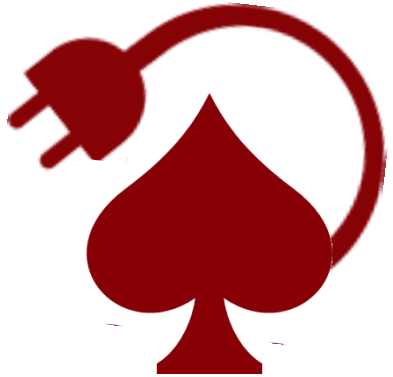
Security & Privacy Architecture DEsign

(SPADE)



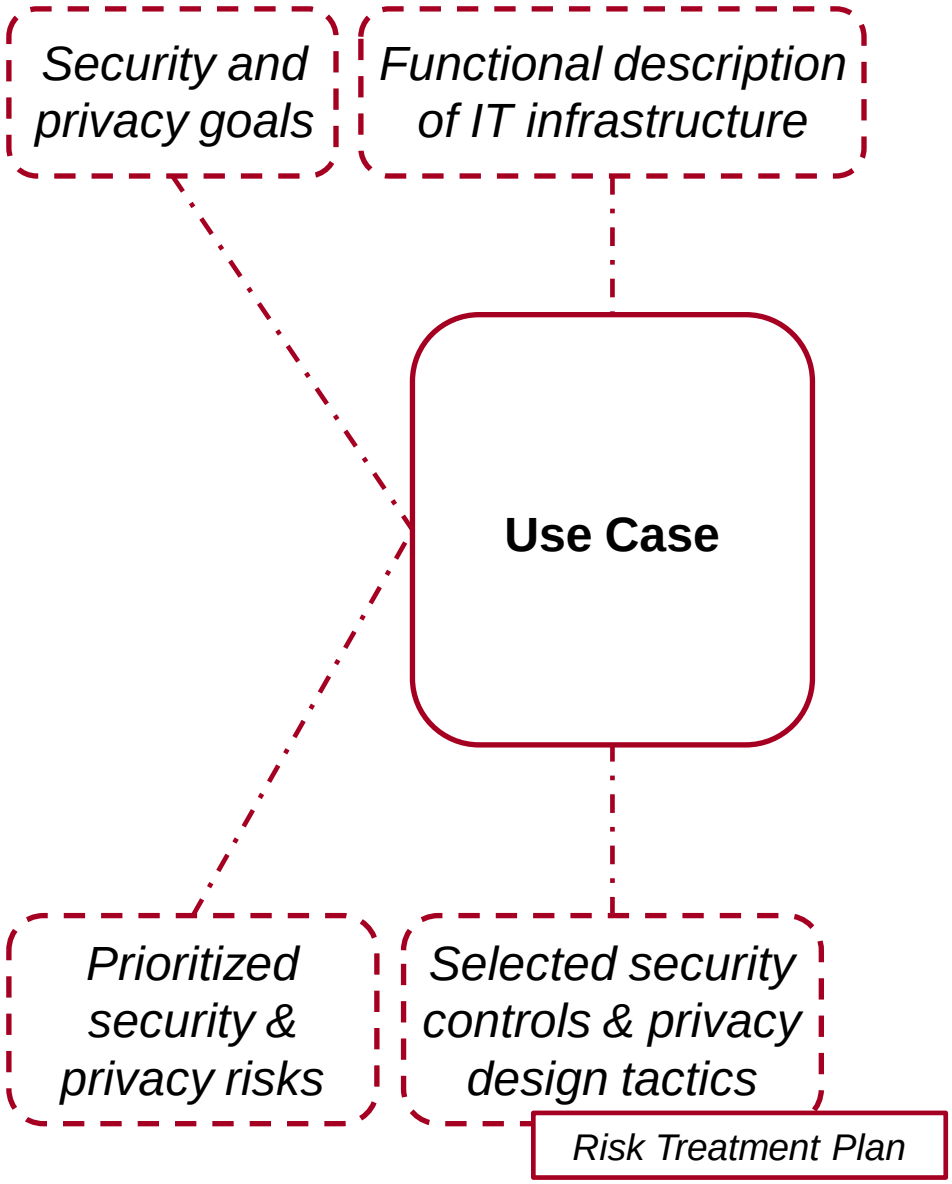
Security and Privacy Architecture DEsign

- **Security and privacy architecture**
  - Structured and modular composition of interconnected, possibly depending and cooperating, security and privacy mechanisms and technologies.

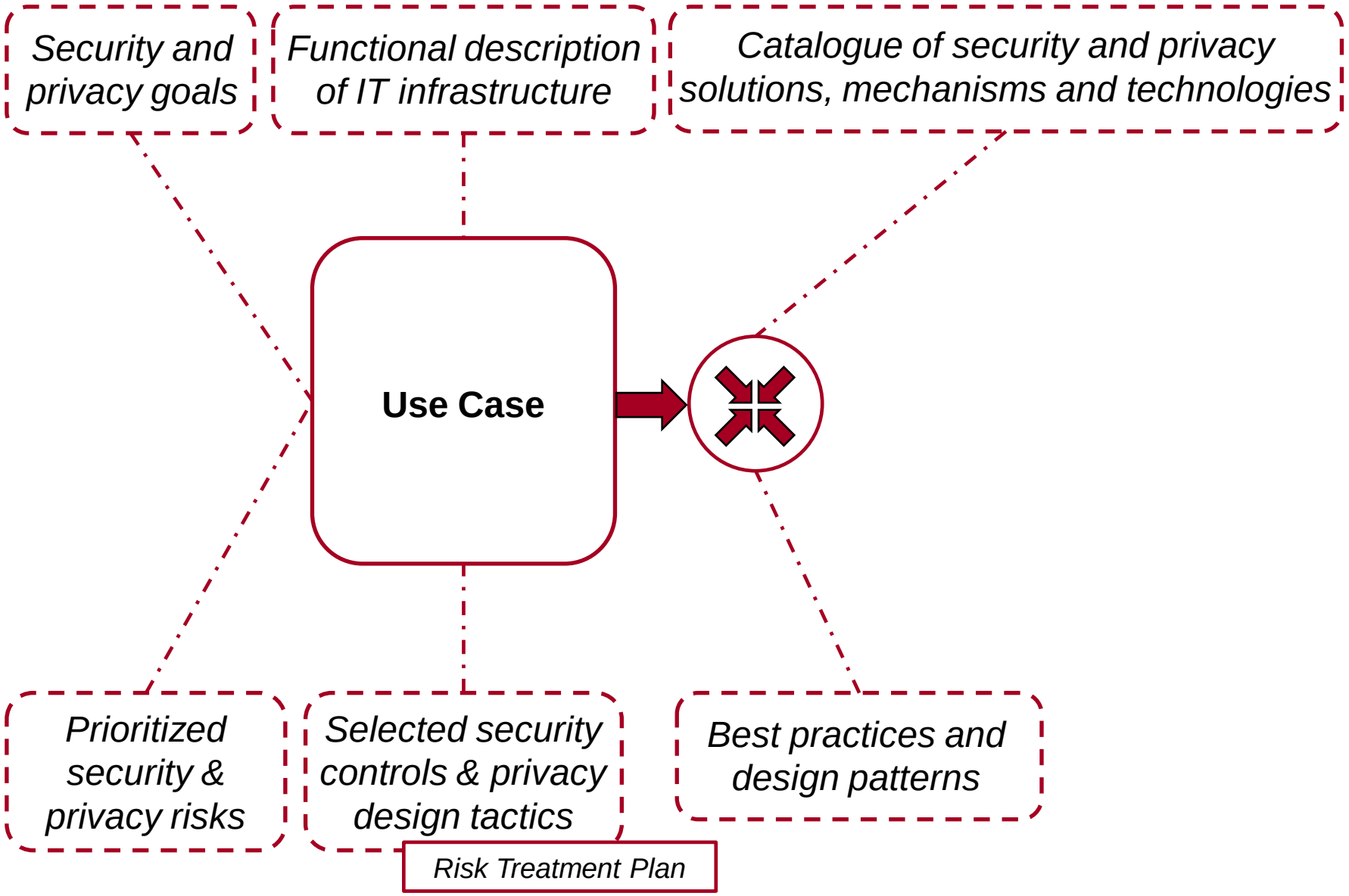
- **Motivation**
  - Secure the IT infrastructure of smart grid use cases
  - Ensure mitigation of security risks and acceptable performance

