Planning Safety Demonstration

Vikash Katta[1], Pontus Ryd[2], Janne Valkonen[3]

[1]Institute for Energy Technology, Norway
[2]Solvina AB, Sweden
[3]VTT Technical Research Centre of Finland Ltd, Finland

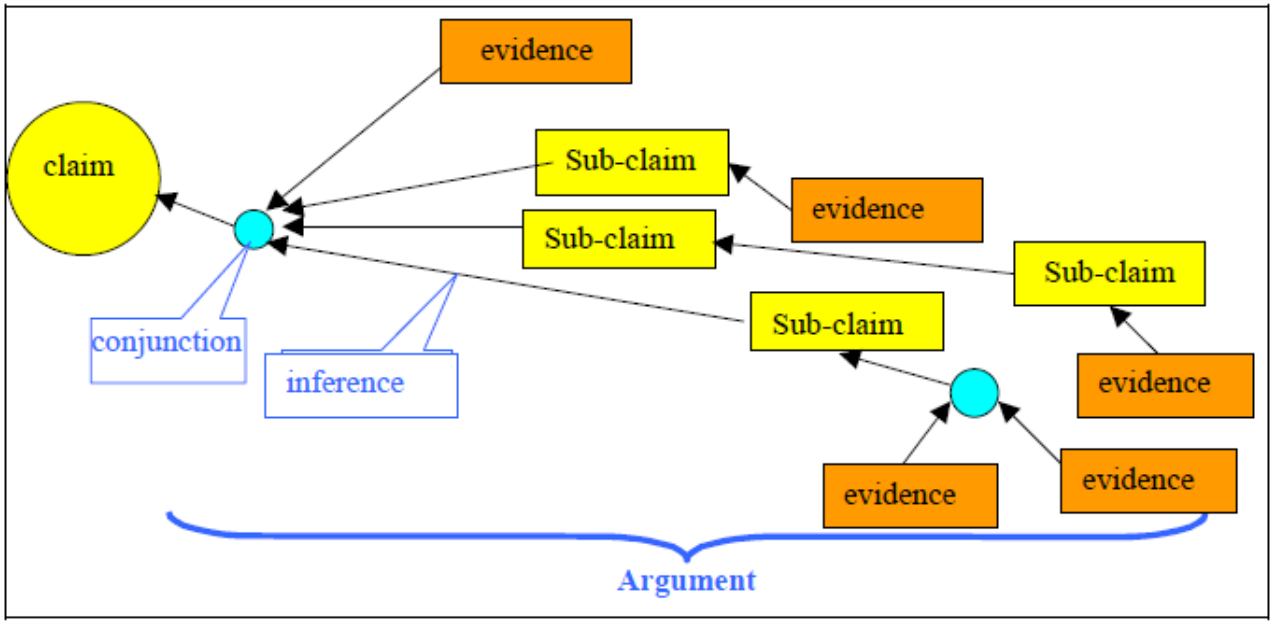
Contents

- Safety demonstration
  - Definitions
  - Challenges
- Nuclear Safety Research (NKS) PLANS project
- Safety demonstration plan guide
- Relevance to other industries

[www.troll.me]

Safety demonstration

- Safety demonstration (safety case)
  - "The set of arguments and evidence elements which support a selected set of claims on the dependability – in particular the safety – of the operation of a system important to safety used in a given plant environment."



[Licensing of safety critical software for nuclear reactors – Common position]

Safety demonstration (cont..)

- Safety (demonstration) plan
  - “A plan, which identifies how the safety demonstration is to be achieved; more precisely, a plan which identifies the types of evidence that will be used, and how and when this evidence shall be produced.”
  - “A safety plan shall be agreed upon at the beginning of the project between the licensor and the licensee.”

[Licensing of safety critical software for nuclear reactors – Common position]

- Safety demonstration plan guide (SDPG)
  - “A guideline or a document describing an approach for how to plan and perform safety demonstration. The guide supports the development of the safety plan.”

[ELFORSK rapport 13:86]

Practices and Challenges in in demonstrating safety of Digital I&C

- Interviews with regulators from 6 countries
  - As a part of OECD Halden Reactor Project
  - Practices and challenges of safety demonstration
- Practice
  - Safety demonstration/case
    - Is required by regulation
    - Not required by regualtion, but regualtor is positive towards it
    - Not required by regualtion, does not want an explicit argumentation
  - Different standards to be complied with
    - IEEE framework
    - IEC/IAEA framework

Challenges

Deficiencies with

- Common understanding between stakeholders
- Convincingly expressing the safety demonstration
- Building confidence
- Documentation overload
- Designing for safety demonstration
- Harmonize safety demonstration with the development process
- Tools for safety demonstration

Common understanding between stakeholders

- Lack of common understanding between stakeholders on:
  - Guiding safety principles, and how these should be achieved
  - Applicable standards and measures
  - Interpretation of regulations
  - Acceptable evidences
  - Expected deliverables
- Lack of communication between the stakeholders, especially at the early stages of the project
  - Right experts (I&C, safety, security) are not involved

Expressing the safety demonstration

- Convincingly express/describe safety demonstration
  - Complete, correct, consistent, and transparent
  - It is not clear how to accurately define (and assess) what these characteristics mean
- Have invalid or missing information, evidence on
  - Application of suitable standards and measures
  - Application of safety principles
  - Description of the interaction with other parts of the system and people, design decisions made
  - Description of strengths and weaknesses of the system
- Not comprehensive
  - Contains complex statements, extraneous details, etc.

