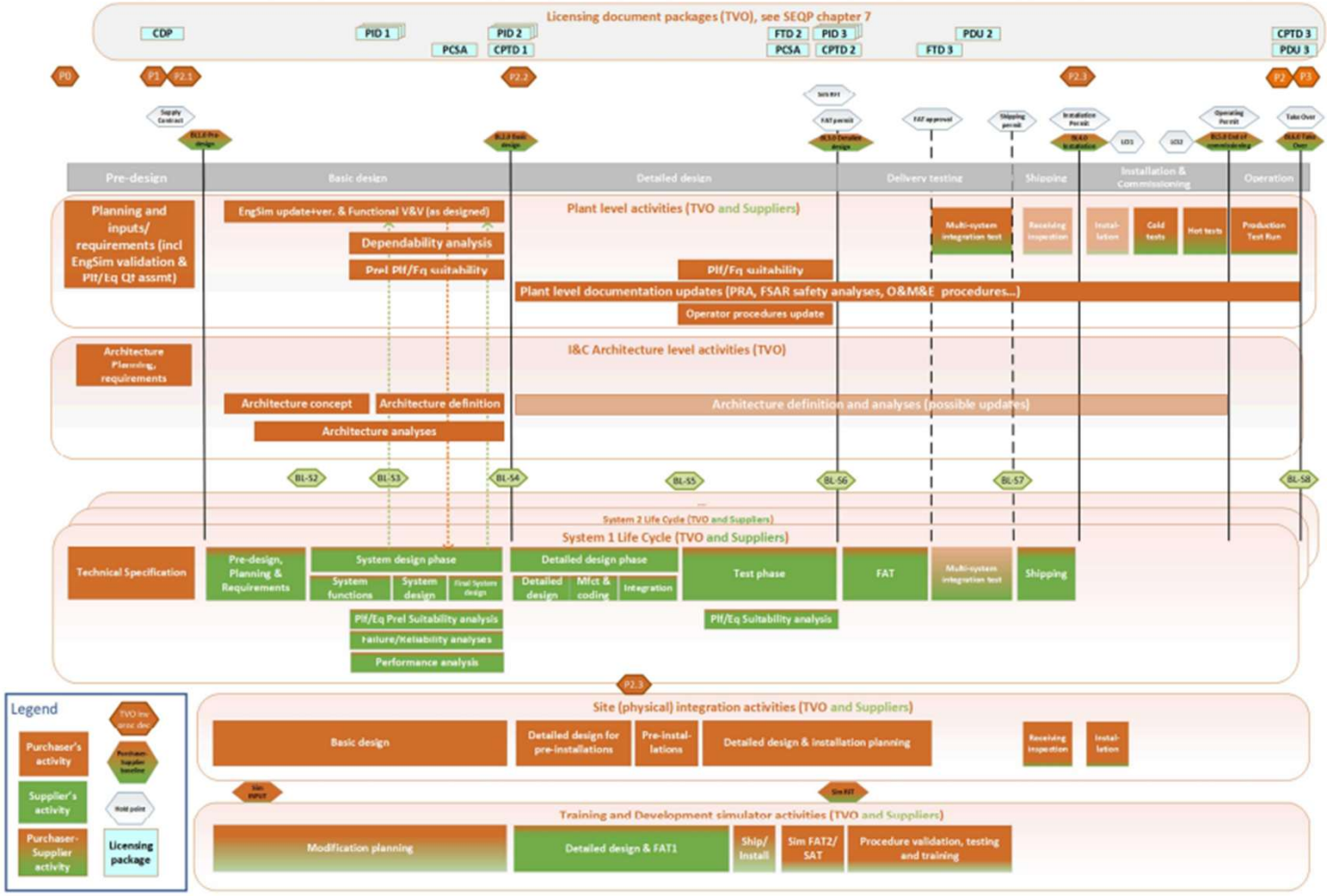
Background of ICMA-program

- Hybrid strategy ended up to the following work packages:
  - COMA-project:
    - Manufacturing of new reactor protection relays and measurement boards
    - Manufacturing of new protection devices
  - DIMA-project:
    - MC&NF: Modernisation of neutron flux measurement and main controllers
    - PCS: Modernisation of process computer system
- RfQ´s to several potential suppliers for each work package
- Shortlisting of suppliers for each work package and assessment of their capabilities (as per Nuclear-SPICE and quality audits) => selection of preferred supplier => delivery contract
- **Lesson learnt 1:** More emphasis needs to be put to the assessment of Suppliers cyber security engineering capabilities – resources, knowhow and processes – already in Supplier selection phase before contracting.
- How about attitude and commitment???