- **Goal**
  - Iterative process to define adequate security and privacy architectures
  - Architectures must be use-case-specific and fulfill related requirements

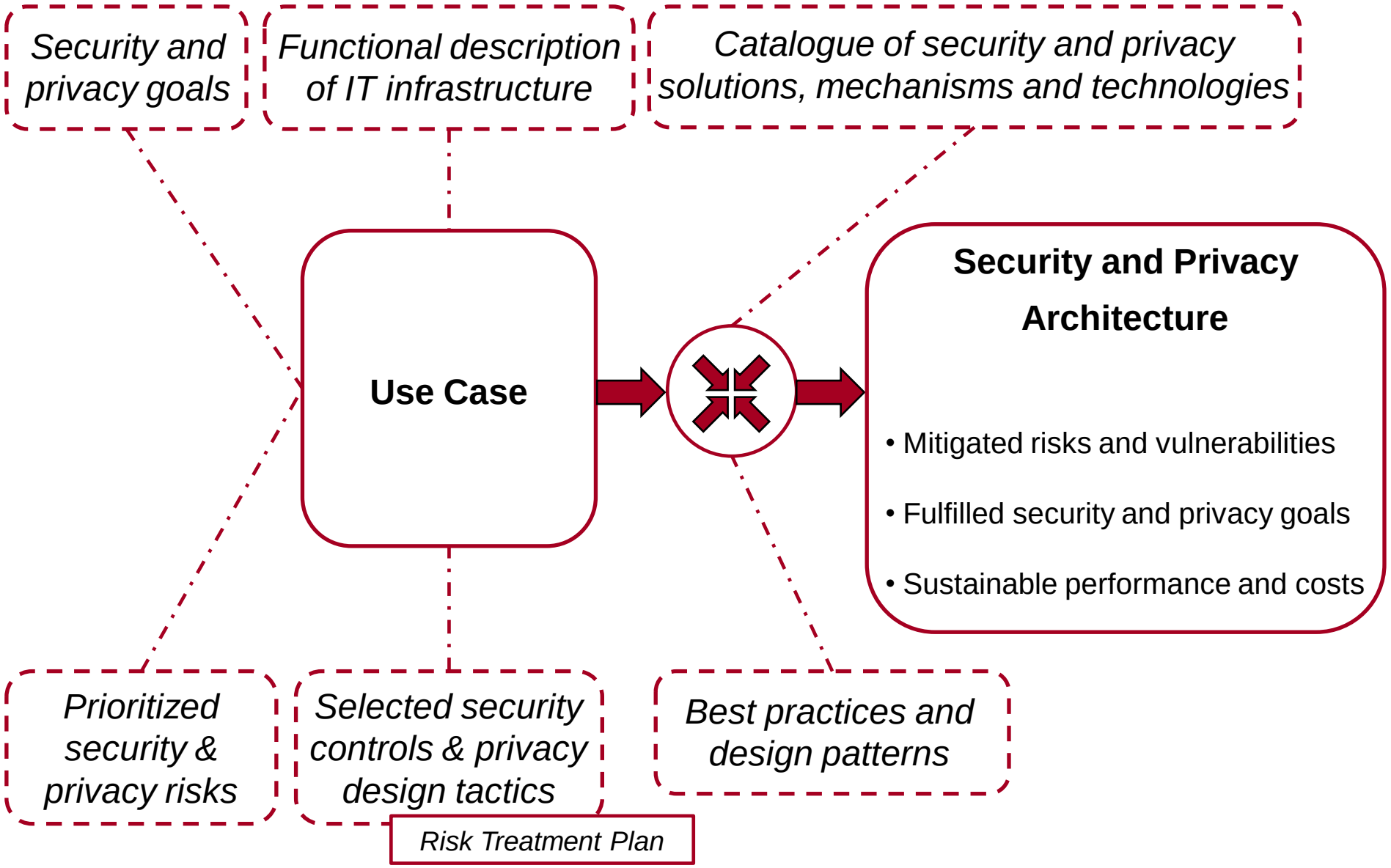
Security and Privacy Architecture DEsign



Security and Privacy Architecture DEsign

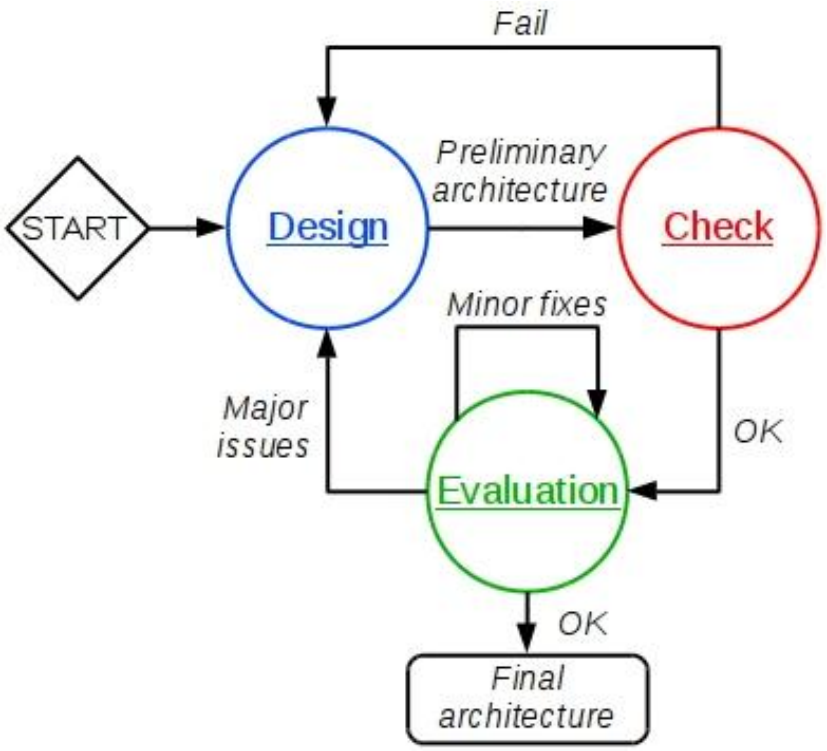


Security and Privacy Architecture DEsign



Security and Privacy Architecture DEsign

- **SPADE**
  - S&P Architecture DEsign process
  - Output: Use-case-specific architecture
  - Fulfillment of security and privacy goals



