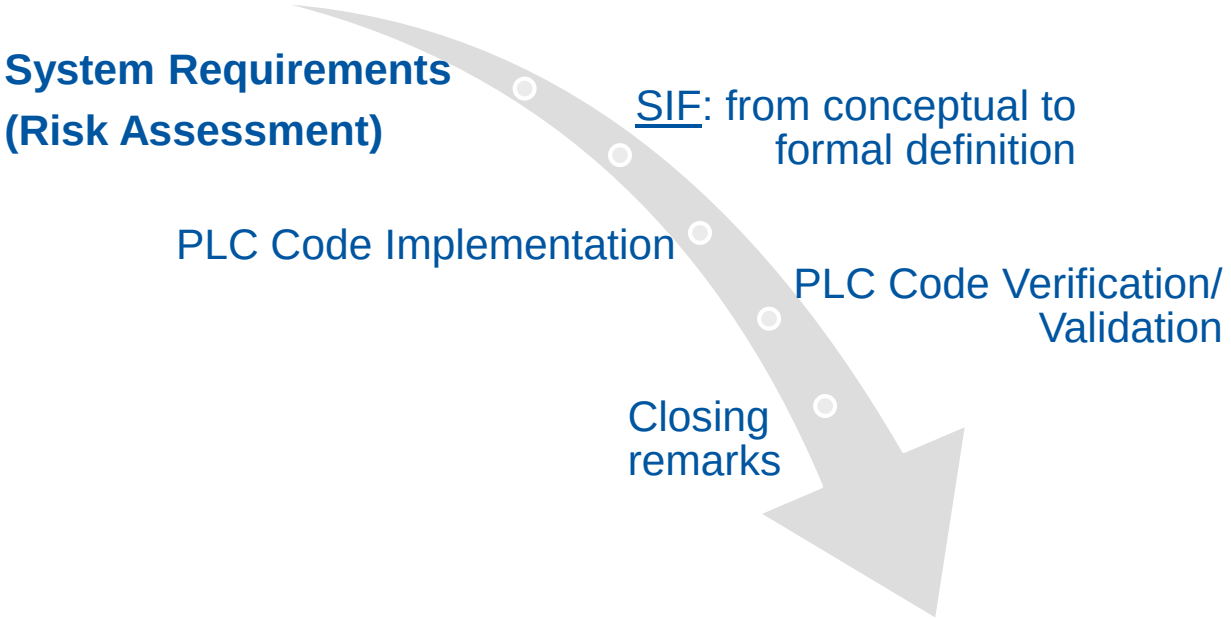
# Safety Instrumented Functions:
## from risk analysis to PLC implementation

**Control & Safety Solutions workshop** – 22th June 2018

F. Havart, T. Ladzinski, P. Ninin, **F. Valentini** (BE-ICS)

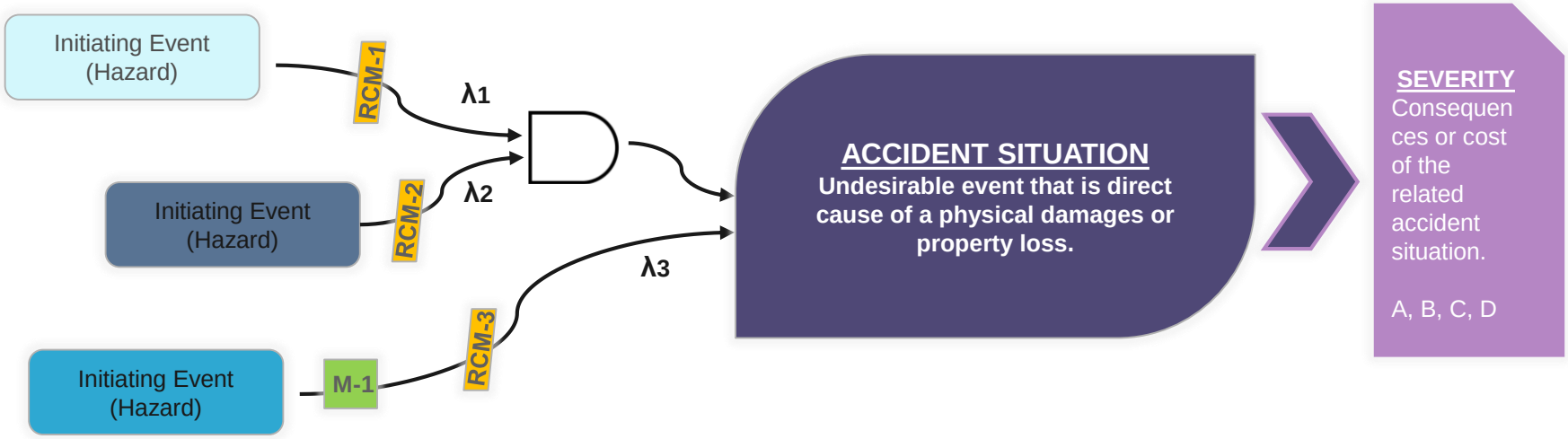
# Outline


System Requirements
(Risk Assessment)
SIF: from conceptual to formal definition
PLC Code Implementation
PLC Code Verification/ Validation
Closing remarks

# Risk Assessment

- What are the most relevant outcomes.
- What is the link between Safety Functions and R.A.
- How it shall be presented in practice.

# Relevant information from the Study




## E/E/PE Control Measures

- **RCM-1**:*Safety action implemented by the SIS to prevent the occurrence of one specific Initiating Event.*
- **RCM-2**:*Safety action implemented by the SIS.*
- **RCM-3**:*Safety action implemented by the SIS.*

## Other control measures

- **M-1**: *Any other preventive engineering control, rules or procedure not part of the SIS.*

## Risk Assessment

| Risk evaluation | | Probability of the hazardous event | | | |
|---|---|---|---|---|---|
| | | Very low (1) | Low (2) | Medium (3) | High (4) |
| Potential severity | Minimal (A) | (A1) RA | (A2) RA | (A3) | (A4) |
| | Low (B) | (B1) RA | (B2) | (B3) RC | (B4) |
| | Medium (C) | (C1) | (C2) | (C3) | (C4) |
| | High (D) | (D1) | (D2) | (D3) | (D4) |

*CERN safety Guideline* OHS-1-0-1. EDMS: 1144042.

# Example from a real use case

3.5 **RSK-05**: BREAK OF THE LASER TRANSFER TUBE

**Hazardous Event**

LOCATION: (*GBAR Experimental Area & outstanding visitor's path*)

Break or partial loss of integrity of the laser transfer line, consisting in a rigid tube or metallic material, used to transfer the 410nm laser beam from the laser room (DLA-1) down to the GBAR experimental area.
An accidental damage to this transfer structure or an improper installation may cause laser beam to propagate, directly or by reflection, into the GBAR laser area and other areas of the AD experimental hall including the near visitor's path.

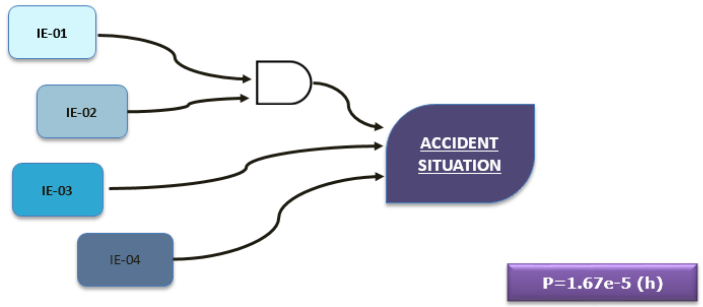
**Applicable Reference Documents**:
[1], [3], [4]

**Potential Severity: [ D ]**

Taking into the account the real power of the laser (10mJ per 11Hz rate) and the distances to be travelled to hit anyone present into the GBAR experimental area or the rest of the AD hall, it can be assumed that the physical injuries (if any) would be superficial and reversible. However the possibility of losing control in such a way of a class 4 laser and potentially impacting against a visitor, not member of CERN personnel, it is considered as Unacceptable and it is here classified with the higher level of severity.

**Applicable Reference Documents**:
[4], [5], [7]

**Probability of the Hazardous Event: [ 3 ]**




| Initiating Event | Assumptions | Event Rate-h (λ) |
|---|---|---|
| **IE-01**: *Co-activity works at proximity of the laser transfer tube and not related with the laser experiment.* | ○ Periodical inspections of all laser lines exposed to the outside are part of the laser team operational procedures. | **5.70E-5** *(1 per 15 years)* |
| **IE-02**: *Accidental mechanical shock against the transfer tube while laser beam inside.* | - | |
| **IE-03**: *Mechanical failure of the laser tube structure due to a wrong conceptual design / assembly work.* | - | **2.28E-6** *(1 per 25 years)* |
| **IE-04**: *Degradation / damage of the laser tube structure caused by a maintenance intervention by the laser experiment's team.* | ○ Quality procedures are followed for intervention of the laser tube. | **2.28E-6** *(1 per 25 years)* |

**Risk Evaluation: [D]x[3]**

| Risk evaluation | | Probability of the hazardous event | | | |
|---|---|---|---|---|---|
| | | Very low (1) | Low (2) | Medium (3) | High (4) |
| Potential severity | Minimal (A) | (A1) | (A2) | (A3) | (A4) |
| | Low (B) | (B1) | (B2) | (B3) | (B4) |
| | Medium (C) | (C1) | (C2) | (C3) | (C4) |
| | High (D) | (D1) | (D2) | (D3) | (D4) |

3.5.1 RISK CONTROL MEASURES

| ID | Description | System | Hazard |
|---|---|---|---|
| RCM-13 | Forbid laser beam extraction from DLA-1 (laser room) upon activation of any emergency stop button inside the GBAR experimental hall. | **PPS** | IE-01<br>IE-02 |
| RCM-14 | Forbid laser beam extraction from DLA-1 (laser room) upon loss of vacuum inside transfer tube. | **PPS** | IE-02 |
| RCM-15 | Classify as EIS (Important Element for Safety) the laser transfer tube and handle it according with safety procedure in use at CERN [8]. | Policy | IE-03<br>IE-04 |
| RCM-16 | Periodical visual inspections of the tube structure (minimum annual) by LSO or DSO. | Inspection | IE-03<br>IE-04 |

# Typical outcomes from Risk Assessment

*Safety Instrumented Functions – Conceptual Description*

- **TYPE 1:** "Interlock **SOMETHING** with **SOMETHING ELSE**"


- **TYPE 2:** "Shutdown **SOMETHING** if Condition is TRUE"

- **TYPE 3:** "Prevent **SOMETHING** to start until Condition is TRUE"

