Institut pour la Maîtrise des Risques
Sûreté de Fonctionnement - Management - Cindyniques

Results of the electrical system dependability benchmark launched by EDF in 2017: demonstration of tools and models

EDF Lab Paris – Saclay

June 14th, 2019

IMdR – 12 avenue Raspail – 94250 GENTILLY
Tél. 01 45 36 42 10 - secretariat@imdr.eu
www.imdr.eu

ABOUT THIS BENCHMARK

In 2017, EDF launched a benchmark designed to compare advanced modeling and calculation tools for the dependability analysis of dynamic systems, that is to say, impossible to represent with static models such as fault trees or Bayesian networks. This benchmark included several use cases, but only two of them were solved with a significant variety of tools. Of these, only one is representative of a real industrial system: the 6.6kV emergency power supply of a nuclear power plant. This example concentrates the great majority of the difficulties that one can encounter in a study of the reliability and availability of a repairable system: reconfigurations with cascades of probabilistic instantaneous transitions, high redundancy level, common cause failures, large differences between the lowest and highest transition rates, multidirectional interactions (due to the propagation of short circuits), looped interactions, existence of deterministic delays due to battery depletion. A precise definition of this test case including reliability data (fake, for confidentiality reasons), as well as a first BDMP modelling are given in an article published at the MARS 2017 workshop (http://mars-workshop.org/mars2017).

Marc.Bouissou@edf.fr

PROGRAM

9h00	***Welcome coffee***
9h30	**Welcome, benchmark history and definition**
10h00	**Solution by KB3-BDMP and Figseq (A*) or YAMS (M*) - *Marc Bouissou (EDF)***
10h45	***Coffee break***
11h15	**Solution 1 by Pycatshoo (M) in textual mode - *Keoni Sanny & Claudia Picoco (Ohio State Univ.), Valentin Rychkov (EDF)***
12h00	**Solution 2 by Pycatshoo (M) with GUI - *Jean-Christophe Houdebine (Aristè)***
12h30	**Partial solution (non repairable version) by STORM (A) - Shahid Khan & Pieter-Joost Katoen (Aachen Univ.)**
13h00	***Lunch***
14h00	**Solution by SimfiaNeo (M) - *Xavier de Bossoreille & Mathilde Machin (APSYS-AIRBUS)***
14h45	**SMT-based safety analysis of redundant power networks (A)" - *Marco Bozzano, Alessandro Cimatti, Mirko Sessa (Fondazione Bruno Kessler), Sergio Mover (Ecole Polytechnique)***
15h30	***Coffee break***
15h45	**Solution by KB3-K6 and Figseq or YAMS - *Anthony Legendre (EDF)***
16h15	**Solution by RiskSpectrum I&AB (A) - *Marc Bouissou (EDF), Pavel Krcal (Lloyd's Register)***

*A : analytical
*M : Monte Carlo simulation

Summary:

**A : analytical*
**M : Monte Carlo simulation*

Solution by KB3-BDMP and Figseq (A) or YAMS (M)

Marc Bouissou (EDF)

