# I&C Architecture
## within NUCLEAR SAFETY

# Main Challenges
## in new builds project

**25/04/2018**

SLOVENSKÉ ELEKTRÁRNE

# Objective

- **I&C Architecture**
  - What is the role within nuclear safety ?
  - What are the requirements driving the I&C architecture ?

- **The main challenges in new builds projects**
  - What is behind nuclear plant complexity ?
  - Why the nuclear plant construction lasts so long ?

# I&C Architecture

# I&C Architecture

## Definitions (IEC, IAEA)

- **I&C Architecture**
  - Organizational structure of the instrumentation and control systems of the plant that are important to safety.
- **I&C System**
  - System, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself.
- **I&C Function**
  - Function to control, operate and/or monitor a defined part of the process.

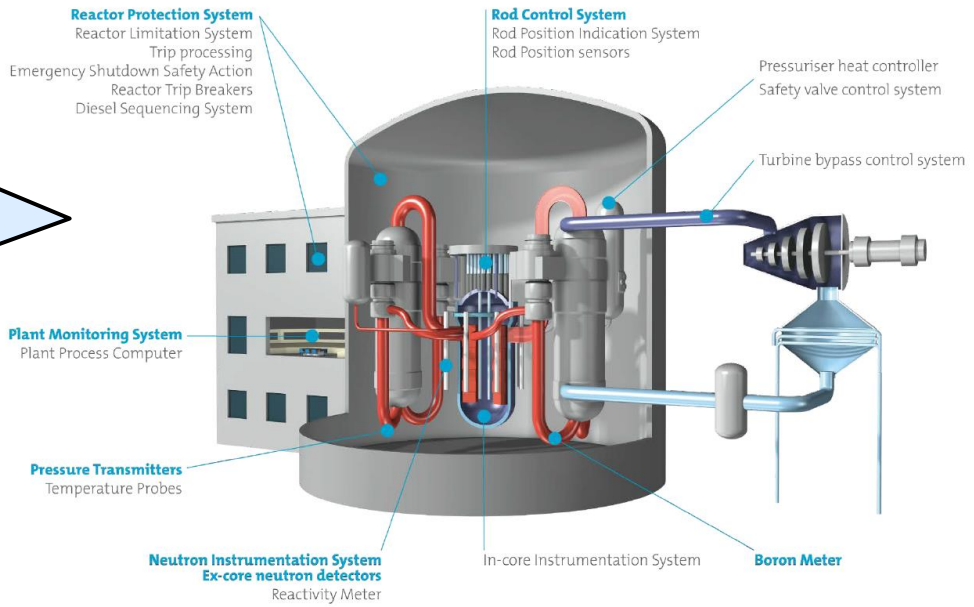
# I&C Architecture

## Definitions (exemplary)

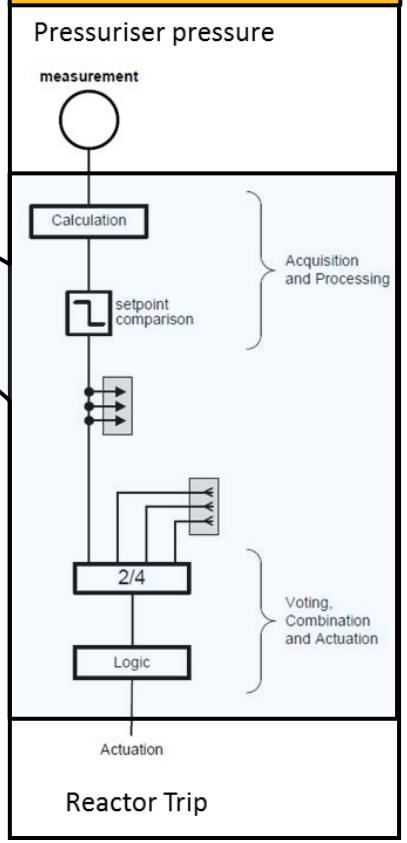
**I&C Architecture**

- RPS
- RCS
- PMS
- NIS
- …

**I&C System**


**I&C Function**



# I&C Architecture

## Role within nuclear safety

SLOVENSKÉ ELEKTRÁRNE

**Defense in Depth Concept**

**Level 01**
- Prevention of abnormal operation

**Level 02**
- Control of abnormal operation

**Level 03**
- Control of accidents within the design basis

**Level 04**
- Severe accident management

**Level 05**
- Off-site emergency

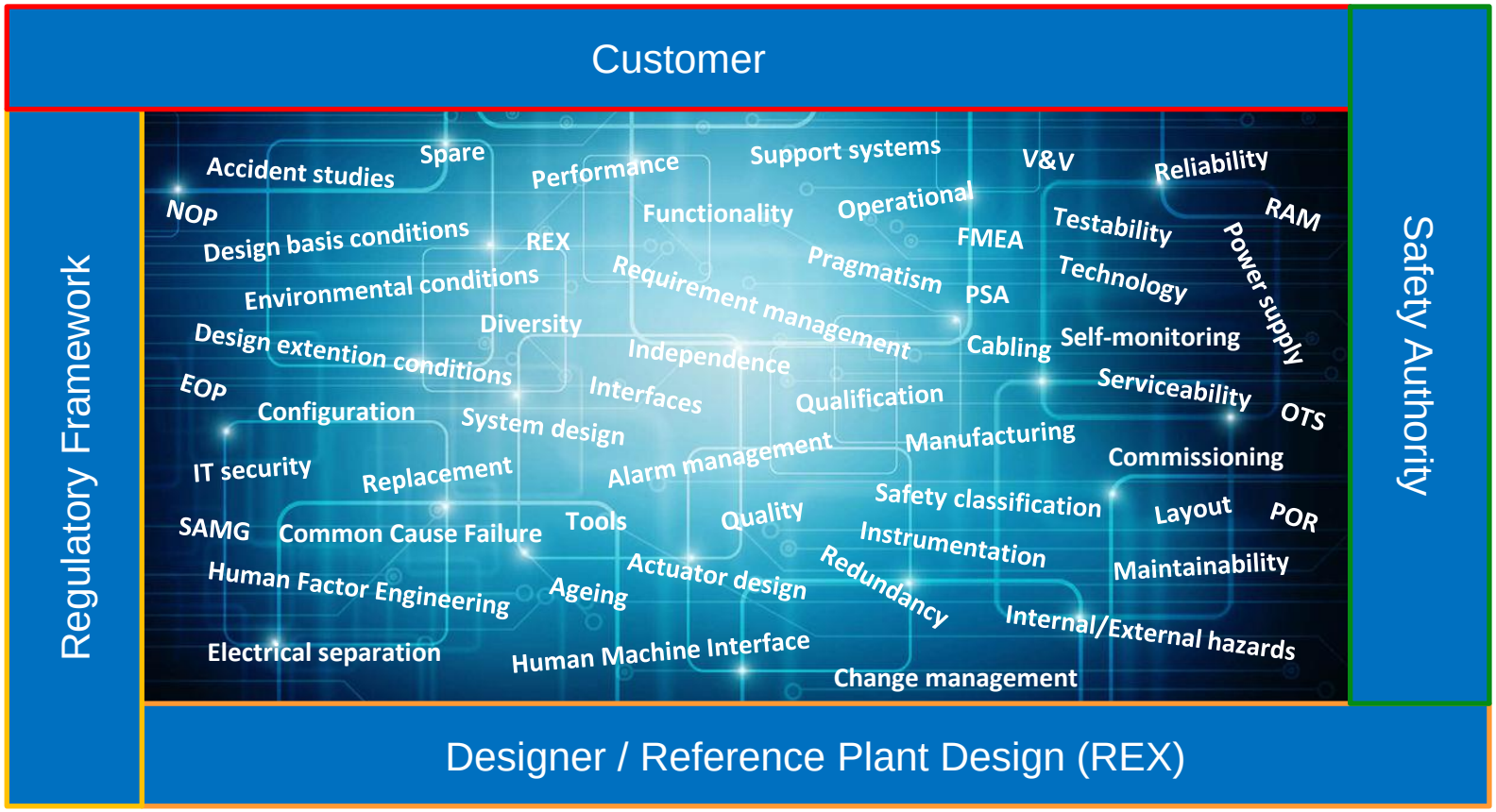
1) One shall not violate any rule
2) There is only single failure
3) The operator is perfect, who never makes any mistake
4) The NC systems do not exist
5) I give a conclusion with certainty