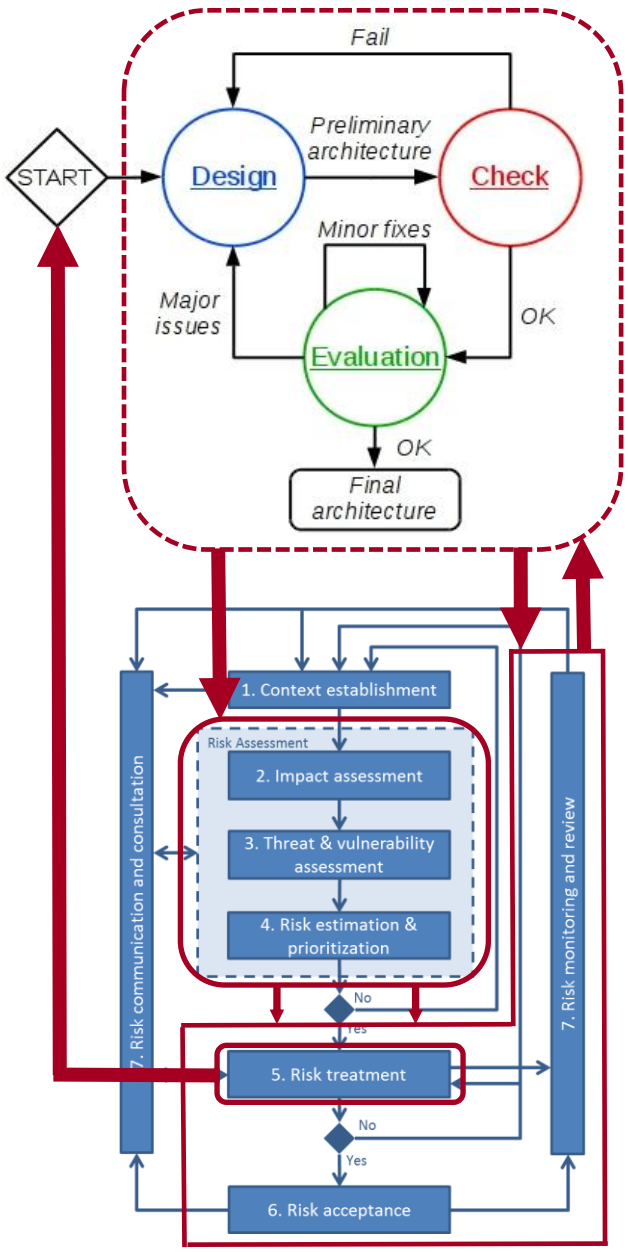
- **Three distinct phases**
  - “Design”, “Check”, “Evaluation”
  - Possible iteration among phases

- **Flexible and adaptable**
  - Improve already existing architectures
  - Design architectures for different systems

Security and Privacy Architecture DEsign

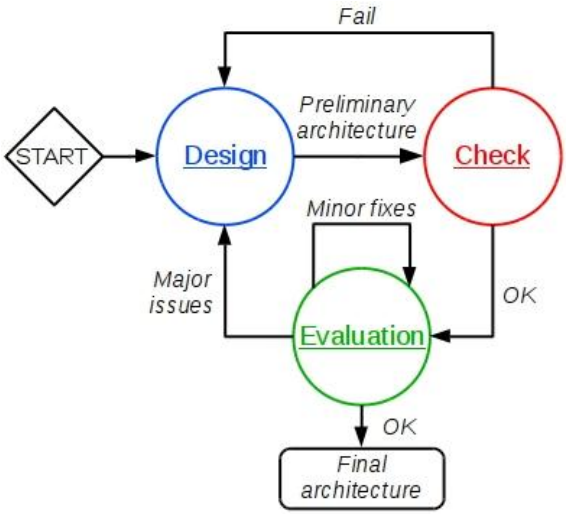
- **Mapping with the Risk Management process**
  - SPADE starts at the end of the Risk Treatment phase
- **Input from Risk Management**
  - List of prioritized risks
  - Risk treatment plan

    (contains intended security controls)
- **SPADE lifetime and roles**
  - Directly cover steps 5-7 of Risk Management
  - Determine how to implement the selected security controls from the risk treatment plan
  - Test solutions and evaluate residual risks



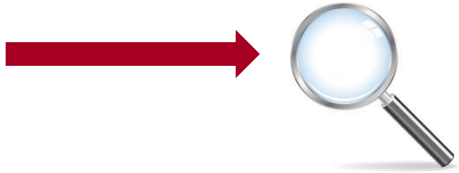
Security and Privacy Architecture DEsign

→ Design



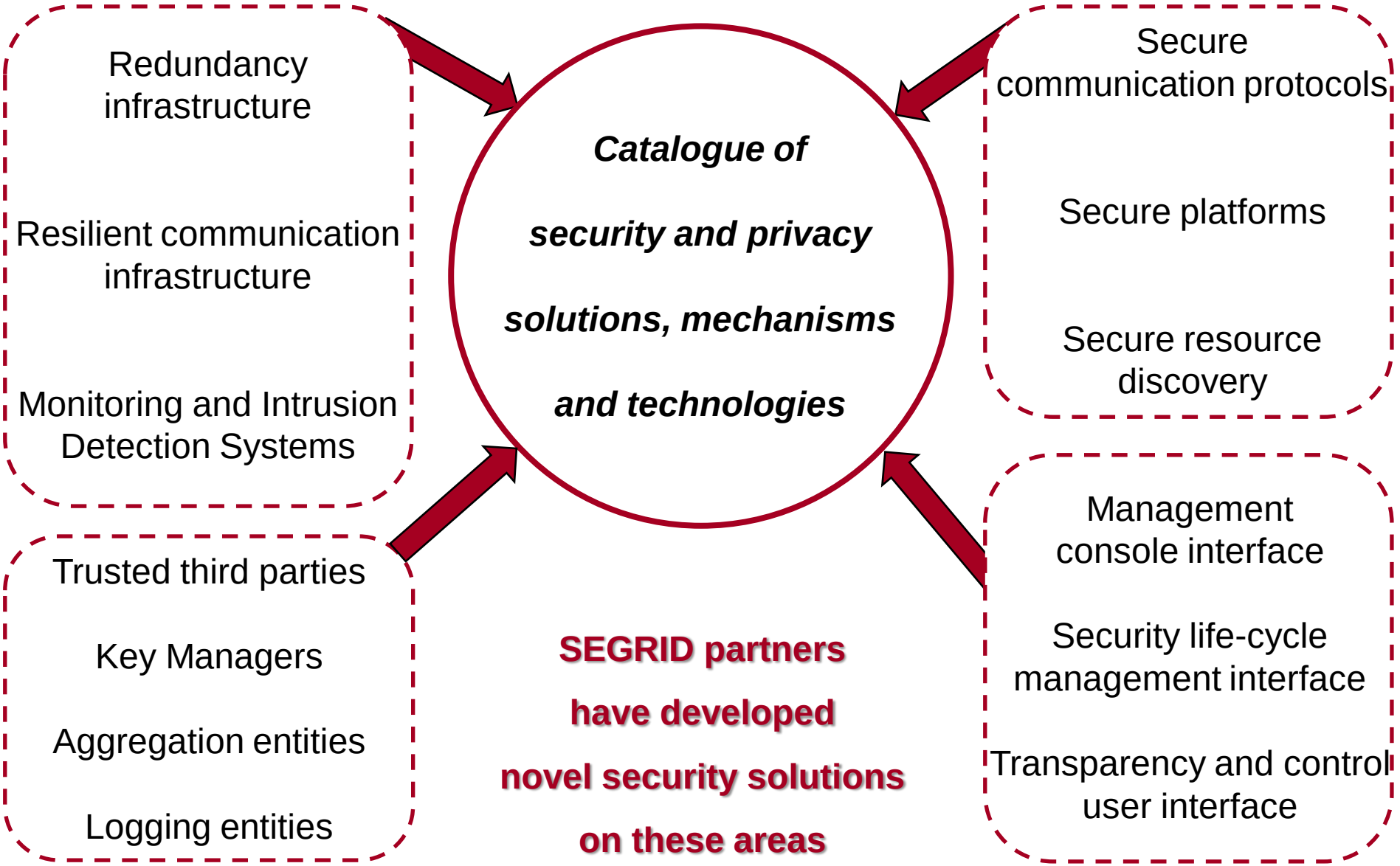
- **Goal**
  - Analysis & synthesis of SPADE inputs
  - Build a first preliminary security and privacy architecture

- **Considered input**
  - *Specific use case* – Functional component and communication flows
  - *Cost and performance requirements* – Maximum costs and minimum performance
  - *Security and privacy goals* – Information and system assets
  - *Prioritized risks and required security controls* – From the early risk assessment
  - *Adversary model* – Capabilities, available information, available resources
  - *Best practices and design patterns* – Guidelines and approaches
  - *Security and privacy controls, mechanisms and technologies*