Harmonize safety demonstration with the development process

- Safety demonstration activities are not well integrated with the development process
  - Design goes ahead of safety demonstration
    - E.g. decision to use software-based systems without considering how this impacts safety, demonstration
- Safety demonstration should be a living document
  - Updated and maintained throughout the development process including operation, maintenance, decomissioning
  - Systems with a long life expectancy, safety demonstration
    - Has to document the history of modifications made
    - Becomes large, difficult to maintain, and difficult to comprehend

Documentation overload

- Lot of documentation
  - Safety demonstration + supporting documentation
  - System that was built by several engineers over many years
  - Reviewed by few regulators
- Difficult to extract the relevant parts needed to perform different jobs or tasks
  - Stakeholders who review (regualtor, independent assessor)
  - Stakeholders who might use it during activities such as operation and maintenance
    - Maintenance personnel: identify parts of the demonstration which state the maintenance tasks required

Suggestions for improvement - Planning

- Prevented by precise planning early in the project
  - Establish a safety plan, preliminary safety case
- Licensee/utility and suppliers plan for safety
- Communicate plans to the regualtor as well as internally within the organisation
- Supports common understanding of how safety will be achieved
  - agreements on guiding safety principles, evidence (artefacts) required, interpretation of regulations, etc

Utility & supplier view

- NKS PLANS project workshop
  - Practices, challenges, possible solutions for safety demonstration

1. Knowledge gap across organisations (utility, supplier, etc) as well as within disciplines of an organisation
   - What is safety demonstration, what are the contents, how to perform it, …
   - Have a plan at early stages of lifecycle, involve right people in planning
   - Better communication and understanding between experts from different disciplines (safey, security, I&C, management) and organisations
2. Multidisciplinary approach for safety demonstration incorporating boundaries and interfaces between various disciplines
   - Interfaces (e.g. I&C and plant design), completeness of I&C requirements towards plant design, information flow across disciplines
   - Integrating safety demonstration with development process
   - Configuration and change management for the whole plant, all changes have to be reviewed by all the relevant departments.
3. Better understanding of safety demonstration and cost-benefits
   - Concepts, relation to safety systems engineering, safety and cost-benefits

Guidance on safety demonstration planning

- Lack of detailed guidance on how to plan for safety demonstration
  - How to perform safety demonstration during development?
  - What kind of evidence (artefacts) are required and collected in each stage of development process?
  - How to organise the evidence and claims in a logical manner?
- Safety Demonstration Plan Guide (ELFORSK rapport 13:86)
  - Developed by Solvina AB
  - Project steering group constitued by expert representatives from Vattenfall, Fortum, OKG, FKA and SSM
  - Provides a high-level strategy on how to perform the demonstration
  - Starting point for PLANS project

NKS-R PLANS project

- Nordic Nuclear Safety Research (NKS) funded

- Aim: Improve guidance on safety demonstration planning for Digital I&C systems in NPPs

PLANS objectives

- Refining the Safety Demonstration Plan Guide, by:
  - Identify type of evidence (artefacts) needed
  - Provide explicit and clear reasoning structure for organising claims and evidence
  - Develop illustrative examples
- Establishing a Nordic network of competence on nuclear Digital I&C safety demonstration, with experts from
  - Regulators, utilities, suppliers, technical consultancy firms and research organisations
  - http:\\nordicnsec.ife.no
- Long term objective:
  - Define a framework for Digital I&C safety demonstration planning
  - Serve as a harmonized foundation between the Nordic countries

Safety Demonstration Plan Guide

A general guide to Safety Demonstration with focus on digital I&C in Nuclear Power Plant modernization and new build projects

Research project initialized and sponsored by Elforsk

Solvina
Energy Excellence

Background to the Guide

- The Guide is to provide a common structure and guidelines for how to perform Safety Demonstration, agreed upon by Swedish utilities and the regulator.
- A common structure would facilitate the exchange of experience between utilities and projects.

Background to Safety Demonstration

- Experiences from complex modernization and new build projects including digital I&C indicates a need for a complement to present licensing approaches.
- US NRC has found the present Standard Review Plan (NUREG 0800) insufficient and develops new review guidelines for digital I&C (RIL-1101).
- The regulators of six European countries have summarized common positions (SSM 2013:08) recommending Safety Demonstration as a possible solution to the problems.
- Safety Demonstration has been applied in Swedish projects with good results.