1) There is no rule, only the probability matters
2) There can be multiple failure or common cause failure
3) Every human makes error, it's just a question of probability
4) Maybe they are less reliable but they do exist in reality
5) I give a result with uncertainty of just one order of magnitude…

**Mr. Deterministic** **Ms. Probabilistic**

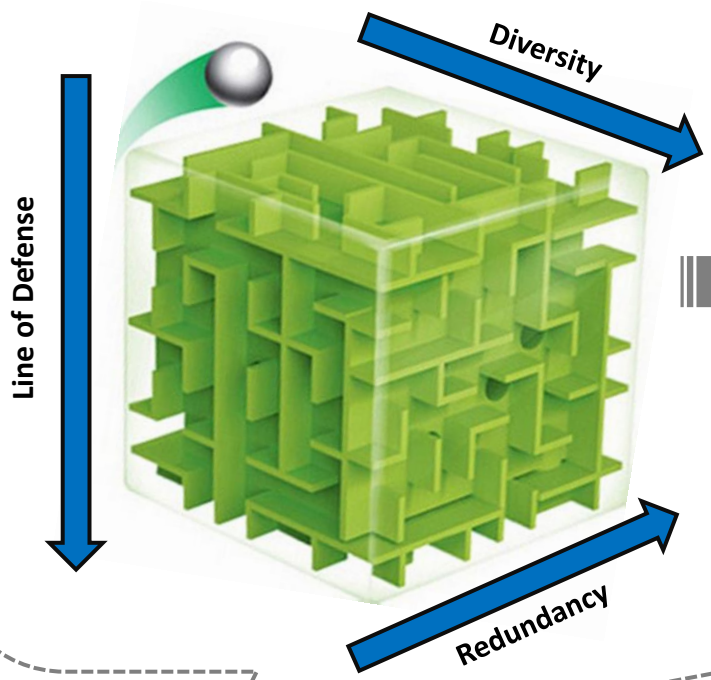
# I&C Architecture

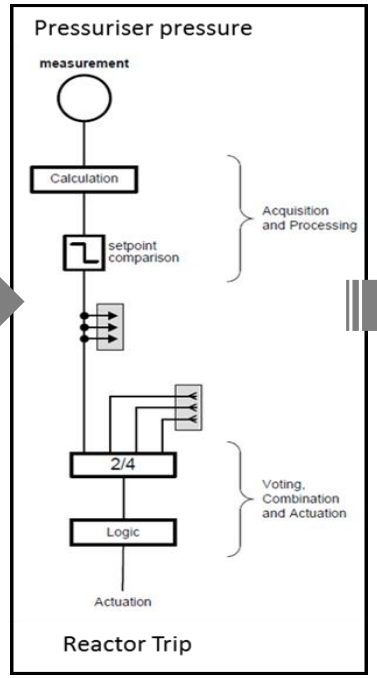
## Requirements complexity

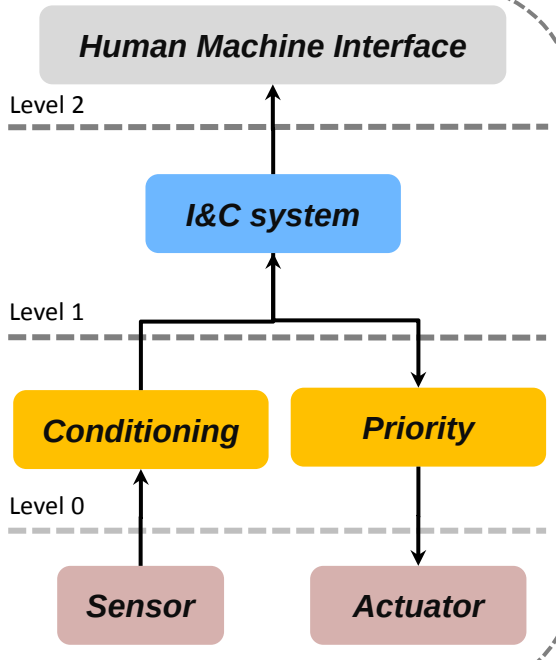


# I&C Architecture

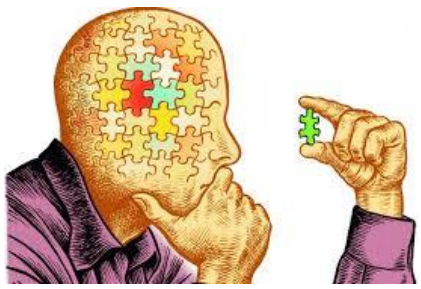
## Simplified safety design principle




**Safety** | **Process I&C Function** | **Application I&C Functions**

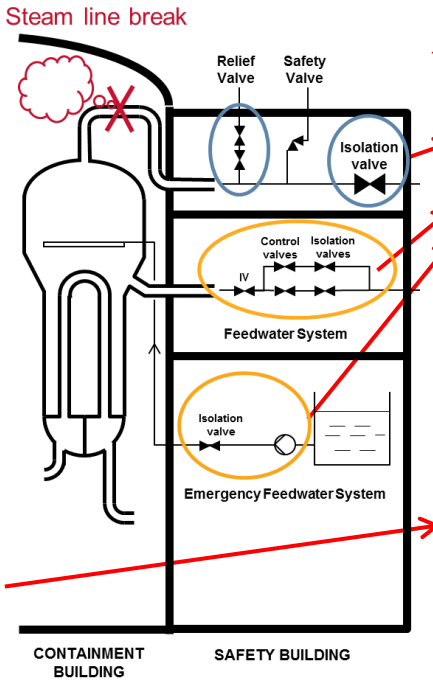


# I&C Architecture

## Functional requirements process

| Line 1 | Line 2 | Line 3 | Line 4 |
|---|---|---|---|

| DBC1 | DBC2 | DBC3 | DBC4 | DEC A | DECB |
|---|---|---|---|---|---|
| • Start-up of plant<br>• Load changes<br>• Load reduction<br>• … | • Turbine trip<br>• Loss of RCP<br>• Fedwater malfunction<br>• … | • SGTR (1 tube)<br>• Small SLB<br>• Boron dilution<br>• … | • Large-break LOCA<br>• SLB<br>• SGTR (2 tubes)<br>• … | • ATWS + LOOP<br>• SBO<br>• TLOCC<br>• … | • Severe accidents (core melt) |