# SYNTHÈSE DES FONCTIONS DE SÉCURITÉ DU SYSTÈME LASS

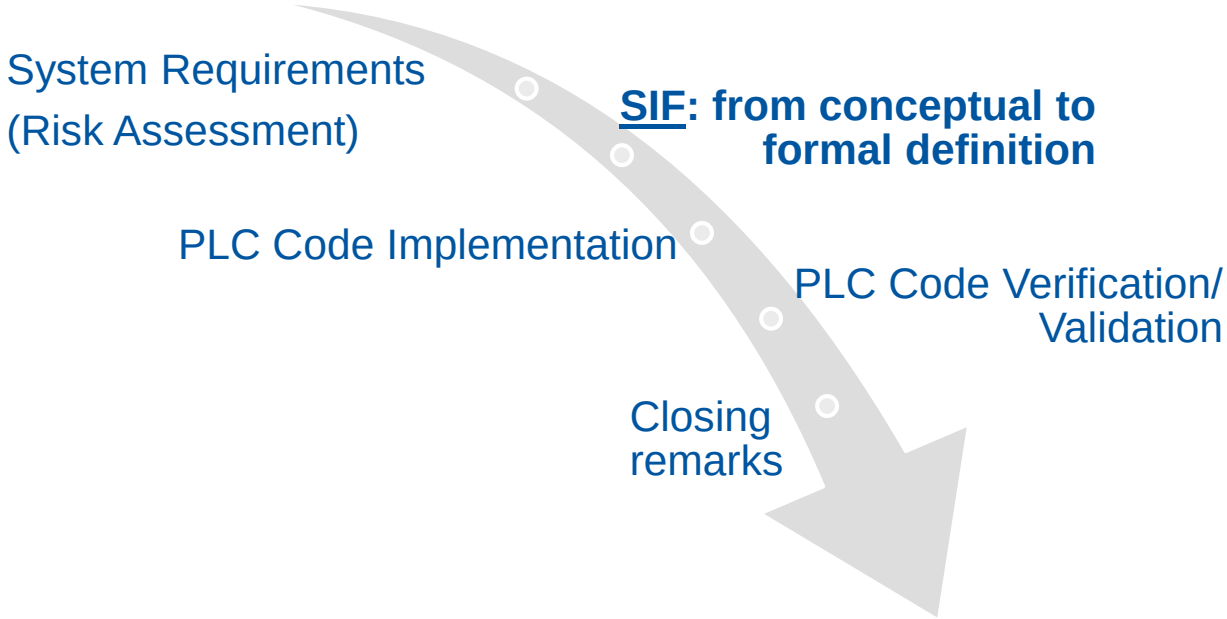
**Mode d'Exploitation du LHC**

| Événement Dangereux | LHC | | | | TI2/TI8 | | | ZIV PAR POINT | | | | ZONE RF / ZONES ADJACENTES RF (POINT 4) | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Accès -> Faisceau | Faisceau | Faisceau -> Accès | Accès | Faisceau TI | Faisceau TI <-> Accès Point X | Accès Point X | Accès Service | Accès Tunnel | Accès Expérience | Délégation Contrôle d'accès Expérience | RF / Électron Stopper | RF/ Électron Stopper <--> Accès | Accès (Zone RF ou Zones adjacentes RF) |
| | Accès : interdit au Ring | | | | Accès : interdit au Point 2/8 (X) | | | Accès : autorisé aux ZIV Service d'un Site | Accès : autorisé aux ZIV Faisceau d'un Site | | | Accès : interdit aux Zones RF ou Zones adjacentes RF du Point 4 | | Accès : autorisé aux Zones RF ou Zones adjacentes RF du Point 4 |
| Autorisation d'accès lorsque le niveau de radiation est trop élevé | | 1.3 - Activer les signaux *Veto Radiation* des Zones d'Accès définis par le service de Radio Protection, après une temporisation suite au passage en mode faisceau. | | | | | | 1.1- Acquérir les signaux *Veto Radiation* des Zones d'Accès, et lorsqu'un veto est présent, maintenir en PS +V l'enceinte de la Zone d'Accès concernée. | | | | | | |
| Intrusion dans une ZIV lorsque l'accès y est interdit | 2- Maintenir en PS+V les entrées aux ZIV. | | | | 2.1- Maintenir en PS+V les entrées aux ZIV du Point X. | | | 1.2- Détecter la PNS d'un EIS-accès dans une Zone d'Accès, et lorsqu'un *Veto Radiation* est présent, envoyer une alarme au CCC | | | | 2.3- | | |
| | | | | | | | | 2.3- Maintenir en PS+V les entrées aux ZIV Faisceau du Site 4. | | | | | | |
| | 3.- Détecter la PNS d'un EIS-accès dans une ZIV et : - Arrêter le faisceau (EIS-fc LHC) et empêcher une nouvelle injection (EIS-fi LHC) | | | | | | | | | | | 3.5 Interrrompre la délégation local RF si désarmement du signal search du secteur formant la zone RF (secteur 8) | | |
| | 3.1- Détecter la PNS d'un EIS-accès dans la ZIV RF (secteur 8) du Point 4 et : - Mettre en PS+V la RF* | | | | 3.2.1- Détecter la PNS d'un EIS-accès dans une ZIV du Point 2 et empêcher une injection en provenance du SPS (safety chaine 5). | | | 3.1 | | | | 3.1 | | |
| | 3.3- Détecter la PNS d'un EIS-accès dans une ZIV adjacente RF (secteur 7 et 9) du Point 4 et : - Mettre en PS+V les ES*. Si au but de 8 sec le ES ne sont pas en PS+V, mettre en PS+V la RF. | | | | 3.2.2- Détecter la PNS d'un EIS-accès dans une ZIV du Point 8 et empêcher une injection en provenance du SPS (safety chaine 3). | | | 3.3 | | | | 3.3 | | |
| | 18.1 | 18 Interdire le transfert de la barrière de l'entrée vers la porte de maintenance si celle-ci n'est pas en PS+V. | 18.1 Interdire le transfert de la barrère de l'entrée vers la porte de maintenance. | | | | | | | | | | | |
| | 19 Détecter la PNS de la porte de maintennace et si elle constitue la barrière de l'entrée active , - désarmer la boite de patrouille du PA et désarmer le Search du secteur franchi; - remettre le PA comme barriere de l'entrée active. | | | | | | | 19.1 Remettre le PA comme barrière de l'entrée active. | | | | | | |
| Présence d'au moins une personne à l'intérieur d'une ZIV | 4.1- En mode d'accès *Général* détecter l'ouverture d'un EIS-accès dans une ZIV, désarmer la boite de patrouille de l'EIS-accès et désarmer le Search du secteur franchi. | | | | | | | | | | | | | |
| | 4.2.1- En mode d'accès *Restreint*, maintenir en PS+V les entrées aux ZIV. Empêcher l'accès si contacte clé mode restreint n'est pas activé. | | | | | | | | | | | | | |
| | 4.2.2- Dans tous les modes d'accès détecter un passage d'urgence forcé dans une ZIV, désarmer la boite de patrouille de l'EIS-accès et désarmer le Search du secteur franchi. Le passage d'urgence forcé au cours d'une patrouille désarmer toutes les boites de patrouille du secteur. | | | | | | | | | | | | | |
| | 4.2.3- Dans tous les modes d'accès, activer le "Search Transfer"dans les ZIV sauf lors du passage du patrouilleur avec la clé patrouille. | | | | | | | | | | | | | |
| | 4.2.4- Lors de l'armement du signal Patrol d'un secteur, désarmer toutes les boites de patrouille du secteur concerné. | | | | | | | | | | | | | |
| | 4.2.5- Lors d'une patrouille, détecter l'ouverture d'un EIS-accès pour un temps prolongé et désarmer les boites de patrouille du secteur. | | | | | | | | | | | | | |
| | 3.- | | | | 3.2.1- | | | 3.1.- | | | | 3.1 | | |
| | 3.1.- | | | | 3.2.2- | | | 3.3.- | | | | 3.3 | | |
| | 3.3.- | | | | | | | | | | | | | |
| | 7.1_ Interdire le transfert à Faisceau, si dans les ZIV, au moins un/e: - *EIS-accès* n'est pas en PS+V ou, - *Boite de Patrouille* n'est pas armée ou, - *Search* n'est pas armée ou, - *BIW* n'a pas marché correctement ou, - *Distributeur des clefs* n'est pas en PS. | | | | 7.2.- Interdire le transfert à Faisceau TI du Site X, si dans les ZIV au moins un/e: - *EIS-accès* n'est pas en PS+V ou, - *Boite de Patrouille* n'est pas armée ou, - *Search* n'est pas armée ou, - *Distributeur des clefs* n'est pas en PS. | | | | 7.3.- Interdire le transfert à Accès OFF ZIV, si dans ces ZIV, au moins un/e: - *EIS-accès* n'est pas en PS ou, - *Boite de Patrouille* n'est pas armée ou, - *Search* n'est pas armée ou, - *Distributeur des clefs* n'est pas en PS. | | | 7.5.- Interdire le transfert à Électron Stopper, si dans ces ZIV Faisceau, au moins un/e: - *EIS-accès* n'est pas en PS+V ou, - *Boite de Patrouille* n'est pas armée ou, - *Search* n'est pas armée ou, - *Distributeur des clefs* n'est pas en PS. | | |
| | 7.7 - Activer les signaux de BIW | | | | | | | 7.4- Interdire le transfert à Accès Service OFF, si dans ces ZIV, au moins un/e: - *EIS-accès* n'est pas en PS ou, - *Boite de Patrouille* n'est pas armée ou, - Search n'est pas armée ou, - *Distributeur des clefs* n'est pas en PS. | | | 7.6.- Interdire le transfert à RF, si dans ces ZIV Faisceau, au moins un/e: - *EIS-accès* n'est pas en PS+V ou, - *Boite de Patrouille* n'est pas armée ou, - *Search* n'est pas armée ou, - *Distributeur des clefs* n'est pas en PS. | | |
| | 8- Acquérir les signaux d'*Arrêt d'Urgence* actionnés dans une ZIV et - Mettre en PS+V les EIS-f circulants et injectés si cela se produit dans les ZIV Faisceau du Point 4: - Mettre aussi en PS+V les ES et RF du Point 4 si cela se produit dans les ZIV du Point 2 ou Point 8: - Mettre en PS les chaines de sécurité 3 ou 5 du SPS | | | | | | | | | | | | | |
| Démarrage intempestif d'EIS-f ou d'EIS-m, lorsque l'accès est autorisé | 9.- | | 9- Maintenir en PS+V *tous* les EIS-f circulants du LHC | | | | | | | | | | | |
| | 9.1.- | | 9.1- Maintenir en PS+V *tous* les EIS-f injectés du LHC (point 2 et 8) | | | | | | | | | | | |
| | | | 9.2- Maintenir en PS+V la chaine de sécurité SPS 5 du TI2 | | | | | | | | | | 13.1- Maintenir en PS+ V les RF en cas d'accès à la Zone RF. | |
| | | | 9.3- Maintenir en PS+V la chaine de sécurité SPS 3 du TI8 | | | | | | | | | | 13.2- Maintenir en PS+ V les ES en cas d'accès | |
| | 10.- | | 10- Détecter la PNS d'au moins un EIS-f circulant et dans ce cas mettre en PS+V les EIS-accès des ZIV | | | | | | | | | | | |
| | 10.1.- | | 10.1- Détecter la PNS d'au moins un EIS-f injecté et dans ce cas mettre en PS+V les EIS-accès des ZIV | | | | | | | | | | | |
| | 10.2.- | | 10.2- Détecter la PNS d'au moins deux EIS-f circulants ou injectés du LHC (dans la même chaine) et dans ce cas déclencher l'évacuation du personnel présent à l'intérieur des ZIV LHC | | | | | | | | | | | |
| | | | 12.1 Détecter la PNS d'au moins un EIS-f de la chaine de sécurité SPS 5 et dans ce cas metttre en PS+V les EIS accès des ZIV du Point 2. Détecter la PNS d'au moins 2 EIS-f de la chaine de sécurité SPS 5 et dans ce cas déclencher l'évacuation du Point 2". | | | | | | | | | | 14.1- Détecter la PNS de la RF et mettre en PS+ V les entrées à la zone RF (Secteur8) | |
| | | | 12.2 Détecter PNS d'au moins un EIS-f de la chaine de sécurité SPS 3 et dans ce cas metttre en PS+V les EIS accès des ZIV du Point 8. Détecter la PNS d'au moins 2 EIS-f de la chaine de sécurité SPS 3 et dans ce cas déclencher l'évacuation du Point 8". | | | | | | | | | | 14.2- Détecter la PNS d'au moins un ES et mettre en PS+V les entrées aux Zones adjacentes RF correspondantes (Secteur 7 et/ou 9) et mettre en PS+V la RF. | |
| | | 15.1- Interdire le transfert à Accès, si PNS d'au moins un EIS-f circulant ou injecté du LHC. | | | 15.2- Interdire le transfert à Accès TIX, si PNS d'au moins une chaine de sécurité SPS | | | | | | | 15.4- Interdire le transfert à Accès Zone RF si PNS de la RF. | | 15.6- Interdire la délégation locale RF, si: -PNS de la RF. |
| | | | | | | | | | | | | 15.5- Interdire le transfert à Accès Zones adjacente RF, si PNS du ES associé. | | |
| | | | | | | | | 8- | | | | | | |

