

## Lesson learnt from the Isograph Training Course

Winterthur 24<sup>th</sup> to 26<sup>th</sup> of July 2017

Miriam Blumenschein, Saskia Hurst and Estrella Vergara - RAS Working Group Meeting -31<sup>st</sup> of August 2017

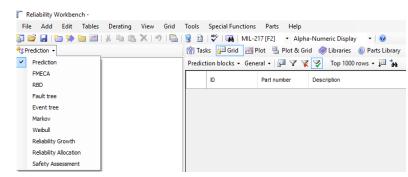


### 1. Isograph for beginners Estrella Vergara



### **Reliability Workbench**

#### Available in CMF Packages: Isograph - RelWorkbench 13.01



#### During installation...

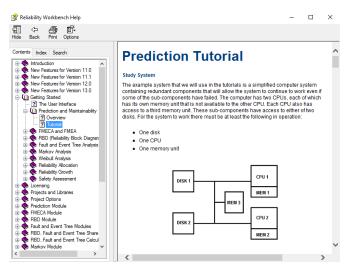
Server		omatic check-ou
ndalone license		
Activate	Status	Repair
Host name or IP address: Port number:	cernvfkn07	

#### Password needed for installation: cernvflxn07

#### **Modules available**

**CERN** licenses

- Prediction Methods
- Failure Mode Effect and Criticality Analysis (FMECA)
- Reliability Block Diagrams (RBD)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Markov Analysis
- Weibull
- Reliability Growth
- Reliability Allocation



Tutorials for each module: Help  $\rightarrow$  Getting Started  $\rightarrow$  Tutorial



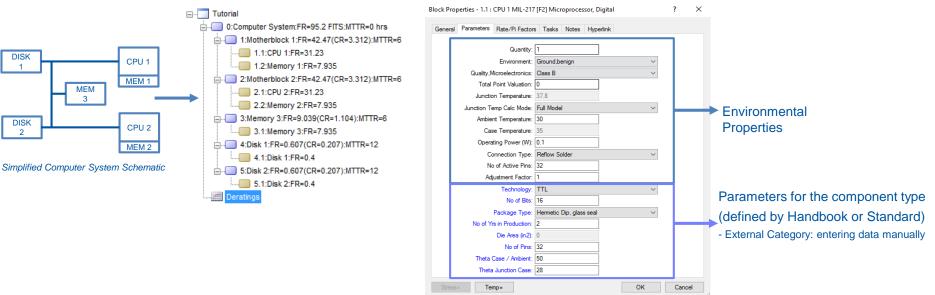
### **Prediction module**

Provide consistent methods of estimating failure rates using Handbooks and standards

Reliability Workbench -			
File     Add     Edit     Tables     Derat       Image: State of the stat	ing View Grid Tools Special Functions Parts Help MIL-217 [F2] Alpha-Numeric Display (%) Tasks Grid Mill Plot & Grid Prediction blocks - General - W V NWC [98] D Part number GiB/; [299B] GiB/; [299C] GiB/; [299C] GiB/; [299C] SN 29500	CERN license: • Telecordia TR/SR • MIL-217 Prediction • NSWC Prediction	<ul><li>Only 1 license:</li><li>217 Plus Prediction</li><li>FIDES Prediction</li></ul>

#### **Project Hierarchy Diagram**

#### **Block Systems and Components Properties**

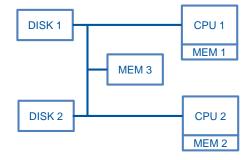


- Entering prediction data manually or using libraries (Project and Library must follow the same Standard or Handbook)
- Possibility to associate maintenance tasks in the prediction hierarchy
- Option to specify the **phases** if the ambient conditions change during the lifetime of the system



### **Prediction module**

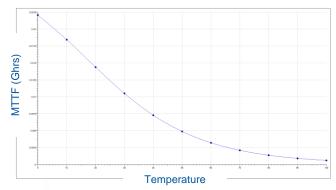
#### Results

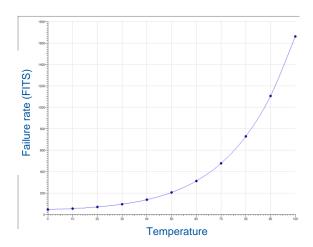


#### Simplified Computer System Schematic

D	Part number	Description	Parent	Category	Sub category	Failure rate	MTTF	MTTR
1	0-1	Motherblock 1		System Block		42.47	0.02354	6
1.1	0-1-1	CPU 1	1	Microprocessor,	TTL	31.23	0.03202	0
1.2	0-1-2	Memory 1	1	Micro, Not EEPROM	ROM	7.935	0.126	0
2	0-2	Motherblock 2		System Block		42.47	0.02354	6
2.1	0-1-1	CPU 2	2	Microprocessor,	TTL	31.23	0.03202	0
2.2	0-1-2	Memory 2	2	Micro, Not EEPROM	ROM	7.935	0.126	0
3	0-3	Memory 3		System Block		9.039	0.1106	6
3.1	0-1-2	Memory 3	3	Micro, Not EEPROM	ROM	7.935	0.126	0
4	0-4	Disk 1		System Block		0.607	1.647	12
4.1	0-4-1	Disk 1	4	External		0.4	2.5	0
5	0-5	Disk 2		System Block		0.607	1.647	12
5.1	0-5-1	Disk 2	5	External		0.4	2.5	0

#### **Plots**







31/08/2017

## Fault Tree Analysis (FTA) · Show interaction to failures Creation of fault trees manually

#### **GATES TYPES**

Symbol	Name	Meaning	Inputs
	OR	TRUE if any input is TRUE	≥2
	AND	TRUE if all inputs are TRUE	≥2
m	VOTE	TRUE if <i>m</i> inputs are TRUE	≥3
	EXCLUSIVE OR	TRUE if one and only one inputs is TRUE	2
	INHIBIT GATE	TRUE if all inputs are TRUE; one input is conditional	≥2
	PRIORITY AND	TRUE if inputs occur in left to right order	≥2
	NOT	TRUE if inputs is FALSE	1
	Transfer In	Inputs appear elsewhere on same page or on another page	
	Transfer Out	Output appears elsewhere on same page or another page	