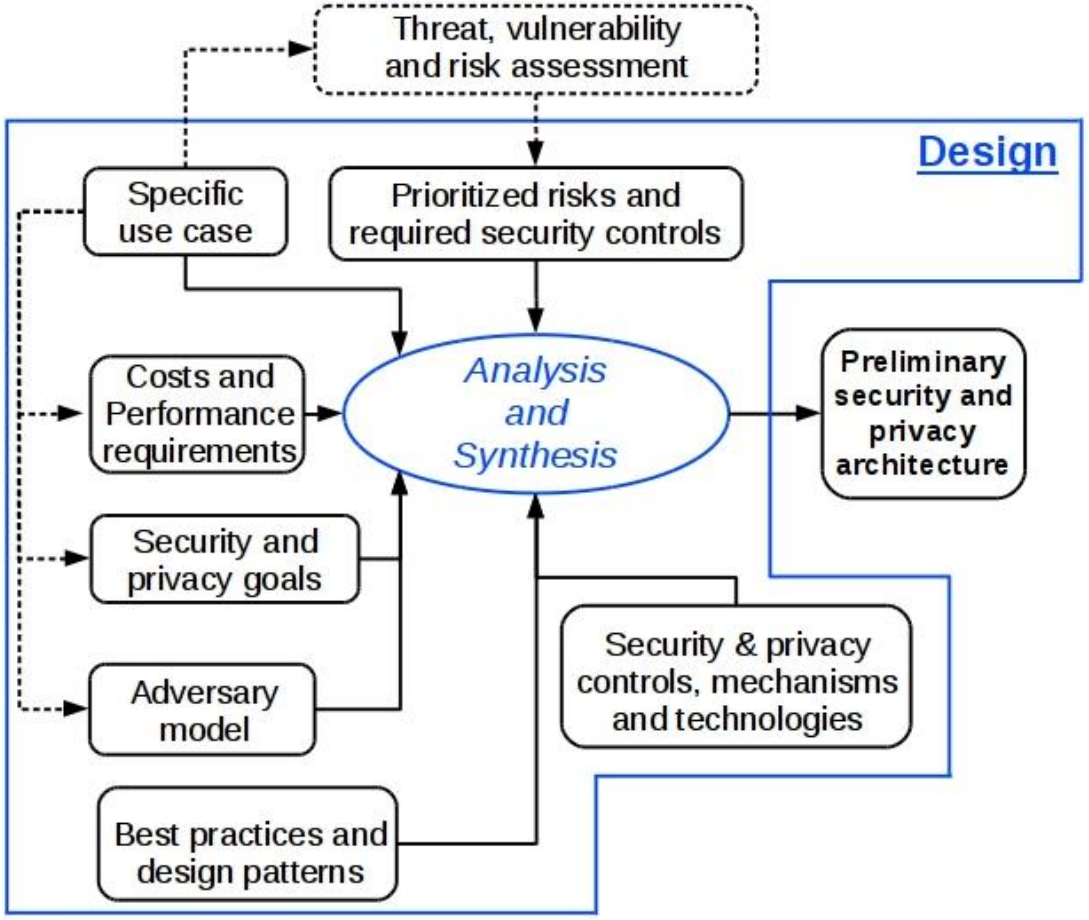
Security and Privacy Architecture DEsign

→ Design



Security and Privacy Architecture DEsign

→ Design



Security and Privacy Architecture DEsign

→ Design (analysis and synthesis)

- **Step 0 – Consider the identified risks**
  - Produced as part of the SEGRID Risk Assessment process
  - Prioritized and along with required security and privacy controls
- **Step 1 – Consider the specific use case**
  - Actual scenario and IT infrastructure
  - Interconnected components
  - Related information and communication flows
- **Step 2 – Define a trust boundary**
  - Partition the use case scenario into two portions (based on goals and risks)
  - Everything above/beyond is out-of-scope and not (required to be) addressed
  - Everything below/within is in-scope and to be secured by SPADE

Security and Privacy Architecture DEsign

→ Design (analysis and synthesis)

- **Step 3 – Select the security and privacy solutions**
  - Goal: produce a secure version of the use case
  - Based on trust boundary, prioritized risks and list of security controls

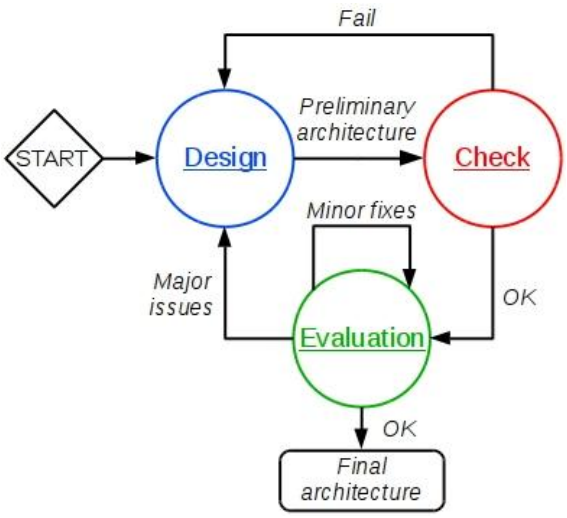
For each pair <*Risk*, *Treatment Actions*>

- Select and combine mitigating security controls, based on the treatment actions
- Justify why the chosen controls are good to address the risk
- Justify how the chosen controls relate to each other and the use case
- Justify how interdependencies/conflicts between controls are addressed

- **Step 4 – Tune and refine the security solutions**
  - Fine tuning of controls, mechanisms and technologies
  - Part of a high-level validation evaluation, before the proper *Check* phase