# To be considered @ this stage

- **Very good synthesis of hundred of pages of R.A.'s prescriptions: it summarizes all SIS critical objectives**;
- SIF are mostly expressed in natural language: ambiguities are possible;
- Lack of details about the physical Input / Outputs: how the *conditions* shall precisely be computed?
- Different SIF can act on the same actuator (output);
- Many possible ways to code the SIF into PLC code;
- Final system validation can be difficult if the PLC code does not follow the SIF specification structure.

# Outline


System Requirements
(Risk Assessment)
SIF: from conceptual to formal definition
PLC Code Implementation
PLC Code Verification/ Validation
Closing remarks

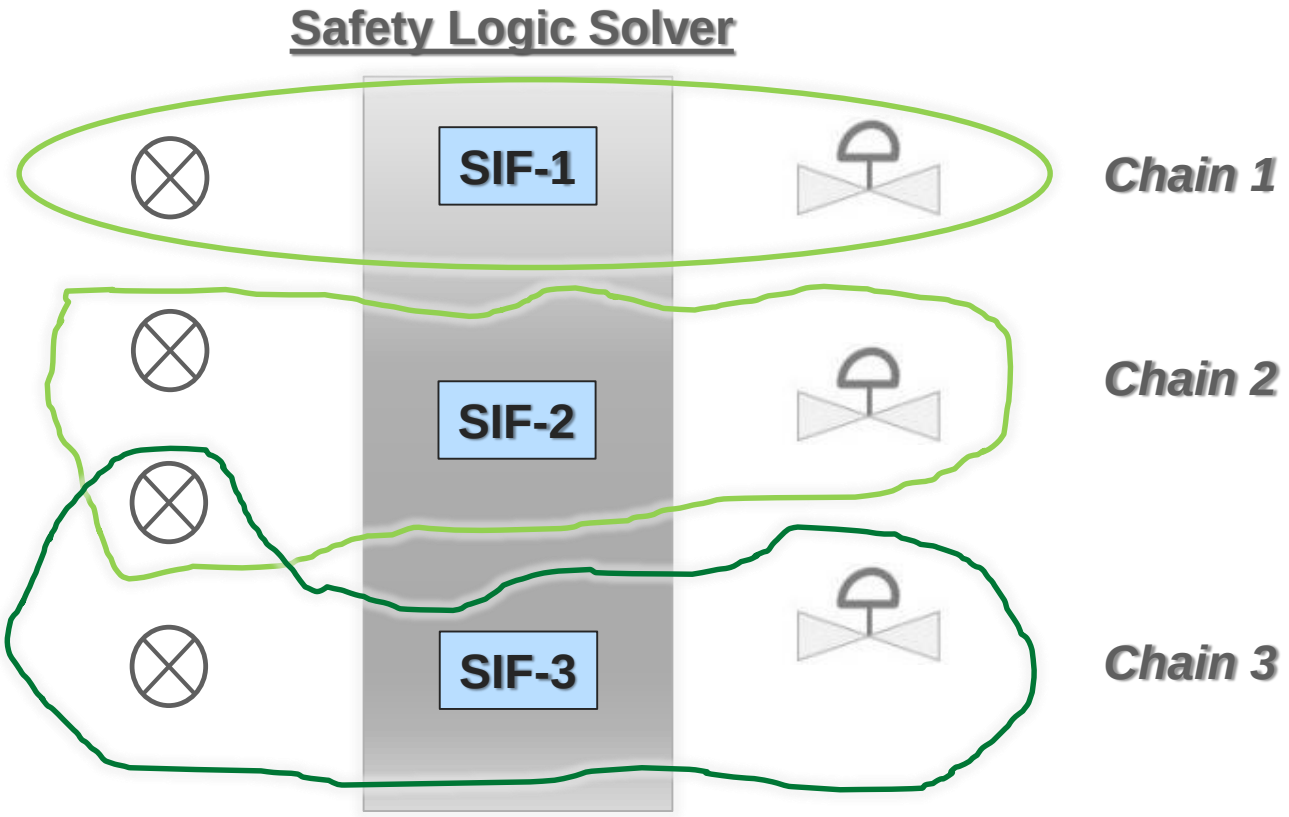
# Safety Instrumented Functions
## From conceptual to logic design

- What they are for, main purpose of SIF.
- What are the main properties.
- What formalism to use.
- Impact of different design approaches.

# Safety Functions definition

**3.2.68**
**safety function**
function to be implemented by an SIS, other technology safety related system or external risk, reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event

NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.



# Main desirable properties for SW coding

- **Unambiguity:**

  *A formal language shall be adopted in order to express in a synthetic and not ambiguous formalism the role of every SIF.*

- **Completeness:**

  *It should be possible to proof that very risk control measure from Risk Assessment has been taken into the account.*

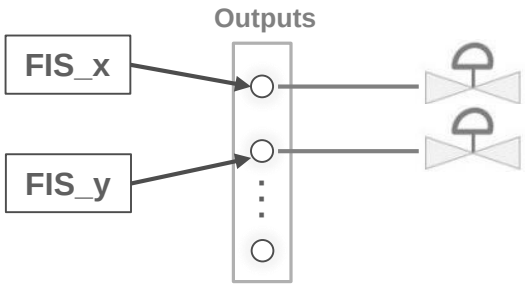
- **Correctness & Consistency:**

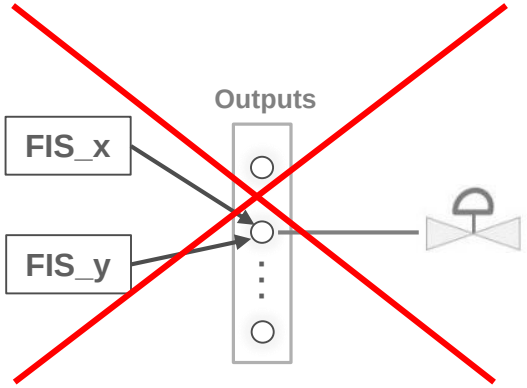
  *The SIF modelling strategy defining the safety behaviour of the system shall ensure:*

  - *The construction of a set with the strictly minimum number of SIF to reach the safety mission of the system.*
  - *The absence of redundant rules.*
  - *The absence of not reachable rules.*
  - *The absence of conflicting rules.*

# Main desirable properties for SW coding

- **Safety action uniqueness:**

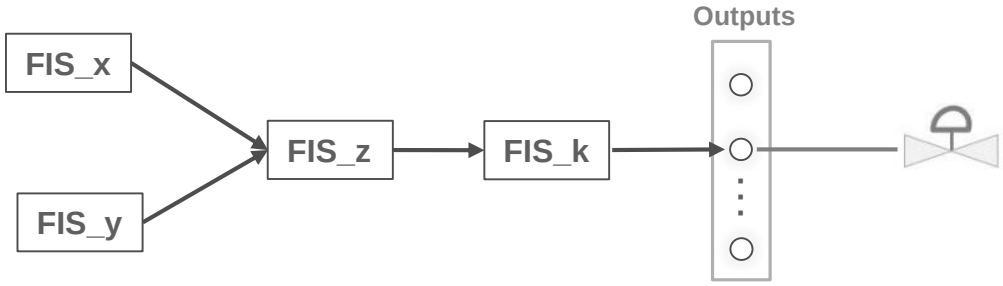


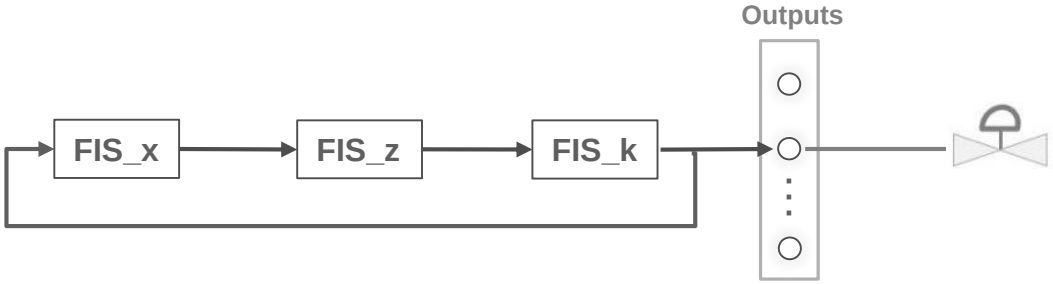
# Main desirable properties for SW coding

- **Independency:**

1. Avoid too complex structures




2. Avoid cycling rules



# Normalization Process for Safety Functions

Interlock **A** with **B** if **condition1**

Shutdown **A** if **condition2**

Prevent **A** to start if **condition3**

| C1 | C2 | C3 | A | B |
|---|---|---|---|---|
| *0* | *0* | *0* | ON | OFF |
| *0* | *0* | *1* | OFF | OFF |
| *0* | *1* | *0* | OFF | OFF |
| *0* | *1* | *1* | OFF | OFF |
| *1* | *0* | *0* | OFF | ON |
| *1* | *0* | *1* | OFF | ON |
| *1* | *1* | *0* | OFF | ON |
| *1* | *1* | *1* | OFF | ON |

