ebg MedAustron

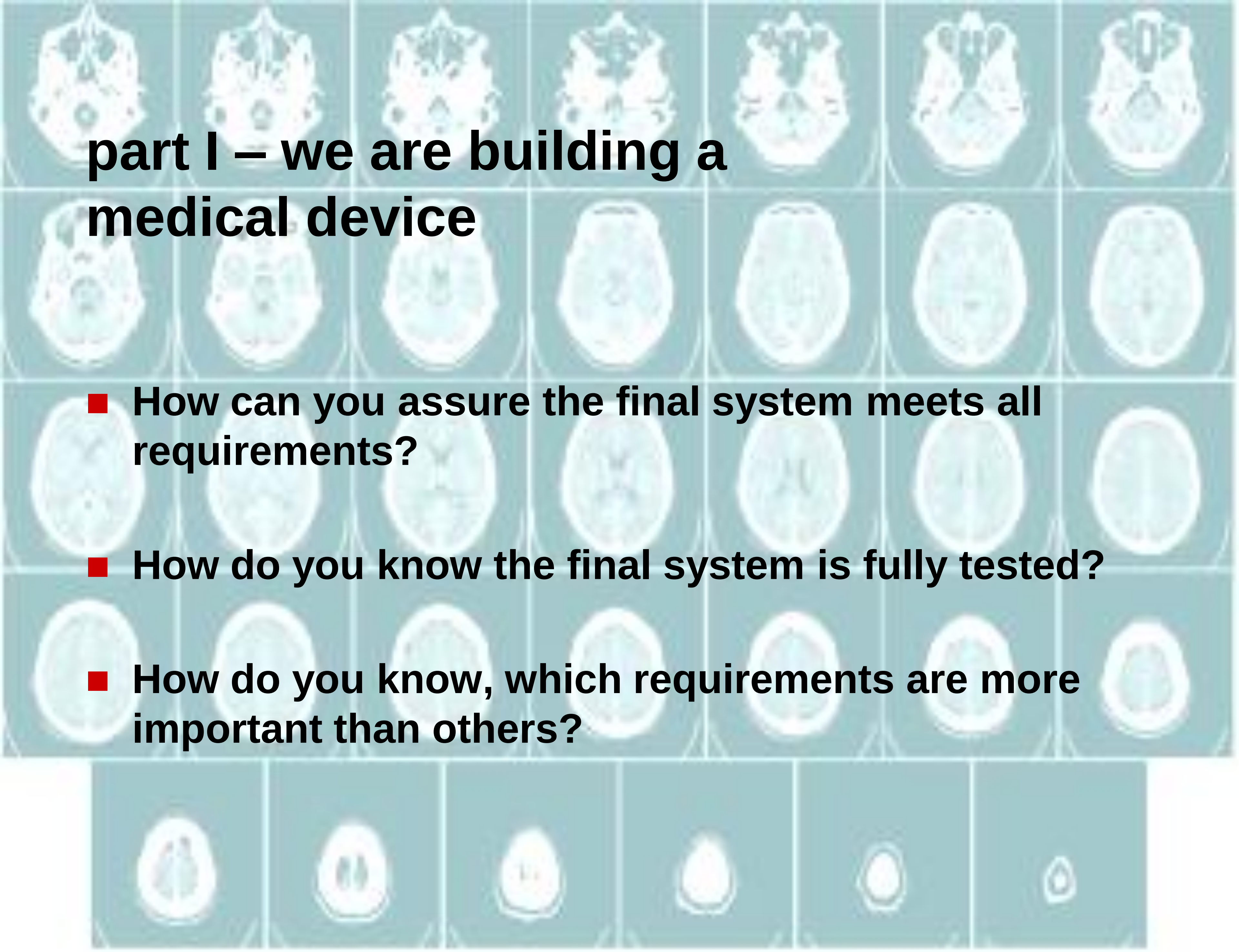
cosylab
CONTROL SYSTEM LABORATORY

Safety demands strict documentation management

(from initial requirements to the final design of the system)

Bojan Zalar (bojan.zalar@cosylab.com)

the best people make cosylab



part I – we are building a medical device

- How can you assure the final system meets all requirements?
- How do you know the final system is fully tested?
- How do you know, which requirements are more important than others?

How to achieve it?

- Requirements must be traceable throughout entire development process
  - all requirements are: agreed, evaluated, and met
    - … therefore we need traceability

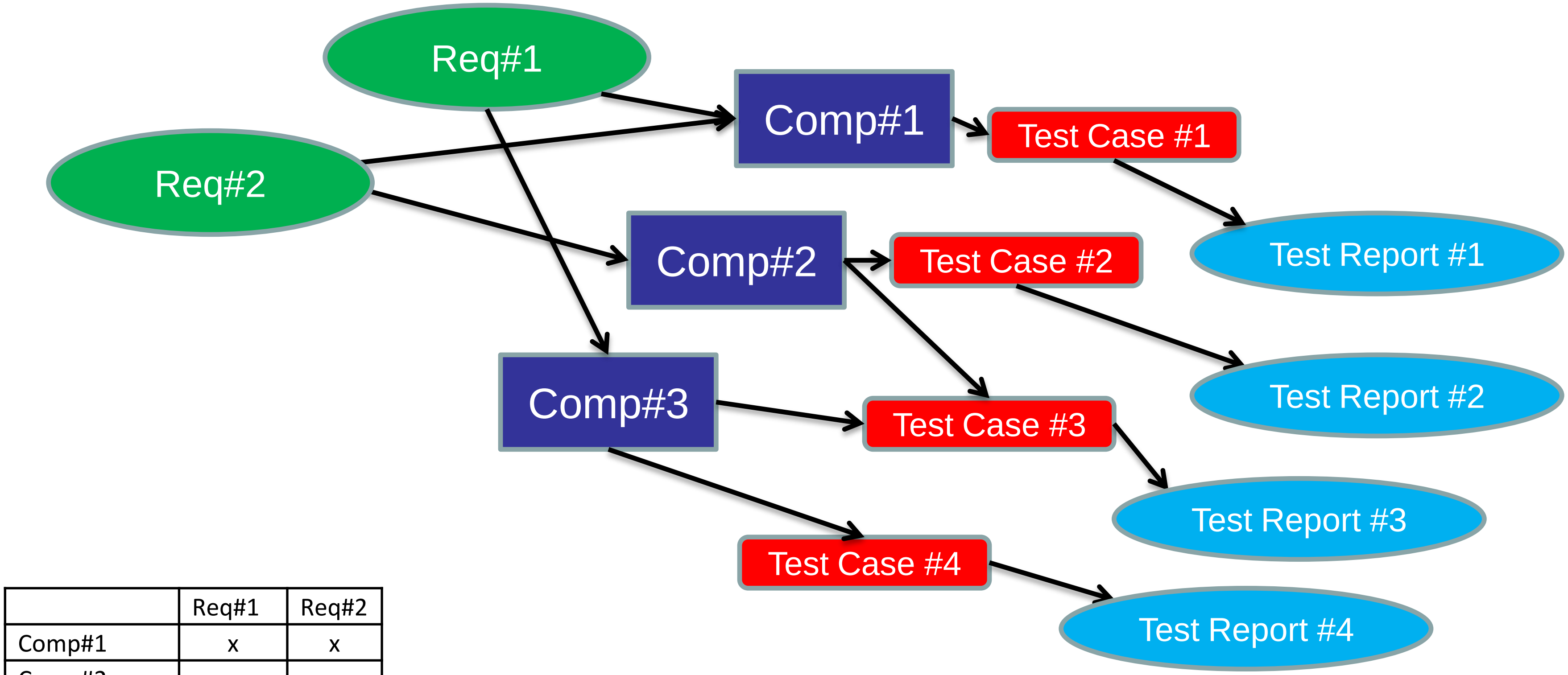
- Risks must be identified and mitigated