Security and privacy architecture

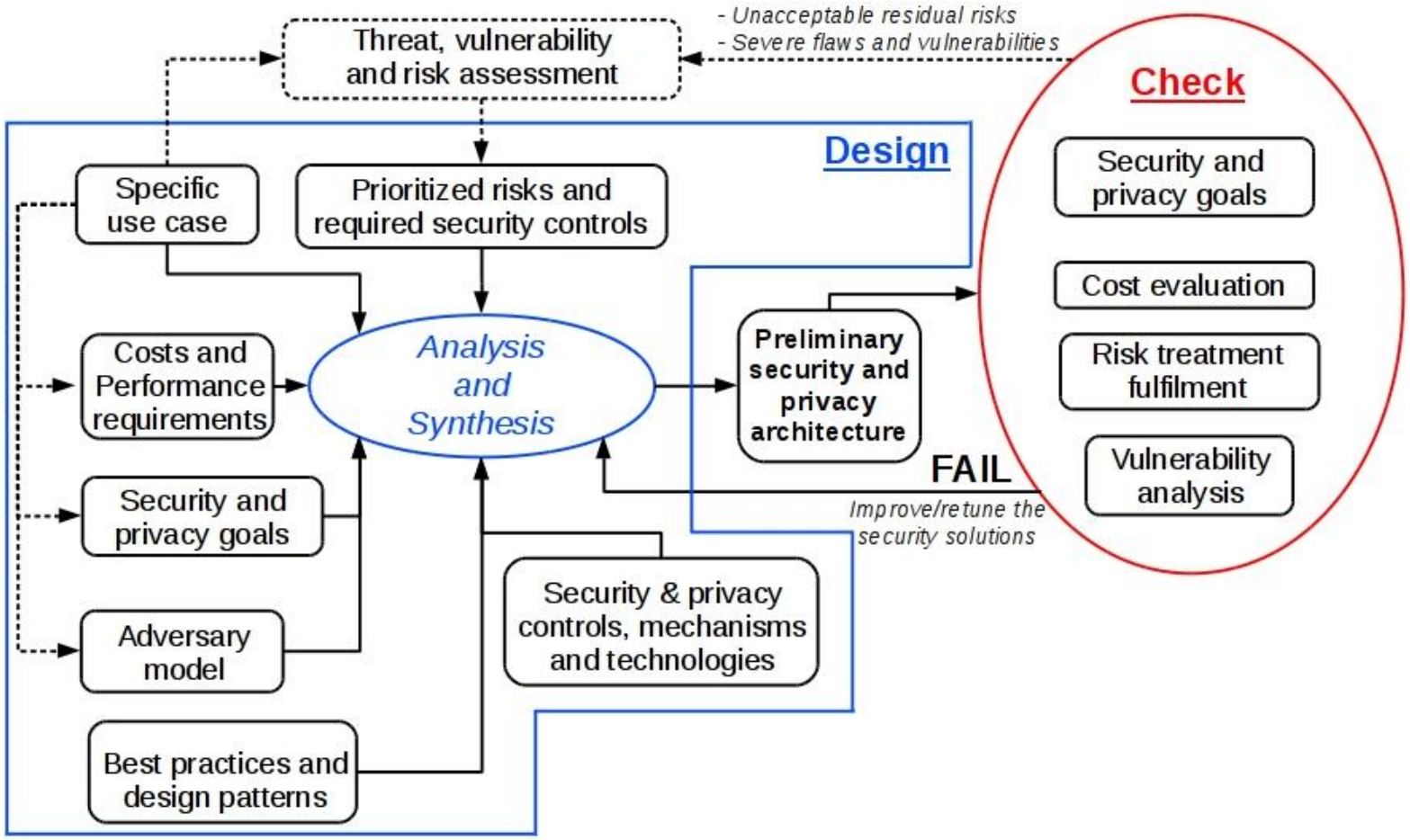
→ Design → Check



- **Goal**
  - Verify that the preliminary architecture fulfils security and privacy requirements, as well as design criteria
- **Considered aspects**
  - Security and privacy goals satisfactorily fulfilled
  - Expected maximum costs not exceeded
  - Risk and threat mitigation – Acceptable residual risks
  - Vulnerability analysis – E.g. securiCAD tool
- **Possible steps back**
  - Redesign the preliminary security and privacy architecture
  - Perform a new Threat and Vulnerability Risk Assessment

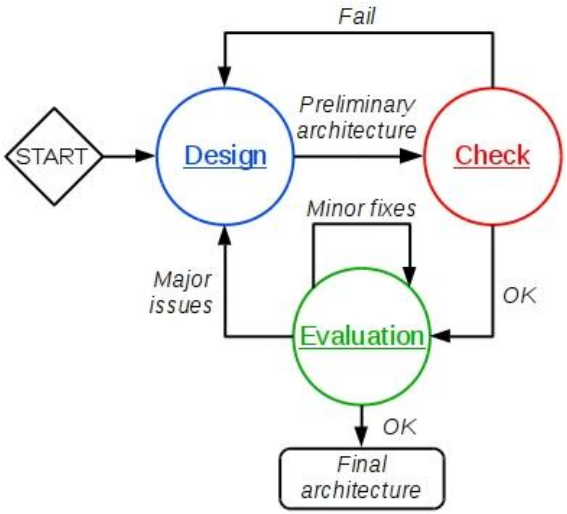
Security and Privacy Architecture DEsign

→ Design → Check



Security and privacy architecture

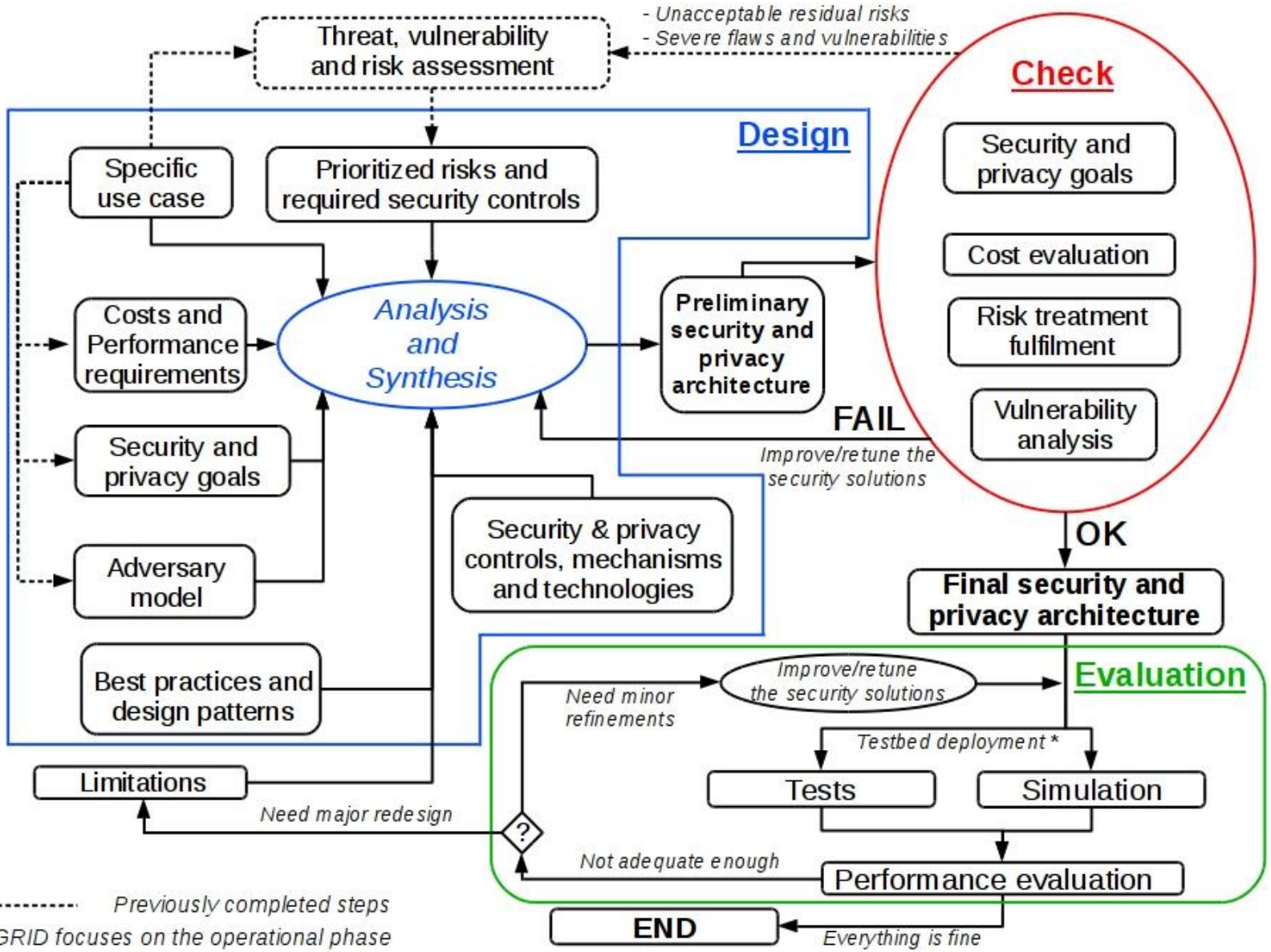
→ Design → Check → Evaluation



- **Goal**
  - Carry out extensive practical tests
  - Assess overall functionality and performance
- **Considered means**
  - Experimental tests on real hardware and testbed
  - Simulation software and other assessment tools
- **Possible outcomes**
  - Required major changes, through a new design
  - Required minor performance improvements, before evaluating again
  - Final security and privacy architecture ready for implementation and deployment