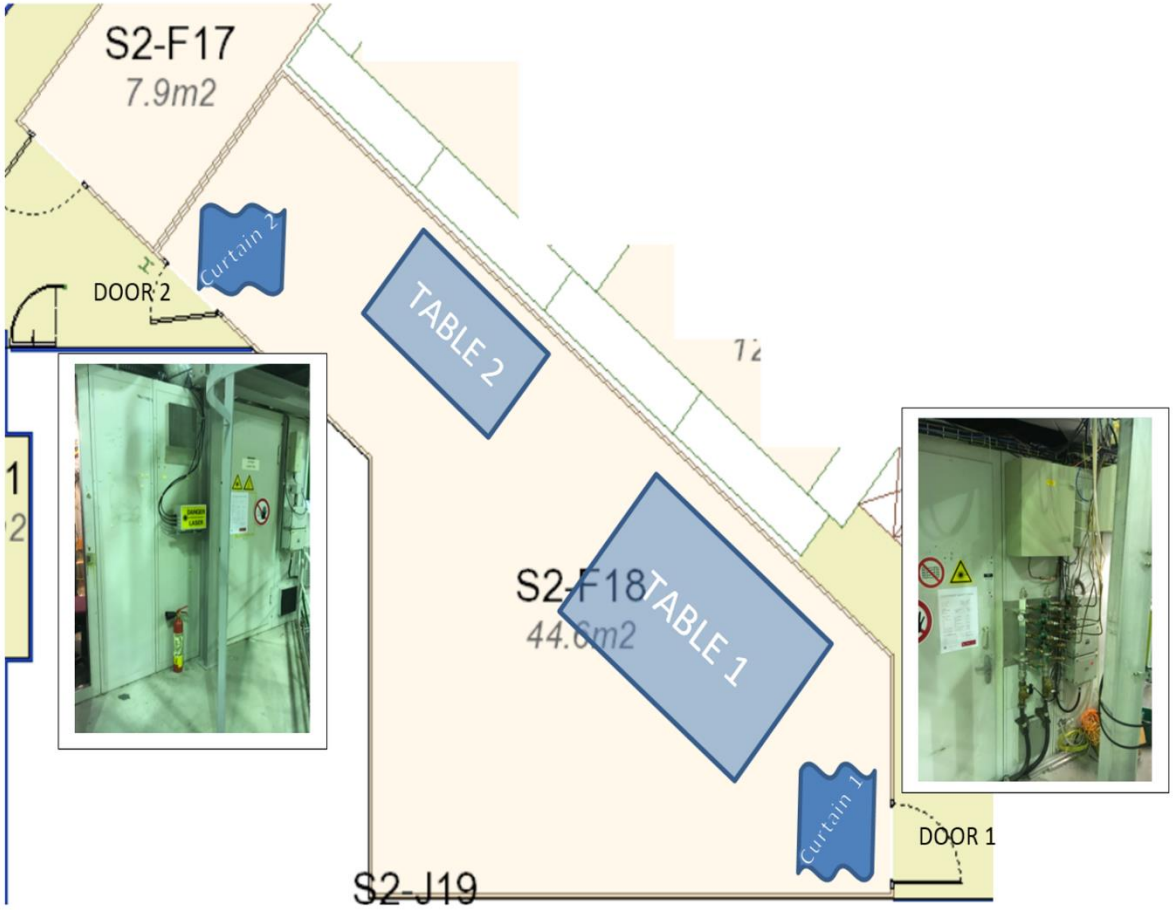
SIF-1: if (*cond1==0 & cond2==0 & cond3==0)* then A → **ON**

SIF-2: if (*cond1==1)* then B → **ON**

# To be considered @ this stage

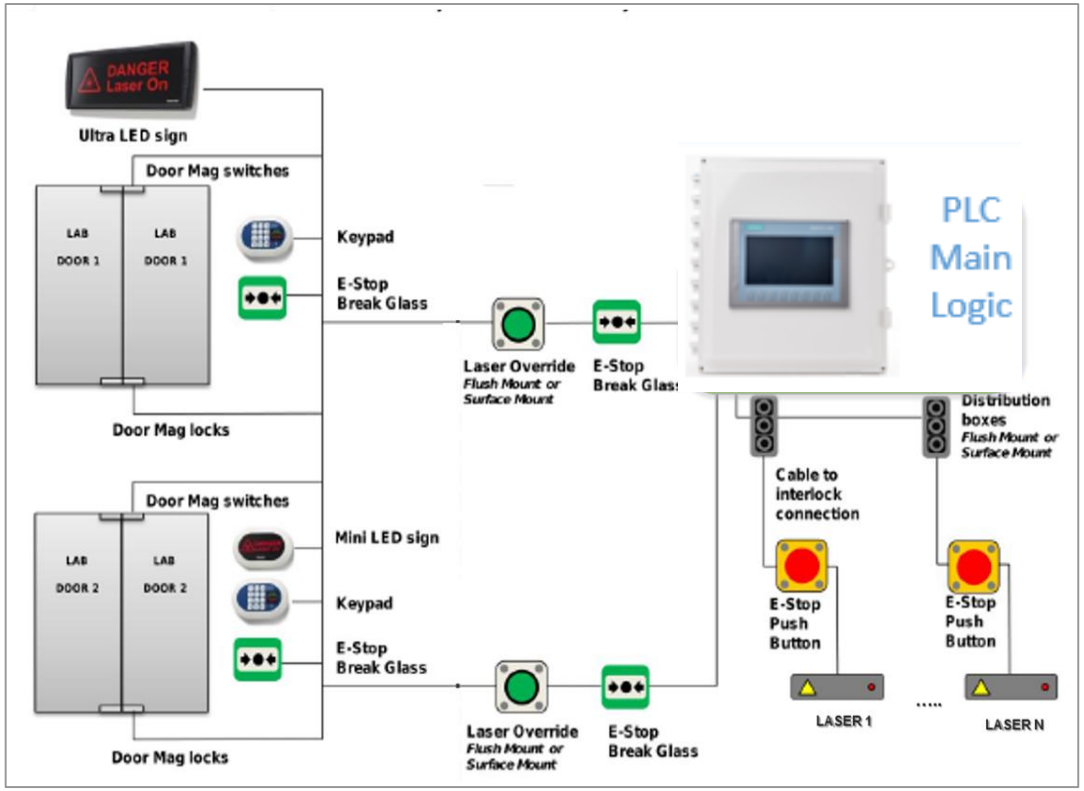
- Not all outcomes from R.A. needs to be implemented in safety;
- The added value for implementing a given R.A. outcome as a SIF shall be demonstrable by the study of the *Hazardous Event* failure scenario.
- Specific risk reductions (**>***10*) can be obtained via a SIL rated SIF **but also** via several independent layers of protection;
- Include into the SIS design ONLY what is not practicable to cover otherwise;
- Especially: avoid mix control with critical safety functionalities. Maintain a clear separation (*PROS/CONS … to discuss*).