- Work-flow environment and tools must support the above

Requirements must be traceable

- All requirements must be met
  - link from initial requirements to final verification
- Every component of the system must be there for a reason
- Proof of traceability:
  - traceability matrix.

All requirements must be met



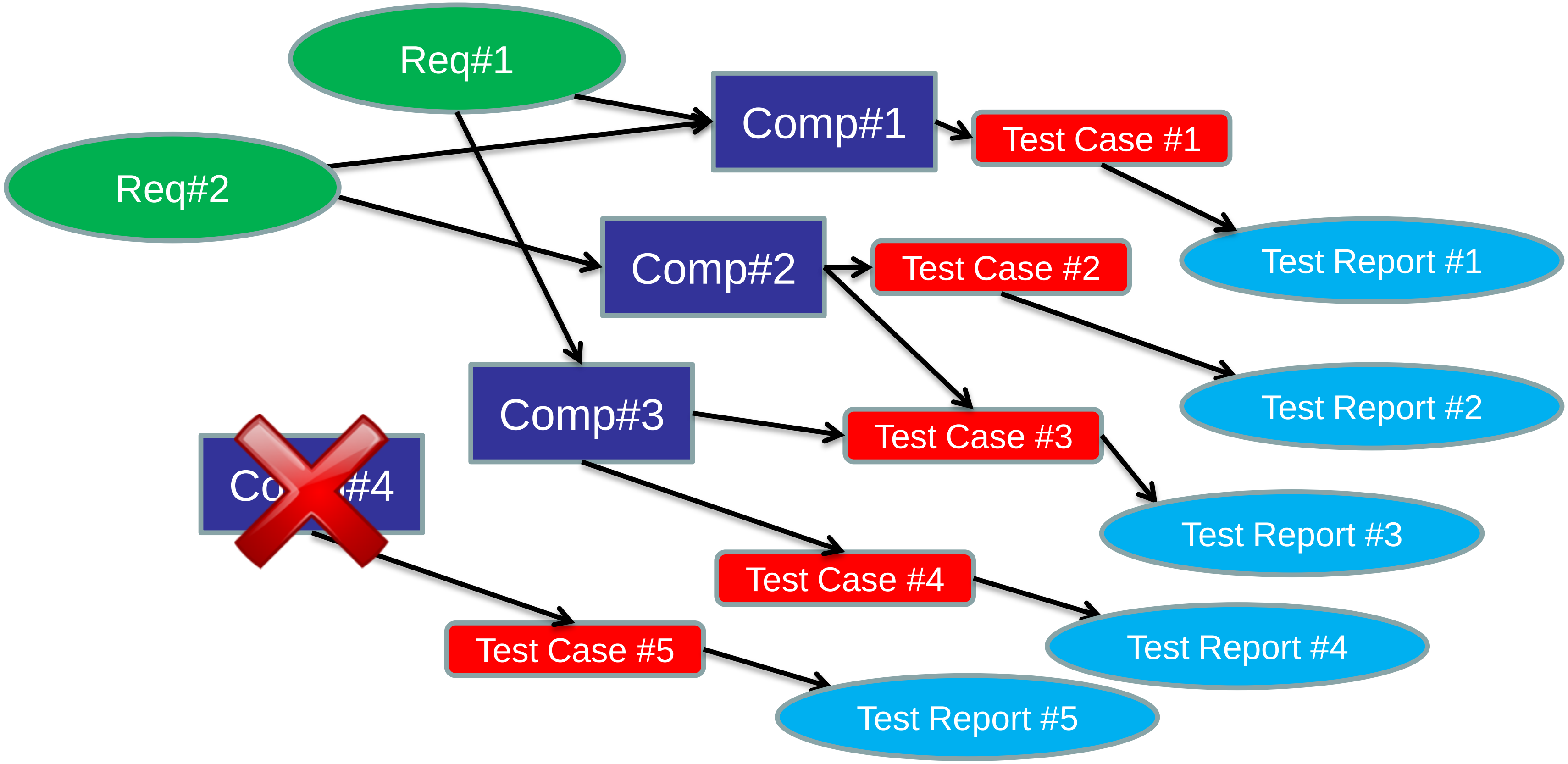
	Req#1	Req#2
Comp#1	x	x
Comp#2		x
Comp#3	x	

	Comp#1	Comp#2	Comp#3
Test Case #1	x		
Test Case #2		x	
Test Case #3		x	x
Test Case #4			x