General	Possible answers	KB3-BDMP	Figseq	YAMS
Existence of detailed user manual (or on line help)	Y/N	Y	Y	Y
Typical time between releases (in months)	months	12	36	24
Users community (web site, forum, user meetings…)	Y/N	Y	N	N
Open source / Free / Commercial / Private	O/F/C/P	C	P	F
Possibility of collaborative work via network	Y/N	N	N	N
Possibility to import/export data (schematics, tabular data)	Y/N	Y	Y (list of constant parameters)	Y (list of constant parameters)
Openness (capacity to cooperate with external libraries)	Y/N	N	N	N
Portability : Windows/Linux/OSX	W, L, O	W	W	W/L
Modelling				
The model includes: high voltage and low voltage parts/high voltage part only	HV&LV/HV	HV&LV	HV&LV	HV&LV
The model takes repairs into account	Y/N	Y	Y	Y
Model size: reusable part (library…) lines of code (incl. XML lines) OR number of nodes in graphics		1762 lines of Figaro + 1581 lines of XML (GUI definition)	15912 lines of Figaro 0 (automatically generated from the BDMP)	15912 lines of Figaro 0 (automatically generated from the BDMP)
Model size: specific part (system topology…) lines of code (incl. XML lines) OR number of nodes in graphics		163 nodes (gates or basic events)		
Similarity between physical system and model	Y/N	N		
Ability to deal with (instantaneous) loops in flow propagation	Y/N	N	Y	Y
Modeling help: interactive simulator	Y/N	Y	Y	N
Modeling help: property verification	Y/N		Y (reachability)	Y (Probabilistic)
Calculations				
Machine used	Ex: intel Core i5 cpu@2.3Ghz		intel Core i5 cpu@2.3Ghz	intel Core i5 cpu@2.3Ghz
Results include Sequences	#of s., cpu time (s)		14 **most probable** sequences in 9s, 3950 seq in 1800s.	143 sequences **among** the most probable (99 after grouping) in 1050s.
Results include Cutsets	# of c., cpu time (s)		Post processing of sequences. Negligible time	N
Results include importance factors	Y/N		N	N
Performances : simulation of 1,000,000 stories with 10,000h mission time	cpu time on a single cpu (s)		Not applicable	420s
Possibility of using parallel machines	Y/N		In some cases	Y

My own criteria			

Notes:

Solution 1 by Pycatshoo (M) in textual mode

Keoni Sanny & Claudia Picoco (Ohio State Univ.), Valentin Rychkov (EDF)

General	Possible answers	PyCATSHOO
Existence of detailed user manual (or on line help)	Y/N	Y
Typical time between releases (in months)	months	6
Users community (web site, forum, user meetings…)	Y/N	Y
Open source / Free / Commercial / Private	O/F/C/P	F
Possibility of collaborative work via network	Y/N	N
Possibility to import/export data (schematics, tabular data)	Y/N	Y
Openness (capacity to cooperate with external libraries)	Y/N	yes (via Python)
Portability : Windows/Linux/OSX	W, L, O	W/L/O
Modelling		
The model includes: high voltage and low voltage parts/high voltage part only	HV&LV/HV	HV&LV
The model takes repairs into account	Y/N	Y
Model size: reusable part (library…) lines of code (incl. XML lines) OR number of nodes in graphics		3600
Model size: specific part (system topology…) lines of code (incl. XML lines) OR number of nodes in graphics		400
Similarity between physical system and model	Y/N	Y
Ability to deal with (instantaneous) loops in flow propagation	Y/N	Y
Modeling help: interactive simulator	Y/N	N
Modeling help: property verification	Y/N	Y
Calculations		
Machine used	Ex: intel Core i5 cpu@2.3Ghz	intel Core i7
Results include Sequences	#of s., cpu time (s)	424 in 7hours
Results include Cutsets	# of c., cpu time (s)	N
Results include importance factors	Y/N	N
Performances : simulation of 1,000,000 stories with 10,000h mission time	cpu time on a single cpu (s)	2520 s
Possibility to use parallel simulations	Y/N	Y

My own criteria			

Notes:

Solution 2 by Pycatshoo (M) with GUI

Jean-Christophe Houdebine (Aristè)

General	Possible answers	Pycatshoo	PycatshooGUI
Existence of detailed user manual (or on line help)	Y/N	Y	N
Typical time between releases (in months)	months	6	
Users community (web site, forum, user meetings…)	Y/N	Y	N
Open source / Free / Commercial / Private	O/F/C/P	Free	Private
Possibility of collaborative work via network	Y/N	N	N
Possibility to import/export data (schematics, tabular data)	Y/N	N	N
Openness (capacity to cooperate with external libraries)	Y/N	Y	
Portability : Windows/Linux/OSX	W, L, O	W, L, O	W (L, O)
Modelling			
The model includes: high voltage and low voltage parts/high voltage part only	HV&LV/HV	HV&LV	HV&LV
The model takes repairs into account	Y/N	Y	Y
Model size: reusable part (library…) lines of code (incl. XML lines) OR number of nodes in graphics		1600 lines of code	
Model size: specific part (system topology…) lines of code (incl. XML lines) OR number of nodes in graphics		1400 lines of xml	290 nodes in graphics
Similarity between physical system and model	Y/N	Y	
Ability to deal with (instantaneous) loops in flow propagation	Y/N	Y	
Modeling help: interactive simulator	Y/N	Y	Y
Modeling help: property verification	Y/N	N	
Calculations			
Machine used	Ex: intel Core i5 cpu@2.3Ghz	intel Core i5 cpu@3.2Ghz	
Results include Sequences	#of s., cpu time (s)	120 in 4h	
Results include Cutsets	# of c., cpu time (s)	N	
Results include importance factors	Y/N	N	
Performances : simulation of 1,000,000 stories with 10,000h mission time	cpu time on a single cpu (s)	1440s	
Possibility of using parallel machines	Y/N	Y	

