STPA Methodology for Hazard Analysis on a Nuclear Application Software

Nazaret López
Safety, Operation and Training Services
Tecnatom S.A.
nlopez@tecnatom.es

WHO WE ARE

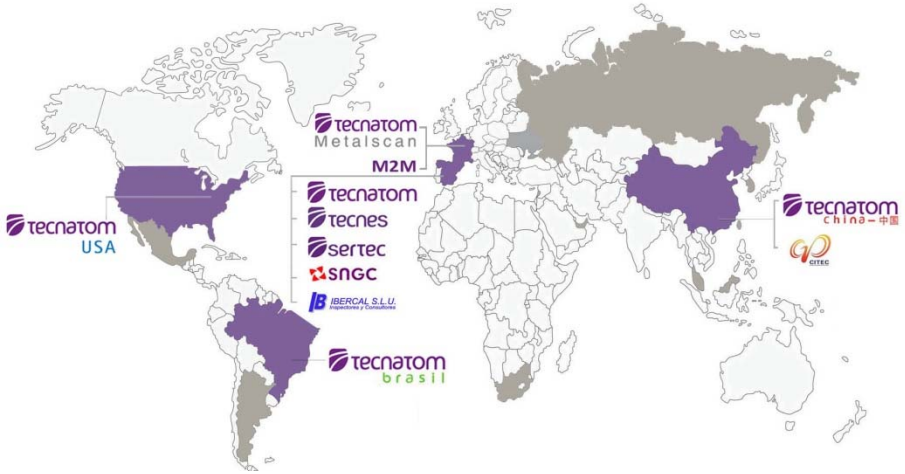
- Areas of activity:

  -Training, Operation and Safety
  -Process engineering
  -Inspection and testing services
  -Product design and development

- Projects in more than 30 countries

- 800 employees worldwide:

  -Headquarters in Spain
  -France
  -Brazil
  -China
  -USA



tecnatom

OUTLINE

1. Context of this work
2. Tecnatom's Advanced Alarm System AAS
3. Application of STPA
4. Conclusions & Future Work

CONTENTS

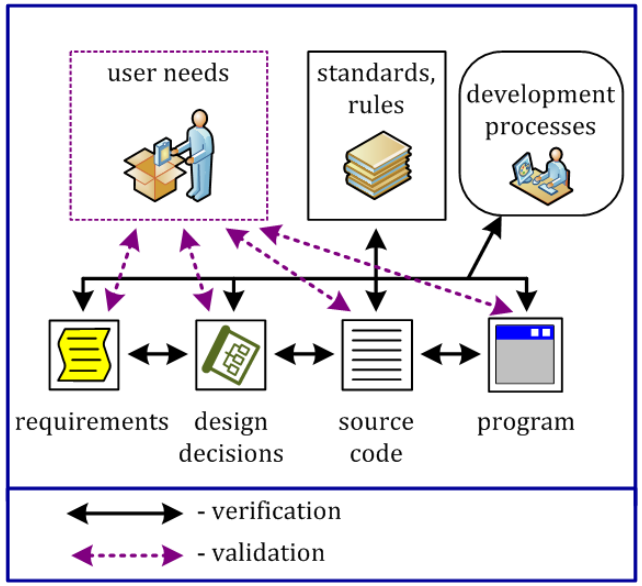
1

1. Context of this work
2. Tecnatom's Advanced Alarm System AAS
3. Application of STPA
4. Conclusions & Future Work

CONTEXT OF THIS WORK

Verification & Validation

Goal: Verification and Validation (V&V) of the Advanced Alarm System through the standard IEEE 1012-2004 (Standard for Software Verification and Validation) endorsed by the R.G. 1.168