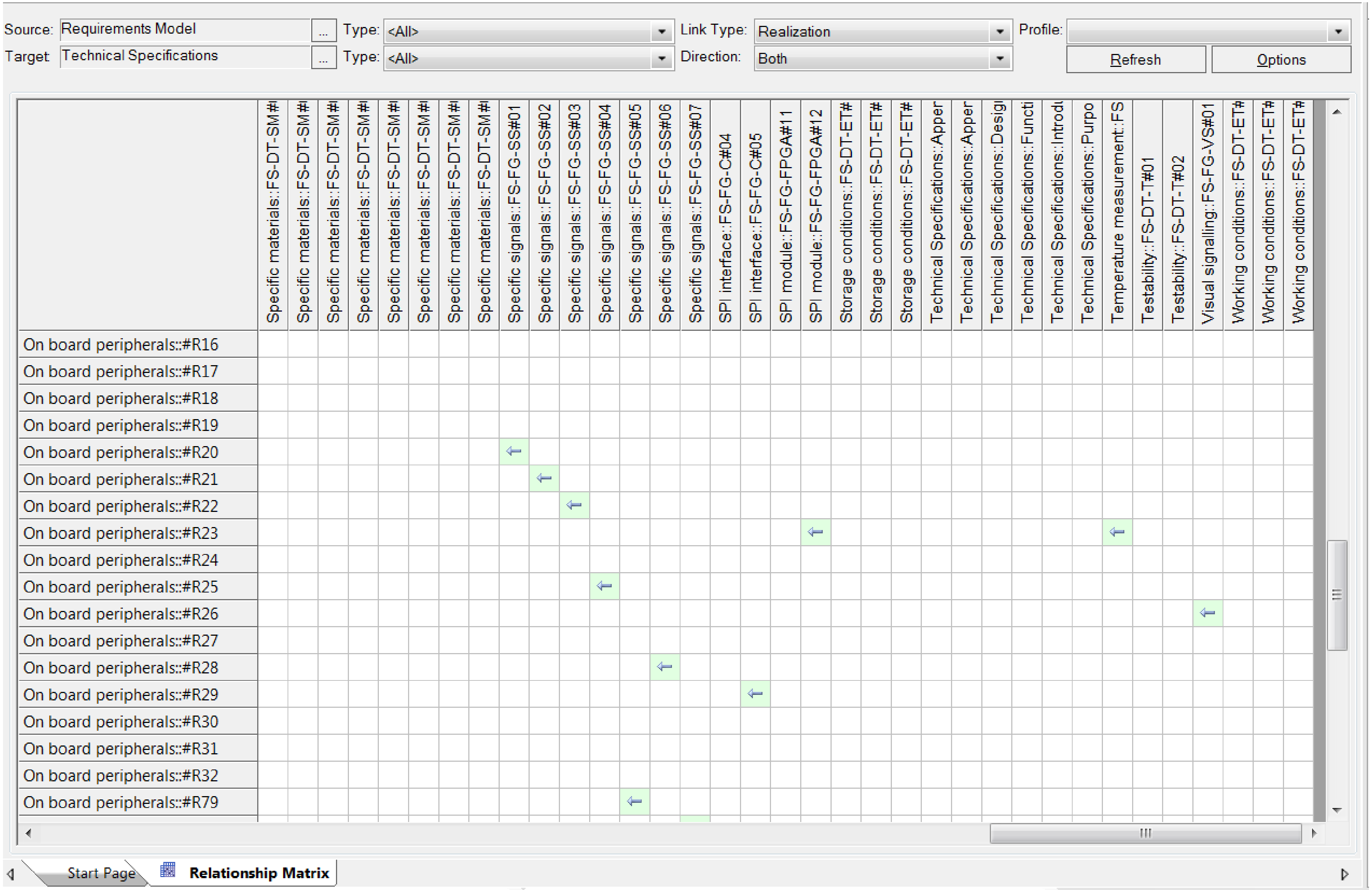
Every component of the system must be there for a reason

- Prevent over-engineering
- Reduce maintenance and upgrade

	Req#1	Req#2
Comp#1	x	x
Comp#2		x
Comp#3	x	
Comp#4		



Traceability matrix



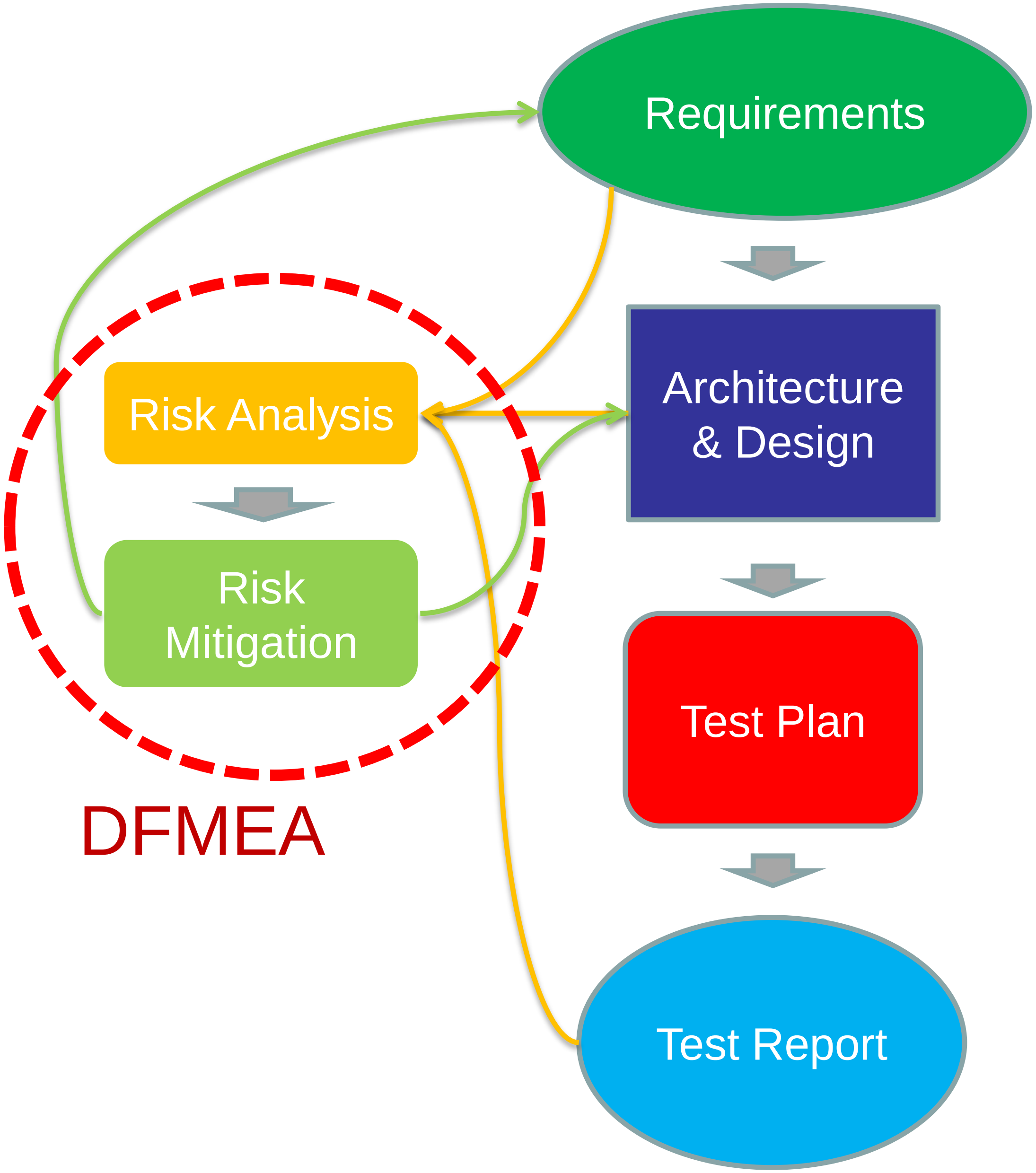
Source: Requirements Model ... Type: <All> Link Type: Realization Profile:

Target: Technical Specifications ... Type: <All> Direction: Both

	Specific materials::FS-DT-SM#	Specific materials::FS-DT-SM#	Specific materials::FS-DT-SM#	Specific materials::FS-DT-SM#	Specific materials::FS-DT-SM#	Specific materials::FS-DT-SM#	Specific materials::FS-DT-SM#	Specific materials::FS-DT-SM#	Specific signals::FS-FG-SS#01	Specific signals::FS-FG-SS#02	Specific signals::FS-FG-SS#03	Specific signals::FS-FG-SS#04	Specific signals::FS-FG-SS#05	Specific signals::FS-FG-SS#06	Specific signals::FS-FG-SS#07	SPI interface::FS-FG-C#04	SPI interface::FS-FG-C#05	SPI module::FS-FG-FPGA#11	SPI module::FS-FG-FPGA#12	Storage conditions::FS-DT-ET#	Storage conditions::FS-DT-ET#	Storage conditions::FS-DT-ET#	Technical Specifications::Apper	Technical Specifications::Apper	Technical Specifications::Desig	Technical Specifications::Functi	Technical Specifications::Introd	Technical Specifications::Purpo	Temperature measurement::FS	Testability::FS-DT-T#01	Testability::FS-DT-T#02	Visual signalling::FS-FG-VS#01	Working conditions::FS-DT-ET#	Working conditions::FS-DT-ET#	Working conditions::FS-DT-ET#
On board peripherals::#R16																																			
On board peripherals::#R17																																			
On board peripherals::#R18																																			
On board peripherals::#R19																																			
On board peripherals::#R20									←																										
On board peripherals::#R21										←																									
On board peripherals::#R22											←																								
On board peripherals::#R23																			←										←						
On board peripherals::#R24																																			
On board peripherals::#R25												←																							
On board peripherals::#R26																																←			
On board peripherals::#R27																																			
On board peripherals::#R28														←																					
On board peripherals::#R29																	←																		
On board peripherals::#R30																																			
On board peripherals::#R31																																			
On board peripherals::#R32																																			
On board peripherals::#R79													←																						

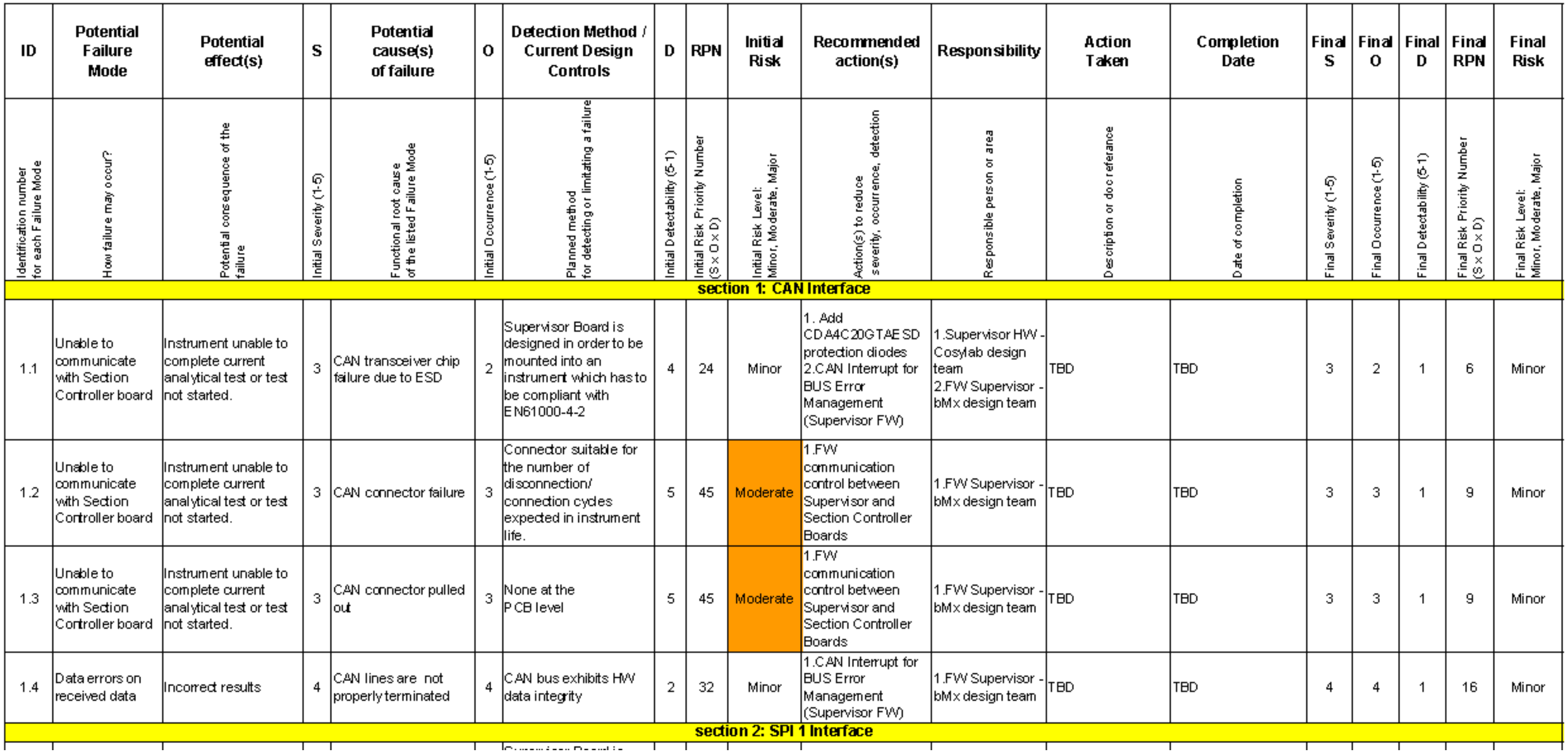
Risks must be identified and mitigated

- Certain device risks can result from faults
- Take appropriate actions to minimize the risks
- Verify that taken actions minimize the risks



DFMEA
Design Failure Mode and Effects Analysis

- Key functions of the design are inspected
- Primary potential failures and causes of each failure are identified
- Actions are taken to reduce final risk