**Isolation functions**
- IV closure on SG pressure
- RV isolation on SG pressure
- FW isolation on SG pressure
- Manual EFWS isolation
- …

**Reactivity Control functions**
- Safety Injection startup on PZR pressure
- Extra Borating System Actuation on SG pressure
- …

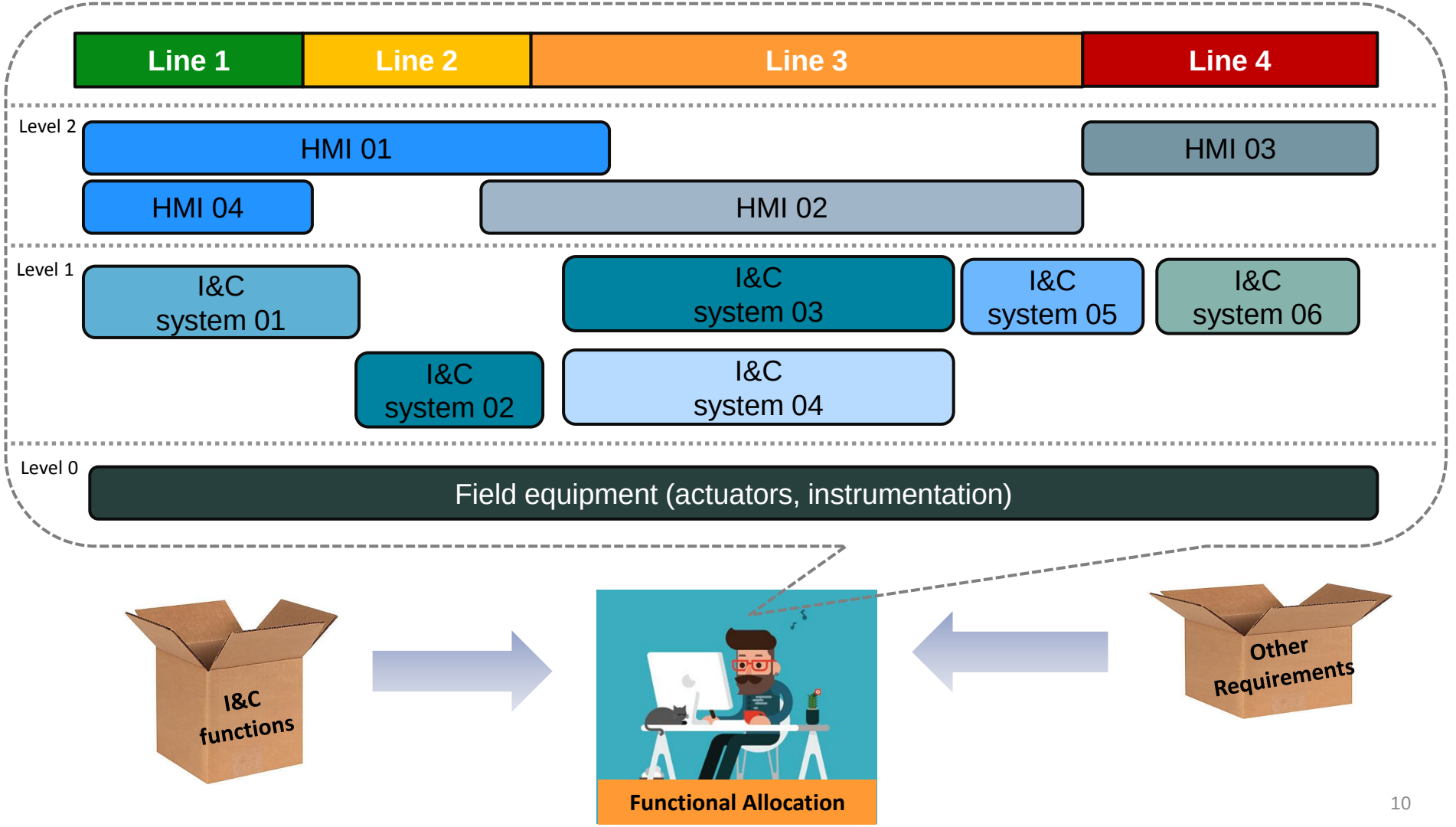
**Function Requirement**
- DiD: 3a
- Safety Category: A
- Safety Class: Class 1
- Seismic Class: SC1
- Redundancy: N + 2
- Power supply: EDG + batteries
- Automatic (within 30 minutes)
- Diversity: No
- Periodic tests: Yes
- Reliability target: $10^{-4}$ fpd
- Periodic tests: Yes
- Response time: 0.5 sec
- Algorithm, Input/Output
- …

**System Level Requirement**
- Functional Diagrams
- Technological, Quality requirements
- resulting from safety class
- HFE, Operational Requirements
- …

**Component Level Requirement**
- Safety Class: Class 1
- Mechanical Quality Class: Q1
- Electrical Class: EE1
- Seismic Class: SC1
- Relevant IEC standards: IEC, etc.
- Environmental conditions: SLB cond.
- Radiation protection: 20 kGy
- …