# A practical example: ATRAP Experiment

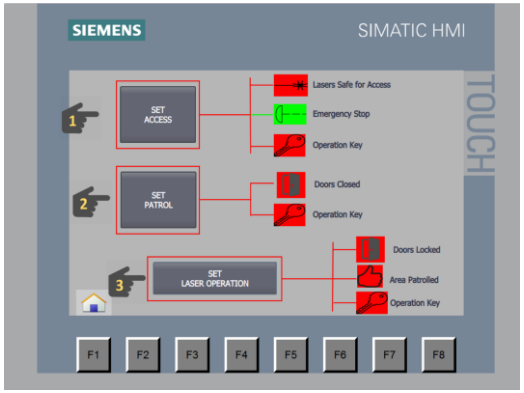


# A practical example: ATRAP Experiment

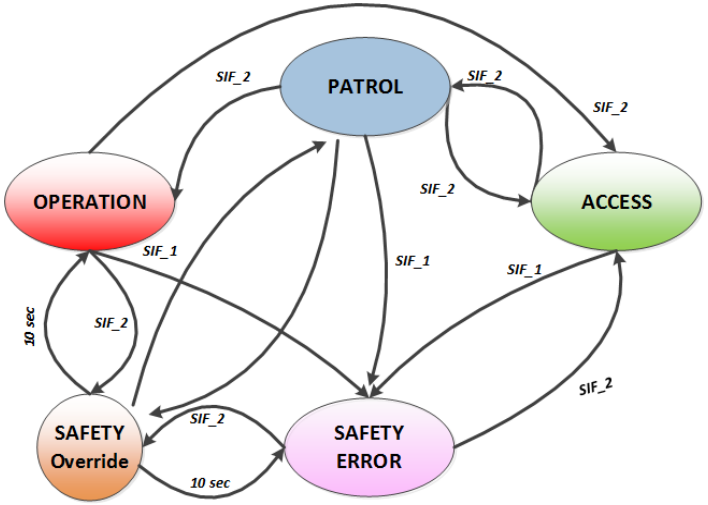
## Laser Room Equipment



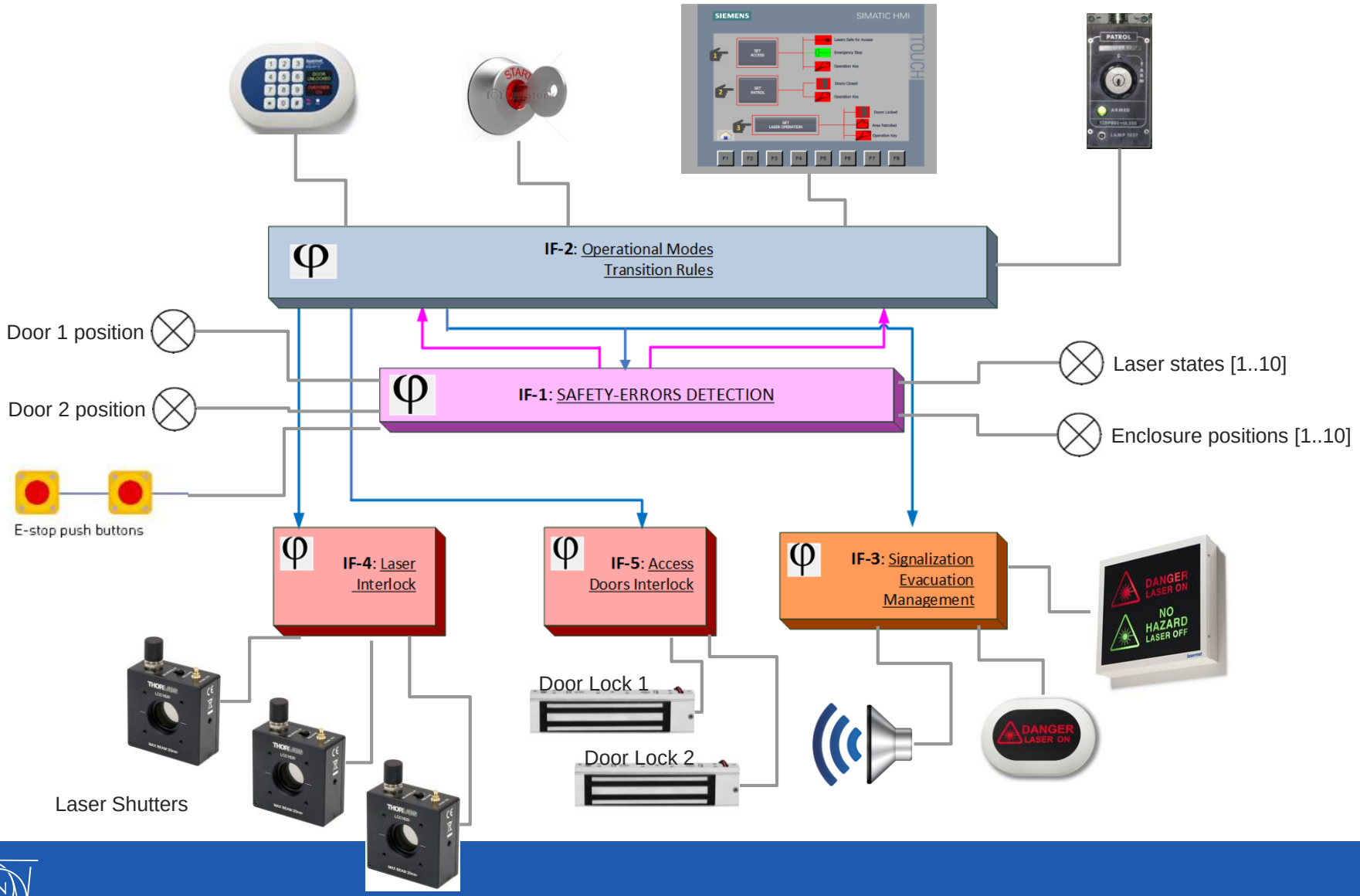

## Local Control Console



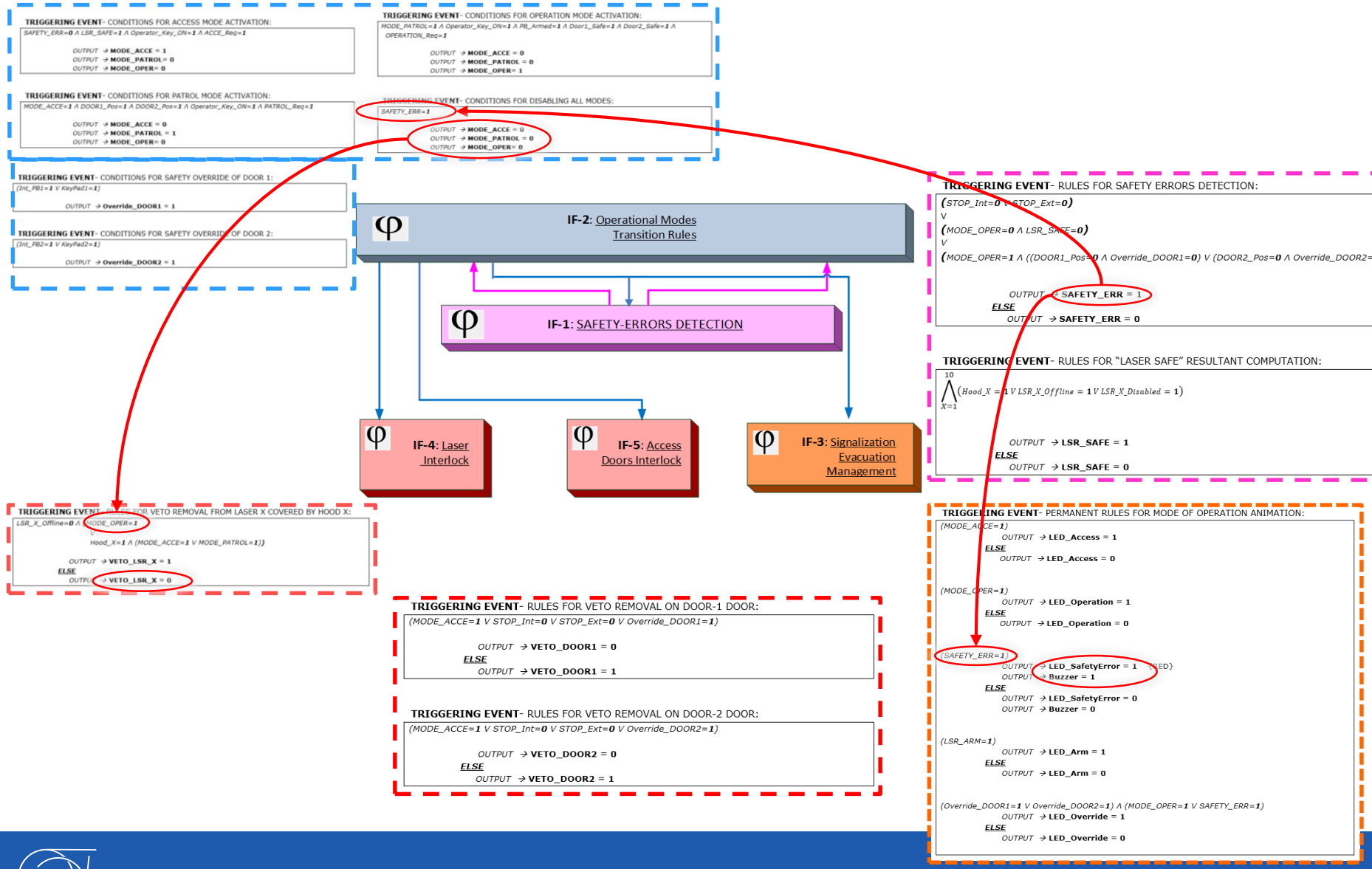

## Operational Modes



# A practical example: SIF Logic Model

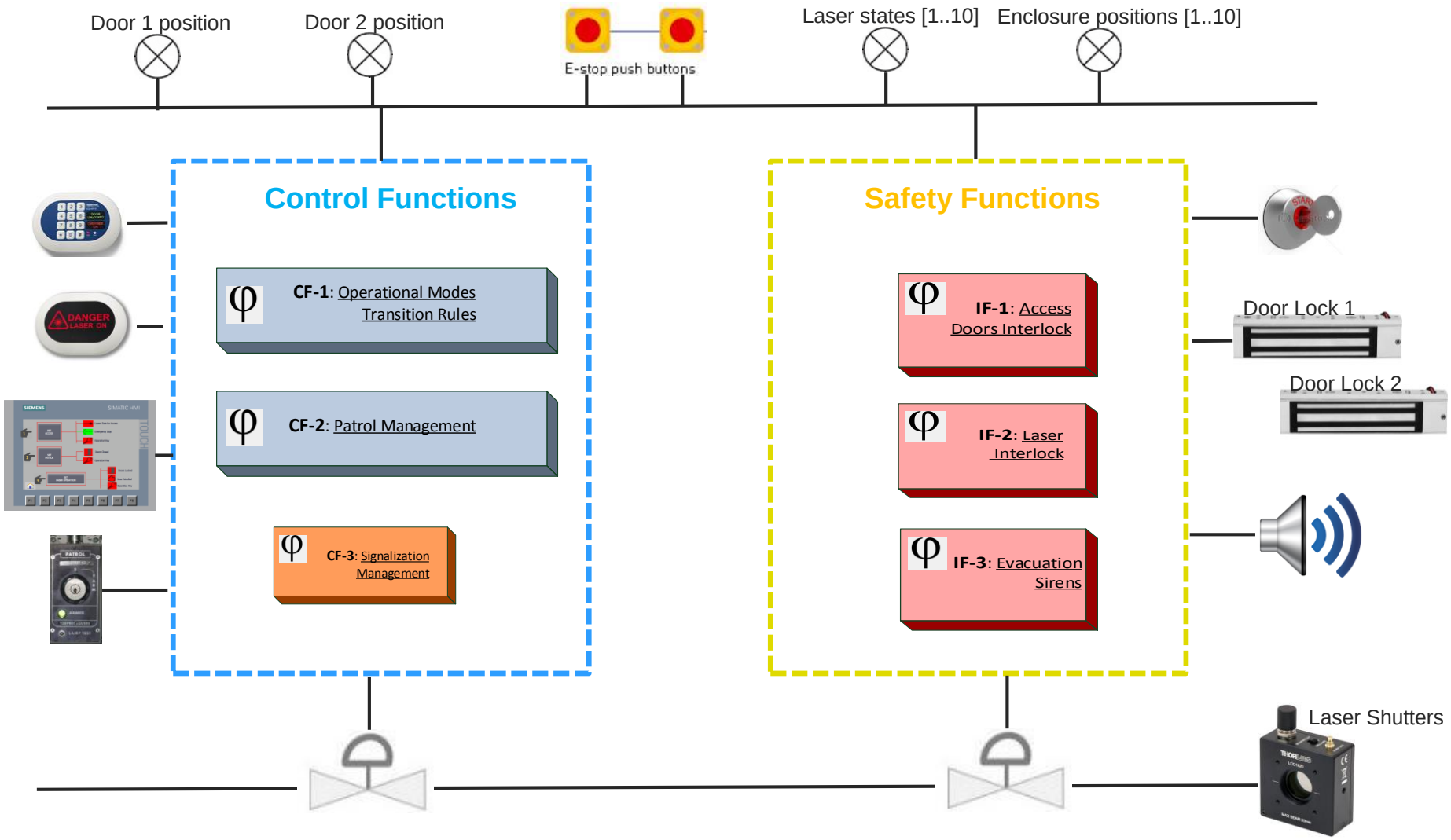


# A practical example: SIF Logic Model

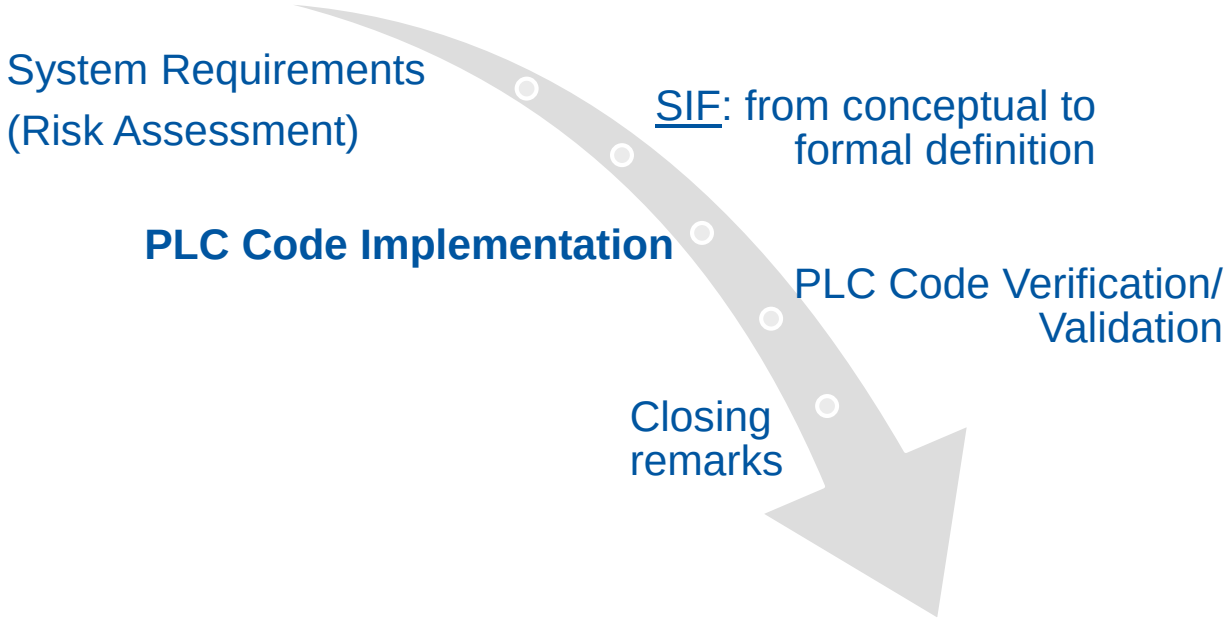



Edms: **1731580**

# A practical example: Alternative Design



# Outline


System Requirements
(Risk Assessment)
SIF: from conceptual to formal definition
PLC Code Implementation
PLC Code Verification/ Validation
Closing remarks