ID	Potential Failure Mode	Potential effect(s)	S	Potential cause(s) of failure	O	Detection Method / Current Design Controls	D	RPN	Initial Risk	Recommended action(s)	Responsibility	Action Taken	Completion Date	Final S	Final O	Final D	Final RPN	Final Risk
Identification number for each Failure Mode	How failure may occur?	Potential consequence of the failure	Initial Severity (1-5)	Functional root cause of the listed Failure Mode	Initial Occurrence (1-5)	Planned method for detecting or limitating a failure	Initial Detectability (5-1)	Initial Risk Priority Number (S × O × D)	Initial Risk Level: Minor, Moderate, Major	Action(s) to reduce severity, occurrence, detection	Responsible person or area	Description or doc referance	Date of completion	Final Severity (1-5)	Final Occurrence (1-5)	Final Detectability (5-1)	Final Risk Priority Number (S × O × D)	Final Risk Level: Minor, Moderate, Major
section 1: CAN Interface																		
1.1	Unable to communicate with Section Controller board	Instrument unable to complete current analytical test or test not started.	3	CAN transceiver chip failure due to ESD	2	Supervisor Board is designed in order to be mounted into an instrument which has to be compliant with EN61000-4-2	4	24	Minor	1. Add CDA4C20GTAESD protection diodes 2.CAN Interrupt for BUS Error Management (Supervisor FW)	1.Supervisor HW - Cosylab design team 2.FW Supervisor - bMx design team	TBD	TBD	3	2	1	6	Minor
1.2	Unable to communicate with Section Controller board	Instrument unable to complete current analytical test or test not started.	3	CAN connector failure	3	Connector suitable for the number of disconnection/ connection cycles expected in instrument life.	5	45	Moderate	1.FW communication control between Supervisor and Section Controller Boards	1.FW Supervisor - bMx design team	TBD	TBD	3	3	1	9	Minor
1.3	Unable to communicate with Section Controller board	Instrument unable to complete current analytical test or test not started.	3	CAN connector pulled out	3	None at the PCB level	5	45	Moderate	1.FW communication control between Supervisor and Section Controller Boards	1.FW Supervisor - bMx design team	TBD	TBD	3	3	1	9	Minor
1.4	Data errors on received data	Incorrect results	4	CAN lines are not properly terminated	4	CAN bus exhibits HW data integrity	2	32	Minor	1.CAN Interrupt for BUS Error Management (Supervisor FW)	1.FW Supervisor - bMx design team	TBD	TBD	4	4	1	16	Minor
section 2: SPI 1 Interface																		

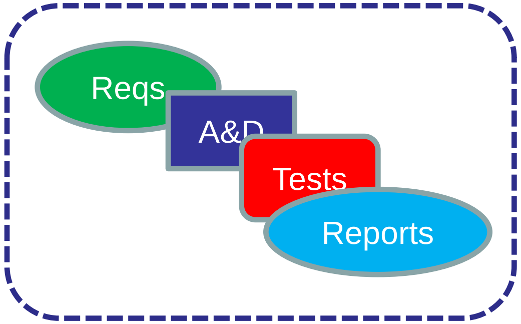
Work-flow environment and tools

- The tool must work well on big projects
- The environment must be set in a way to allow tracking changes and keeping team aligned

The tool must work well on big projects

- MS Word is not enough, we need specialized tools
- Custom made applications are too expensive
- Enterprise Architect can easily handle big projects

Implementing The model in Enterprise Architect



The model

- □ **People**
  - Architects
  - Developers
  - Testers

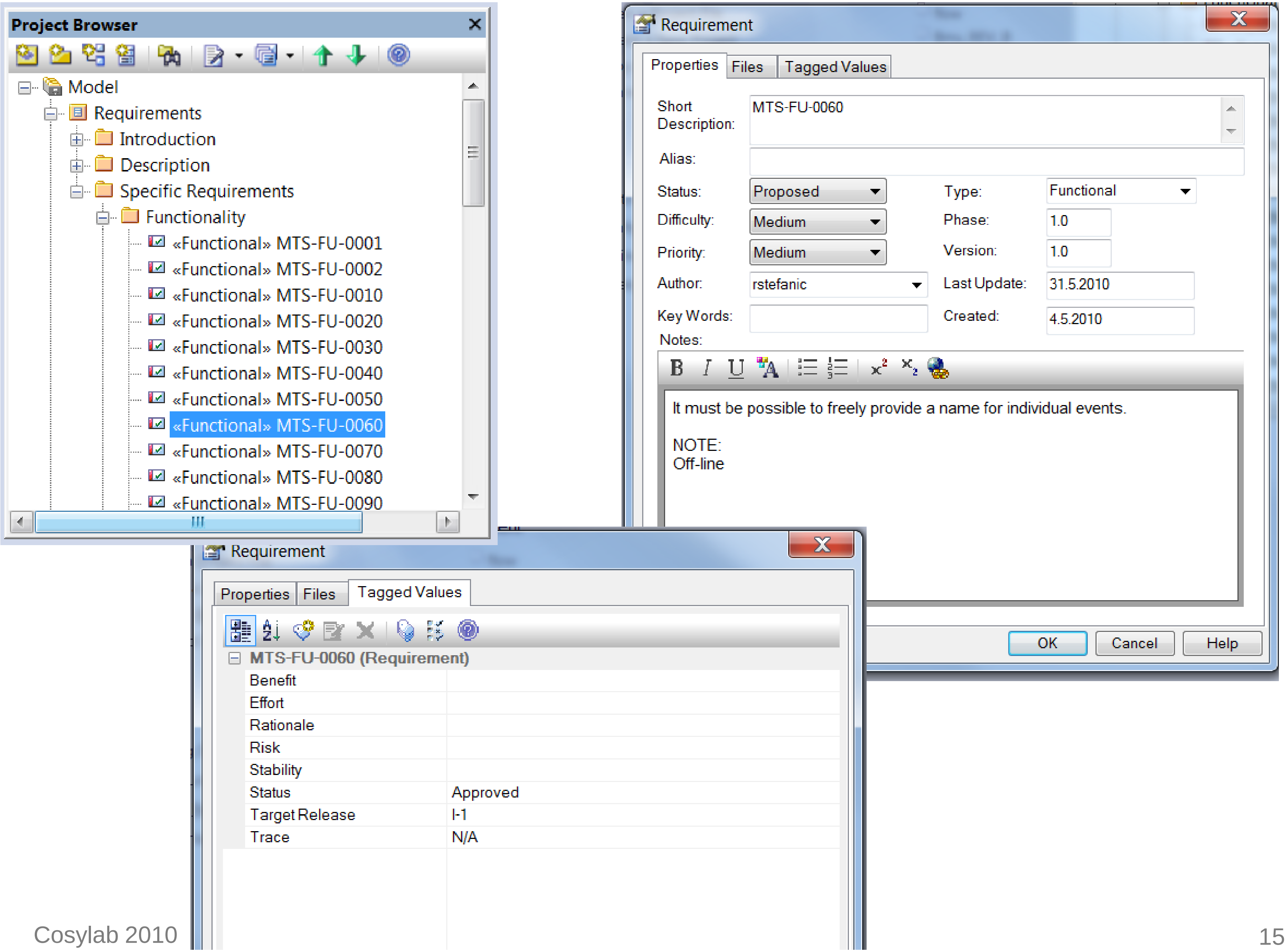
- □ **Documents**
  - Requirements
  - Architecture & Design
  - Test Plan
  - Test Report
  - Traceability Matrix

part II – hands-on in practice

Collect information

- Adding/modifying requirements
  - Attributes, Figures
- Linking requirements to Architecture and Test Cases
  - No requirement is forgotten
  - Each Component is there for a reason

Collect information



Project Browser

- Model
  - Requirements
    - Introduction
    - Description
    - Specific Requirements
      - Functionality
        - «Functional» MTS-FU-0001
        - «Functional» MTS-FU-0002
        - «Functional» MTS-FU-0010
        - «Functional» MTS-FU-0020
        - «Functional» MTS-FU-0030
        - «Functional» MTS-FU-0040
        - «Functional» MTS-FU-0050
        - «Functional» MTS-FU-0060
        - «Functional» MTS-FU-0070
        - «Functional» MTS-FU-0080
        - «Functional» MTS-FU-0090

Requirement

Short Description:	MTS-FU-0060		
Alias:			
Status:	Proposed	Type:	Functional
Difficulty:	Medium	Phase:	1.0
Priority:	Medium	Version:	1.0
Author:	rstefanic	Last Update:	31.5.2010
Key Words:		Created:	4.5.2010

Notes:

It must be possible to freely provide a name for individual events.