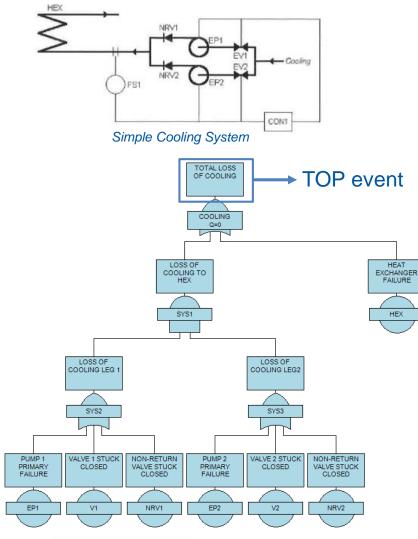
#### **EVENT TYPES**

Symbol	Name	Meaning
	BASIC	Basic event
	UNDEVELOPED	A system event which is yet to be developed
	CONDITIONAL	Conditional event connected to an inhibit gate
	HOUSE	Definitely operating or definitely not operating
	DORMANT	Failure not immediately revealed; latent/ hidden failure



### Fault Tree Analysis (FTA)

- Show interaction to failures
- Creation of fault trees manually thought gates



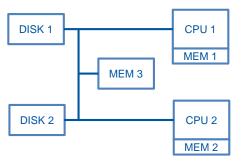
General Appearan	ce Notes Anchored La	abel Hyperlink		
ID	: SYS1			
Description	: LOSS OF COOLING TO	HEX		
Description	LOSS OF COOLING TO	- HEX		
Туре		~	Tag: Automatic	`
Vote number	OR AND		Page	
Modularization	VOTE			
Modularization	I NOT XOR			
	INHIBIT			
	PRIORITY			
	NULL	ſ		

- No limit of gates or events ("Page" checkbox)
- Special Function: Multiple Project option:
  - ID must be coherent
  - Connection between gates (no events)
- Minimal Cut Set:
  - Minimum combination of events which cause TOP event
  - First step of Analysis
  - Produced using Boolean algebra

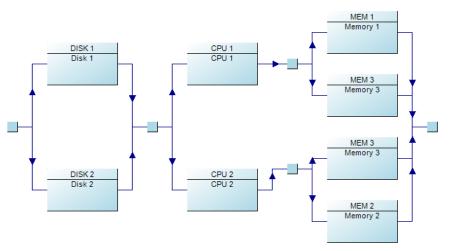


## Reliability Block Diagram (RBD)

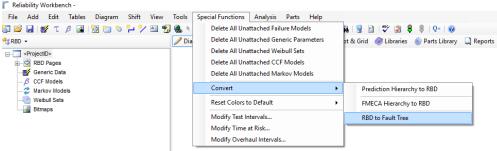
- · Used to predict the reliability of entire systems
- Similar to FTA:
  - RBD → Process (availability) / FTA → Hazards



Simplified Computer System Schematic



- Flow from left to right easy to read
- · Blocks connected in series/ parallel
- Option to Copy-Paste to duplicate a block (e.g. "MEM 3")
- Special functions: RBD to FTA, Prediction to RBD and FMECA to RBD

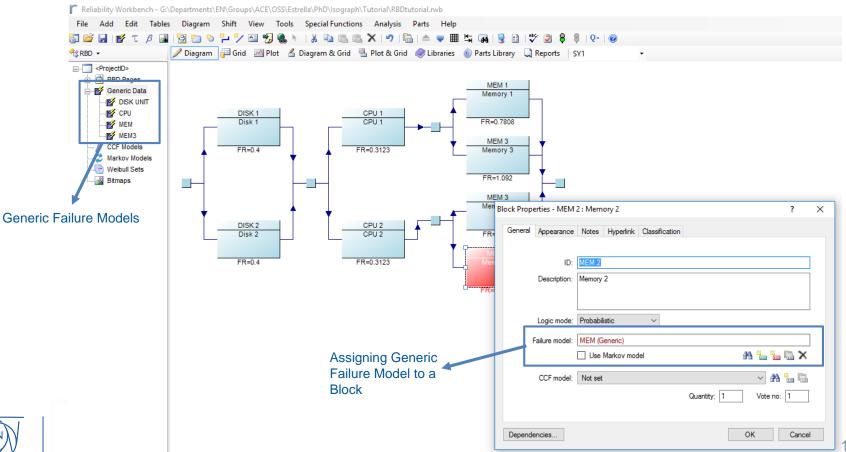




## Reliability Block Diagram (RBD)

#### ASSIGNING FAILURE MODELS TO BLOCKS

- · Failure and repair date is entered in a failure model
  - Local Failure Model: attached to one block only
  - Generic Failure Model: can be attached to multiple blocks
- Applicable for FTA as well



### Reliability Block Diagram (RBD)

#### **PERFORMING AN ANALYSIS - Results**

#### Summary

Results for block SY1		
Summary O Impo	ortance O Cut sets	O Appearance
Parameter	Point Value	
Unavailability	2.861E-12	
Frequency	1.717E-06	
CFI	1.717E-06	
Number expected fail	1.717E-06	
Unreliability	1.717E-06	
MTTF	Not calculated	
MTTR	Not calculated	
Total down time	2.861E-12	
Mean unavailability	2.861E-12	
Risk reduction factor	3.495E+11	
Q/T	2.861E-12	
Used method	Cross product	
Number of compact s	5	

