Reliability measurements, risk and safety assessment

Lorenzo Ciani

Consiglio DINFO – 28 marzo 2018

- 2005 Laurea in Ingegneria Elettronica
- 2006-2008 Dottorato di ricerca in "Ingegneria industriale e dell'affidabilità"
- 2012 TUV – Functional Safety Engineer – Id 5062/12
- 2008-2017 Assegnista di ricerca con continuità
- 1 ottobre 2017 RTD – A SSD ING-INF/07 Misure Elettriche ed Elettroniche

Didattica

- Attività di supporto didattico con seminari, esercitazioni di laboratorio ed assistenza agli esami per i seguenti corsi: Affidabilità e Controllo di Qualità, Diagnostica e Sicurezza dei Sistemi
- AA 2017-18 Diagnostica e Sicurezza dei Sistemi (LM Elettronica, Elettrica ed Automazione, Telecomunicazioni e Biomedica)

- **IEEE Senior Member**

- **TPC**: IEEE I2MTC, IEEE MEMEA, IMEKO World Congress, IMEKO TC10, ESREF, …

- 2015 **IEEE Instrumentation and Measurement Society "Outstanding Young Engineer Award**" - *For his contribution to the advancement of instrumentation and measurement in the field of reliability analysis*

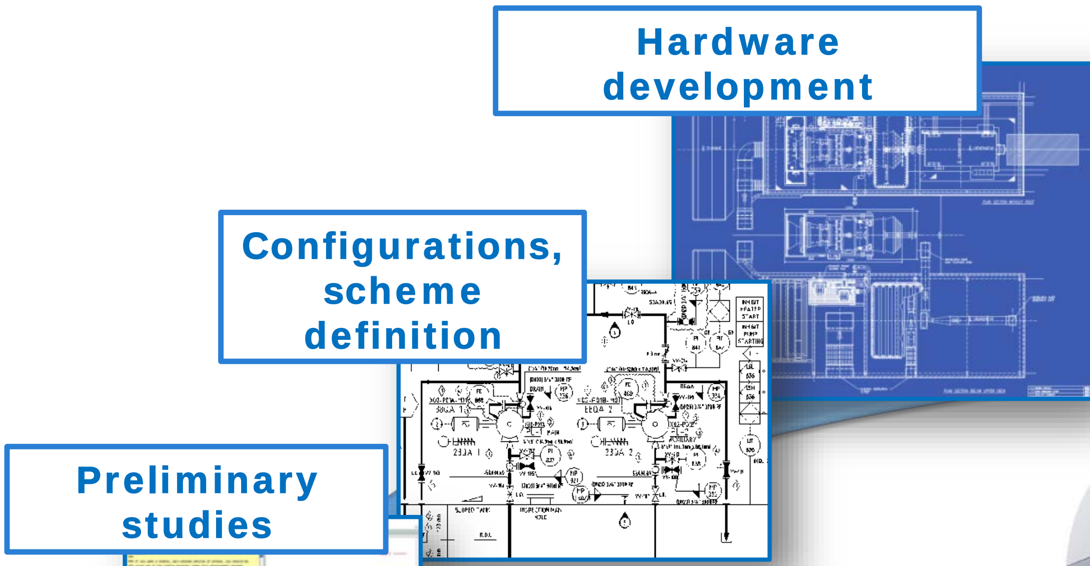
- **Associate Editor** per IEEE Transactions on Instrumentation and Measurement (IEEE TIM) e IEEE Access
  Guest Editor per Measurement - Journal of the International Measurement Confederation (IMEKO)
  Membro dell'**Editorial Board** di ACTA IMEKO