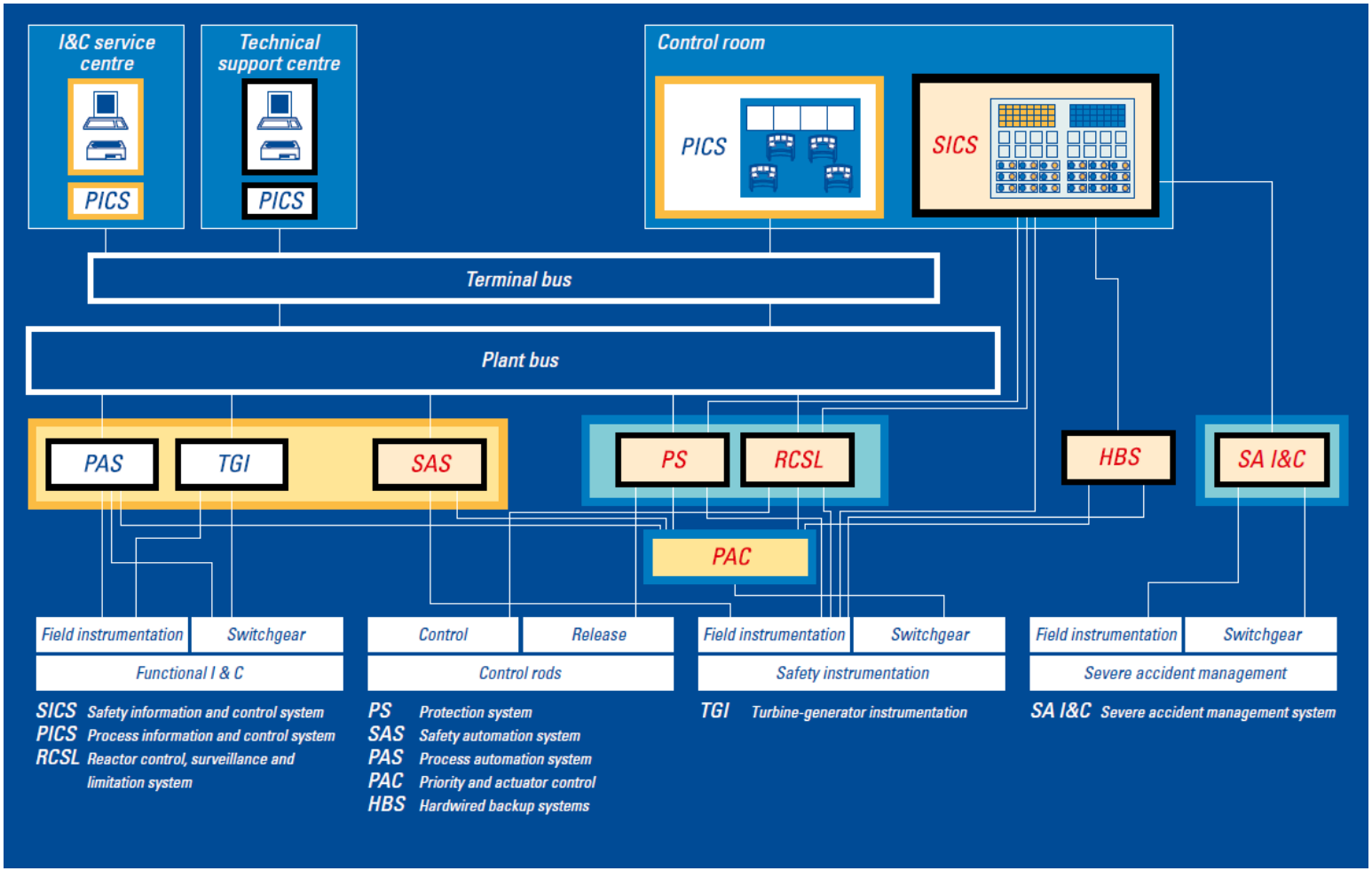
# I&C Architecture

## Functional allocation and definition of application I&C functions



# I&C Architecture

## Example

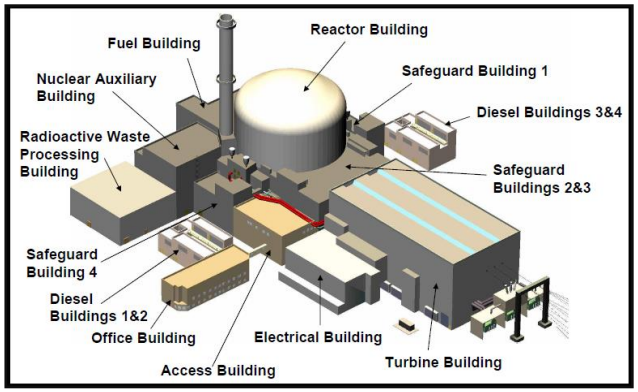


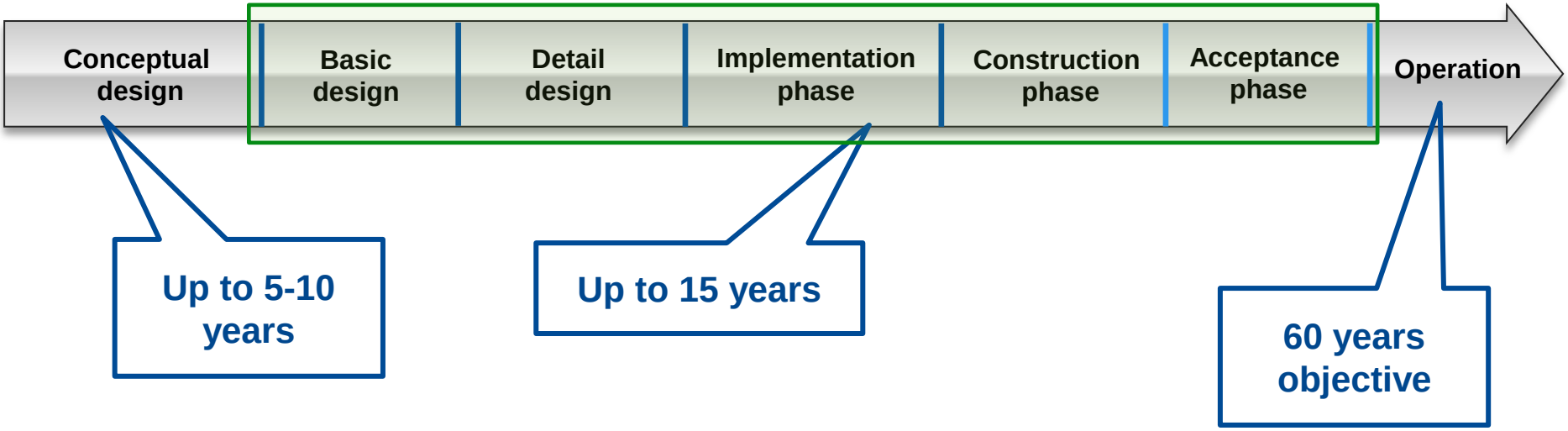

Reference: https://www.tvo.fi/uploads/julkaisut/tiedostot/ydinvoimalayks_OL3_ENG.pdf