Security and privacy architecture

→ Design → Check → Evaluation



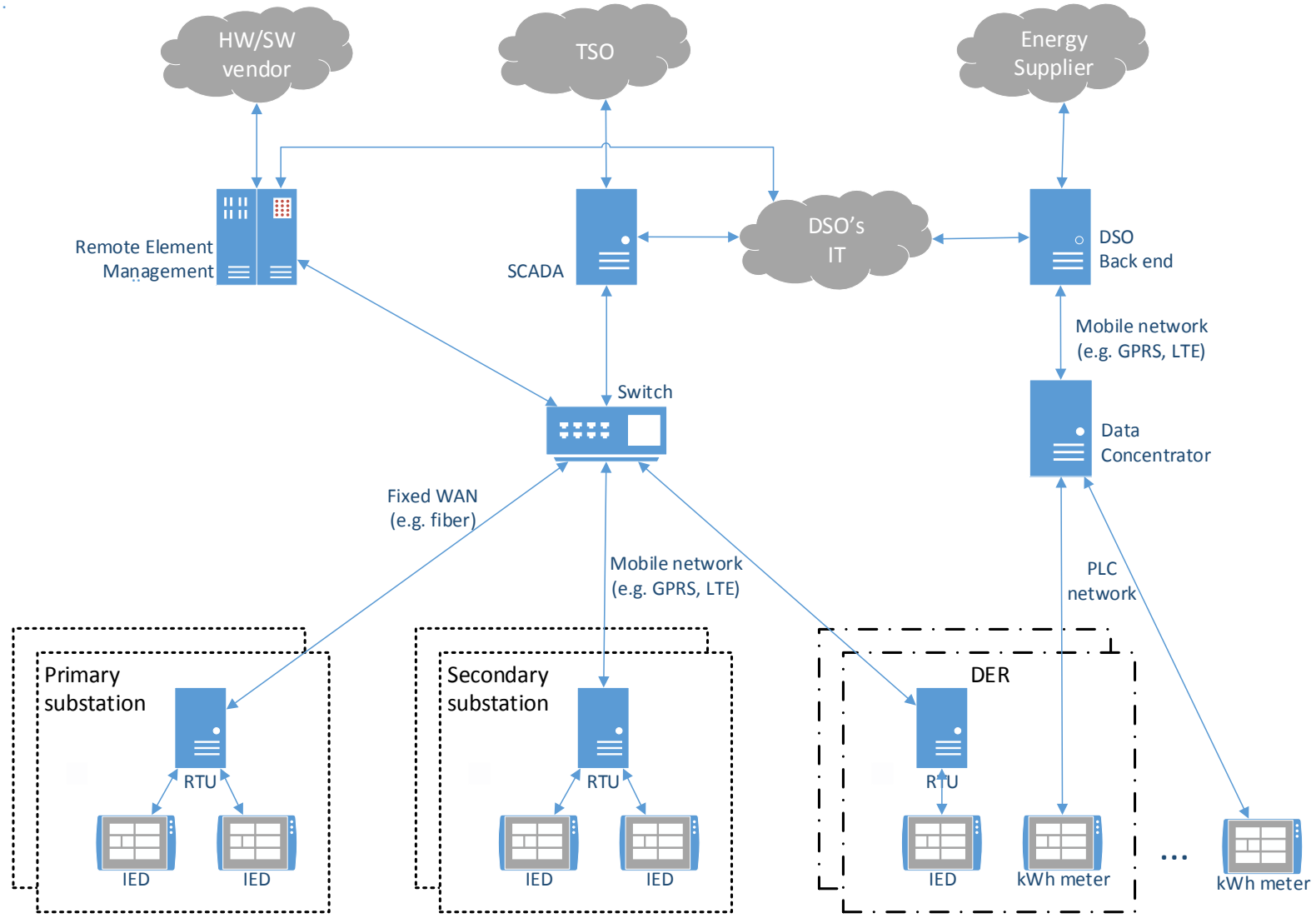
Security and Privacy Architecture DEsign

- **Example on SEGRID Use case 2 – Scenario 2**
  - Load balancing renewable energy centrally
  - Balancing MV renewable energy centrally

- **Focus on the SPADE Design phase**
  - The outcome is the preliminary security and privacy architecture
  - Purely illustrative example (outcomes may likely be more complex)

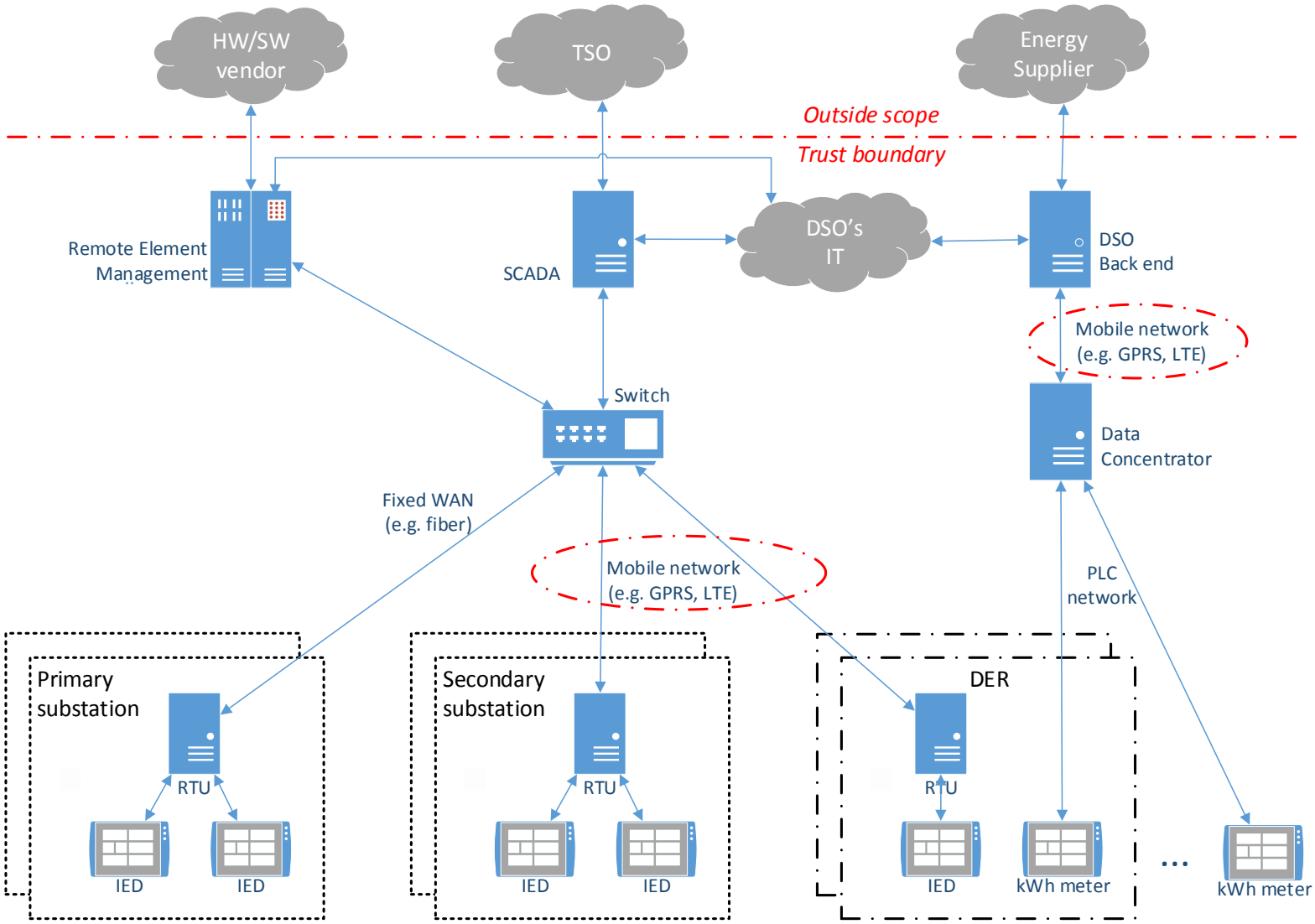
Security and Privacy Architecture DEsign