tecnatom

CONTEXT OF THIS WORK

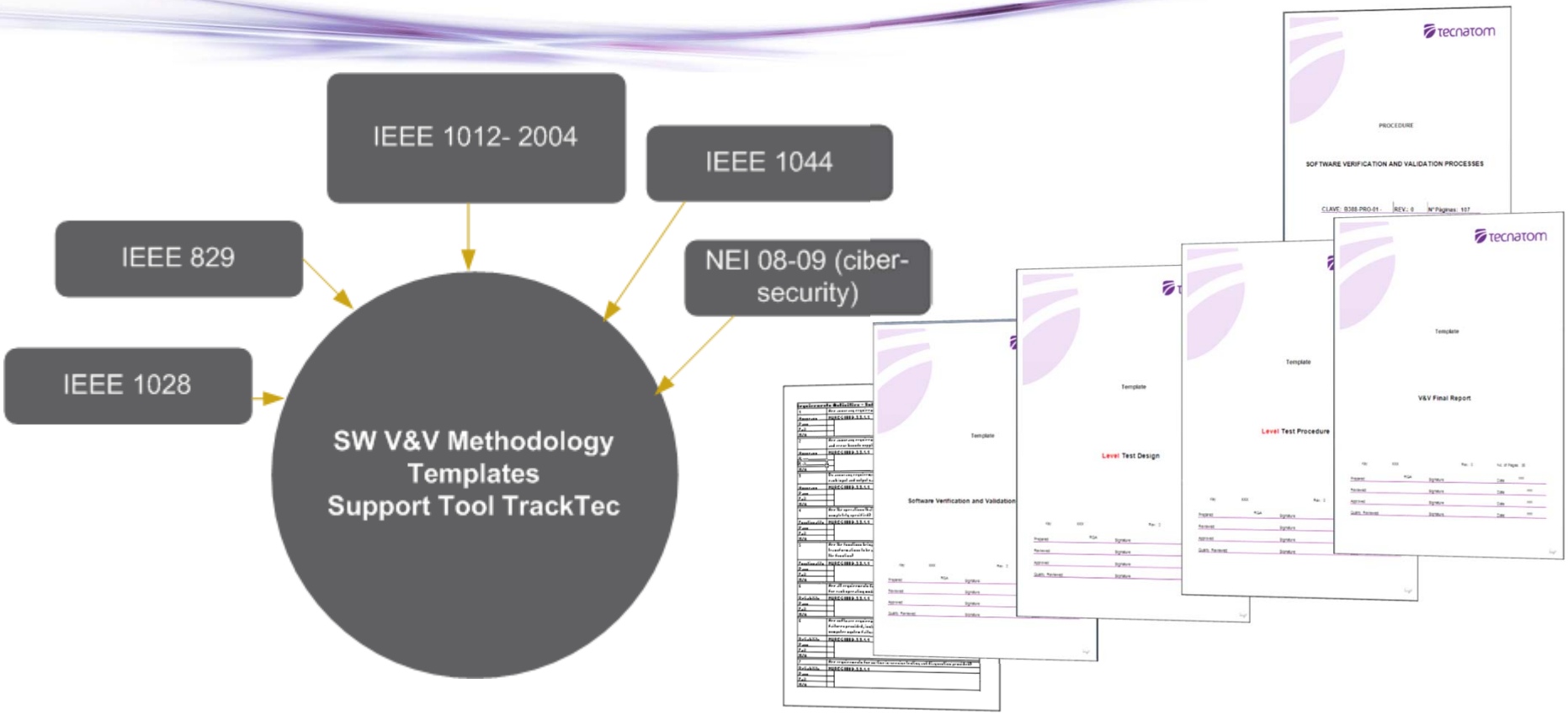
Verification & Validation

Kitty Hawk, North Carolina, USA, December 1903