My own criteria			

Notes:

Partial solution (non repairable version) by STORM (A)

Shahid Khan, Pieter-Joost Katoen (Aachen Univ.)

General	Possible answers	STORM
Existence of detailed user manual (or on line help)	Y/N	Y
Typical time between releases (in months)	months	6
Users community (web site, forum, user meetings…)	Y/N	N
Open source / Free / Commercial / Private	O/F/C/P	O, F
Possibility of collaborative work via network	Y/N	N
Possibility to import/export data (schematics, tabular data)	Y/N	Y
Openness (capacity to cooperate with external libraries)	Y/N	Y
Portability : Windows/Linux/OSX	W, L, O	L, O
Modelling		
The model includes: high voltage and low voltage parts/high voltage part only	HV&LV/HV	HV&LV
The model takes repairs into account	Y/N	N
Model size: reusable part (library…) lines of code (incl. XML lines) OR number of nodes in graphics		
Model size: specific part (system topology…) lines of code (incl. XML lines) OR number of nodes in graphics		195 Lines of Galileo Code (Manually written using BDMP2DFT translation rules). This corresponds to 200 nodes (basic events, static and dynamic gates) in the GUI
Similarity between physical system and model	Y/N	N
Ability to deal with (instantaneous) loops in flow propagation	Y/N	N
Modeling help: interactive simulator	Y/N	N
Modeling help: property verification	Y/N	Y
Calculations		
Machine used	Ex: intel Core i5 cpu@2.3Ghz	Intel Core i5 cpu@2.6 GHz
Results include Sequences	#of s., cpu time (s)	N
Results include Cutsets	# of c., cpu time (s)	N
Results include importance factors	Y/N	Y (partial)
Performances : simulation of 1,000,000 stories with 10,000h mission time	cpu time on a single cpu (s)	Not applicable
Possibility of using parallel machines	Y/N	N

My own criteria			

Notes:

Solution by SimfiaNeo (M)

Xavier de Bossoreille, Mathilde Machin (APSYS-AIRBUS)

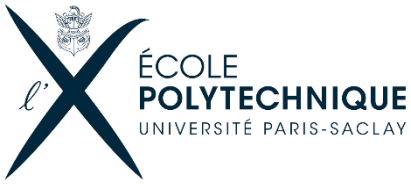
General	Possible answers	SimfiaNeo
Existence of detailed user manual (or on line help)	Y/N	Y
Typical time between releases (in months)	months	6
Users community (web site, forum, user meetings…)	Y/N	Y
Open source / Free / Commercial / Private	O/F/C/P	C
Possibility of collaborative work via network	Y/N	Y
Possibility to import/export data (schematics, tabular data)	Y/N	Y
Openness (capacity to cooperate with external libraries)	Y/N	N
Portability : Windows/Linux/OSX	W, L, O	W/L
Modelling		
The model includes: high voltage and low voltage parts/high voltage part only	HV&LV/HV	HV&LV
The model takes repairs into account	Y/N	Y
Model size: reusable part (library…) lines of code (incl. XML lines) OR number of nodes in graphics		17 classes in library (about 800 lines in AltaRica)
Model size: specific part (system topology…) lines of code (incl. XML lines) OR number of nodes in graphics		92 nodes in graphics: 75 instances of classes + 17 specific components
Similarity between physical system and model	Y/N	Y
Ability to deal with (instantaneous) loops in flow propagation	Y/N	N
Modeling help: interactive simulator	Y/N	Y
Modeling help: property verification	Y/N	N
Calculations		
Machine used	Ex: intel Core i5 cpu@2.3Ghz	intel Core i5 cpu@2.6Ghz
Results include Sequences	#of s., cpu time (s)	Y
Results include Cutsets	# of c., cpu time (s)	N
Results include importance factors	Y/N	N
Performances : simulation of 1,000,000 stories with 10,000h mission time	cpu time on a single cpu (s)	1200s
Possibility of using parallel machines	Y/N	N