### **Cut Sets:** Combination of component block failures that will cause system failure

🔘 Summa	ary O Importance	Cut sets      Appearance
No.	Q	Minimal cut set
1	1.778E-12	DISK 1.DISK 2
2	1.084E-12	CPU 1.CPU 2
3	9.862E-18	CPU 1.MEM 3.MEM 2
4	2.466E-17	MEM 1.MEM 3.MEM 2
5	9.862E-18	MEM 1.CPU 2.MEM 3

#### Importance: Block's contribution to the unavailability of the system

Event ID	Fussell-Vesely	Bimbaum	Barlow-Proschan	Sequential	Risk Reduction Worth	Risk Achievement .
DISK 2	0.6213	1.333E-06	0.3106	0.3106	2.64	4.66E+05
DISK 1	0.6213	1.333E-06	0.3106	0.3106	2.64	4.66E+05
CPU 1	0.3787	1.041E-06	0.1894	0.1894	1.61	3.638E+05
CPU 2	0.3787	1.041E-06	0.1894	0.1894	1.61	3.638E+05
MEM 3	1.551E-05	1.219E-11	7.755E-06	1.551E-05	1	5.261
MEM 2	1.206E-05	1.326E-11	6.032E-06	1.206E-05	1	5.635
MEM 1	1.206E-05	1.326E-11	6.032E-06	1.206E-05	1	5.635

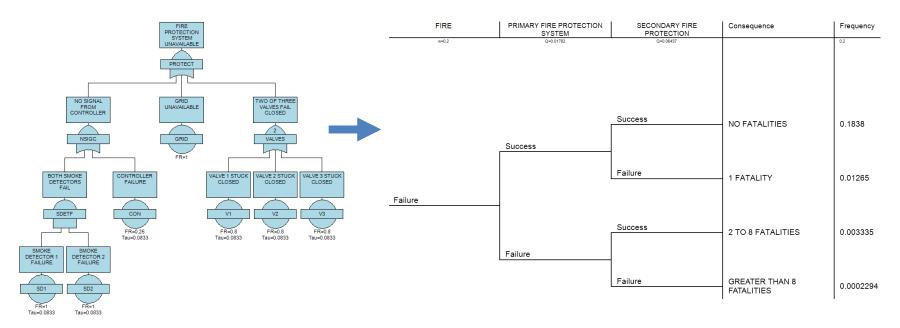


### Event Tree Analysis (ETA)

- · Identifies outcomes of initiating event
- ETA & FTA closely linked:
  - FTA can be used to quantify events in ETA sequence
  - Use cut sets and same quantitative methodology

#### Fault Tree created in FTA module

#### **Event Tree Analysis**





### Failure Mode Effect and Criticality Analysis (FMECA)

#### • Rates failure modes by danger

Dat	e: 05/07/201	17		FMEA CIBDS: Failure chain all levels			
d	Component	Component FM	Effect immidiate	Effects +1	Effects +2	Effects +3	Effects on LBDS
.1.1.	P1	not considered	Not considered				
.1.1.	P2	not considered	Not considered				
.1.1.	IC26	Input open	Incorrect transfer of CIBDS monitoring data from Monitoring_FPGA to MenA20 processor	1.1.3 Incorrect monitoring information	1.16 Incorrect monitoring information	7 Incorrect monitoring information CIBDS	Incorrect monitoring information CIBDS
		Output open	Incorrect transfer of CIBDS monitoring data from Monitoring_FPGA to MenA20 processor	1.1.3 Incorrect monitoring information	1.16 Incorrect monitoring information	7 Incorrect monitoring information CIBDS	Incorrect monitoring information CIBDS
		Supply open	Incorrect transfer of CIBDS monitoring data from Monitoring_FPGA to MenA20 processor	1.1.3 Incorrect monitoring information	1.16 Incorrect monitoring information	7 Incorrect monitoring information CIBDS	Incorrect monitoring information CIBDS
		Output stuck low	Incorrect transfer of CIBDS monitoring data from Monitoring_FPGA to MenA20 processor	1.1.3 Incorrect monitoring information	1.16 Incorrect monitoring information	7 Incorrect monitoring information CIBDS	Incorrect monitoring information CIBDS
		Output stuck high	Incorrect transfer of CIBDS monitoring data from Monitoring_FPGA to MenA20 processor	1.1.3 Incorrect monitoring information	1.16 Incorrect monitoring information	7 Incorrect monitoring information CIBDS	Incorrect monitoring information CIBDS
.1.1. IC22	IC22	Input open	Incorrect transfer of CIBDS monitoring data from Monitoring_FPGA to MenA20 processor + No transfer of CIBDS rearm controlling data from MenA20 processor to Monitoring_FPGA	1.1.3 Incorrect monitoring information 1.1.11 Remote + BIS freq: no effect 1.1.21 Remote + no Bis freq: no effect 1.1.42 Remote + Transition to BIS freq: arming is blocked 1.1.51 Local + no BIS freq: no effect 1.1.31 Remote + Transition to no BIS freq: no effect	1.16 Incorrect monitoring information 1.17 No effect 1.13 Arming procedure blocked	7 Incorrect monitoring information CIBDS 8 No effect 10 Arming procedure blocked	Incorrect monitoring information CIBDS No effect Arming procedure blocked
		Output open	Incorrect transfer of CIBDS monitoring_FPGA to MenA20 processor + No transfer of CIBDS rearm controlling data from MenA20 processor to Monitoring_FPGA	1.1.3 Incorrect monitoring information 1.1.11 Remote + BIS freq: no effect 1.1.21 Remote + no Bis freq: no effect 1.1.42 Remote + Transition to BIS freq: arming is blocked 1.1.51 Local + no BIS freq: no effect 1.1.31 Remote + Transition to no BIS freq: no effect	1.16 Incorrect monitoring information 1.17 No effect 1.13 Arming procedure blocked	7 Incorrect monitoring information CIBDS 8 No effect 10 Arming procedure blocked	Incorrect monitoring information CIBDS No effect Arming procedure blocked