Use case 2 - Scenario 2



Security and Privacy Architecture DEsign

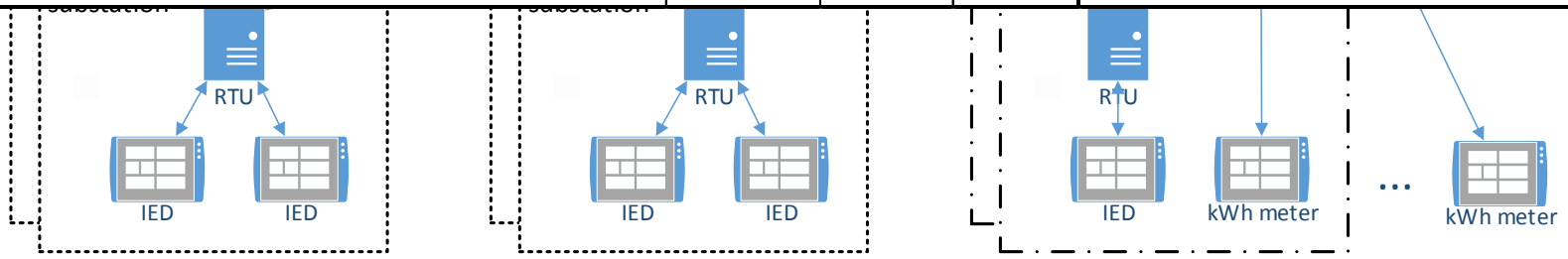
Use case 2 - Scenario 2



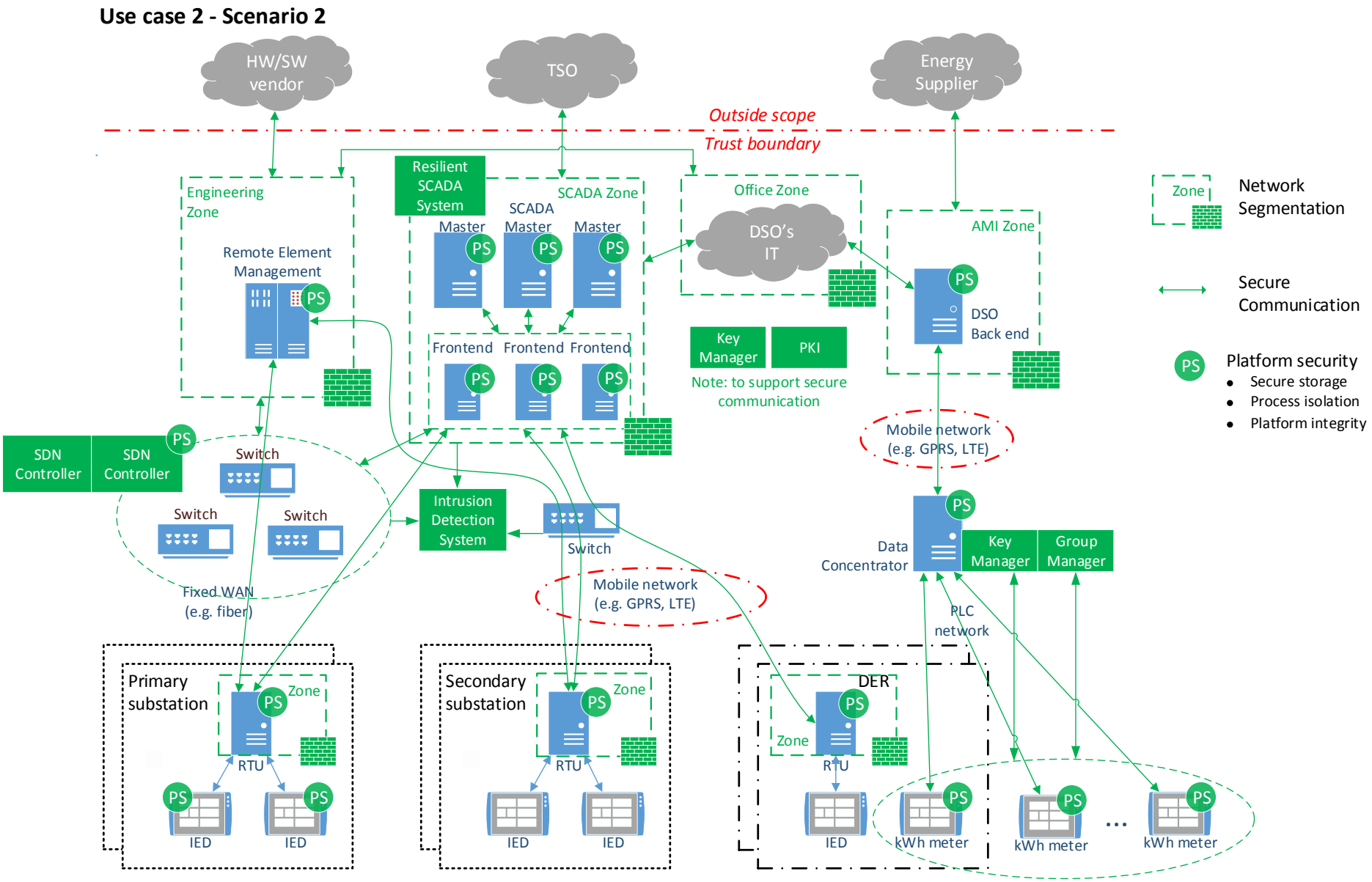
Security and Privacy Architecture DEsign

Example of Prioritized Risks & Risk Treatment Plan

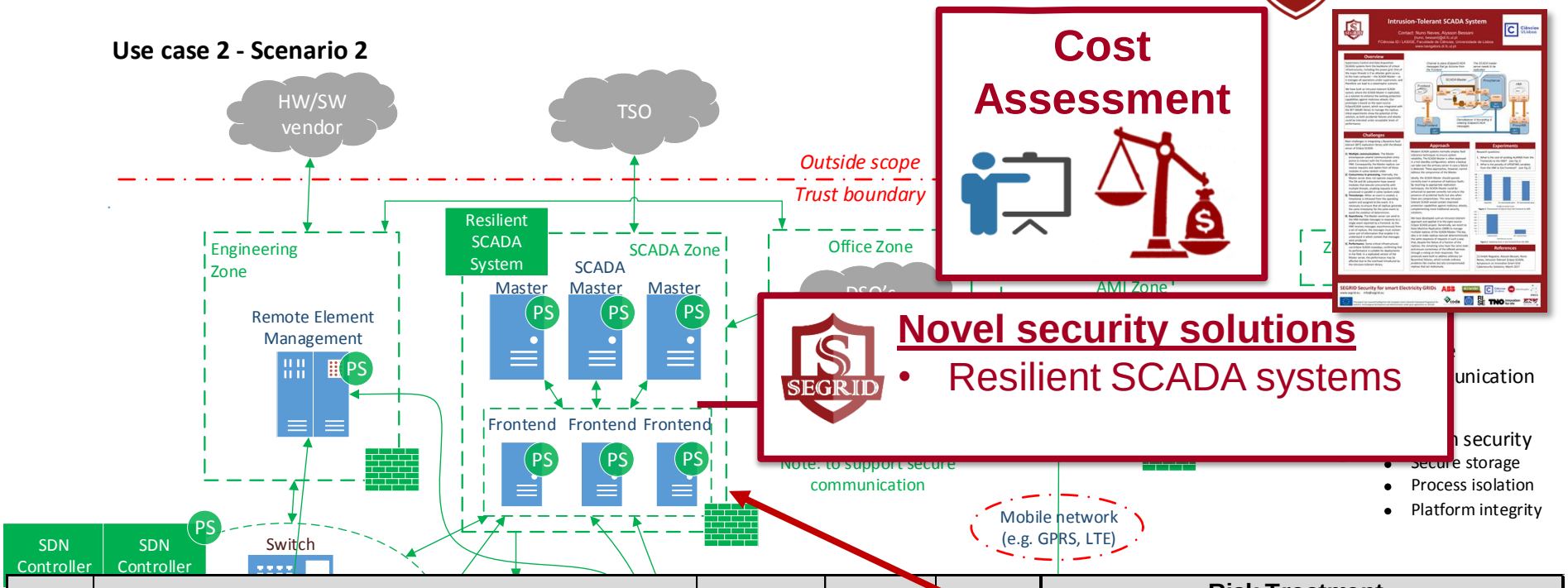
ID	Threat	Likelihood	Impact	Risk	Risk Treatment - Selected Security Controls
UKR 2016	Attackers deliver malware launcher to the SCADA zone of the Utility. The launcher has been programmed with knowledge of the RTU protocols used by the utility. The launcher issues commands according to protocol standards to open high voltage breakers which creates blackouts in part of a major city of the attacked country	Possible	Very high	**Critical**	**FR 3: Data integrity** - *Ensure the integrity of the IACS to prevent unauthorized manipulation.* **FR 7: Resource availability -** *Ensure the availability of the control system against the degradation or denial of essential services.* **…**
UKR 2015	Attackers leverage legitimate credentials to obtain access to three DSOs, use remotely operated breakers to disconnect power, and wipe additional systems using KillDisk malware at the end of the attack. Corruption of firmware of serial-to-ethernet devices at substations, and follow-up attacks to interfere with restoration efforts.	Possible	Very high	**Critical**	**FR 3: Data integrity -** *Ensure the integrity of the IACS to prevent unauthorized manipulation.* **FR 5: Restrict data flow** **…**
UC2_T*n*	Denial of Service attack on the WAN causing the commnication between primary substation and SCADA to be interrupted.	Possible	Medium	**Major**	**FR 7: Resource availability** - *Ensure the availability of the control system against the degradation or denial of essential services.* **SR 7.2 – Management of network resources** **…**
…	…	…	…	…	…