# Main challenges in new build projects

# Main challenges in new build projects

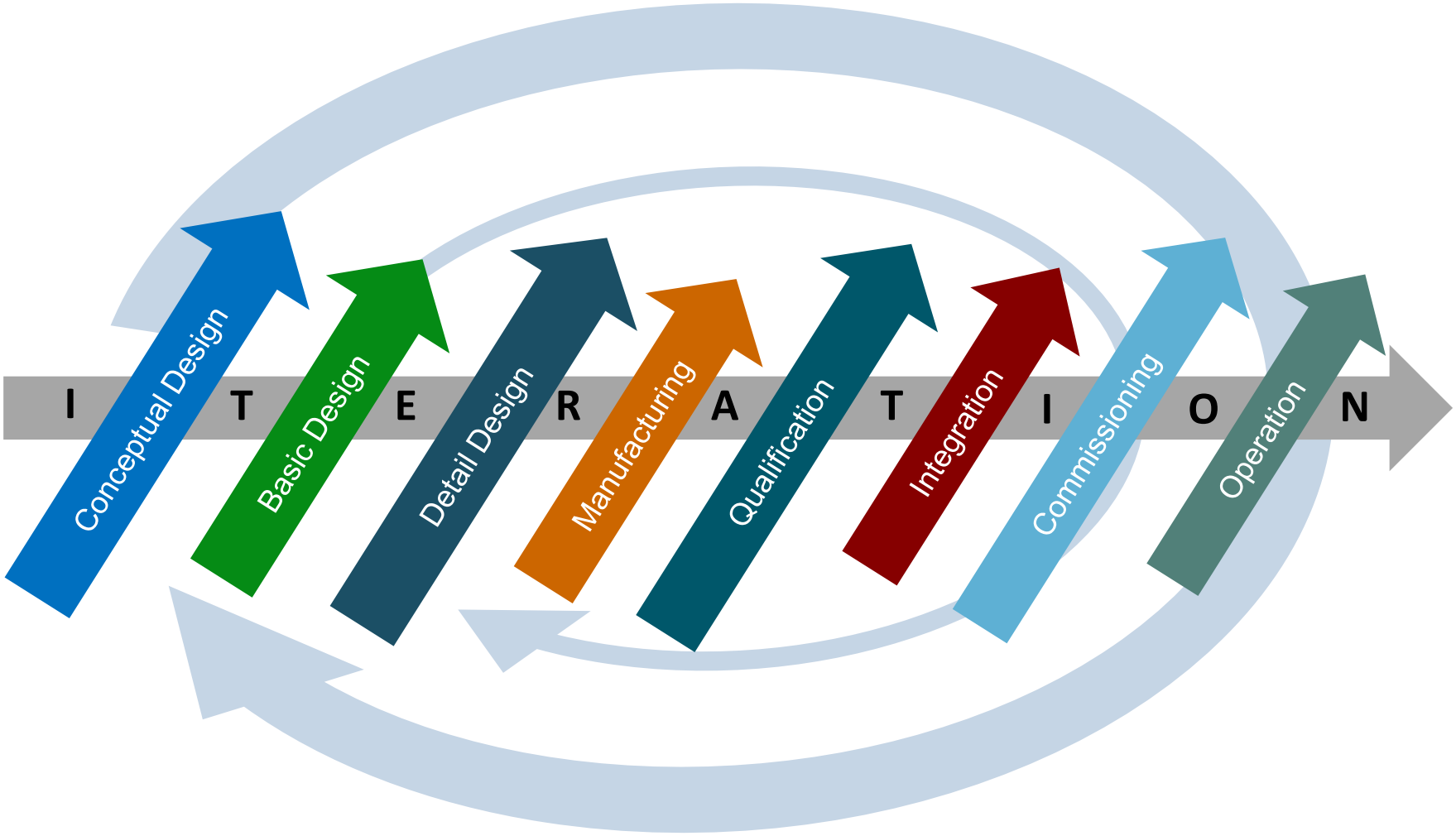
## Project view



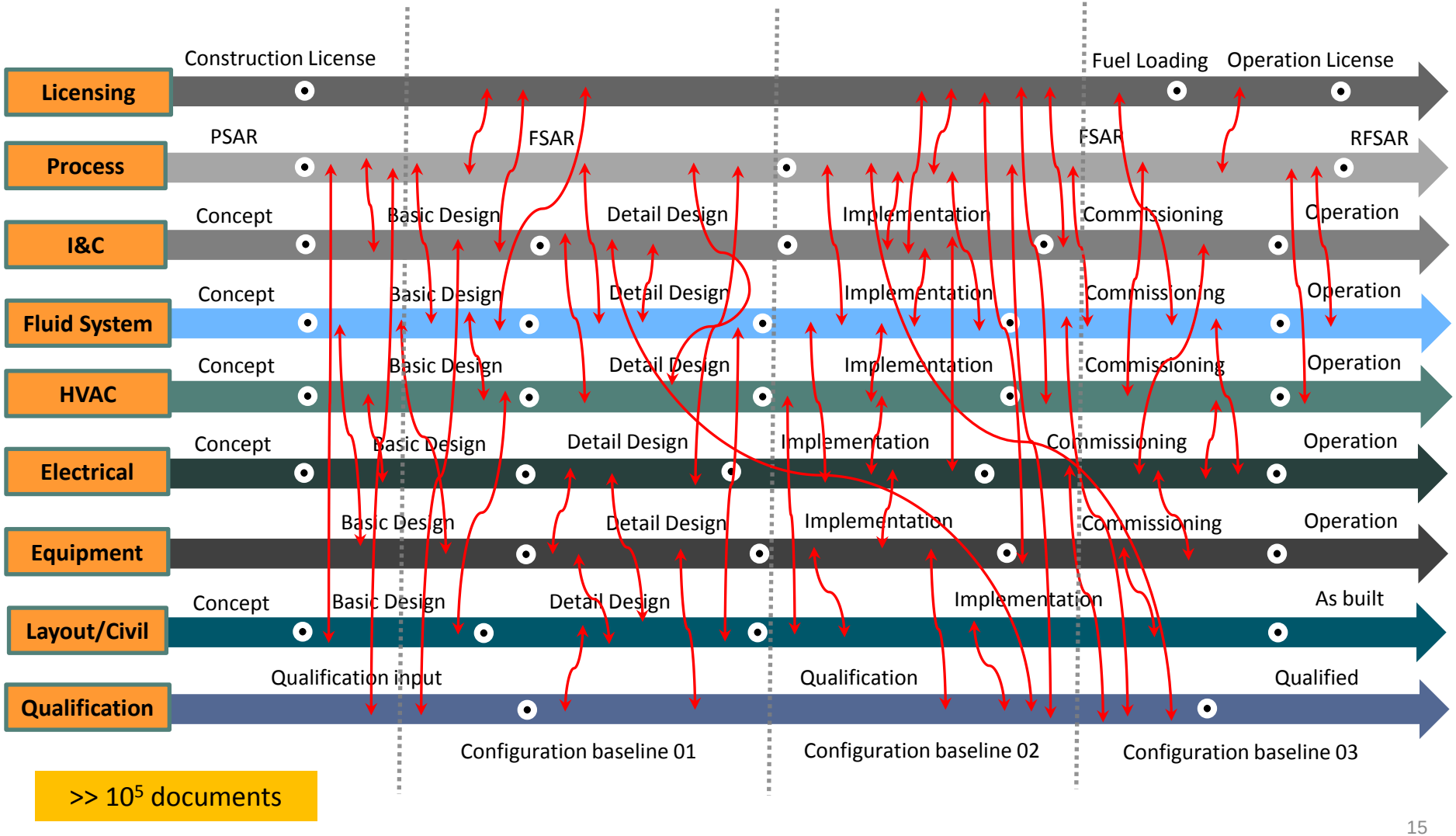
# Main challenges in new build projects

## Iterative design - Schedule



# Main challenges in new build projects

## Input Data Management / Configuration Management



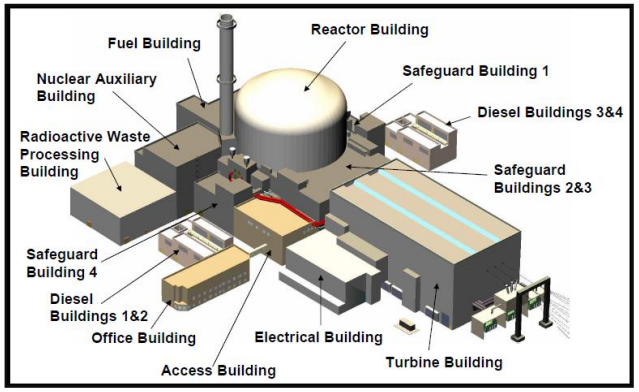

>> $10^5$ documents

# Main challenges in new build projects

## Design Changes

SLOVENSKÉ ELEKTRÁRNE