DIMA-project scope

- TVO has established a DIMA-project for modernisation of Olkiluoto 1/2 I&C systems as follows:
  - Neutron Flux measurement system (system 531)
    - Power Range Monitoring (system 531.2)
      - Cat. A functions realised in hardwired technology (non-programmable, non-networked)
      - Cat. B functions using digital technology
    - Source and Intermediate Range Monitoring (system 531.1)
      - Cat. B functions using digital technology
  - Main controllers (Digital - Cat. B/C)
    - Reactor Power Controller (system 535)
    - Reactor Level/Feedwater Controller (system 537)
    - Reactor Pressure Controller (system 461)
  - Process Computer system (System 527, Cat. C)

DIMA-project lifecycle and product hierarchy



DIMA-project – Pre-design phase

- According to the “normal” v-lifecycle project was started by defining management plans (project, quality, schedule, requirement management, configuration management, etc…)
- Both parties shall establish the plans and as far as possible refer to the existing quality management system. However, their application is project specific and needs clarification.
- **Lesson learnt 2**: Cyber security management plan shall be established and synchronised with other management plans to define cyber security roles and responsibilities, activities and deliverables as well as scheduling. This needs to be performed both by the Supplier and the Customer.

DIMA-project – Pre-design phase

- In the beginning - when defining detailed stakeholder requirements – TVO´s maintenance unit was participating. However, due to contract reasons and maybe lack of understanding, many comments were not included into actual design concept.
- This led to questionable architecture and on the other hand frustration in the organisation.
- **Lesson learnt 3:** Gather stakeholders and their viewpoints already in the beginning of the project before contract signature – also cyber security and ICS-experts.

DIMA-project – (Beginning of) Basic Design phase

- According to the ISO 15288, stakeholder requirements shall be analysed to define actual system requirements.
- TVO established high level cyber security requirements for systems and information security requirements for suppliers (stakeholder requirements).
- In addition, TVO established a Security Concept to describe security principles to be applied in the modernised systems.
- **Lesson learnt 4:** Purchaser shall have Security Concept established as document infrastructure. Establishing project specific Security Concept / Security Architecture will lead to delays and technical risks. Preferred solutions shall be proposed by the Purchaser already in the contract phase.

DIMA-project – (Beginning of) Basic Design phase

-
-

Intentionally left blank

- **Lesson learnt 5:** Both the Purchaser and the Supplier shall have sufficient and knowledgeable resources from the very beginning of the project.
- => In general, management need to commit to the cyber security resource and knowhow development.

DIMA-project – Basic Design phase

- Intentionally left blank
- **Lesson learnt 6:** There is a need for integrated systems engineering that will connect all designs into one product or all designers to one project.

DIMA-project – Basic Design phase

- In the basic design phase, it was clearly noted, that some of the TVO´s own infrastructure is not mature.
- New processes and procedures needed to be developed – leading also into internal disputes and resource questions/gaps.
- New processes were introduced to organisation
- **Lesson learnt 7:** Cyber Security management system needs to be established in the organisational level. Defining the principles differently in each project will lead to waste of resources and sub-optimal system configurations.

DIMA-project – Detailed Design phase

Intentionally left blank

- **Lessons learnt 8**: Ensure common target and “will” throughout the organisation => ensure effective leadership and overall ownership.
  - Cyber Security without properly functioning system is useless, digital system without Cyber Security is dangerous – we need both.

DIMA-project – Delivery testing phase

Intentionally left blank

- Leads to principal problems: if you change something due to cyber security, is previous testing for main functionality still valid?
- How to assess the need for regression testing…?

- **Lesson learnt 9**: Product needs to be managed as a single entity over the lifecycle. There is a need for integrated systems engineering not only in design phase, but also in the V&V activities – including cyber security.

But why this all has happened?

- Is cyber security still in its own bubble?
  - Maybe less than before, but still too much
- Is it about sharing the information and awareness across the organization or about participation and integration of cyber security experts?
- **Lesson learnt 10**:
  - The latter one. Cyber security experts needs to come to factories and plant site where the actual systems are designed, tested and maintained.
  - Awareness does not only arise from training and lecturing but from doing, showing and guiding – hands-on.

Summary

- Lesson learnt:
  - Ensure Cyber Security involvement already in the beginning of the project
  - Ensure sufficient management commitment => resources and knowhow
  - Establish Cyber Security Management Program in company level
  - Integrate Cyber Security to other parts of project / product
    - Also – come down from the ivory tower of cyber security
  - Ensure efficient leadership, collaboration and common goals

Thank you!