Study Committee D2

Information Systems and Telecommunication

Paper 10713_2022

ROLE OF DIGITAL ENGINEERING AND DIGITAL TWIN TECHNOLOGY IN CYBERSECURITY OF ELECTRICAL GRID

Djenana CAMPARA, KDM Analytics

Dr. Nikolai MANSOUROV, KDM Analytics

Andrea HRUSTEMOVIC, JP Elektroprivreda BiH

Mr. Adnan AHMETHODZIC, JP Elektroprivreda BiH

Dr. Meludin VELEDAR, BH K CIGRE

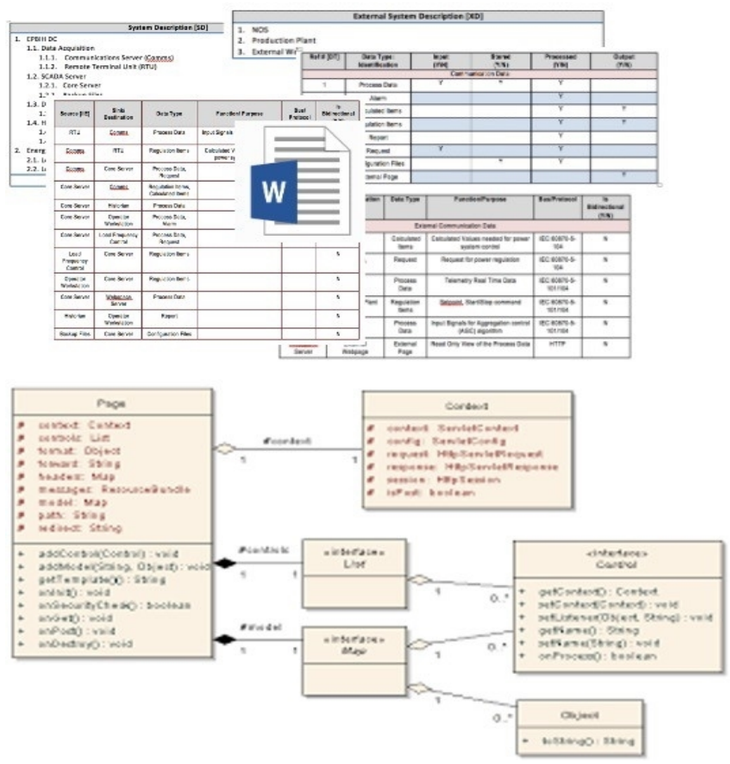
Motivation

- Daily increase in cyber threats faced by Global Electric Power systems causing this IT enabled interconnected and interdependent conglomerates to require risk assessment capabilities for understanding intricate hostile attack options, assessing vulnerabilities, and facilitating decision-making; including decisions related to investment into appropriate security controls.
- Current, antiquated manual risk assessment practices will leave systems unprotected and in constant re-active mode
- Goal: a Pro-active, Assurance-driven Digital Risk Assessment at Industrial Scale

Method/Approach

- One of the key requirements for achieving the goal of Digital Risk at Industrial Scale is structured representation of a System that includes
  - Representation of existing/legacy systems by transforming informally obtained information into structured data via a set of pre-defined tables in MS Word
  - Engineering of a new system by applying Digital Engineering process and further extending into Digital Twin
- These approaches are bringing risk assessment into the digital world, enabling digital risk assessment that can be obtained on demand, with high accuracy

Experimental setup & test results

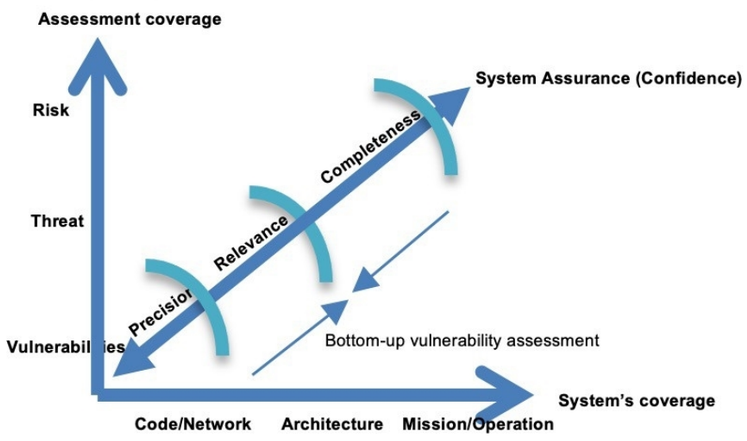


Discussion

- After performing risk assessment of several systems in 3 different ways by different people: manual, automated by utilizing transformed unstructured to structured data (manual transformation) and applying digital engineering, we concluded the following
  - Manual approach (laborious task, long hours) to threat modeling and risk assessment was too liberal, too subjective and too limited in details (only handful of attacks were considered) to compare cross-systems' results
  - System information presented in structured data enables automation in risk assessment process, with tolerance in a level of provided details and with comparable cross-systems' results
- Digital engineering framework is naturally extended to include fully digital risk assessment with enough granularity to move into cybersecurity risk assessment (mapping risks and threats on vulnerabilities identified through vulnerability assessments).