**Conceptual Design**




**Design Changes**

**Final Design**

# Main challenges in new build projects

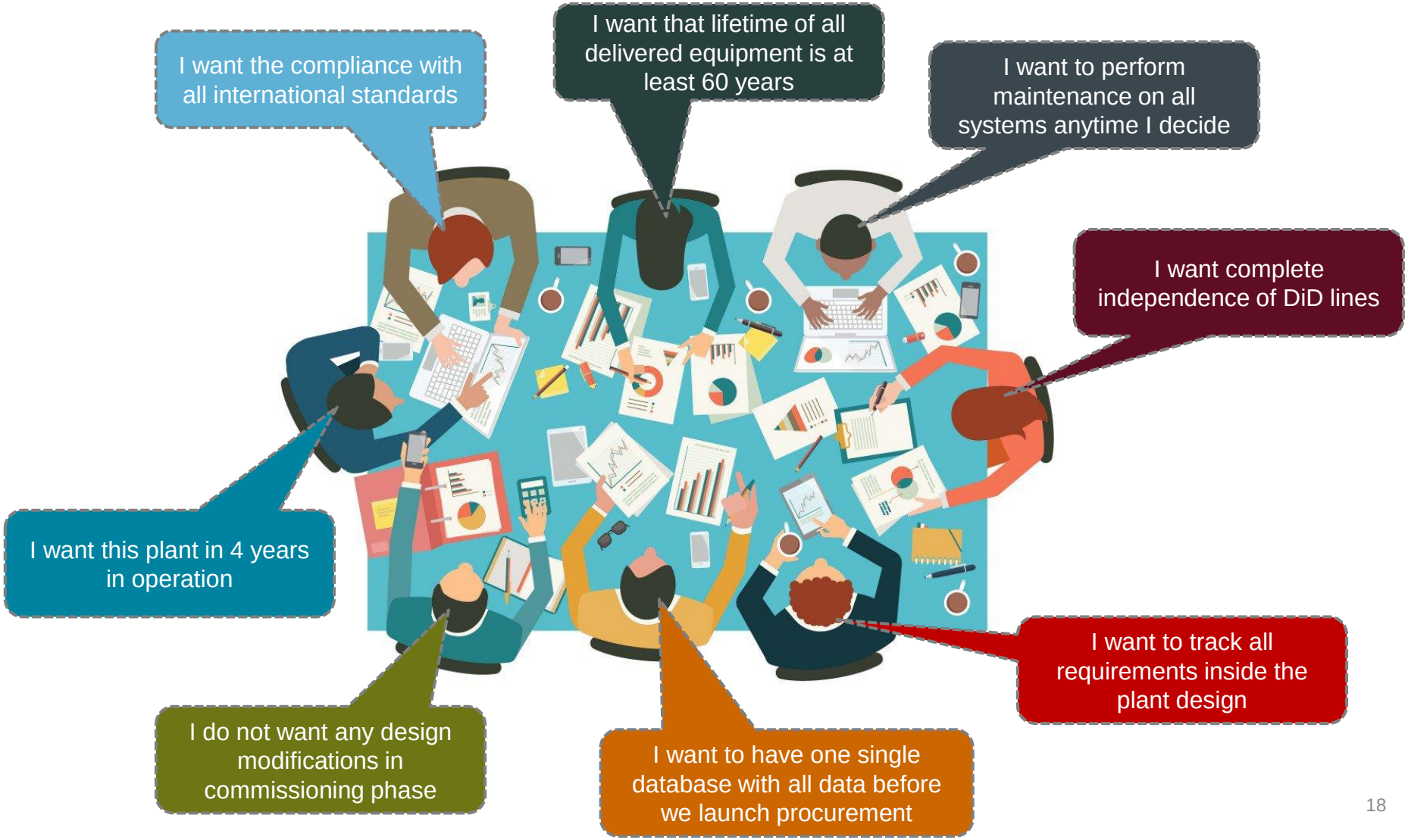
## Missing Requirements

**Cable Routing (example)**

- *Requirements from Electrical Layout and Systems ???*
- *Requirements from Fire Protection ???*
- *Requirements from I&C Systems ???*
- *Requirements from Safety ???*
- *Building analyses requirements ???*
- *Radiation Protection (RP) Requirements ???*
- *Requirements from Civil/Layout ???*
- *Requirements from Fire Hazard Analyses ???*
- *Requirements coming from HEPB Analyses ???*
- *Qualification requirements ???*
- *…*