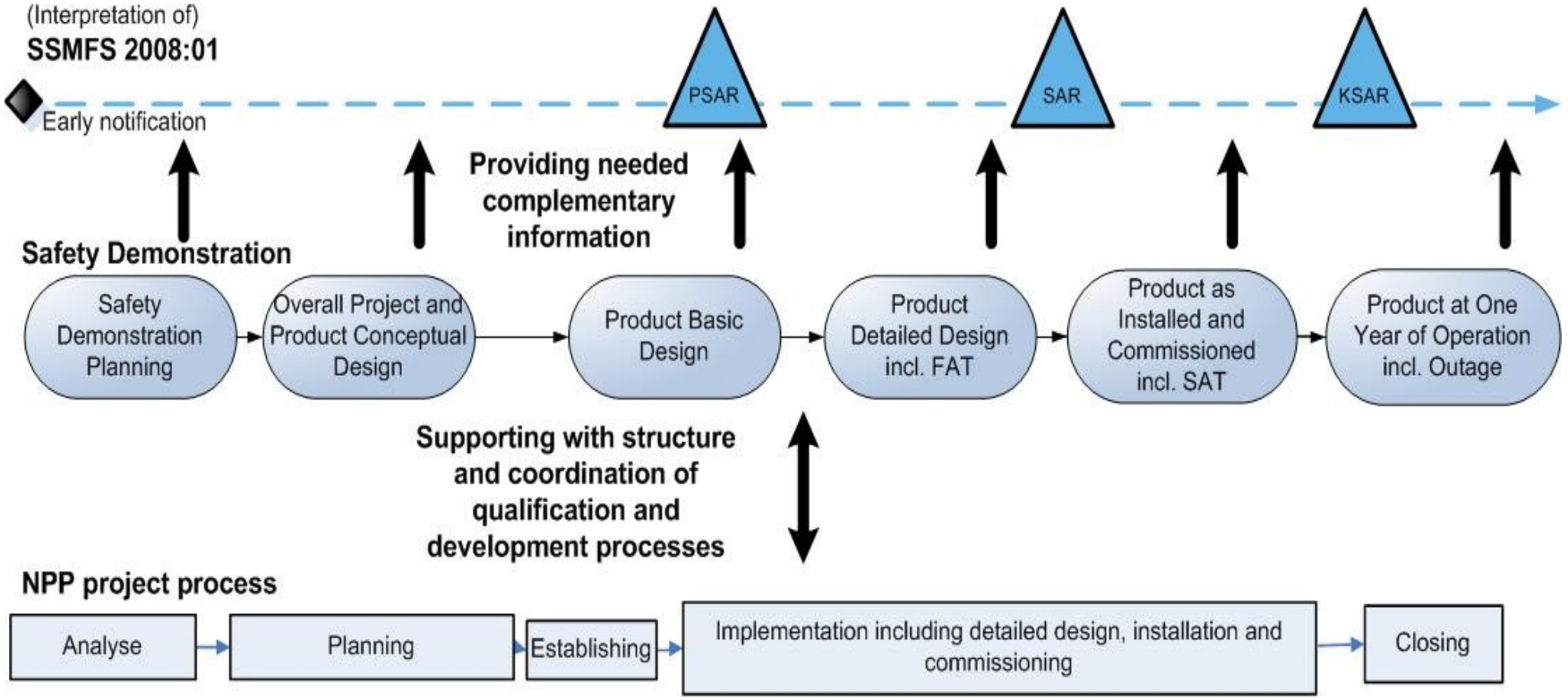
Cornerstones of Safety Demonstration

- Continuous communication and **stepwise approval** of results **according to agreed plan** between the project stakeholders (supplier, NPP project, licensee and regulator).
- Planning and communication to be started **early** in the project.
- **Graded approach** meaning to demonstrate safety with level of detail commensurate to importance to safety.
- Qualify **not only adequate product** but **also work processes, organization and competence** of people involved. All proven adequate - separately and in combination - and in all of the system life cycle phases.