tecnatom

CONTEXT OF THIS WORK

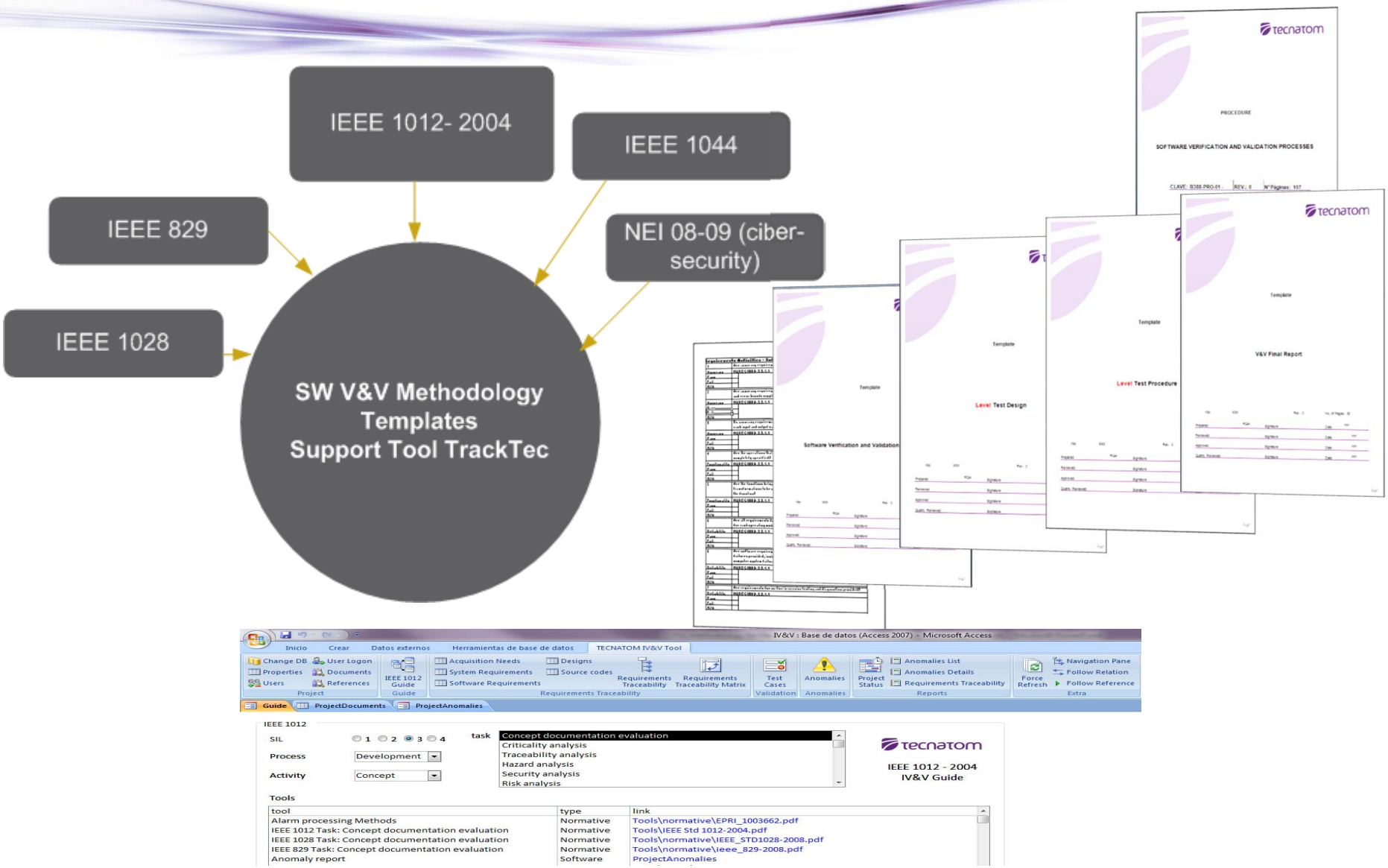
Tecnatom approach in V&V (IEEE 1012-2004)