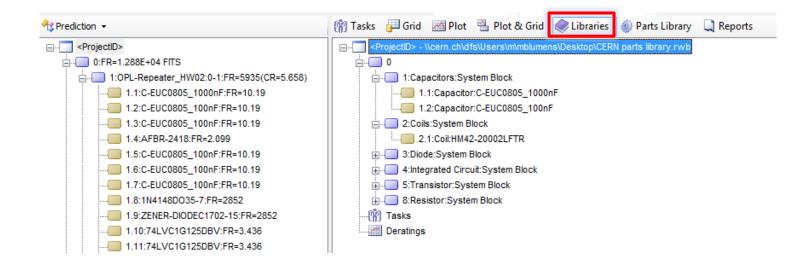
### 2. Compendium of useful features Miriam Blumenschein

Prediction – FMECA – Fault Tree



#### 1. Component library

- Construct a project from a library:
  - File ► Attach Library
  - Drag and drop parts or structures to system structure
  - No automatic update if library is modified
- Build a library: create components in prediction (blue fields)
- Common CERN library?

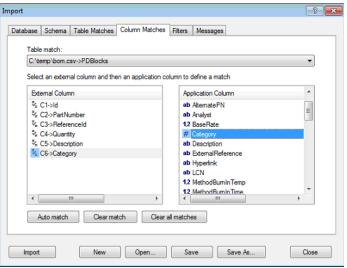




#### 2. Import of bill of material:

- Easy to import: blue fields (component properties) part number, ID, quantity, description and category
- Manual chapter "Importing a Bill of Materials"
- Not (yet) easy to import: black fields (operating environment), filled in manually
- Common Excel format of BOM ?

Id	PartNumber	Quantity	Description	Category
1	0-1	1	OPL-Repeater_HW02	MIL-BK
2	0-2	1	OPL-Trans_1414_HW02	MIL-BK
3	0-3	1	OPL-REC-2418_HW02	MIL-BK
1.1	C-EUC0805_1000nF	1		MIL-CR
1.2	C-EUC0805_100nF	1		MIL-CR
1.3	C-EUC0805_100nF	1		MIL-CR
1.4	AFBR-2418	1		MIL-LB
1.5	C-EUC0805_100nF	1		MIL-CR





#### 3. Rename option

- Objects under the current tree control selection will be renamed based on the name of their parent
- Select parent block ► Tools ► Rename ► Blocks under selection



#### 4. View option:

- Determination of the data which is displayed in the project tree control
- Project Options ► View ► check "Show category"; "Show component part; ... number"

Project Options	8
Project General Phases View Notes Connections Data Links	s Precision
Show standard	Show failure rate
Show category	Show MTTF
Show system part number	Show MTTR
Show component part number	Show unavailability
Show LCN	Show availability
Show reference ID	Show contribution
Show analyst	Show FYM
Show quantity	Show maintenance tasks



#### 5. Help option in dialog boxes

• "?" on the top right in each dialog opens corresponding chapter of the manual

Block Properties - 1.1 MIL-217 [F2] Capacitor	? ×	Reliability Workbench Help	
General Parameters Rate/Pi Factors Tasks Notes Hyperlink ID: 1.1 Description:		Hide Back Print Option Contents Index Search Type in the keyword to find:	category if you are familiar with a specific keyword.  Part number A part number number or you may use the 'Part Selection' facility to locate an existing part in the project or library. The 'Part Selection' facility may be accessed by selecting the Part selection button:
Category: Capacitor Keyword: MIL-CR Part number: C-EUC0805_1000nF CAuto search project Auto search library	A	Select Topic to display:	Part selection button When you type in an existing part number (with the Auto Search Project or Auto Search Library options selected), the program will automatically change the category field to display the part category and copy the part parameters over to the
Alternate part no: LCN: Reference ID:			new component or system block.  Auto search project If selected the program will automatically search for matching project parts when the user types in a part number.
Ansket-	Cancel	Display	Auto search library If selected the program will automatically search for matching library parts when the user types in a part number.

#### 6. Part number

Several Functions are linked to the part number

- Blue fields = component properties: same properties for same part number
- Black fields = operating environment: independent of part number
- Part Selection facility, Auto search project, auto search library, Auto Add Apportioned Failure Modes, Linked block, ...



#### 7. Unit of failure rate

• Project Options ► General ► Units

8. Change component parameters	8.	Change	component	parameters
--------------------------------	----	--------	-----------	------------

- Temperature, Environment, ...
- Select section in tree control ► Special Functions ► change temperature/ MIL-217 environment

OR

- Export block properties to Excel (table PDBlocks; columns PartNumber, ParamValuesKey), find and replace properties in Excel, import Excel file
- 9. Project Options, Special Functions and Tools change from one module to the other, always worth having a look at
- 10. Recommendation: Always create system structure in the prediction module, even if no prediction is performed

Project Options		? ×
Project General Phases V	ew Notes Connections Data Links Precision	
System ID:	0	
System description:	LBDS	
System lifetime (hrs):	0 Target failure rate: 0	
	Units Failure rates: Failures per 10**9 hours v MTTRs: Hours v	

Table: PDBlocks			
Application Column		Exported Application Column	
1.2 AdjustFact			
ab AlternatePN	>>>	# Category	
ab Analyst		ab PartNumber	
1.2 Availability		ab ParamValuesKey	
1.2 BaseRate			
TF BelowHSelect			
ab CategoryDescription			
TF Component			
1.2 ConnRate	<		
1.2 Contribution	<u>`</u>		
1.2 Current Stress	<b>T</b>		
< III	• ***	< III	Þ



### From one module to another

#### 1. Data conversion

- prediction hierarchy to FMECA, RBD, fault tree
- FMECA hierarchy to RBD, fault tree
- RBD to fault tree
- Common way: Prediction to FMECA to Fault Tree
- Special Functions > Convert pull-down menu

#### 2. Data links

Needs to be defined before the data conversion!