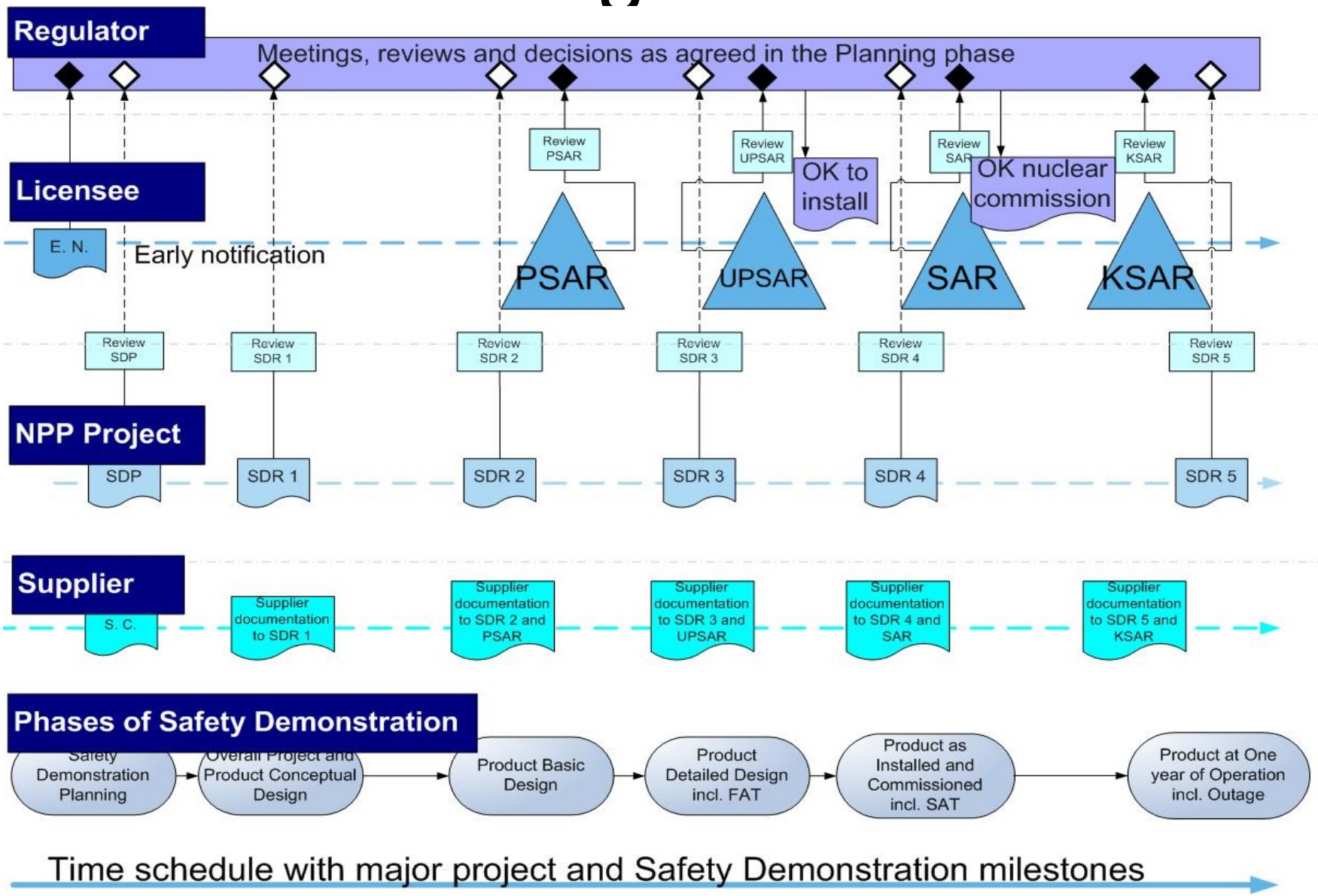
Contents of the Guide

1. Introduction
2. Life cycle and contents of Safety Demonstration
3. Safety Demonstation Planning phase
4. Safety Demonstration Qualification phases
5. Safety Subject Areas – Contents of Safety Demonstration
6. Specific challenge areas for digital I&C
7. References
8. Templates

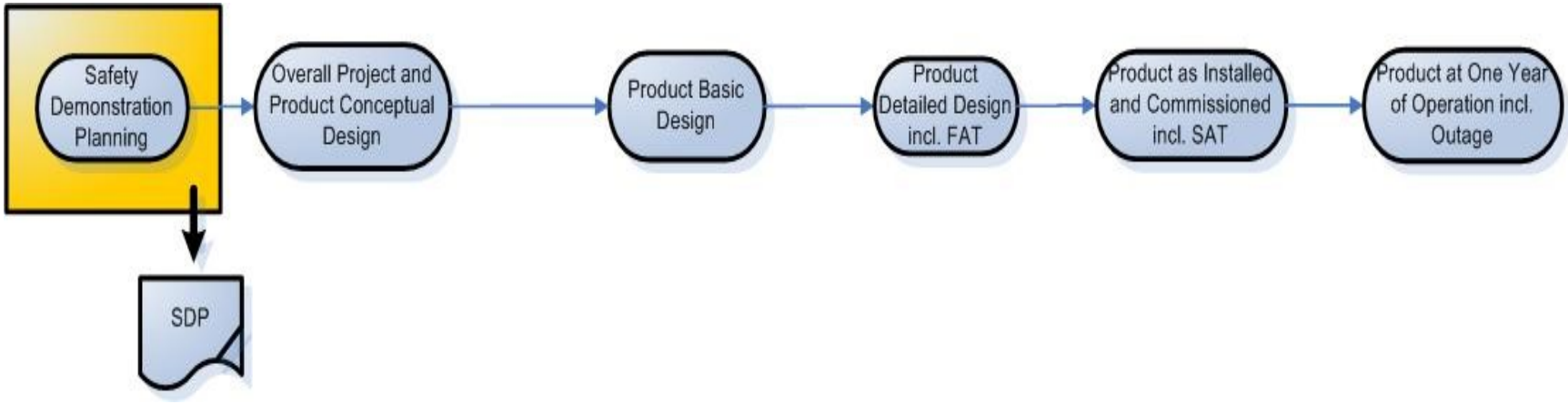
Safety Demonstration complements the present licensing approach and integrates it with the normal project design control