My own criteria			

Notes:

SMT-based safety analysis of redundant power networks (A)

Marco Bozzano, Alessandro Cimatti, Mirko Sessa (Fondazione Bruno Kessler), Sergio Mover (Ecole Polytechnique)



General	Possible answers	XSAP, nuXmv, HyCOMP, DIA editor
Existence of detailed user manual (or on line help)	Y/N	Y
Typical time between releases (in months)	months	12
Users community (web site, forum, user meetings…)	Y/N	N
Open source / Free / Commercial / Private	O/F/C/P	C (free for accademic use)
Possibility of collaborative work via network	Y/N	N
Possibility to import/export data (schematics, tabular data)	Y/N	Y
Openness (capacity to cooperate with external libraries)	Y/N	N
Portability : Windows/Linux/OSX	W, L, O	W,L,O
Modelling		
The model includes: high voltage and low voltage parts/high voltage part only	HV&LV/HV	HV
The model takes repairs into account	Y/N	N
Model size: reusable part (library…) lines of code (incl. XML lines) OR number of nodes in graphics		Number of library components: 4 Number of HyDI code lines per components: 10
Model size: specific part (system topology…) lines of code (incl. XML lines) OR number of nodes in graphics		Number of components instantiated in the HV model: 66
Similarity between physical system and model	Y/N	Y
Ability to deal with (instantaneous) loops in flow propagation	Y/N	Y
Modeling help: interactive simulator	Y/N	Y
Modeling help: property verification	Y/N	Y (reachability and temporal properties)
Calculations		
Machine used	Ex: intel Core i5 cpu@2.3Ghz	Intel(R) Xeon(R) CPU E3-1246 v3 @ 3.50GHz
Results include Sequences	#of s., cpu time (s)	Y (it is included in the computation of the Cutsets)
Results include Cutsets	# of c., cpu time (s)	Y, 480 seconds
Results include importance factors	Y/N	N
Performances : simulation of 1,000,000 stories with 10,000h mission time	cpu time on a single cpu (s)	Not applicable
Possibility of using parallel machines	Y/N	N

My own criteria			

Notes:

Solution by KB3-K6 and Figseq or YAMS

Anthony Legendre (EDF)

General	Possible answers	KB3-K6 2.0	Figseq
Existence of detailed user manual (or on line help)	Y/N	Y	Y
Typical time between releases (in months)	months		36
Users community (web site, forum, user meetings…)	Y/N	Y	N
Open source / Free / Commercial / Private	O/F/C/P	P	P
Possibility of collaborative work via network	Y/N	N	N
Possibility to import/export data (schematics, tabular data)	Y/N	Y	Y (list of constant parameters)
Openness (capacity to cooperate with external libraries)	Y/N	N	N
Portability : Windows/Linux/OSX	W, L, O	W	W
Modelling			
The model includes: high voltage and low voltage parts/high voltage part only	HV&LV/HV	HV&LV	HV&LV
The model takes repairs into account	Y/N	Y	Y
Model size: reusable part (library…) lines of code (incl. XML lines) OR number of nodes in graphics		1600 lines of Figaro + 3000 lines of XML (GUI definition)	30900 lines of Figaro 0 (automatically generated from the K6 2.0 KB)
Model size: specific part (system topology…) lines of code (incl. XML lines) OR number of nodes in graphics		97 nodes (electrical component or logical component)	
Similarity between physical system and model	Y/N	Y	
Ability to deal with (instantaneous) loops in flow propagation	Y/N	Y	Y
Modeling help: interactive simulator	Y/N	Y	Y
Modeling help: property verification	Y/N		Y (reachability)
Calculations			
Machine used	Ex: intel Core i5 cpu@2.3Ghz	intel Core i5-7200U cpu@2.5Ghz	intel Core i5 cpu@2.3Ghz
Results include Sequences	#of s., cpu time (s)		Y
Results include Cutsets	# of c., cpu time (s)		Post processing of sequences. Negligible time
Results include importance factors	Y/N		N
Performances : simulation of 1,000,000 stories with 10,000h mission time	cpu time on a single cpu (s)		Not applicable
Possibility of using parallel machines	Y/N		in some cases