tecnatom

CONTEXT OF THIS WORK

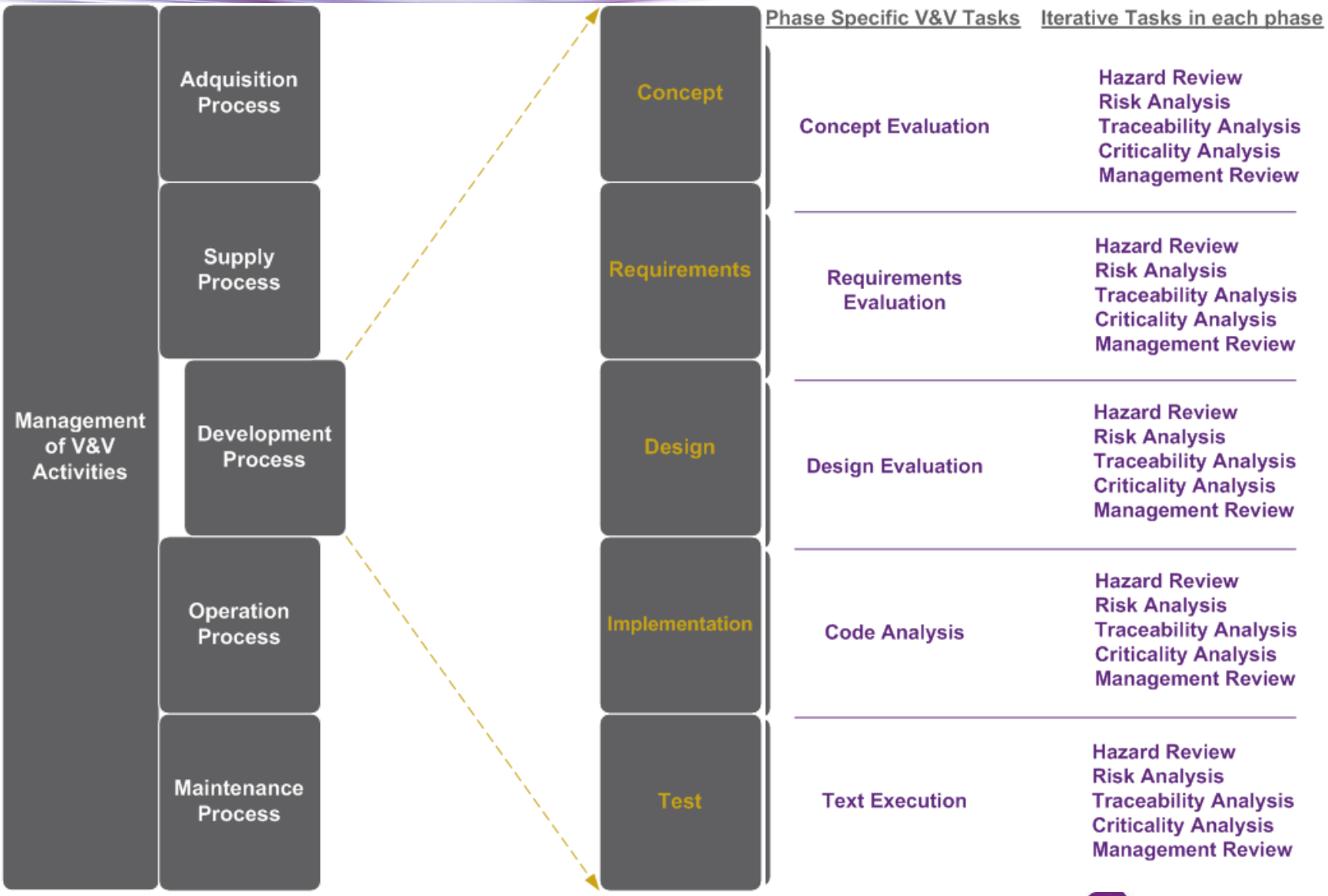
Tecnatom approach in V&V (IEEE 1012-2004)



tecnatom

CONTEXT OF THIS WORK

Tecnatom approach in V&V (IEEE 1012-2004)



tecnatom

tecnatom

1. Context of this work
2. Tecnatom's Advanced Alarm System AAS
3. Application of STPA
4. Conclusions & Future Work

2 CONTENTS

TECNATOM'S ADVANCED ALARM SYSTEM AAS

Modular System

Integration

Information Treatment

User Interface

Operation Support

tecnatom

TECNATOM'S ADVANCED ALARM SYSTEM AAS

Software Integrity Level

- IEEE 1012 defines an acceptable four level method of quantifying software integrity levels (SIL)
- This standard uses software integrity levels to determine the V&V tasks to be performed
- We have assigned SIL 3 to the AAS
- Non-safety related Augmented Quality (Guideline for the Acceptance of Commercial Grade Design and Analysis Computer Programs Used in Nuclear Safety-Related Applications: Revision 1 of 1025243. EPRI)