Overview diagram



Planning phase

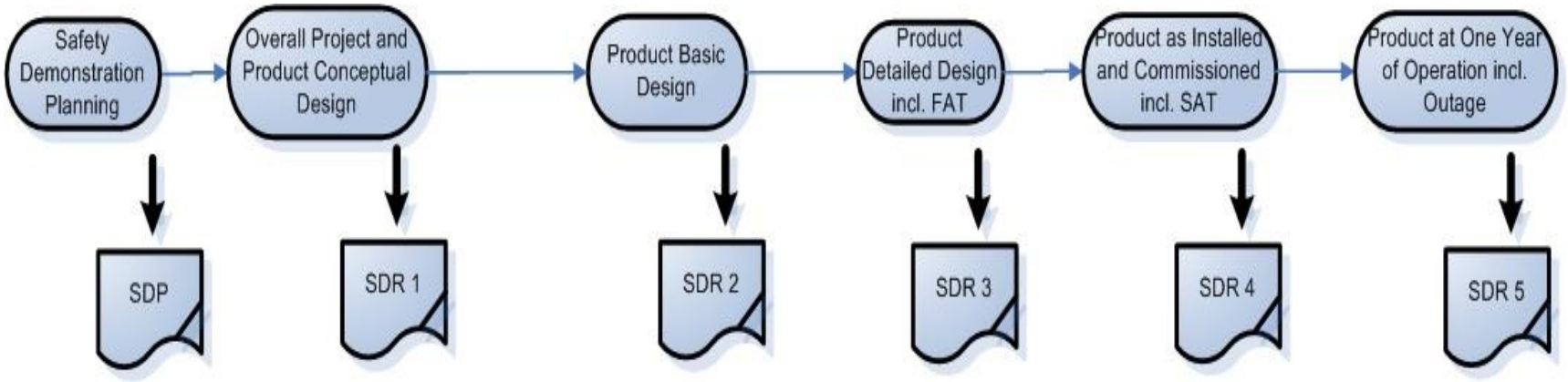


Important outcome of the planning phase:

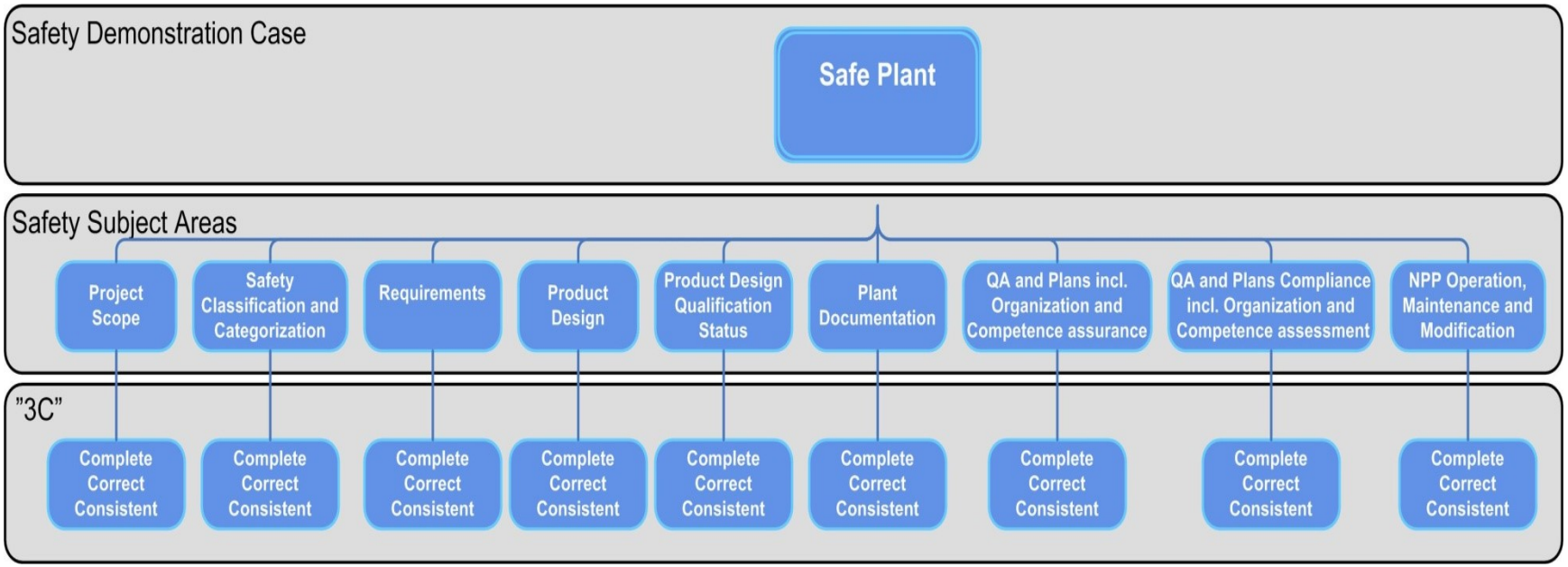
- Safety Demonstration Plan – SDP with overview diagram
- Safety Demonstration Case **Definition** including demonstration strategies
- Scope and requirements for Qualification phases

Qualification phases

1. Overall Project and Product Conceptual Design
2. Product Basic Design
3. Product Detailed Design including FAT
4. Product as Installed and Commissioned including SAT
5. Product at One Year of Operation including Outage



Safety Case



SSAs are safety aspects that together form the overall safety case.

Safety Subject Areas

The set of SSAs to select for a specific Safety Demonstration must always be decided case by case for each individual project.

Standard Safety Subject Areas are suggested by the Guide and described with;

Purpose and scope defining the area.

Strategy advising how to perform the demonstration of the area.

Examples of specific evidence to be used and possible reference to relevant standards.

SSAs are defined and assessed in the planning phase and thereafter re-assessed (with possible adjustment if necessary) in each qualification phase.