Project Options	? 💌
Project General Phases View Notes Connections Data Links Precision	
Assign data link when downloading parts  Assign data link on inter-module copy within project  Assign data link when downloading generic failure models  Prediction to FMECA Data Copy  Add new sub-system blocks  Add new sub-system blocks  Add new component blocks	
Delete missing blocks  Prediction to RBD/FT Data Copy and Transfer      Include component blocks      Imansfer MTTR	
FMECA to RBD/FT Data Copy           Include component blocks           Include failure modes           Include rout failure modes	
ОК	Cancel

- Data links will be automatically created between objects when copying between modules
- Customize data conversion: Project options 
   Data links 
   check "Assign data link on inter-module copy within project"
- Prediction to FMECA: Edit > Transfer linked data > run the FMECA simulation
- FMECA to Fault Tree: Run the FMECA simulation Edit ► Transfer linked data ► run the Fault Tree simulation

#### 3. Update of system structure

- Failure modes remain
- Prediction to FMECA: Special Functions ► Convert pull-down menu



### **FMECA-module**

#### 1. Apportionment table

- Lists a component type (defined by the <u>part number</u>) and its failure modes and %
- Apportionment table can be imported from excel
- Add failure modes to existing blocks: Add ► Auto Add Apportioned Failure Modes OR
- Add apportioned block
- Common CERN apportionment table?

File Add Edit Tables View Grid Tools Spe		
🖥 📂 🗶 I 🛅 🔤 🐃 🐂 🍋 🗼 🦲 🖪 🖳 I 🐰		
Apportionment Table	Apportionment Properties - FA1 : C-EUC0805_1000nF 😵 🔀	C-EUC0805_1000nF Ceramic X 📳 🛃
ID filter: Description filter	General Failure Modes General Failure Modes	
Use part numbers	Description	Apportionment %
ID Cescription	ID: FA1 Short circuits	70
FA1         C-EUC0805_1000nF Ceramic X7R/X5R 6.3 General purpose/Non-encapsulated 70 AVX           FA10         R-EU_M0805_270R Metal film 70 Vishay	Function apportionment Open circuits	10
FA11         R-EU_M0805_330R Metal film 70 Vishay           FA12         R-EU_M0805_11K Metal film 70 Vishay           FA13         R-EU_M0805_147 Metal film 70 Vishay           FA14         R-EU_M0805_10K Metal film 70 Vishay           FA15         IRF7413 Microwave - M05/FET small signal Non-drift 50 30 Vishay           FA2         C-EUC0080 100nF Cerramic X7RX/SR 50 General purpose/Non-encapsulated 70 AVX	Description: C-EUC0805_1000nF Ceramic X7R/X5R 6.3 General purpose/Non-encapsulated 70 AVX	20
FA3 Universal Non-drift 70 FA4 ZENER-DIODEC1702-15 Reference Non-drift 70 FA5 74LVC16125 CM0S BLogic Non-drift 70 70	Part No: C-EUC0805_1000nF	•
Add Edit Delete Delete All	OK Cancel	OK Cancel





### **FMECA-module**

- 2. Severity matrix
  - Tabulates the number of failure mode contributors in each severity category for each block in the system
  - Exported as excel file
  - If severity categories are defined as system failure modes: number of root contributors per system failure mode
  - Special Functions ► Export ► Severity Matrix

#### 3. Criticality matrix

- Tabulates the severity category and criticality for each failure mode
- Special Functions ► Export ► Criticality Matrix

Block	Dia de Dia activita a			Component Block	Failure Mode	Severity	O-WW-
Name	Block Description		Mode ID	Description	Description	Category	Criticality
1	POWER SUPPLY	0 0 7 11	1.1.1	CAPACITOR, FIXED CK	Shorted (Electrical)	IV	0.069375
1.1	CAPACITOR, FIXED CK	0 0 1 3	1.1.2	CAPACITOR, FIXED CK	Change of Value	IV	0.0555
1.2	CAPACITOR, FIXED CB	0 0 2 2	1.1.3	CAPACITOR, FIXED CK	Open (Electrical)	III	0.006938
1.3	CAPACITOR, FIXED CK	0 0 2 2	1.1.4	CAPACITOR, FIXED CK	Other	IV	0.006938
1.4	RESISTOR, FIXED RCR	0 0 0 2	1.2.1	CAPACITOR, FIXED CB	Shorted (Electrical)	III	3.40543
1.5	RESISTOR, FIXED RC	0 0 0 2	1.2.2	CAPACITOR, FIXED CB	Open (Electrical)	III	0.729735
			1.2.3	CAPACITOR, FIXED CB	Change of Value	IV	0.48649
1.6	I.C., DIGITAL	0 0 2 0	1.2.4	CAPACITOR, FIXED CB	Other	IV	0.243245
2	CPU BOARD	3038					
2.1	I.C., DIGITAL	0 0 0 1	1.3.1	CAPACITOR, FIXED CK	Shorted (Electrical)	III	0.055985
		0001	1.3.2	CAPACITOR, FIXED CK	Change of Value	IV	0.044788
2.2	CAPACITOR, FIXED CK	2011					



#### 1. System lifetime

- Unit of system lifetime corresponds to unit of failure
- Project Options ► Calculation

#### 2. Failure and repair models

- 17 model types with different failure and repair characteristics
- <u>Rate models:</u> Constant failure and repair rate
  - Input Rate Model: failure rate  $\lambda$  and repair rate  $\mu$ 
    - $\mu$  = 0: non-repairable components
  - Input <u>Rate/MTTR</u>: failure rate λ and MTTR MTTR = 0: failures are immediately repaired
- <u>Dormant failure model: non repairable components between inspections</u>
  - Three methods: mean (default), max (worst case), IEC 61508
- Local failure model (for one event): Primary Event Properties ► Local Failure Model ► Failure Model Properties
- Generic failure model (for any event): Add ► Failure model ► Failure Model Properties