My own criteria			

Notes:

Solution by RiskSpectrum I&AB (A)

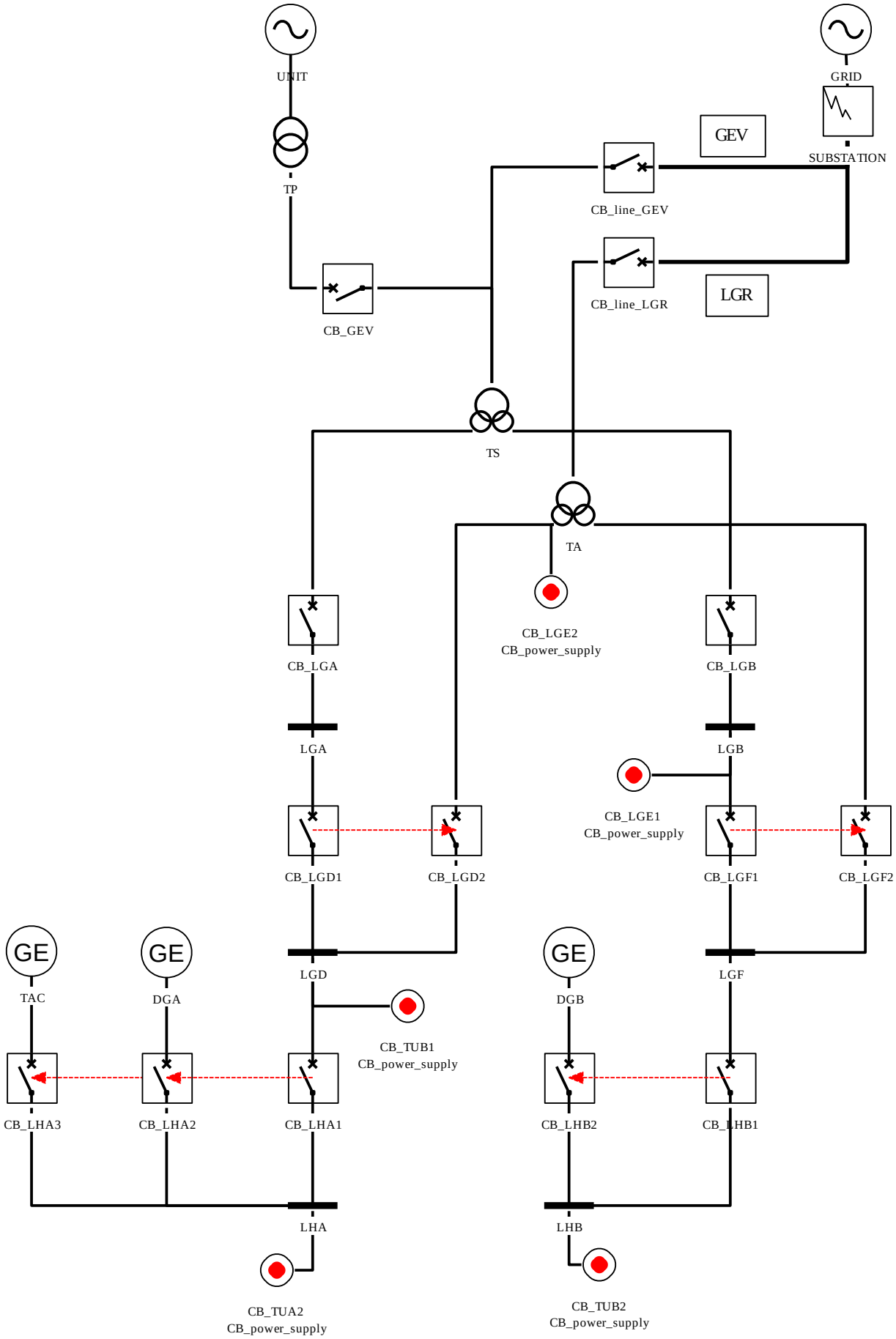
Marc Bouissou (EDF), Pavel Krcal (Lloyd's Register)