# PLC Code Implementation

- What properties shall have the PLC software.
- How to pass from the SIF logic model to the PLC code.
- What development strategy can be employed

# PLC code implementation: main properties

- **Maintainability:**

  *Different PLC systems developed inside the same organization shall have the same code structure and the same coding convention.*

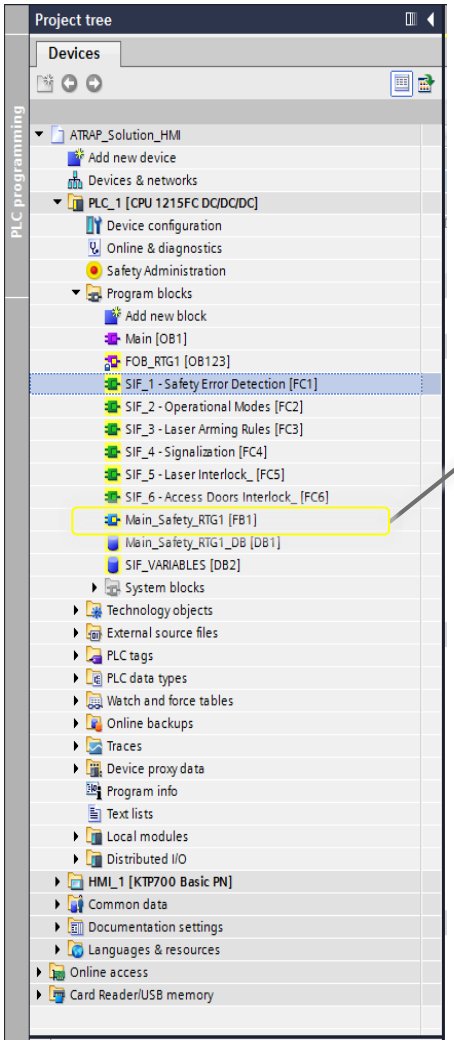
- **Coherence with specs:**

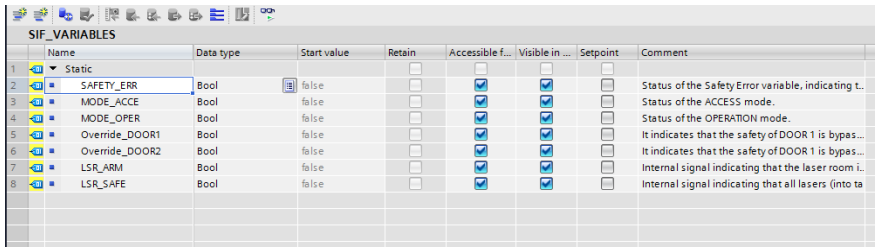
  *The code's blocks functionalities shall be clearly identifiable in respect of the requirements of the functional specification.*

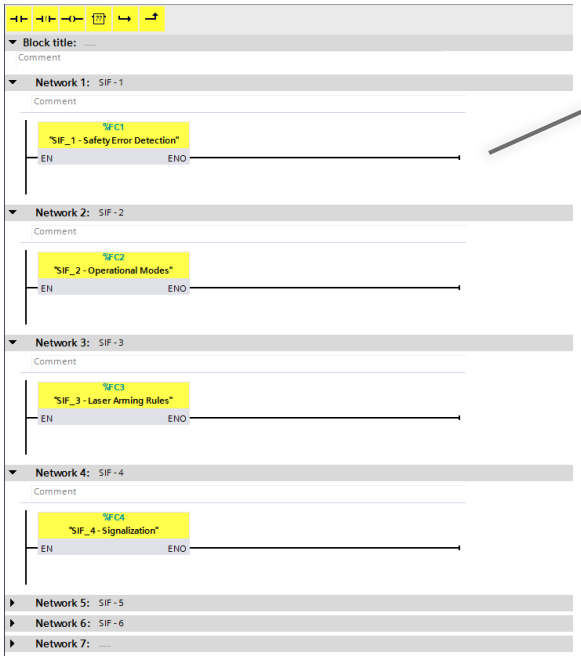
- **Testability:**

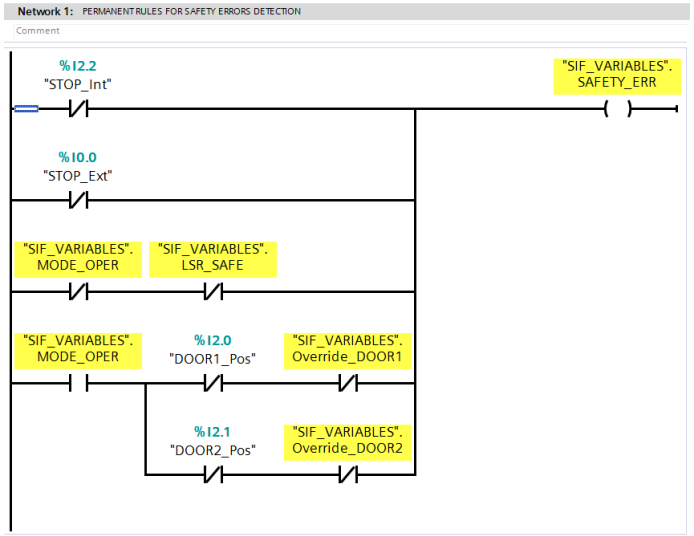
  *The code structure shall allow to easy identify relevant test UNITS and make it easily possible to test them: e.g. every unit shall be testable independently from the others.*