Description	SIL
Software element must execute correctly or grave consequences will occur. No mitigation is possible.	4
Software element must execute correctly or the intended use of the software will not be realized, causing serious consequences. Partial to complete mitigation is possible.	3
Software element must execute correctly or an intended function will not be realized, causing minor consequences. Complete mitigation possible.	2
Software element must execute correctly or intended function will not be realized, causing negligible consequences. Mitigation not required.	1

tecnatom

tecnatom

1. Context of this work
2. Tecnatom's Advanced Alarm System AAS
3. Application of STPA
4. Conclusions & Future Work

3

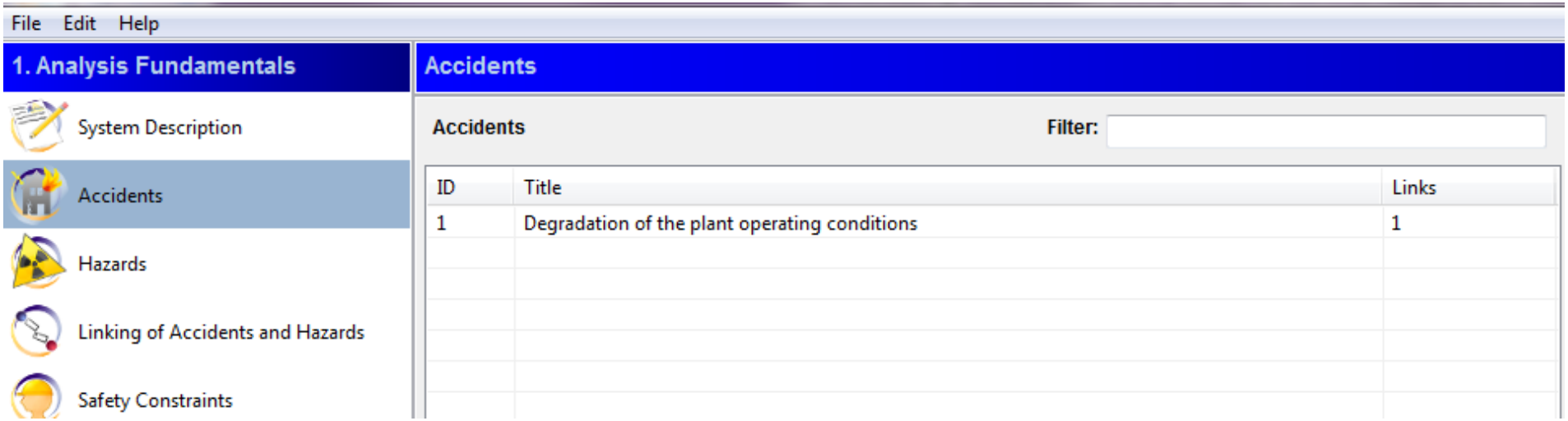