General	Possible answers	KB3-BDMP	RS-I&AB (Beta)
Existence of detailed user manual (or on line help)	Y/N	Y	Y
Typical time between releases (in months)	months	12	First release in a near future
Users community (web site, forum, user meetings…)	Y/N	Y	Y
Open source / Free / Commercial / Private	O/F/C/P	C	C
Possibility of collaborative work via network	Y/N	N	N
Possibility to import/export data (schematics, tabular data)	Y/N	Y	Y
Openness (capacity to cooperate with external libraries)	Y/N	N	N
Portability : Windows/Linux/OSX	W, L, O	W	W
Modelling			
The model includes: high voltage and low voltage parts/high voltage part only	HV&LV/HV	HV&LV	HV&LV
The model takes repairs into account	Y/N	Y	Y
Model size: reusable part (library…) lines of code (incl. XML lines) OR number of nodes in graphics		1762 lines of Figaro + 1581 lines of XML (GUI definition)	
Model size: specific part (system topology…) lines of code (incl. XML lines) OR number of nodes in graphics		163 nodes (gates or basic events)	257 nodes (gates or basic events) FT automatically generated from the BDMP
Similarity between physical system and model	Y/N	N	N
Ability to deal with (instantaneous) loops in flow propagation	Y/N	N	N
Modeling help: interactive simulator	Y/N	Y	Y (setting event/gate values)
Modeling help: property verification	Y/N		Y (reachability)
Calculations			
Machine used	Ex: intel Core i5 cpu@2.3Ghz		intel Core i5 cpu@2.3Ghz
Results include Sequences	#of s., cpu time (s)		
Results include Cutsets	# of c., cpu time (s)		467474 cutsets in 8s (exhaustive) 2370 first in 2s
Results include importance factors	Y/N		Y
Performances : simulation of 1,000,000 stories with 10,000h mission time	cpu time on a single cpu (s)		Not applicable
Possibility of using parallel machines	Y/N		N