Overview of phase report content and focus

	Planning Phase	Qualification phases				
SSA	Safety Demonstration Planning	Overall Project and Product Conceptual Design	Product Basic Design	Product Detailed Design including FAT	Product as Installed and Commissioned incl SAT	Product at One Year of Operation incl Outage *
Project Scope	S	F	C	C	C	-
Safety Classification and Categorization	S	F	C	C	C	C
Requirements	S	F	C	C	C	C
Product Design	S	I	F	F	C	C
Product Design Qualification Status	S	-	F	F	F	C
Plant Documentation	S	-	I	F	F	C
QA and Plans incl. Organization and Competence Assurance	S	F	C	C	C	C
QA and Plans Compliance incl. Organization and Competence assessment	S	I	F	F	F	I
Operation, Maintenance and Modification	S	-	-	I	F	F

Qualification phase scope and requirements

SSA	Overall Project and Product Conceptual Design	Scope	Requirements
Project Scope	**F**	Project scope definition (including Product, technical documentation, instructing documentation, competences	Project scope definition "3C" and agreed by all stakeholders.
Safety Classification and Categorization	**F**	Overall principles for safety classification and categorization	Safety classification and categorization principles "3C" as defined
Requirements	**F**	Overall high-level requirements specification	High level requirements "3C", e.g. that I&C requirements originate with traceability from the Plant design basis (may require significant iteration) and that relevant portions of chapter 6 challenge areas are properly reflected.
Product Design	**i**	Product Architectural Design (or Conceptual Design)	The design version identified and assessed for "3C". *
Product Design Qualification Status	**-**	Not in scope this phase unless chosen to add	If applicable, any V&V records identified support product design qualification at present status
Etc. for all SSA			

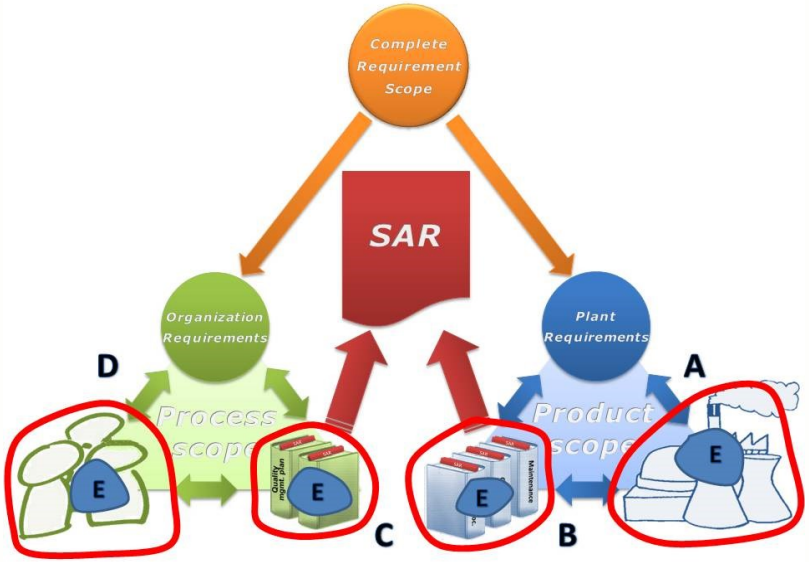
Example: **Table 4-1** Presenting the focus for the Safety Demonstration in the *Overall Project and Product Conceptual Design* qualification phase. Table not complete in this picture.

Example questions in SDPG guidance

1. How explicit is product **scope (functional, physical and geographical) defined with boundaries/interfaces**? How and when is it documented, agreed and communicated? How strongly applied along the project and plant life cycle?

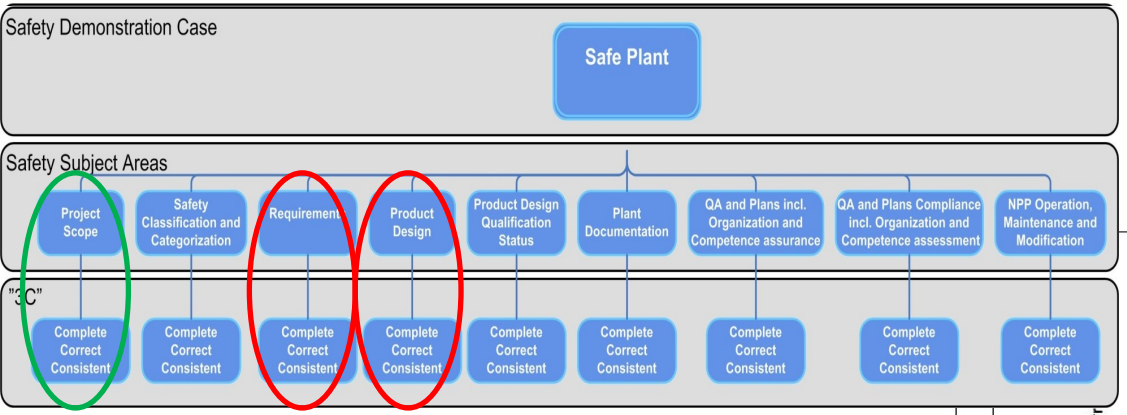
SAFETY SUBJECT AREAS

- Project **Scope**
- Safety Classification and Categorization
- Requirements
- Product Design
- …