CONTENTS

APPLICATION OF STPA

Basic steps in STPA

Step 0: Establishing the system engineering

Define what accidents will be considered



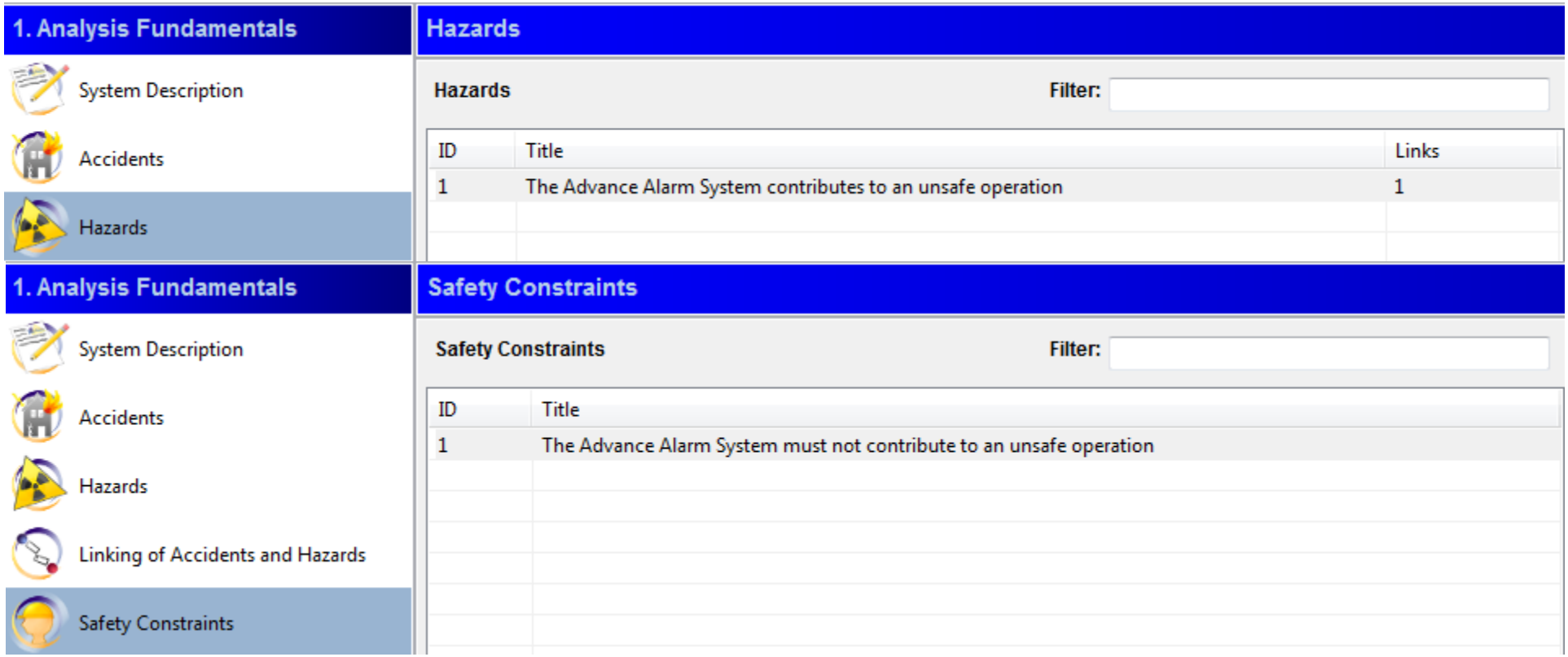
tecnatom

APPLICATION OF STPA

Basic steps in STPA

Step 0: Establishing the system engineering

Define the software hazards and safety constraints



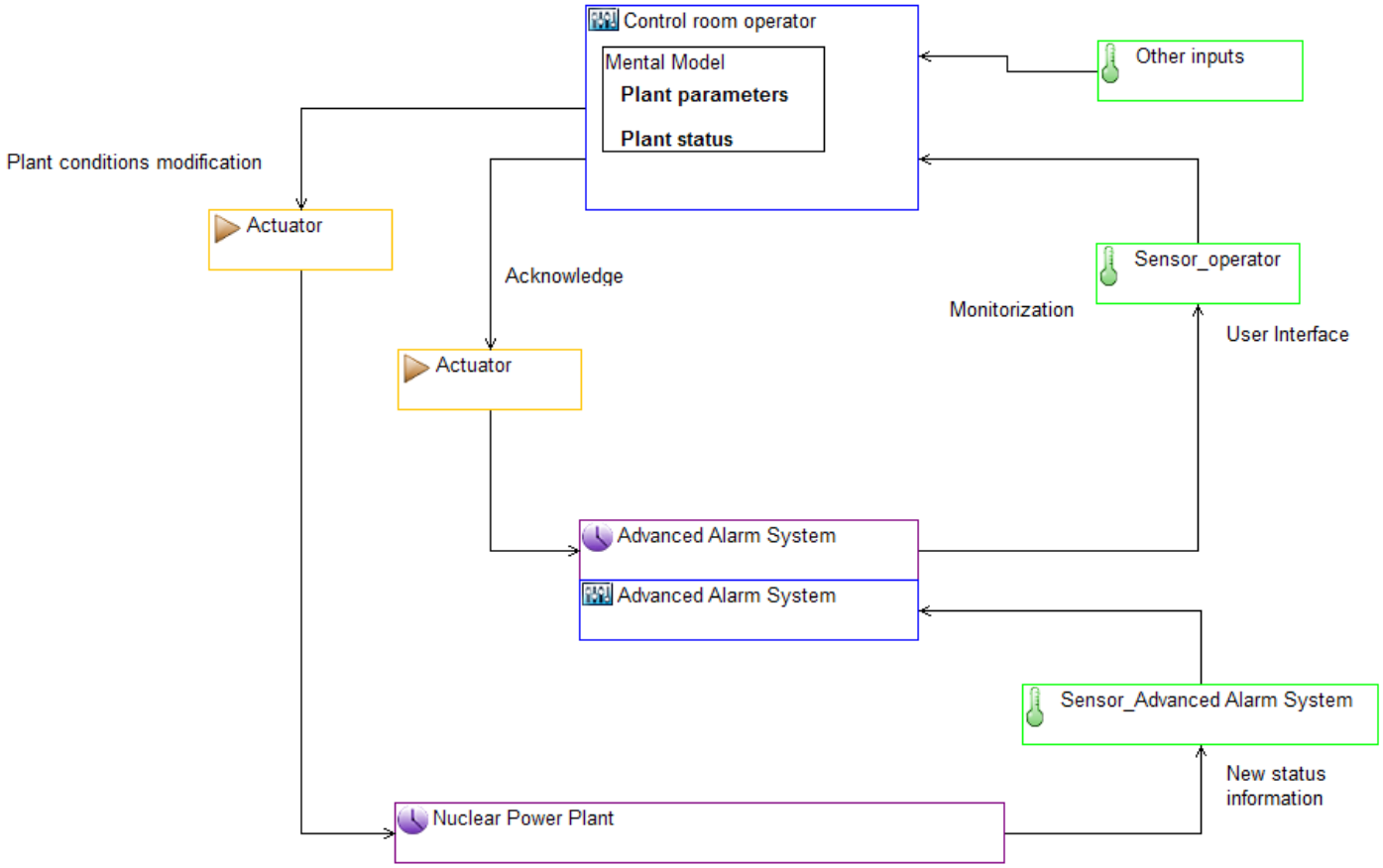
tecnatom

APPLICATION OF STPA

Basic steps in STPA

Step 0: Establishing the system engineering

Define the functional control structure of the AAS



tecnatom

APPLICATION OF STPA

Basic steps in STPA

Step 1: Identifying Unsafe Control Actions

There are four types of unsafe control actions

Unsafe Control Actions Table

Control Action	Not providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stopped too soon or Applied too long
Modify the plant operating conditions	The control room operator does not modify the plant conditions when a plant alarm condition exists	The control room operator modifies wrong the plant conditions when a plant alarm condition exists	The control room operator modifies the plant conditions too late or too early when a plant alarm condition exists	The control room operator does not modify completely the plant conditions when a plant alarm condition exists
	[H-1]	[H-1]	[H-1]	[H-1]
		The control room operator modifies the plant conditions when it does not exist a plant alarm condition		
	Add not given UCA	[H-1]	Add wrong timing UCA	Add stopped too soon UCA