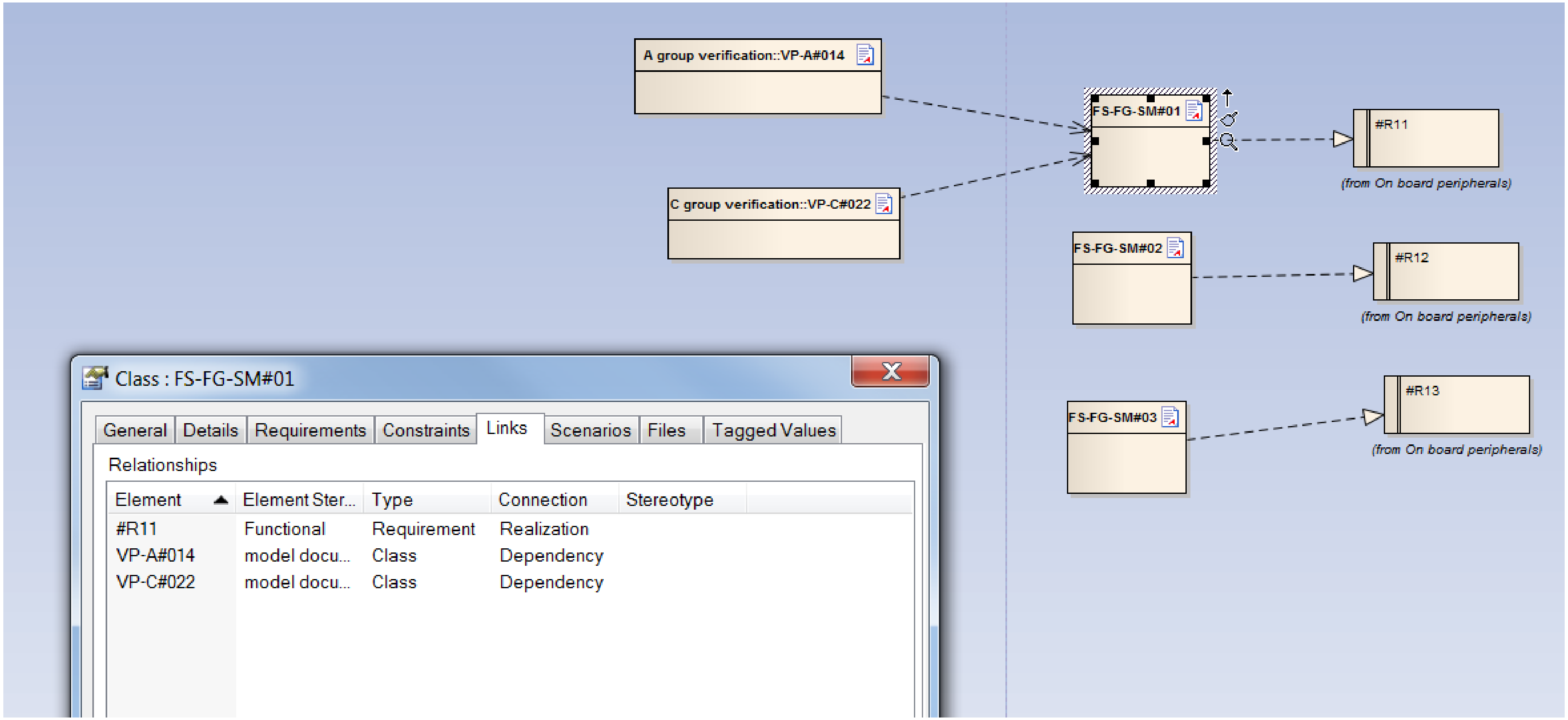
NOTE:
Off-line

Requirement

MTS-FU-0060 (Requirement)

Benefit	
Effort	
Rationale	
Risk	
Stability	
Status	Approved
Target Release	I-1
Trace	N/A

Traceability



Element	Element Ster...	Type	Connection	Stereotype
#R11	Functional	Requirement	Realization	
VP-A#014	model docu...	Class	Dependency	
VP-C#022	model docu...	Class	Dependency	

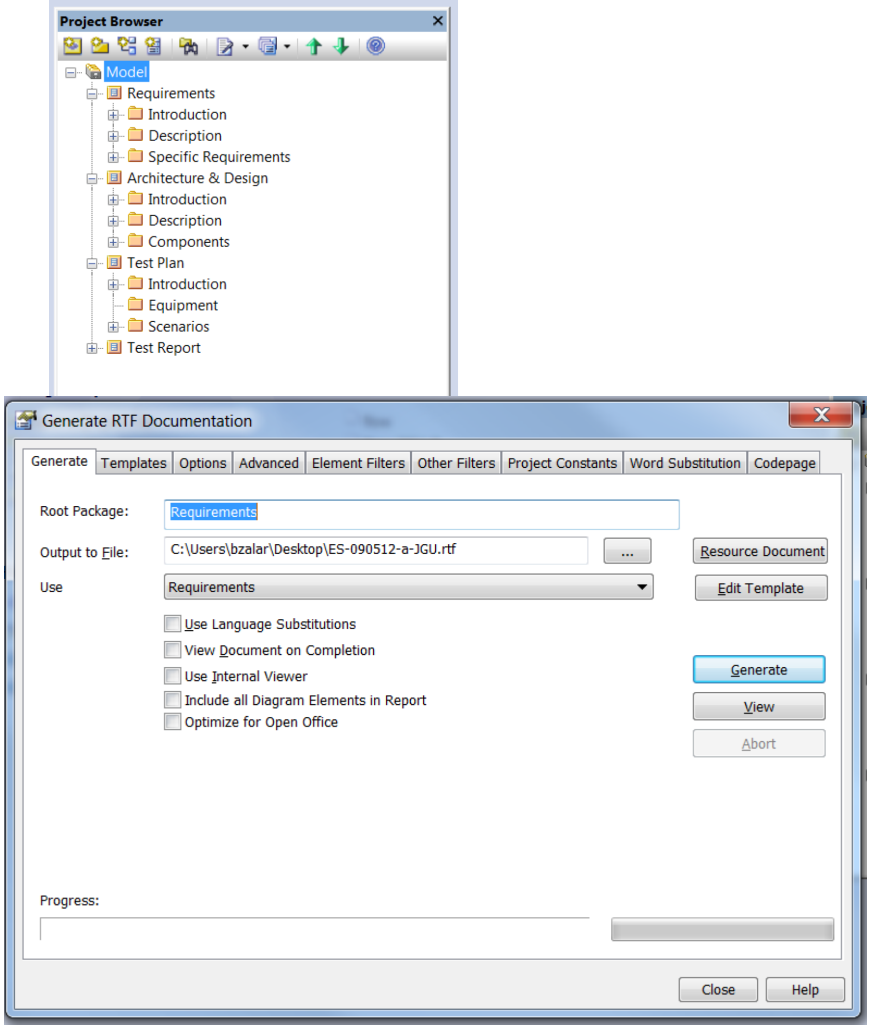
Generate reports covering different perspectives