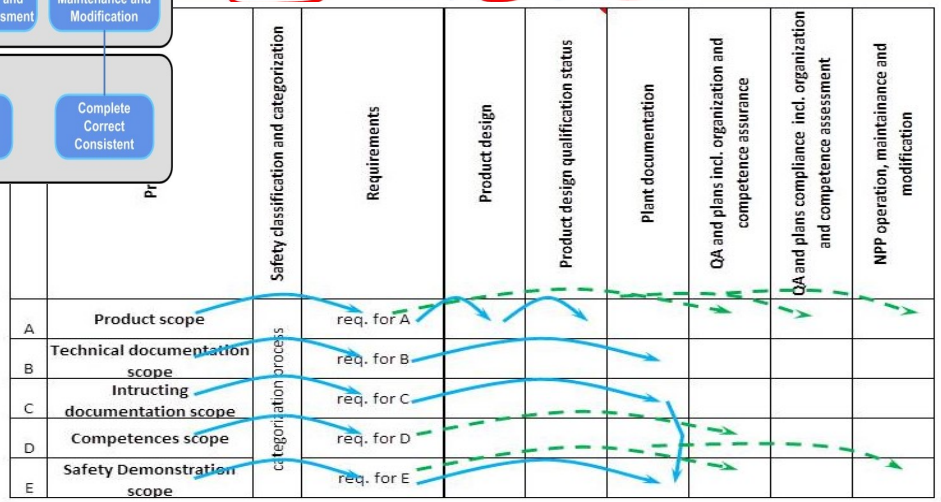
Example questions in SDPG guidance

2. Do you demonstrate that the requirements specification is **complete** in relation to scope and that product design is complete in relation to scope and requirements? If so, how? (If not, how claim safety?)



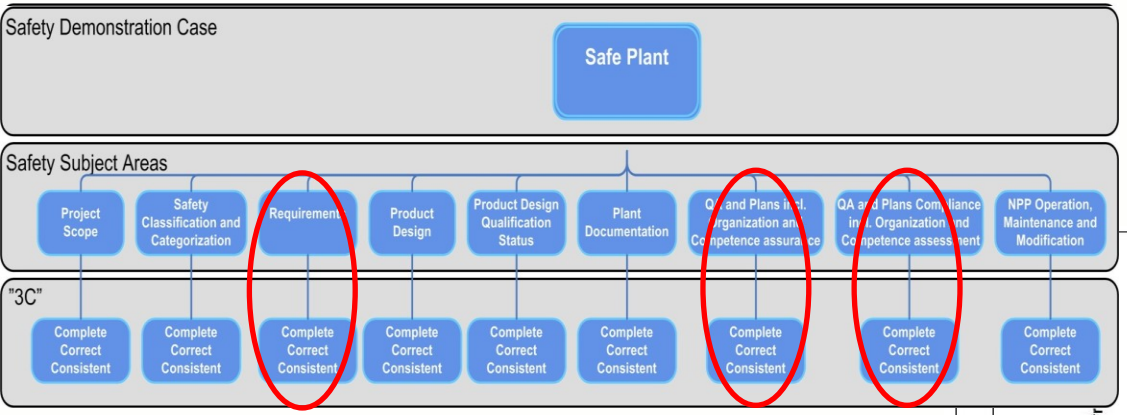
Reqts **complete**
wrt scope?
wrt input?

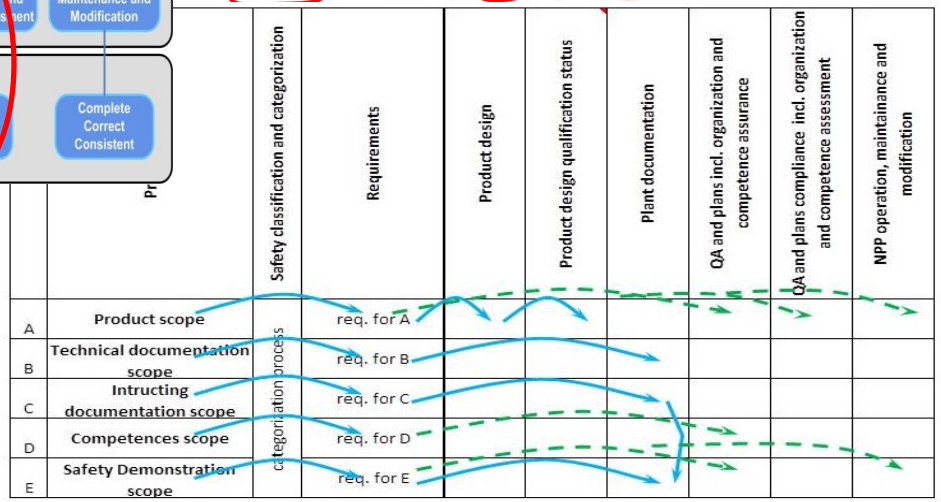
Design **complete**
wrt scope?
wrt reqts?



Example questions in SDPG guidance

3. How do you know that I&C requirements are **consistent with plant design**? Do you demonstrate? If so how? (If not, how claim safety?) During project – After project, along life cycle?





Reqts **consistent** and traceable wrt input?

Reqts maintained **consistent** and traceable thru LC (CM process def and appli) wrt input?