Conclusion

- The risk assessment and cybersecurity for the energy sector are in need of a paradigm shift in order to overcome the gaps caused by manual risk assessment techniques.
- Success of the effort is largely determined by the choice of the input specification. In this paper we argued, that the input format must be aligned with the technologies that are already being adopted in the industry for "digital engineering", model-based systems engineering and for building digital twins.



Study Committee D2

Information Systems and Telecommunication

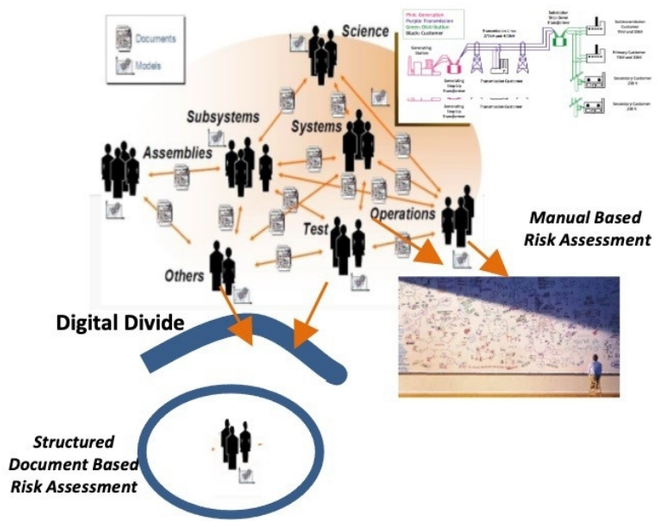
Paper 10713_2022

ROLE OF DIGITAL ENGINEERING AND DIGITAL TWIN TECHNOLOGY IN CYBERSECURITY OF ELECTRICAL GRID

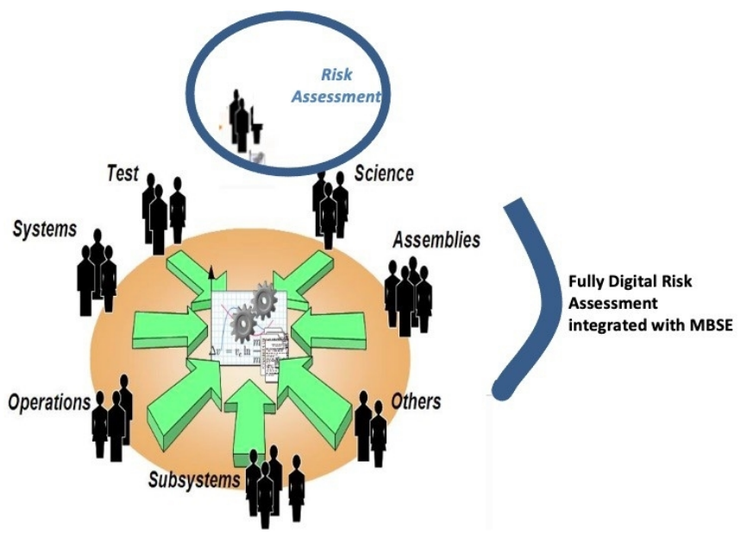
continued

Document Based System Engineering vs. Model Based System Engineering

- Antiquated manual risk assessment practices could be transformed into digital when System information is delivered in the form of structured document