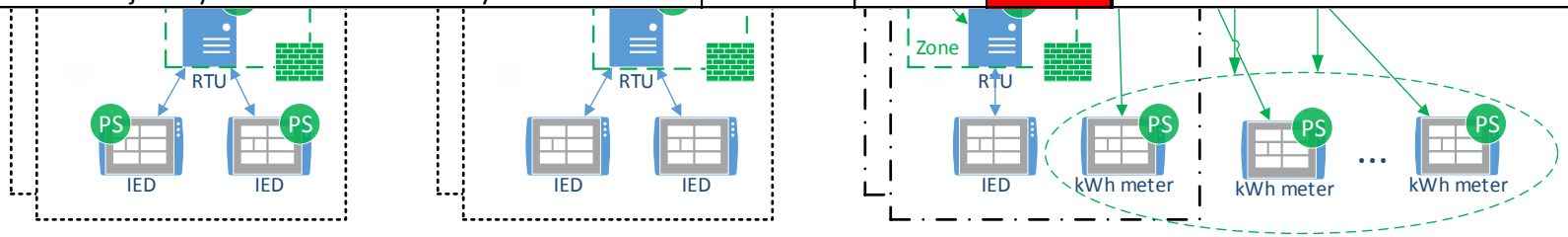
Security and Privacy Architecture DEsign



Security and Privacy Architecture DEsign

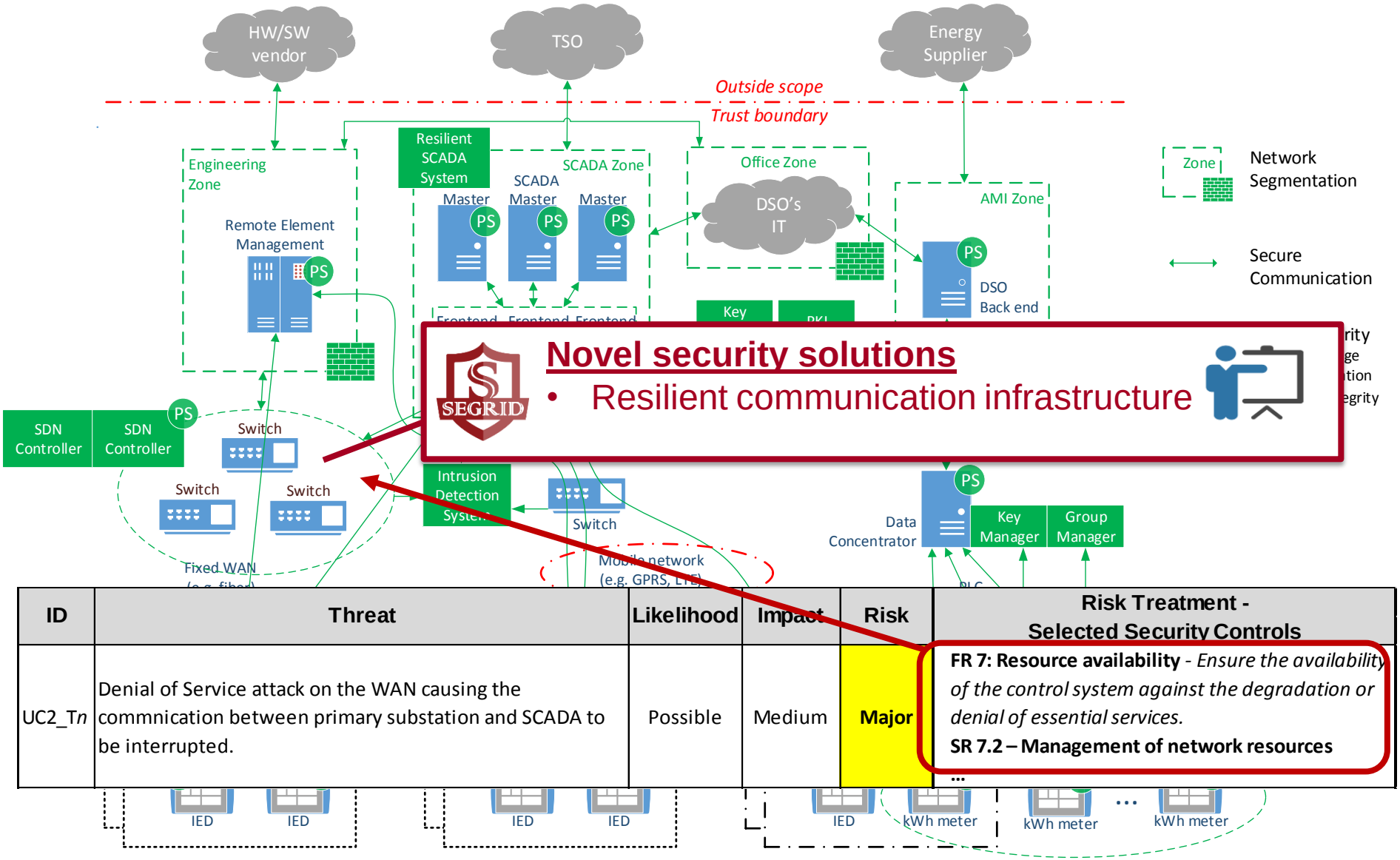


ID	Threat	Likelihood	Impact	Risk	Risk Treatment - Selected Security Controls
UKR 2016	Attackers deliver malware launcher to the SCADA zone of the Utility. The launcher has been programmed with knowledge of the RTU protocols used by the utility. The launcher issues commands according to protocol standards to open high voltage breakers which creates blackouts in part of a major city of the attacked country	Possible	Very high	**Critical**	**FR 3: Data integrity** - *Ensure the integrity of the IACS to prevent unauthorized manipulation.* **FR 7: Resource availability** - *Ensure the availability of the control system against the degradation or denial of essential services.* ...



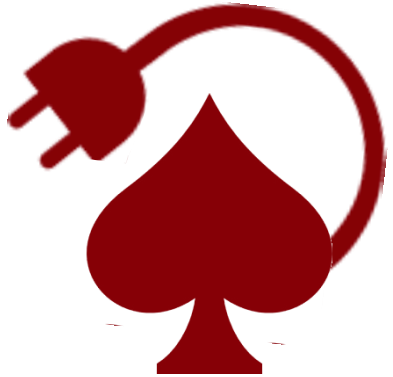
Security and Privacy Architecture DEsign

Use case 2 - Scenario 2



Novel security solutions

- Resilient communication infrastructure

ID	Threat	Likelihood	Impact	Risk	Risk Treatment - Selected Security Controls
UC2_T*n*	Denial of Service attack on the WAN causing the commnication between primary substation and SCADA to be interrupted.	Possible	Medium	**Major**	**FR 7: Resource availability** - *Ensure the availability of the control system against the degradation or denial of essential services.* **SR 7.2 – Management of network resources**

Thank you!