#### 3. Calculation methods:

- Cross Product, Esary-Proschan (Bertsche), Rare, Optimum Upper Bound (default), Lower Bound
- Project Options ► Set Generations ► Custom Options

% Difference									
Event Q	<b>Cross Product</b>	Esary-Proschan	Rare	Lower Bound					
0.5	0%	4.5%	45%	9.1%					
0.1	0%	0.69%	2.5%	0.085%					
0.01	0%	0.0096%	0.029%	0.000098%					

#### 4. Result Summary

- CFI: Conditional Failure Intensity corresponds to  $\lambda$  (t) (Bertsche):
  - probability per unit time that the component or system experiences a failure at time t, (operating, or was repaired to be as good as new, at time zero and operating at time t).
- Unconditional Failure Intensity or Failure Frequency  $\omega(t)$  Frequency:
  - probability per unit time that the component or system experiences a failure at time t, (operating at time zero).
- CFI-λ(t), ω(t) Difference: the CFI has an additional condition that the component or system has survived to time t.



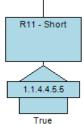
#### 5. Quantity of gates

- Specifying a quantity of *n* is equivalent to including *n* identical gates underneath an gate, with no common cause failures, in the fault tree diagram.
- Quantity values may only be specified for gates that have Modularization set to "Forced on" (default = automatic).

Gate Properties - 1.1.4.22 : ATL - Send "1" instead of PULSE_TO_TDU to LBDS_TDU	Gate Properties - 1.1.4.22 : ATL - Send "1" instead of PULSE_TO_TDU to LBDS_TDU	ATL - Send "1"
General Appearance Notes Anchored Label Hyperlink	General Appearance Notes Anchored Label Hyperlink	instead of PULSE_TO_TDU to LBDS_TDU
ID: 1.1.4.22 Description: ATL - Send "1" instead of PULSE_TO_TDU to LBDS_TDU	ID: 1.1.4.22 Description: ATL - Send "1" instead of PULSE_TO_TDU to LBDS_TDU	1.1.4.22
Type: OR  Tag: Automatic  Vote number: 2 Page	Type: OR  Tag: Automatic  Vote number: 2	R11 - Short IC4 - Output 5 IC13D - Output stuck high stuck high
Modularization: Automatic   Retain results Include in partial analysis	Modularization: Forced on  Retain results Quantity: 2 Include in partial analysis Quantity vote no: 1	1.1.4.4.5.5 1.1.4.4.2.25 1.1.4.4.1.19
Dependencies OK Cancel	Dependencies OK Cancel	FR=0.25312150 FR=0.0188 FR=0.01304 0457594

#### 6. House event

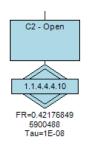
- Used for "what if": switches branches on (Q = 1) and off (Q = 0)
- Primary event properties ► Type ► House; logic mode True or False





#### 7. Event symbols dormant

- Option to visualize the failure model
- Primary event properties ► Type ► Dormant



#### 8. Append facility

- Alternative to library
- Batch append: transfer all the fault tree structures from a group of projects in one go
- Partial append: append parts of a single project by selecting individual gates
- If branches need to be combined in different fault trees and the event ID needs to remain
- Special Functions ► Append

#### 9. MTTF

- By default not calculated
- Calculation requires numerical integration methods to be employed and may be time consuming for large numbers of minimal cut sets
- Project Options ► Calculation ► MTTF/MTBF/MTTR calculations ► Method ► Standard



#### 10. Importance analysis

- Helps determine:
  - Event contribution to TOP event
  - TOP event sensitivity to event changes
  - Weak areas in the system
- 6 different importance measures, most useful (?) Fussell-Vesely Importance (contribution to system Q)