- Templates are defined according the EBG/MedAustron styles
  - Easy changing, creating new ones

- Generating a MS Word document form the model is simple

- Easily Searching for the specific information in the model
  - Search/Generate for Approval Requirements

Generate reports covering different perspectives



Project Browser

- Model
  - Requirements
    - Introduction
    - Description
    - Specific Requirements
  - Architecture & Design
    - Introduction
    - Description
    - Components
  - Test Plan
    - Introduction
    - Equipment
    - Scenarios
  - Test Report

Generate RTF Documentation

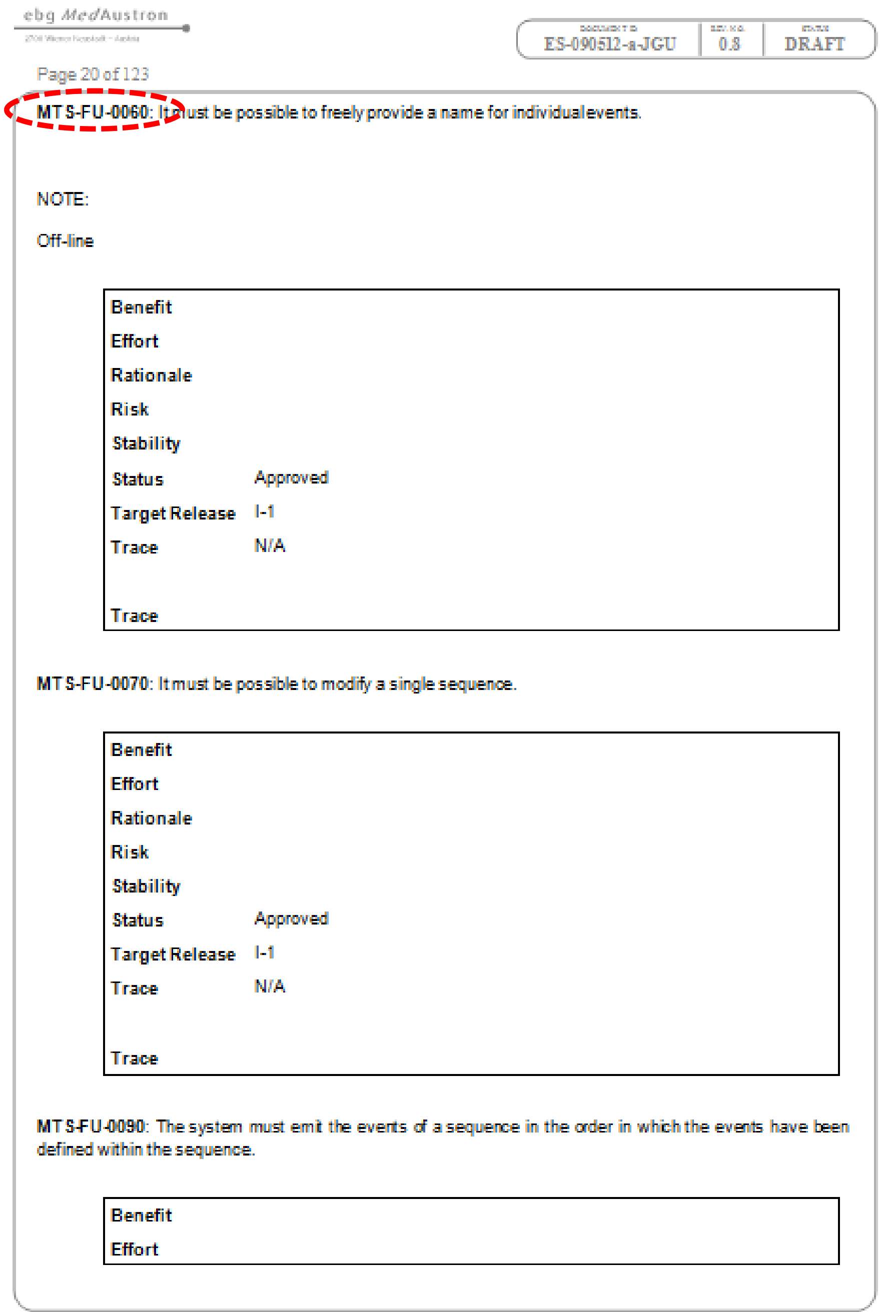
Root Package: Requirements

Output to File: C:\Users\bzalar\Desktop\ES-090512-a-JGU.rtf

Use: Requirements

- □ Use Language Substitutions
- □ View Document on Completion
- □ Use Internal Viewer
- □ Include all Diagram Elements in Report
- □ Optimize for Open Office

...
Resource Document
Edit Template
Generate
View
Abort
Progress:
Close
Help



ebg MedAustron

DOCUMENT ID	REV. NO.	STATUS
ES-090512-a-JGU	0.8	DRAFT

Page 20 of 123

MTS-FU-0060: It must be possible to freely provide a name for individual events.

NOTE:

Off-line

Benefit	
Effort	
Rationale	
Risk	
Stability	
Status	Approved
Target Release	I-1
Trace	N/A
Trace	

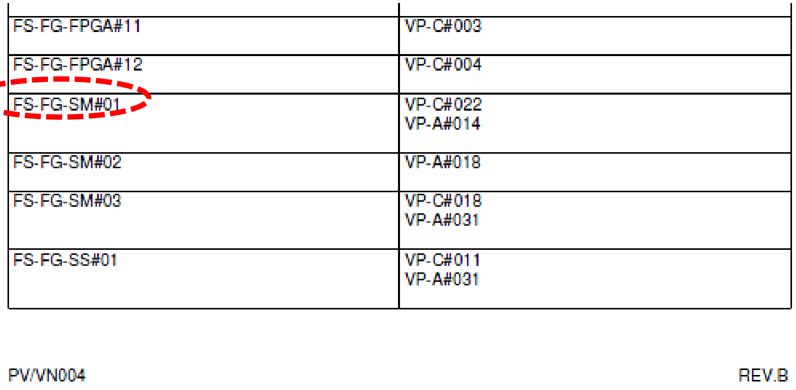
MTS-FU-0070: It must be possible to modify a single sequence.

Benefit	
Effort	
Rationale	
Risk	
Stability	
Status	Approved
Target Release	I-1
Trace	N/A
Trace	

MTS-FU-0090: The system must emit the events of a sequence in the order in which the events have been defined within the sequence.

