3rd European STAMP Workshop, Amsterdam October 2015



STPA Methodology for Hazard Analysis on a Nuclear Application Software

Nazaret López

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



• 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



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





- 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





CONTEXT OF THIS WORK

Verification & Validation





Kitty Hawk, North Carolina, USA, December 1903







CONTEXT OF THIS WORK Tecnatom approach in V&V (IEEE 1012-2004) Tecnatom IEEE 1012-2004 **IEEE 1044** SOFTWARE VERIFICATION AND VALIDATION PROCESSES CLAVE: 8388-PRO-01 - REV: 0 Nº Páginas: 1 Tecnatom NEI 08-09 (ciber-**IEEE 829** security) 1 **IEEE 1028** V&V Final Report SW V&V Methodology Level Test Proced Level Test Design Templates Support Tool TrackTec IV&V : Base de datos (Access 2007) - Microsoft A Herramientas de base de datos TECNATOM IV&V Tool Change DB & User Logon Properties Documents Supervise Requirements Supervis Anomalies List Navigation Pane Anomalies Project Anomalies Details Project Status Requirements Traceability Force Refresh Follow Reference SS User Requirements Traceabilit Extra IEEE 1012 cept doo SIL ◎1 ◎2 ●3 ◎4 τεςηστομ Criticality analysis Process Development 💌 Traceability analysis Hazard analysis Security analysis IEEE 1012 - 2004 Activity Concept -IV&V Guide Risk analysis Tools type Normative Normative tool link Alarm processing Methods IEEE 1012 Task: Concept documentation evaluation Tools\normative\EPRI_1003662.pdf Tools\IEEE Std 1012-2004.pdf IEEE 1028 Task: Concept documentation evaluation Normative Tools\normative\IEEE STD1028-2008.pdf IEEE 829 Task: Concept documentation evaluation Normative Tools\normative\ieee_829-2008.pdf Anomaly report Software ProjectAnomalies Proprietary & Confidential 2015 Tecnatom S.A.

All Rights Reserved



CONTEXT OF THIS WORK

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







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



TECNATOM'S ADVANCED ALARM SYSTEM AAS

Modular System





Τεςποτομ

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





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



Basic steps in STPA

Step 0: Establishing the system engineering

Define what accidents will be considered

File Edit Help						
1. Analysis Fundamentals	Accidents					
System Description	Accidents					
Accidents	ID	Title	Links			
Hazards	1	Degradation of the plant operating conditions	1			
Linking of Accidents and Hazards						
Safety Constraints						



Basic steps in STPA

Step 0: Establishing the system engineering

Define the software hazards and safety constraints

1. Analysis Fundamentals	Hazards			
System Description	Hazards	Filter:	Filter:	
Accidents	ID	Title	Links	
	1	The Advance Alarm System contributes to an unsafe operation	1	
📂 Hazards				
1. Analysis Fundamentals	Safety C	Constraints		
System Description	Safety Co	onstraints Filter:		
Accidents	ID	Title		
	1	The Advance Alarm System must not contribute to an unsafe operation		
Hazards				
Linking of Accidents and Hazards				
Safety Constraints				





Basic steps in STPA

Step 0: Establishing the system engineering

Define the functional control structure of the AAS





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 plan 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] oo	[H-1]	•• [H-1]	00 [H-1] 00			
		The control room operator modifies the plant conditions when it does not exist a plant alarm condition	X				
	Add not given UCA +	[H-1]	Add wrong timing UCA	+ Add stopped too soon UCA +			



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)





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





THANK YOU

Nazaret López

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



www.tecnatom.es