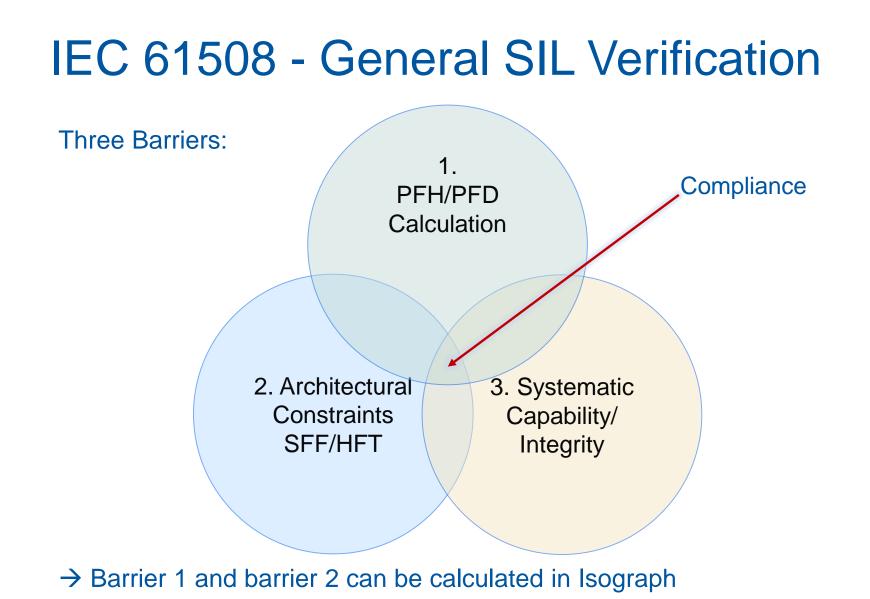
#### 11. Confidence analysis

- Introduces uncertainty in component Q
- Project Options ► Confidence



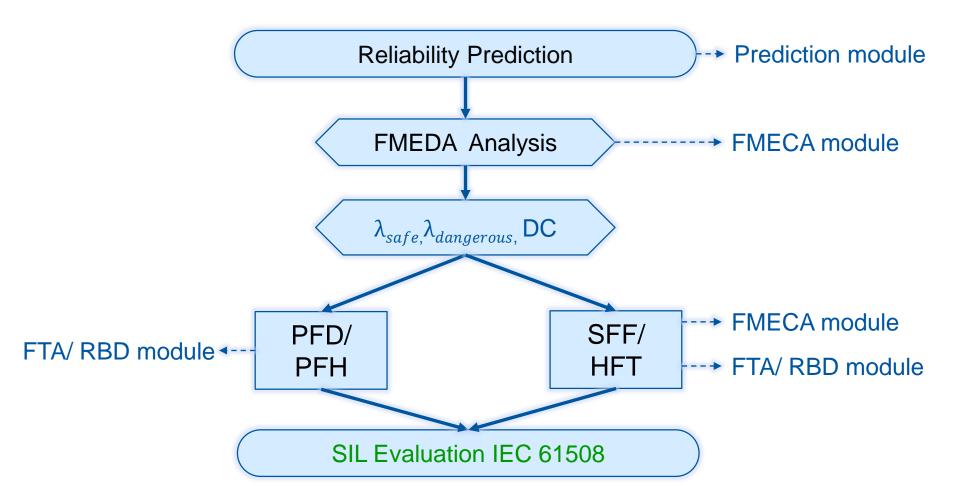
# 3. Isograph and the IEC 61508 Standard Saskia Hurst





CERN

### IEC 61508 - SIL Quantitative Calculation





### FMEDA (Failure Modes, Effects and Detectability Analysis)

- Takes into account:
  - Failure rates of components,
  - Failure mode probabilities,
  - Failure effect of each failure mode,
  - Diagnostic coverage:

 $SC(Safe\ Coverage) = \frac{\lambda_{SD}}{\lambda_{SD} + \lambda_{SU}}; DC\ (Dangerous\ Coverage) = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}},$ 

• Division into safe  $\lambda_S$  and dangerous  $\lambda_D$  and detectable and undetectable failure rates  $(\lambda_{SD}, \lambda_{SU}, \lambda_{DD}, \lambda_{DU})$ 

ID	Description		Contributors defined		Effects (higher level)	Alpha	Beta	Detectable		Dangerous coverage %	Safe coverage %	Detected safe failure rate	Undetected safe failure rate	Detected dangerous failure rate	Undetected dangerous failure rate	Safe failure fraction
2.1.2.7.1	(CC) C80 - short	Yes	N/A	No 24V	1 No alert CROME 2.1 No measurement	49	1	Yes	100	50	0	0	0	0.000949133	0.000949133	0.5
2.1.2.7.2	(CC) C80 - change in value	Yes	N/A		16 No effect CROME 2.16 No effect CMPU	29	1	No	0	0	0	0	0.00112346	0	0	1
2.1.2.7.3	(CC) C80 - open	Yes	N/A		16 No effect CROME 2.16 No effect CMPU	22	1	No	0	0	0	0	0.000852283	0	0	1



### IEC 61508 - SFF Calculation

- Calculation in the FMECA module of Isograph by doing a FMEDA
- SFF is the ratio of safe and dangerous detected failures to the total failure rate
- Safe Failure Fraction (SFF) for a component:

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}}$$

• Safe Failure Fraction (SFF) for a subsystem (safety function):

$$SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD} + \sum \lambda_{DU}}$$



### IEC 61508 - HFT Calculation

• Calculation in the Fault Tree module of Isograph

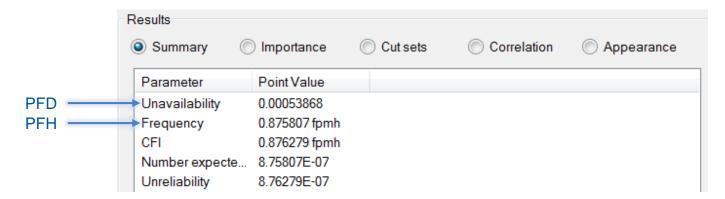
roject Op	tions								9 X
Project	General	Sets Generation	Calculation	Phases	Confidence	Consequences	Event Groups	View	Notes Co · ·
	_								
		Show grid			L L	Show HFT v			
	V 5	Show event failure p	arameters			Show seque	-		
	S	Show event repair p	arameters			Show anchor	red labels		
	<b>S</b>	Show failure model I	Ds			🔲 Disable des	cription reformat	t	
	<b>S</b>	Show CCF model ID	s			Disable des	criptions		
	<b>S</b>	Show CCF paramete	ers			🔲 Use IEC sym	bols		
	V 5	Show CCF tags				📃 Disable pagi	ing		
	V 5	Show ID borders				Disable trans	sfer tags		
	<b>v</b> s	Show repeat bars				_	-		
	Disp	played gate results:				Grid snap:			
	Free	quency		•		Off			•
	Disp	played event results	e.			Pop-up text:			
	Una	vailability and frequ	lency	•		Notset			•
	Ma	aximum tree control	page levels:	6			Line we	eight 1	
							Footer ma	rgin: 2	×
								Ж	Cancel

- Hardware Fault Tolerance (HFT) is the maximum number of faults that can be tolerated before the loss of the safety function
- i.e. HFT = N means that N + 1 faults will cause a loss of the function
- Isograph selects HFT by calculating SFF and cross referencing it against the SIL target for the gate (tables 2 and 3 from IEC 61508-2)



### IEC 61508 - PFH/PFD Calculation

- Calculation in the Fault Tree module or RBD module in Isograph
- Probability of dangerous Failure per Hour PFH (continuous or high demand mode)
  - $\rightarrow$  Frequency  $\omega$  in Isograph
- Probability of dangerous Failure on Demand PFD (low demand mode)
  - $\rightarrow$  Unavailability Q in Isograph





- Set IEC 61508 requirement by either defining
  - Required SIL or
  - Required risk reduction factor

Gate Properties - 0 : CRO	OME	? ×
General Appearance	Notes Anchored Label Hyperlink IEC 61508	
	IEC 61508 SIL requirement Level 2  Required risk reduction factor: 100	
Dependencies	OK	Cancel