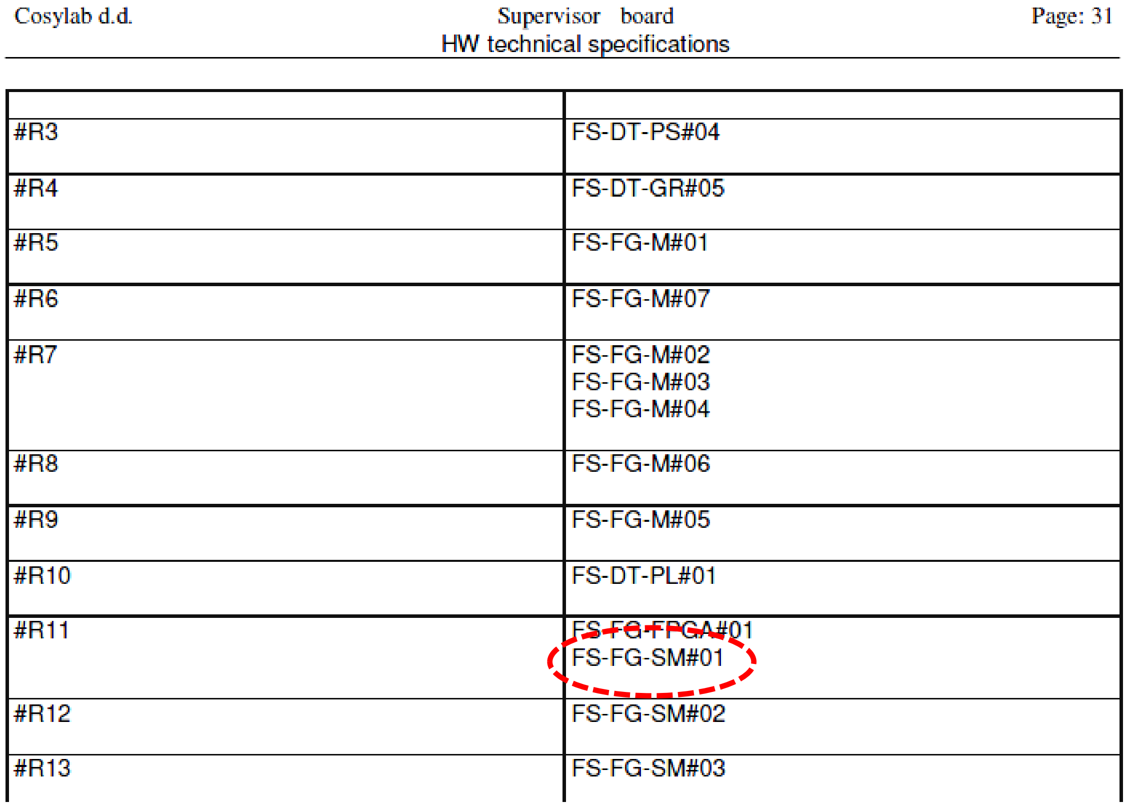
Benefit	
Effort	

Traceability matrix



FS-FG-FPGA#11	VP-C#003
FS-FG-FPGA#12	VP-C#004
FS-FG-SM#01	VP-C#022 VP-A#014
FS-FG-SM#02	VP-A#018
FS-FG-SM#03	VP-C#018 VP-A#031
FS-FG-SS#01	VP-C#011 VP-A#031

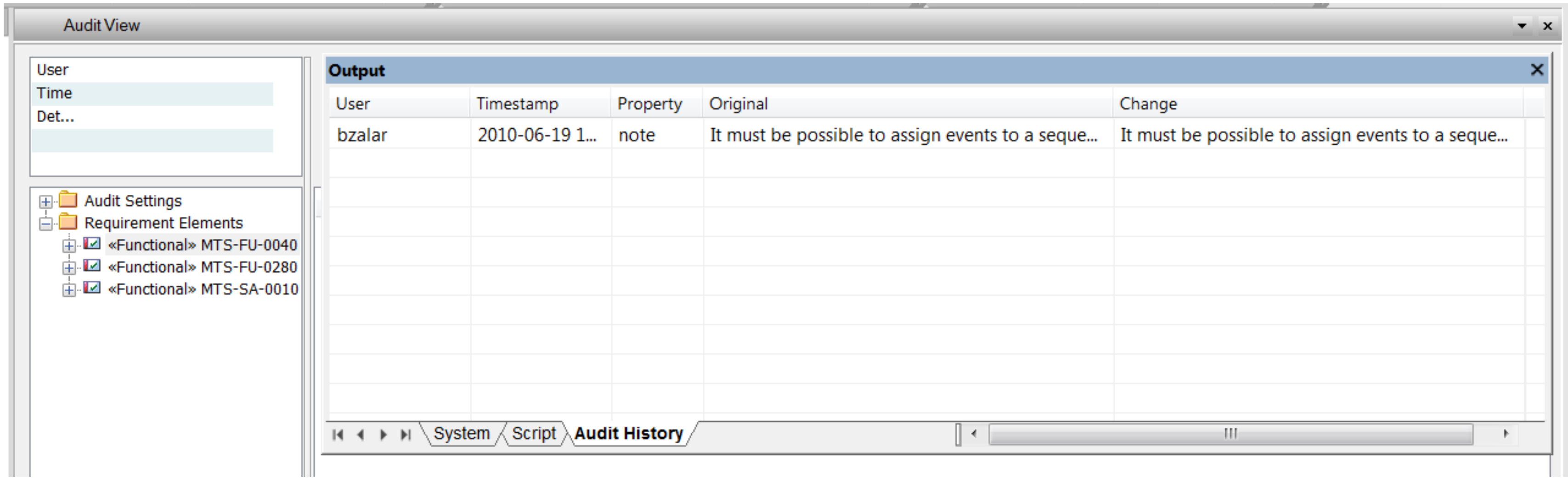
PV/VN004 REV.B



Cosylab d.d. Supervisor board HW technical specifications Page: 31

#R3	FS-DT-PS#04
#R4	FS-DT-GR#05
#R5	FS-FG-M#01
#R6	FS-FG-M#07
#R7	FS-FG-M#02 FS-FG-M#03 FS-FG-M#04
#R8	FS-FG-M#06
#R9	FS-FG-M#05
#R10	FS-DT-PL#01
#R11	FS-FG-FPGA#01 FS-FG-SM#01
#R12	FS-FG-SM#02
#R13	FS-FG-SM#03

Auditing - track model changes



- Audit Settings
- Requirement Elements
  - «Functional» MTS-FU-0040
  - «Functional» MTS-FU-0280
  - «Functional» MTS-SA-0010

User	Timestamp	Property	Original	Change
bzalar	2010-06-19 1...	note	It must be possible to assign events to a seque...	It must be possible to assign events to a seque...

We are building medical device

- Requirements must be traceable throughout entire development process
- Risks must be identified and mitigated
- Work-flow environment and tools must support the above