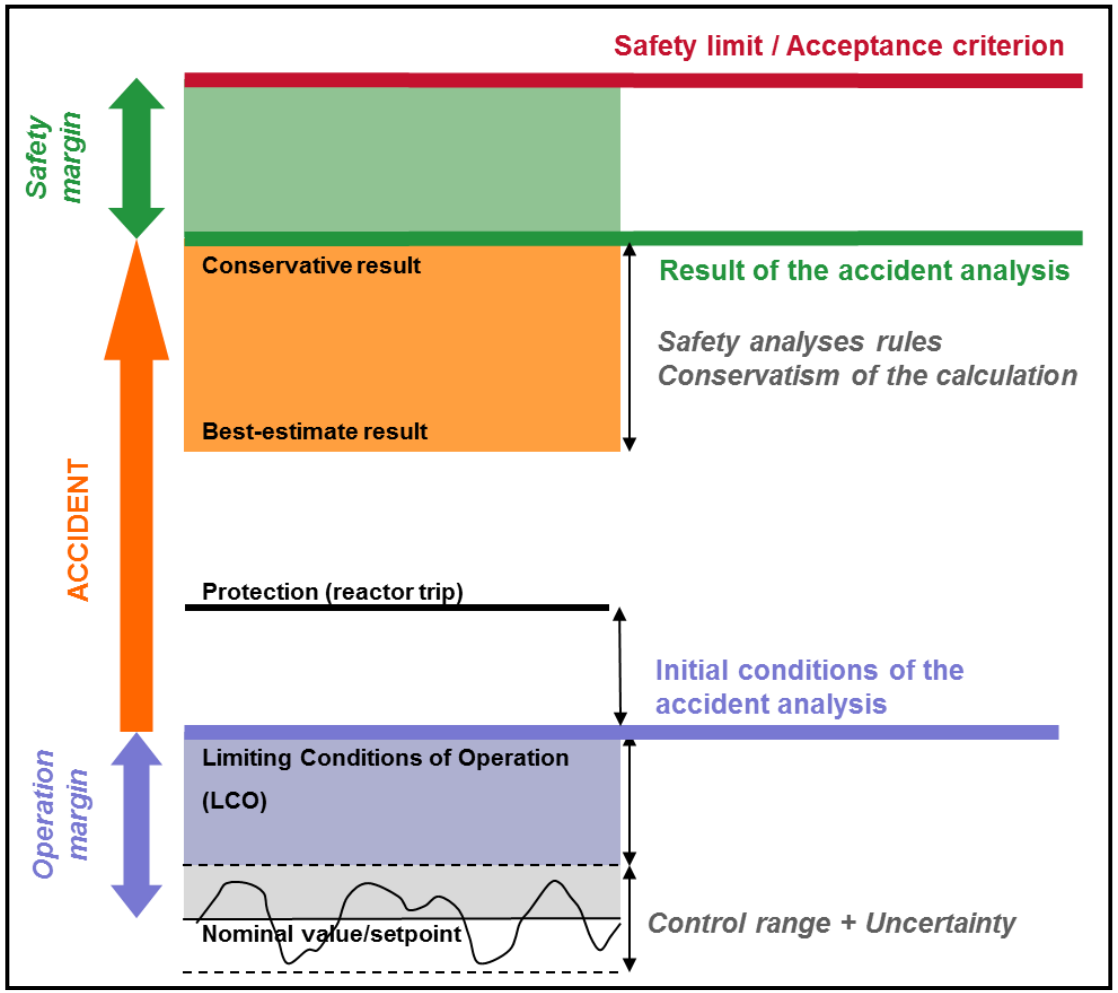
# Main challenges in new build projects

## Unrealistic Requirements



# Main challenges in new build projects

## Safety Limits





Following **only** safety standards would result in design that is not operable

# Main challenges in new build projects

## Interfaces / Common Language

SLOVENSKÉ ELEKTRÁRNE

### Engineering language

This I&C function shall have uncertainty 0,5% of measuring range

**Ms. Process**

HM…
- It is clear…

**Mr. I&C**

### Cultural aspect

Well, your solution is quite interesting

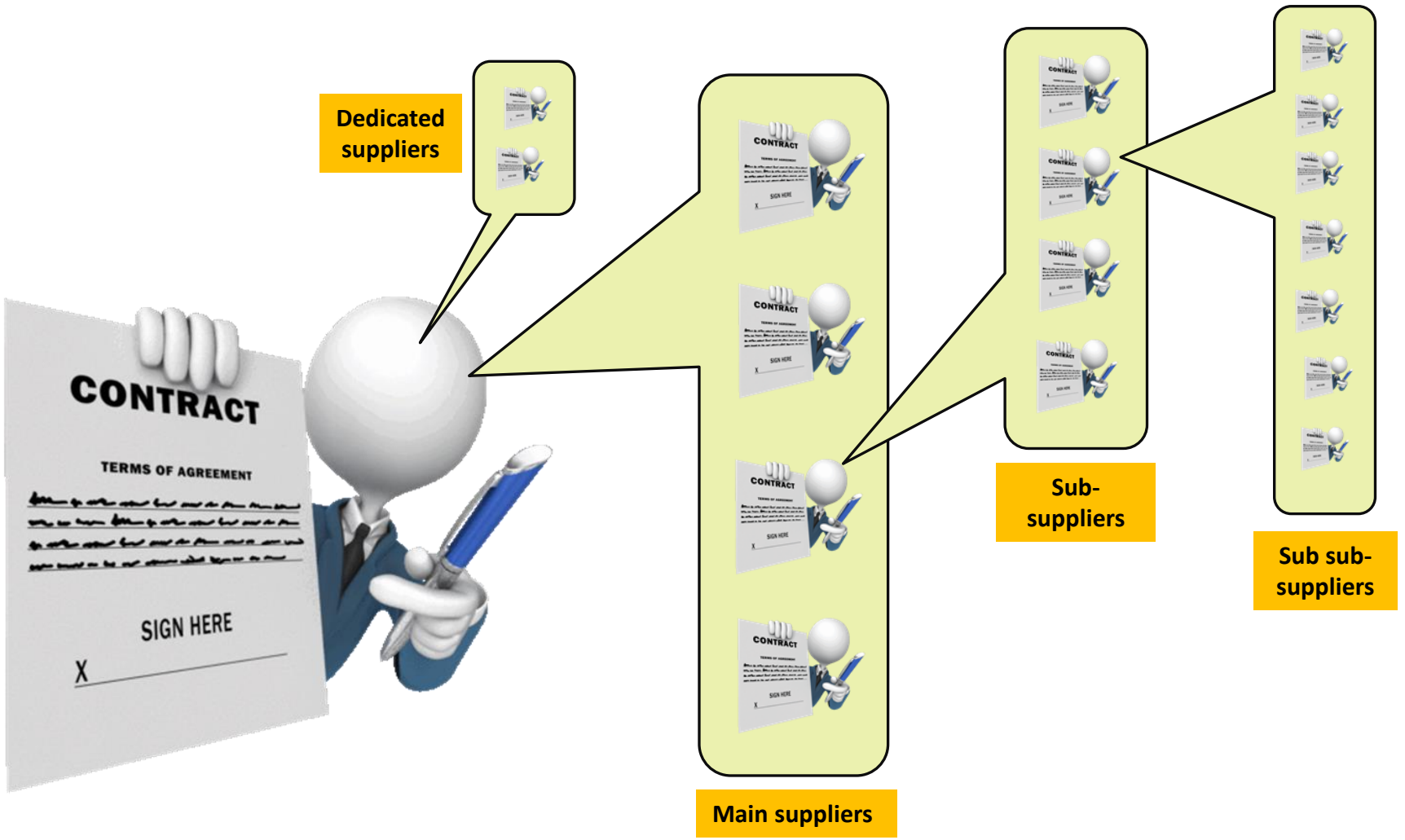
**Ms. UK**

Great, she likes it. I will launch the development within our design

**Mr. France**

# Main challenges in new build projects

## Contract split / Supplier chains



# Main challenges in new build projects

## 10 Tips to remember

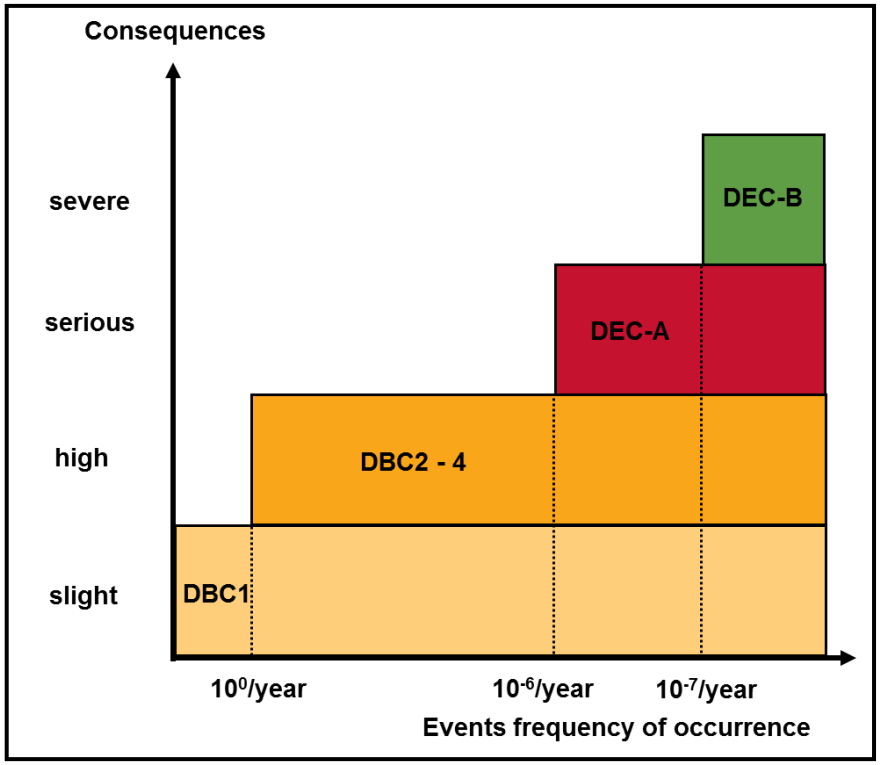
SLOVENSKÉ ELEKTRÁRNE

1. Keep safety always as first objective
2. Propel transparent communication with Local Safety Authority
3. Do not reinvent the wheel. Take lesson learned from the other plants
4. Try to understand the whole picture before you move one hand
5. Make good balance between safety and operation
6. Try to limit the interfaces as much as possible
7. Do not underestimate the cultural/company differences
8. Double-check the impact analysis of complex design changes
9. Remember that engineering is an iterating process
10. People do mistakes, define the process to limit them