SSAs – claim, context, evidence

Requirements SSA

- Claim: Applicable requirements (design, standards, work process, competence) are identified.
  - Context: Project scope specification, Requirements specification
  - Evidence: Requirements specification review, QA review, Traceability matrix

- Claim: I&C requirements are traceable to plant level requirements
  - Context: project scope specification, requirements specification
  - Evidence: Traceability matrix

SSAs – claim, context, evidence

- Claim: I&C requirements are traceable to functional, system design, detailed design requirements.
  - Context: Requirements specification, Design description
  - Evidence: Traceability matrix

- Claim: All hazardous conditions are identified and are acceptable.
  - Context: Requirements specification, System level hazards
  - Evidence: Hazard log, Hazard analysis report, Hazard analysis report review, Traceability matrix

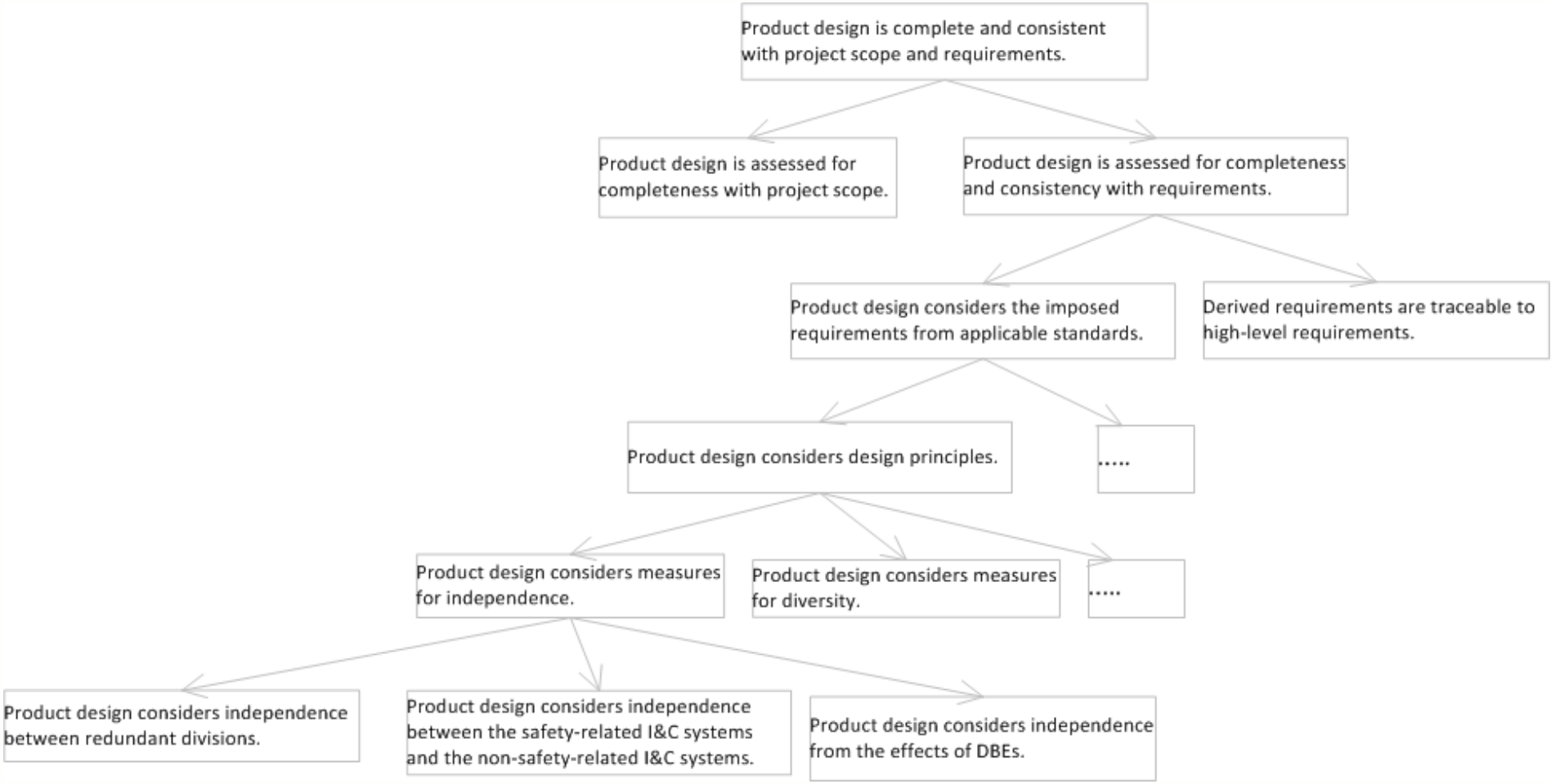
SSAs – claim, context, evidence

Product Design SSA

- Claim: Applicable version of product design is identified.
  - Context: Design description, requirement specification
  - Evidence: Design review, CM report

- Claim: Product design is complete and consistent with project scope and requirements.
  - Context: Design description, requirement specification, standards
  - Evidence: Design review, traceability matrix

Claim decomposition



- Should define and relate context and evidence

Relevance to other industries

- Automotive
  - To learn from?
- Railway
  - Safety case is mandatory and widely used
  - Looking into reuse, modular safety case
- Air traffic management
  - Upcoming EU regulations might require safety case
  - Safety case is not widely practiced
  - Lack of awareness on safety case
  - Lack of management participation
  - Safety cases focus mostly on compliance to standards

Conclusions

- Safety demonstration/case allows to see overall system safety at a shallow level
  - Identify what is required and what is missing
  - Complement with (in-depth details/evidence) documentation from engineering activities.
  - Focus on important aspects/areas that allows to make conclusions on safety
  - Make important information explicit, instead of a reviewer going through vast amount of documentation
- Safety Demonstration Plan Guide (application of it) is a starting point for safety demonstration
- Put forward the plans/approach for reasoning on safety, including claims, required evidence
  - Making your plans visible!
  - Agree/disagree upon aspects

Thank you!