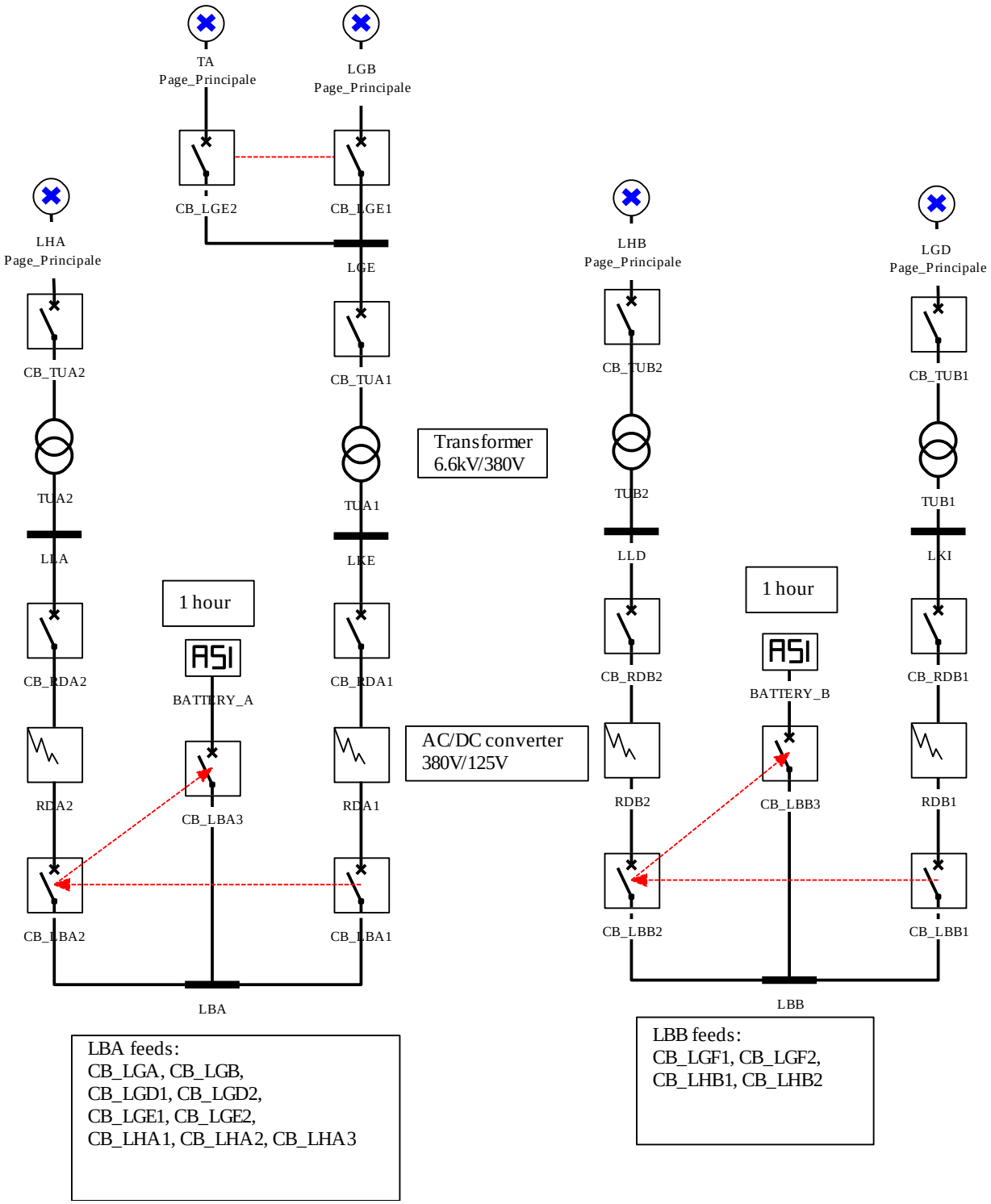
My own criteria			

Notes:

High voltage part



Low voltage part



Reliability data

Component type/failure mode	gamma Probability of failure on demand	lambda/h Failure rate (constant)	mu/h Repair rate (constant)
Circuit breaker/refuse to open (all voltages)	2.00E-04		1/5
Circuit breaker/refuse to close (all voltages)	2.00E-04		1/5
CB_GEV, CB_line_GEV, CB_line_LGR short circuit		1.00E-07	1/5
Circuit breaker/short circuit (all other high voltage circuit breakers)		5.00E-07	1/5
Circuit breaker/short circuit (all low voltage circuit breakers)		1.00E-06	1/5
Bus bar short circuit (high voltage)		2.00E-07	1/50
Bus bar short circuit (low voltage)		5.00E-07	1/50
Transformer short circuit (TP, TS, TA)		5.00E-06	1/200
Transformer short circuit (TUA1, TUA2, TUB1, TUB2)		2.00E-07	1/10
Diesel generators/long failure	2.00E-03	5.00E-04	1/200
Diesel generators/short failure		2.00E-03	1/10
TAC	2.00E-03	1.00E-03	1/200
GRID failure in function		1.00E-05	1/10
UNIT (normal operation) failure in function		1.00E-04	1/10
UNIT (house load operation)	0.2	0.1	1/20 after GRID repair
SUBSTATION		1.00E-06	1/20
Lines GEV, LGR/short circuit		2.00E-05	1/5
AC/DC converter (RDA1, RDA2, RDB1, RDB2)		1.00E-06	1/3
Simultaneous failure of DGA and DGB by CCF	2.00E-04	5.00E-05	1/400
Simultaneous failure of GEV and LGR by CCF due to bad climatic conditions		1.00E-06	1/200

Detailed definition of the benchmark: refer to http://mars-workshop.org/mars2017

Institut pour la Maîtrise des Risques

IMdR

12 avenue Raspail – 94250 GENTILLY

Tél. : 01 45 36 42 10

www.imdr.eu