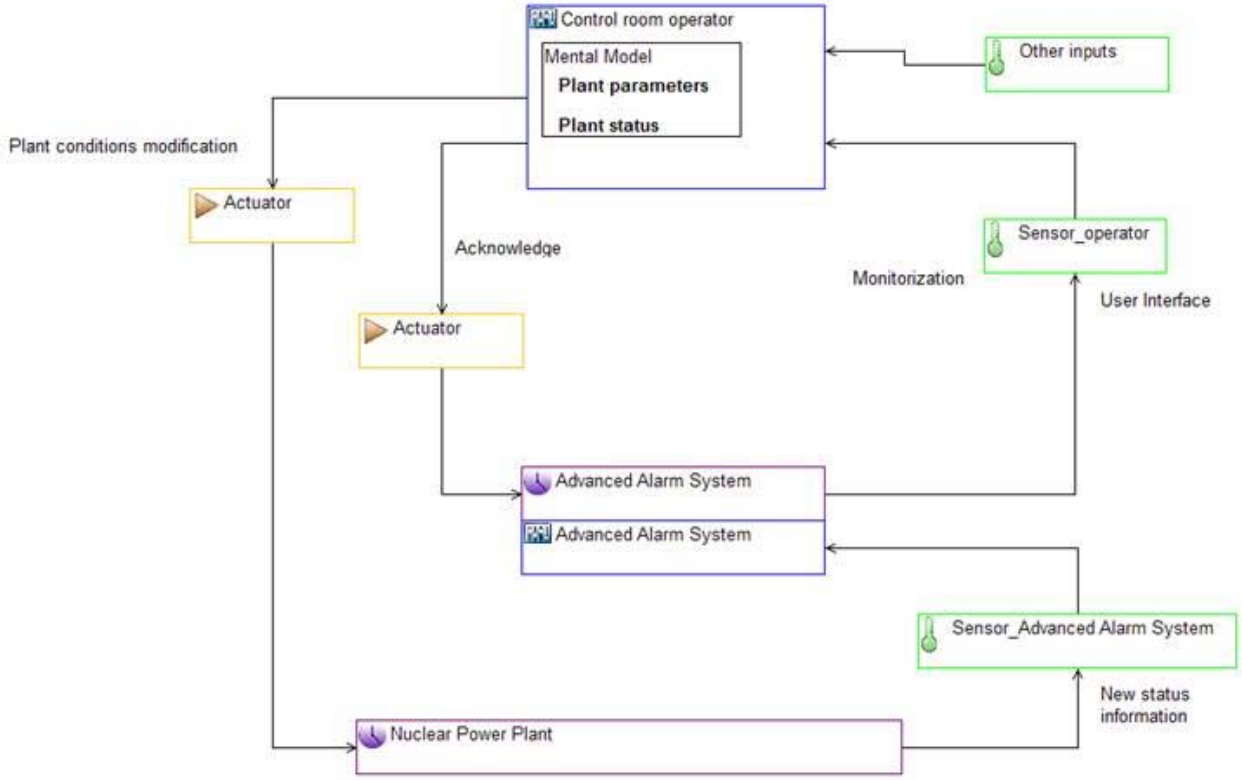
tecnatom

APPLICATION OF STPA

Basic steps in STPA

Step 2: Identifying Causes for Unsafe Control Actions

Determine how each potentially hazardous control could happen



The AAS provides inadequate, missing or delayed information (inadequate, missing or delayed feedback to the controller)

The communication channel between the AAS and the plant systems is inadequate, missing or delayed (inadequate, missing or delayed feedback to the AAS)

tecnatom

tecnatom

1. Context of this work
2. Tecnatom's Advanced Alarm System AAS
3. Application of STPA
4. Conclusions & Future Work

4 CONTENTS

CONCLUSIONS AND FUTURE WORK

- The current STPA exercise is only a first attempt for us at getting experience using the STPA methodology

- STPA makes possible to identify safety constraints and causal factors for early software design phase

- Conceptually STPA is very useful to find early hazardous scenarios, more complexity when refining in successive stages

- Future work: Hazard analysis with STPA iteratively across the software development lifecycle (more functions and interfaces will appear adding complexity)

tecnatom

THANK YOU

Nazaret López
Safety, Operation and Training Services
Tecnatom S.A.
nlopez@tecnatom.es

www.tecnatom.es

@tecnatom