# Support slides

# Support slide

## DBC/DEC

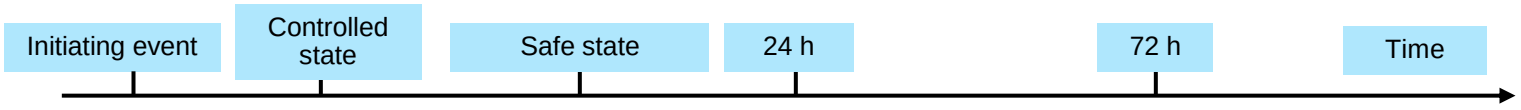



| DBCs | Safety Objectives | | |
|---|---|---|---|
| | Reactivity control | Core cooling | Confinement of radioactive material |
| DBC1 | I&C Functions of Preventive Line | | |
| DBC2 | | | |
| DBC3 | I&C Functions of Mainline | | |
| DBC4 | | | |
| DEC A | I&C Functions of Risk Reduction Line | | |
| DEC B | I&C Functions for Severe Accidents | | |

# Support slide

## Controlled/ Safe State

- **Controlled state**
  - Core subcritical
  - Residual heat removal ensured
  - Core coolant inventory stabilized or increasing
- **Safe shutdown state**
  - Core subcritical
  - Residual heat removal durably ensured
  - Radioactivity releases are within acceptable limits



# Support slide

## Classification overview

| National or International Standard | Classification of the importance to safety | | | |
|---|---|---|---|---|
| IEC 61226 | Cat. A / Class 1 | Cat. B / Class 2 | Cat. C / Class 3 | Unclassified |
| France | F1A | F1B | F2 | Unclassified |
| Finland | SC2 | SC3 | EYT/STUK | EYT |
| UK | Cat. A / Class 1 | Cat. B / Class 2 | Cat. C / Class 3 | Unclassified |
| Russia | Class 2 | Class 3 | | Class 4 |
| USA | Systems Important to Safety | | | Non-nuclear Safety |
| Canada | Category 1 | Category 2 | Category 3 | Category 4 |
| Japan | PS1/MS1 | PS2/MS2 | PS3/MS3 | Non-nuclear Safety |
| IAEA NS-R-1 | Safety | Safety Related | | Systems Not Important to Safety |