• Dormant failure model  $\rightarrow$  IEC 61508

roject Options	2 ×					
Project General Sets Generation Calculation Phases Con	nfidence Consequences Event Groups View Notes Co					
System lifetime System lifetime: 1	Time-dependent analysis					
MTTF/MTBF/MTTR calculations Method: Off	No. of intermediate time points: 20 Importance calculations V Use rare approximation					
CCF analysis ✓ Perform CCF analysis ✓ Adjust independent Q	Dormant failure model Model: EC 61508   Sort cut sets Sort method: No sort Maximum sorted sets: 100000					
Use minimum Q in group <ul> <li>IEC 61508 Failure Models</li> <li>Only model spurious trip failures</li> </ul>						
<ul> <li>Only index spanets up tailets</li> <li>Include DD failures for spurious trip</li> <li>Exclude DD failures in frequency</li> </ul>						
	OK Cancel					

Logic for average: 1. Product of the function (Fault Tree Logic)
 2. Average of the result



• Default setting: calculation of PFD/PFH with dangerous failure rate  $\lambda_{DU}$ 

Project Options	? ×				
Project General Sets Generation Calculation Phases Confi	dence Consequences Event Groups View Notes Co				
System lifetime System lifetime: 8760	Time-dependent analysis On No. of intermediate time points: 20				
MTTF/MTBF/MTTR calculations Method: Off	Importance calculations Use rare approximation Dormant failure model Model: IEC 61508				
CCF analysis ✓ Perform CCF analysis ✓ Adjust independent Q Use minimum Q in group					
IEC 61508 Failure Models  Only model spurious trip failures Include DD failures for spurious trip Exclude DD failures in frequency	Sort method: No sort				
	OK Cancel				

- *"Only model spurious trip failure"*: calculation of PFH/PFD with  $\lambda_S$
- *"Only model spurious trip failure"* and *"Include DD failures for spurious trip"*: calculation of PFH/PFD with  $\lambda_S$  and  $\lambda_{DD}$



• For continuous or high demand functions (PFH): "Exclude DD failures in frequency"

Project Options	? ×				
Project General Sets Generation Calculation Phases Conf	idence Consequences Event Groups View Notes Co				
System lifetime System lifetime: 8760	Time-dependent analysis On No. of intermediate time points: 20 Importance calculations Vuse rare approximation Dormant failure model Model: IEC 61508				
MTTF/MTBF/MTTR calculations Method: Off					
CCF analysis ✓ Perform CCF analysis ✓ Adjust independent Q Use minimum Q in group					
<ul> <li>IEC 61508 Failure Models</li> <li>Only model spurious trip failures</li> <li>Include DD failures for spurious trip</li> <li>✓ Exclude DD failures in frequency</li> </ul>	Sort method: No sort				
	OK Cancel				

→ Calculation of the frequency (PFH) with only dangerous undetectable failures  $\lambda_{DU}$  according to IEC 61508 standard



• Model type: IEC 61508

F	ailure Model Properties - IEC : Cor	nponent 1			? X			
Ш	General Notes Hyperlink							
	ID:	IEC				EC 61508 Parameter Converter	C C C C C C C C C C C C C C C C C C C	X
Ш	Generic data group:	Not set			<b>•</b>			1
Ш	Description:	Component 1				Total failure rate: 1	-06	per hr
H						Dangerous failure %: 50	)	
	Model type:	IEC 61508 -	Туре А		<b>-</b>	Dangerous coverage %: 60		
	Failure rate:		perhr			Safe coverage %: 0		
			perm			Safe failure fraction (%): 80	)	
	Failure rate Std/Erf.			Normal	<b>•</b>	Dangerous detected failure rate: 3E	E-07	per hr
	MTTR:	8	hrs			Dangerous undetected failure rate: 2E	E-07	perhr
	MTTR Std/Erf.	0		Normal	-	Safe detected failure rate: 0		, per hr
	Test interval:	8760	hrs					
	Dangerous failure %:	50				Safe undetected failure rate: 5E	E-07	perhr
	Dangerous coverage %:						Convert	J
							ОК	]
	Safe coverage %:							, ]
	Proof test coverage %:	100					Cancel	J
	Overhaul interval:	10	hrs					
L	Dependencies	Data Link Inactive		ОК	Cancel			



### **Common Cause Failures**

β Factor Model (used in IEC 61508) 

6	CCF Model Properties - CC1	2 ×		IEC	61508=6 CCF Determination - CC1	<u>ନ୍</u> ×	
	General Notes Hyperlink				System & Testing Separation Diversity Complexi	ty Assessment Procedures Competence Environmental ()	
Ш	ID:	CC1	11		Logic subsystem	>= 99%	
H					Sensors or final elements	>= 90%	
Ш	CCF model group:	Not set				>= 60%	
	Description:				Check this box if the equipment under control is put into a safe state before a non-simultaneous common cause failure can effect all the channels. The time taken to assure this safe state should be less than the claimed diagnostic test interval.		
Ш	CCF model type:	Beta   Apply IEC model IEC settings			Logic subsystem test interval	Sensors or final elements test interval	
Ш	Beta	0.05			<ul> <li>Less than 1 minute</li> </ul>	<ul> <li>Less than 2 hours</li> </ul>	
Ш	Dota				Between 1 and 5 minutes	Between 2 hours and 2 days	
Ш					Greater than 5 minutes	Between 2 days and 1 week	
Ш						Greater than 1 week	
l		OK Cancel				OK Cancel	

Calculates the proportion of event failures due to common cause  $Q_1 = (1 - \beta) \cdot Q_T;$  QCCF =  $\beta \cdot Q_T$ 

 $Q_1$ : Q due to independent failure,  $Q_T$ : Total Q,  $Q_{CCF}$ : Q due to common cause failure

β-factor can be determined by "Apply IEC model" with a • questionnaire which is implemented in Isograph