# PLC code implementation: a possible strategy

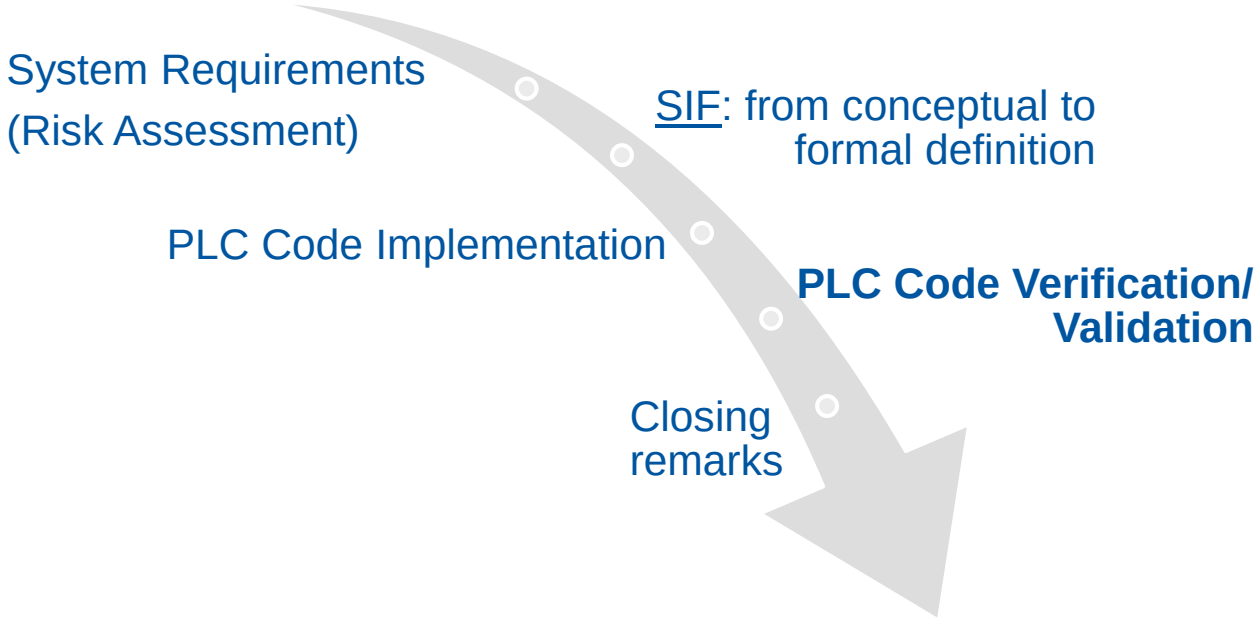


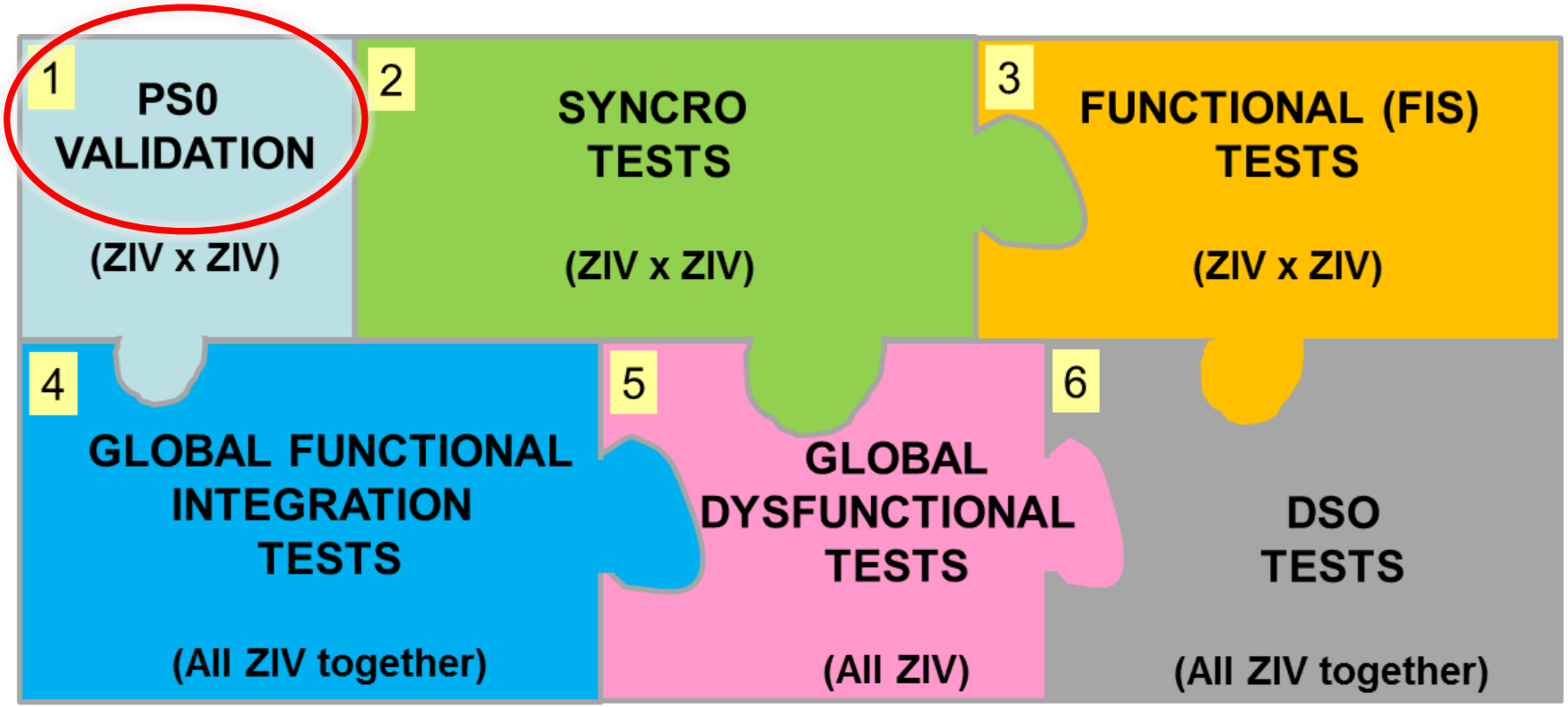
# Outline


System Requirements
(Risk Assessment)
SIF: from conceptual to formal definition
PLC Code Implementation
PLC Code Verification/ Validation
Closing remarks

# PLC Code Verification & Validation

- How to define PLC software unit tests?
- How to ensure that unit tests are relevant for the validation of a specific SIF?
- How to ensure the system does what it is supposed to?
- How to estimate the quality of the tests: *test coverage*?
- Practical tests execution.

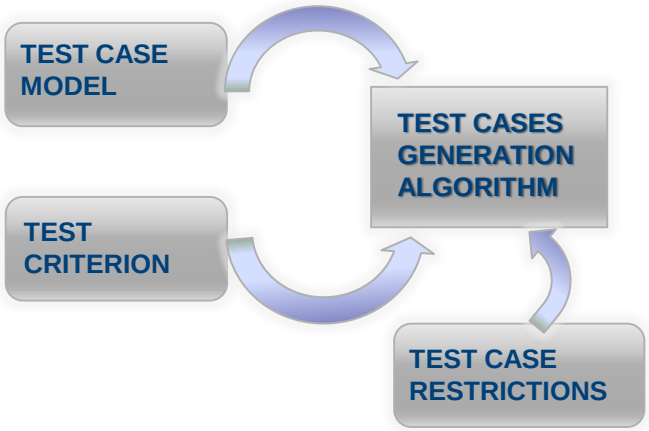
# PLC code V & V: main properties



# PLC code V & V: main properties

**Test Criterion:**

***Verify FIS outputs for all possible events triggering the FIS interlock actions.***




| FIS CODE | TEST CASE SCENARIO | CATEGORY |
|---|---|---|
| FIS_1 | ACTIVATION OF THE REPLI MODE FOR THE ZIV | SAFETY |

**TEST CASE MODEL:**

$\Phi_{1\_1} = ((MODE\_Acc = 1 \vee MODE\_TFA = 1 \vee MODE\_Tra = 1) \wedge ACC\_Tst = 0 \wedge ACC\_TfT = 0 \wedge EISb\_Pos = 0) \vee (MODE\_Acc = 0 \wedge EISa\_Safe = 0)$

**TEST CASE RESTRICTIONS:**

$R_1 = (MODE\_Acc=1 \wedge MODE\_TFA=1) \vee (MODE\_Acc=1 \wedge MODE\_Tra = 1) \vee (MODE\_TFA=1 \wedge MODE\_Tra = 1)$

$R_2 = (ACC\_Tst=1 \wedge ACC\_TfT=1)$

$R_3 = (MODE\_Acc=0) \wedge (ACC\_Tst=1 \vee ACC\_TfT=1)$

**TEST CASE GENERATION MODEL:**

$$\omega : (\Phi_{1\_1} = 1) \wedge (R_1 = 0) \wedge (R_2 = 0) \wedge (R_3 = 0)$$

**SYSTEM VERIFICATION PROPERTY:**

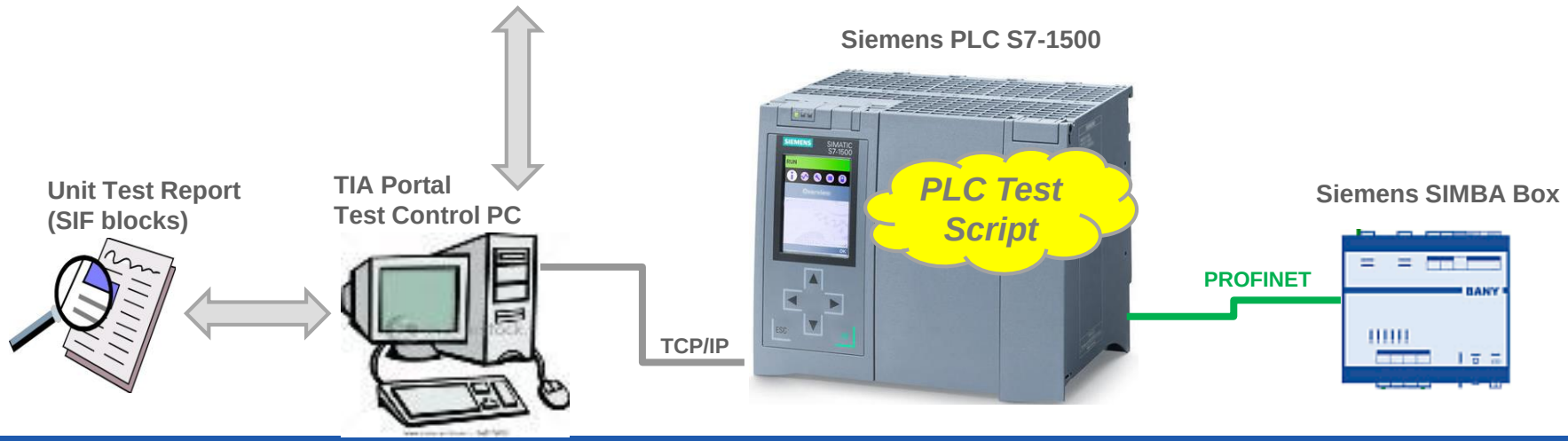
$$(MODE\_Rep = 1)$$

| | | | | | |
|---|---|---|---|---|---|
| **Total Variables:** | *7* | **Total State Space:** | *128* | **Scenario State Space:** | *10* |
| **I/O Types:** | *DIGITAL* | **Test Impact:** | *PLC ZIVx PLC OKC* | **Execution Strategy:** | *MANUAL* |

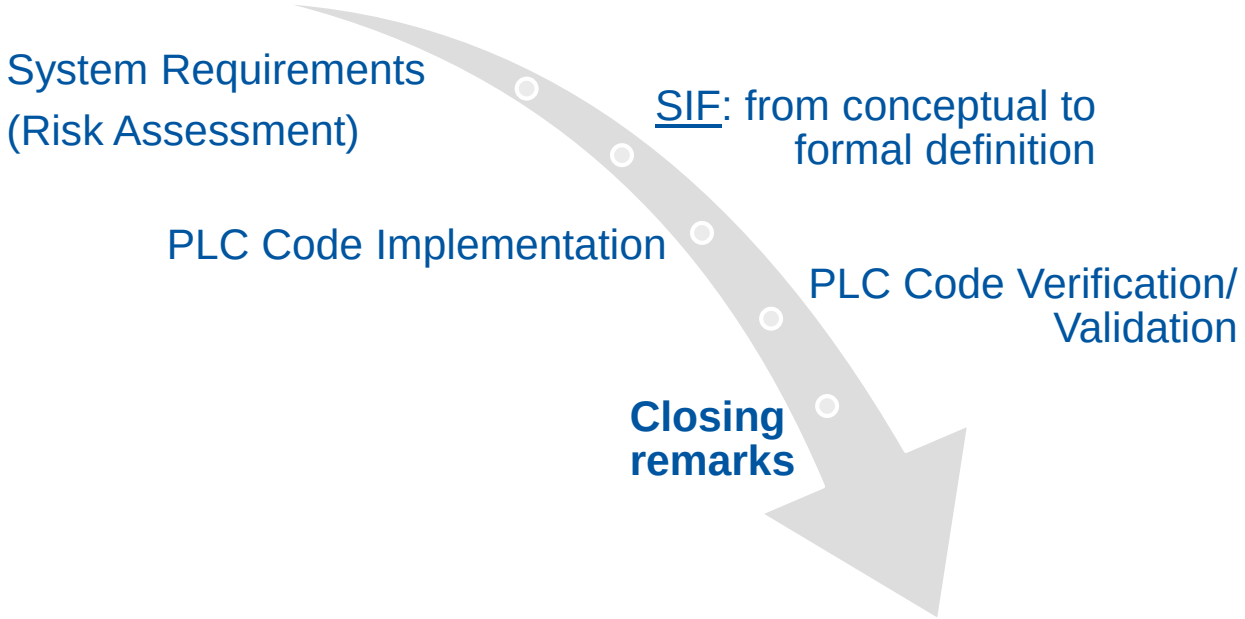
# PLC code V & V: main properties

## Test Instances auto-generated by MATLAB:

| | MODE_Acc | MODE_TFA | MODE_Tra | ACC_Tst | ACC_ITT | ElSb_Pos | ElSa_Safe | RESULTS |
|---|---|---|---|---|---|---|---|---|
| Test 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | |
| Test 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Test 3 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | |
| Test 4 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | |
| Test 5 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | |
| Test 6 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | |
| Test 7 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | |
| Test 8 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | |
| Test 9 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | |
| Test 10 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | |



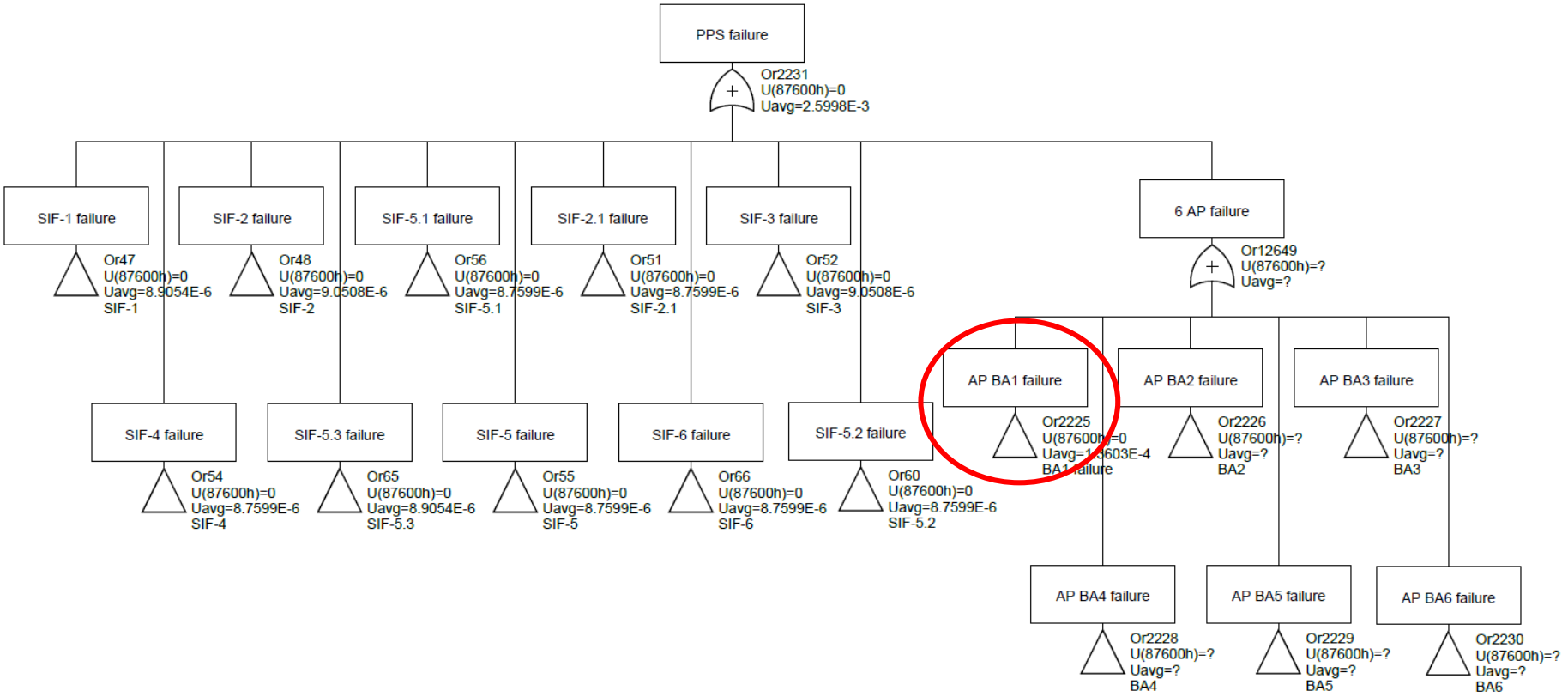
# Outline


System Requirements
(Risk Assessment)
SIF: from conceptual to formal definition
PLC Code Implementation
PLC Code Verification/ Validation
Closing remarks

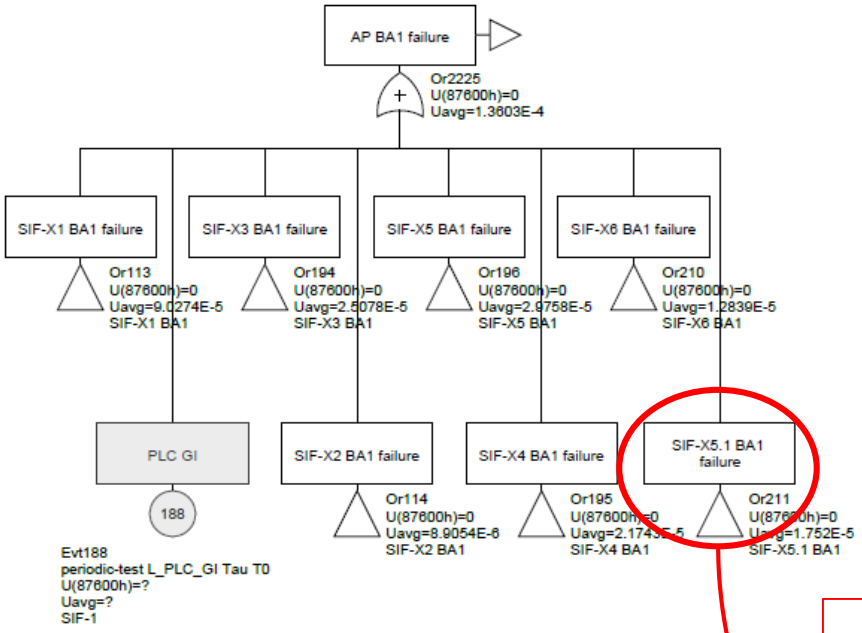
# Closing Remarks

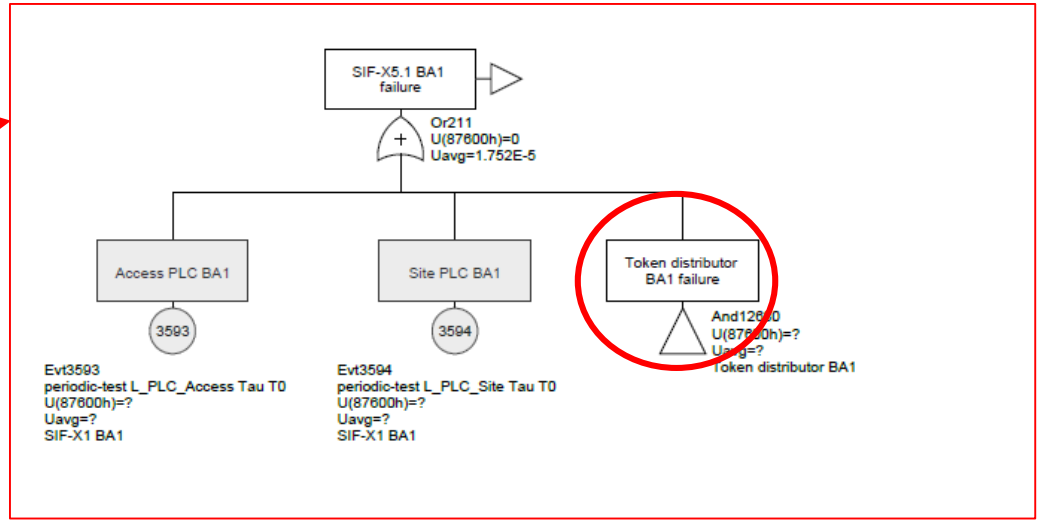
- SIL VERIFICATION
  - FTA approach: typically thousands of nodes are needed to model a complex systems.
  - Large usage of approximating hypotheses: *failure rates of components, probability distribution, calculations, system design.*
  - Impact of these approximations on final results is not easily accountable, but it grows with the complexity of the system.

# Closing Remarks

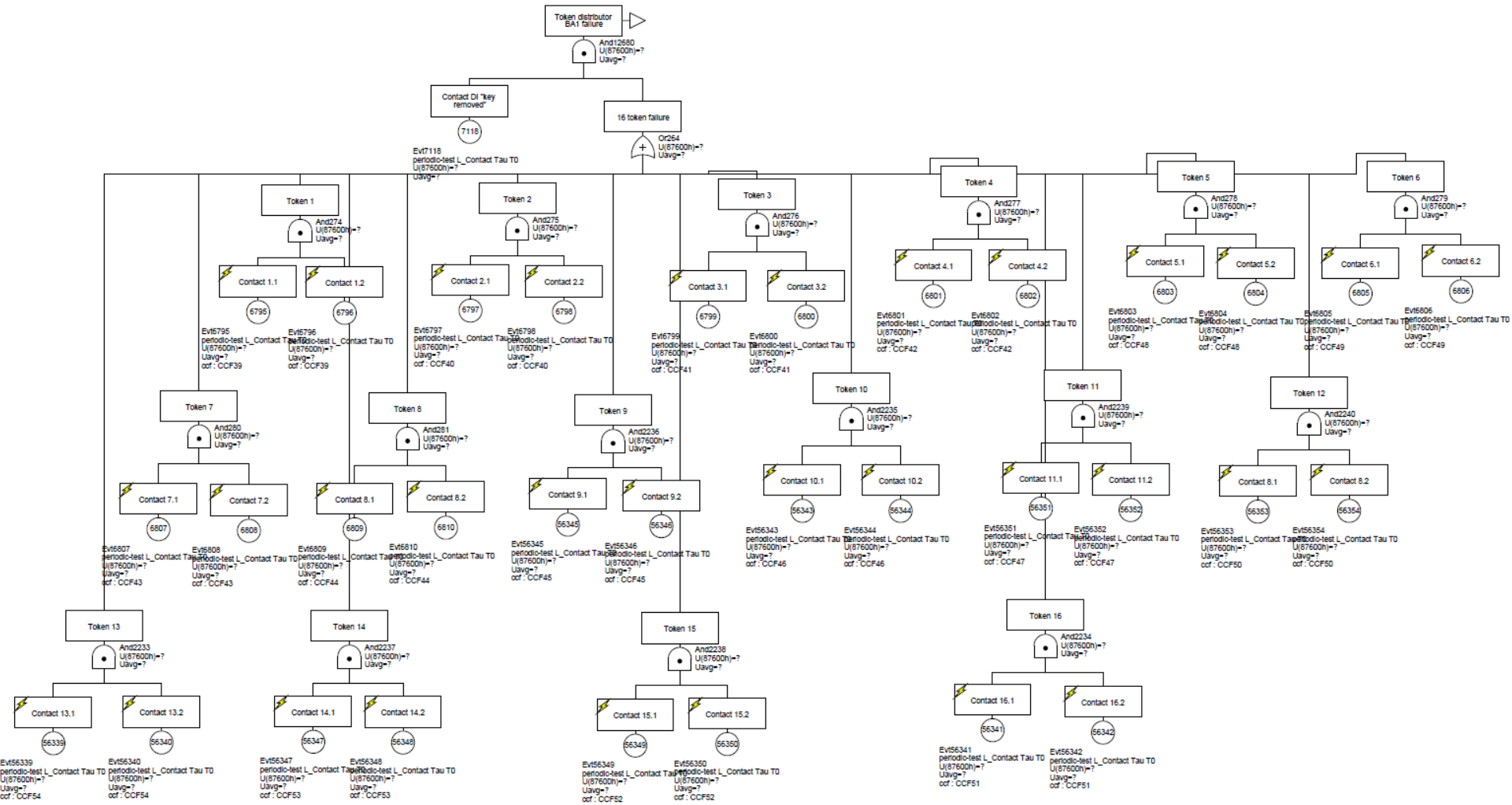


# Closing Remarks



# Closing Remarks



# Closing Remarks

- KEYPOINTS FOR COMPLEX SYSTEMS DESIGN
  - Keep a clear separation between Safety and Standard control.
  - Make the safety part as simple as possible: do not include in the SIS functionalities what can be done in standard if NO added value. It makes easy to proof SIL and to validate SIS.
  - Norm 61511 is helpful for systems of reduced/average scale, however for complex systems nuclear **norm 61513** can bring real added value focusing more on other aspects than SIL:
    - *Usage of redundancy and diversity of SIS devices;*
    - *Prescriptions against external aggressions;*
    - *Guidelines to avoid common **causes** & **modes** of failures.*

# THANK YOU FOR YOUR ATTENTION

## Any Questions?


CERN