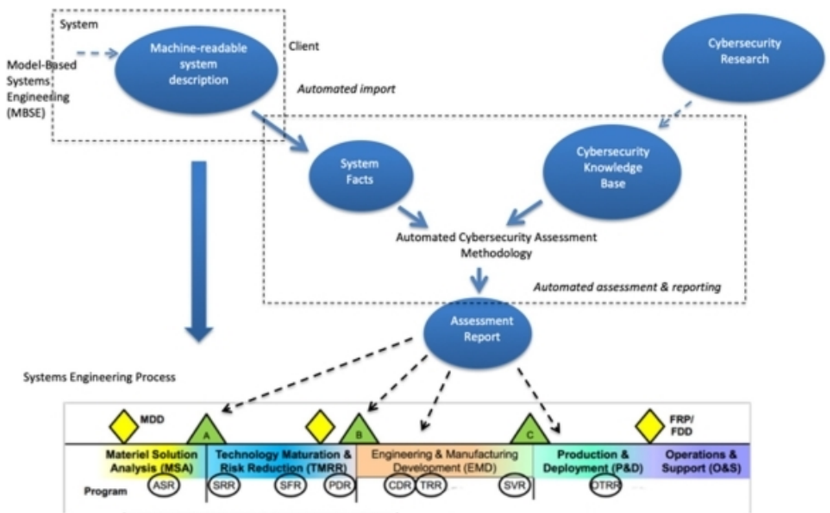


- Model Based System Engineering enables fully digital risk assessment



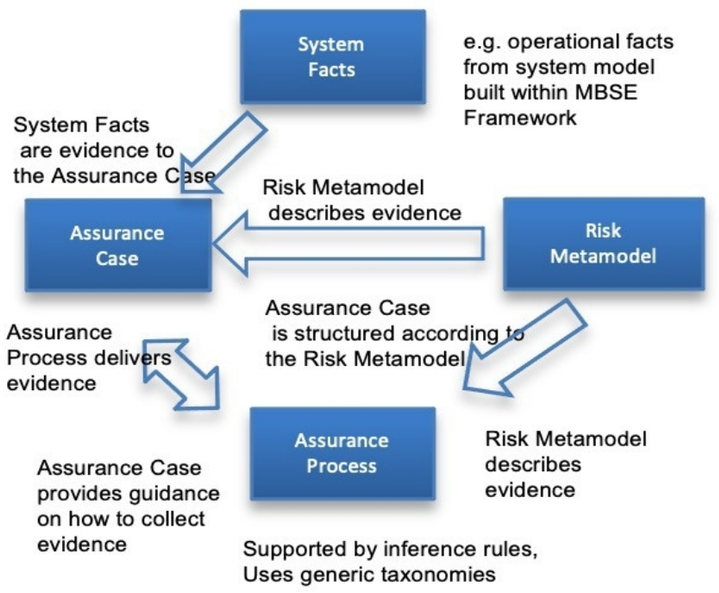
Separation of Domains

- System/Operational Architecture vs. Cybersecurity Knowledge
- Separation of Domains enables experts in each field to focus and contribute to the respective knowledge area



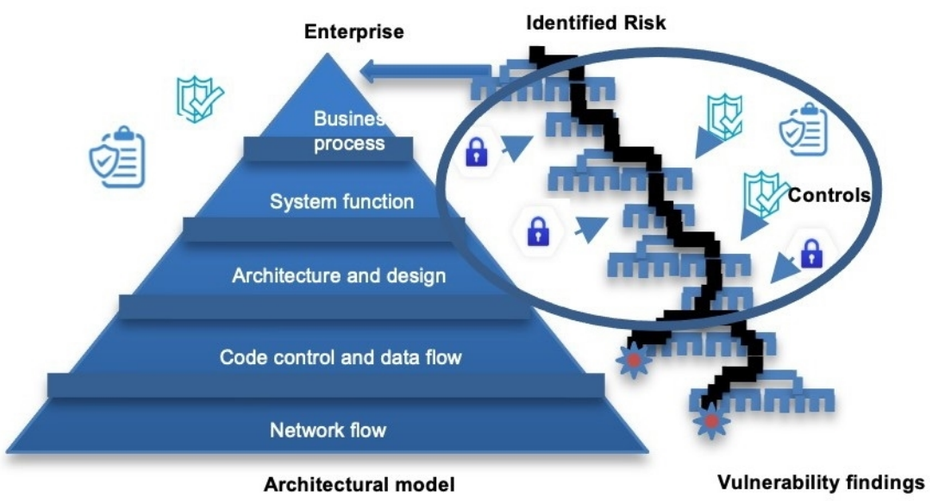
Integration with System Assurance

- Integrating System Assurance with Risk Assessment Methodology to assess confidence in System information and Risk outcome



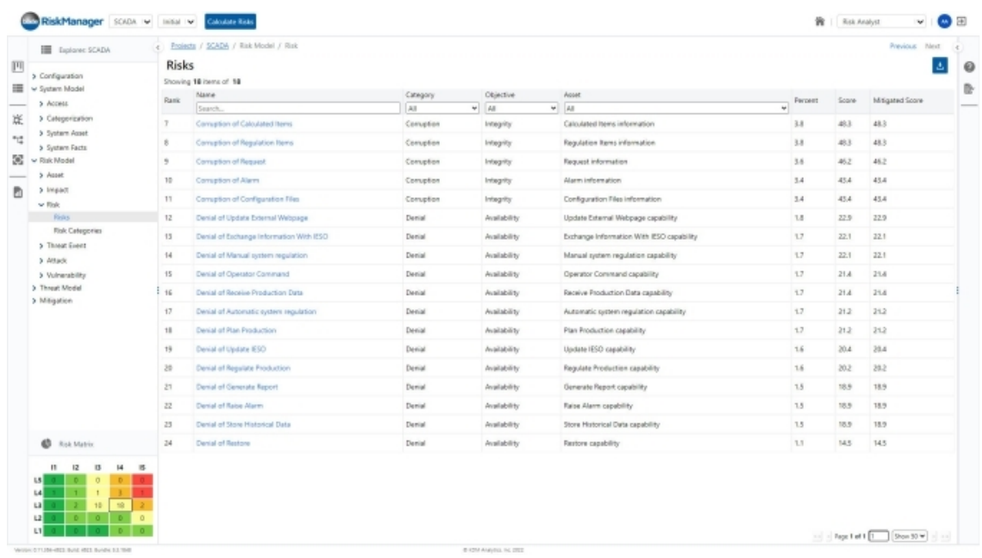
Automating end-to-end process

- Enables automated generation of attack tree with systematic enumeration of attack paths
- Connects code and network vulnerabilities with operational risk through identified attack path



Fully Quantifiable Risk Results

- Systematic, Comprehensive, Repeatable Results



http://www.cigre.org