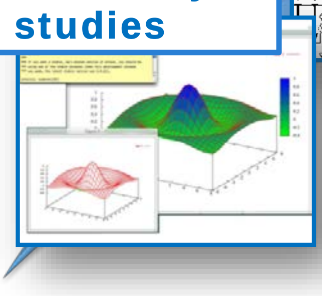
- **CEI IEC TC 56 Dependability**

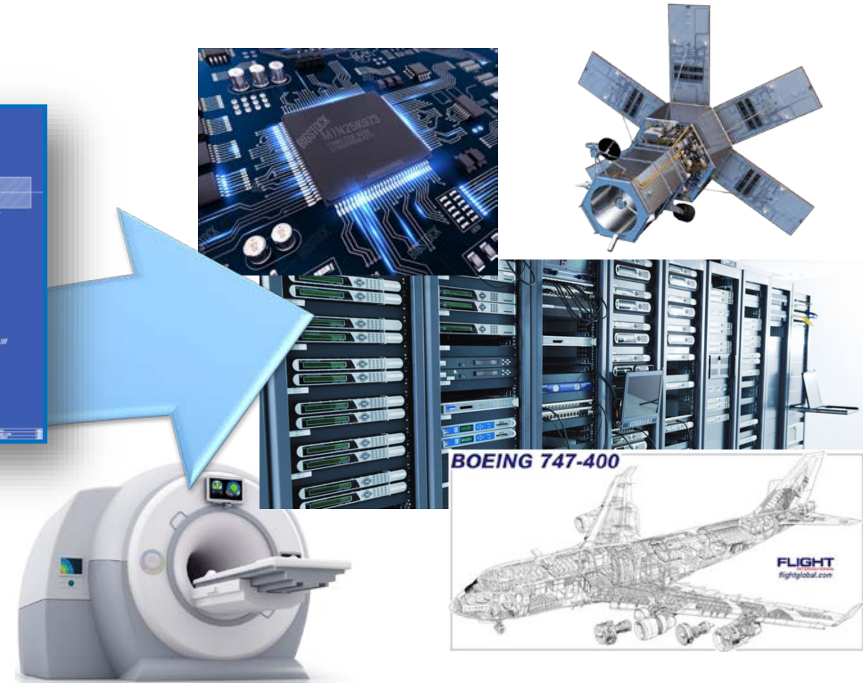
- **PRIN 2006, 2008; Progetto PRSE 2007 – 2010; POR CREO FESR 2007 – 2013**; ...

- **ASN : 28.03.2017 abilitazione II fascia nel settore concorsuale 09/E4**

Reliability, Availability, Maintainability and Safety (RAMS)







Reliability improvement in complex system design stage:

- **Time reduction** for improvement
- **Comparison** of multiple configurations/solutions
- **Validation** of design choices
- Achievement of **reliability target**
- Guarantee **availability and safety** performance

Fields of application:
railway, biomedical, automotive, avionics, energy (PV, Wind), oil&gas, power electronics, automation, ICT

Industry collaborations:
ALSTOM, Autostrade per l'Italia, Biomerieux, Brembo, Borri Industrial Power Solutions, Comesa, Ducati Motor Holding, ECM, ENEL, Esaote, Easytech, GE-Nuovo Pignone, GE Transportation, General Project, Intecs, **Laboratorio CETACE-Analytical***, Leone, Progress Rail SESA, Sirio Panel, TERNA, Trenitalia, VDS srl.

*Laboratorio congiunto

Collaboration with Italian University and Research Centre**:**

- Dipartimento di Ingegneria, Università del **Sannio**
- Dipartimento di Elettronica, Informazione e Bioingegneria, **Politecnico di Milano**
- Dipartimento di Fisica, Università degli Studi di **Milano**
- Dipartimento di Ingegneria dell'Energia, dei Sistemi, del Territorio e delle Costruzioni, Università di **Pisa**
- Dipartimento di Scienze, Università degli Studi **Roma Tre**
- Dipartimento di Ingegneria industriale e dell'informazione e di economia, Università degli Studi dell'**Aquila**
- **IRA-INAF**, Medicina (BO) – Arcetri (FI)

International collaboration with University and Research Centre:

- Division of Operation and Maintenance Engineering - **Luleå University** of Technology, Sweden
- **TECNALIA Corporation**, La Almunia de Doña Godina, Zaragoza (Zaragoza), Spain
- MTA SZTAKI - **Hungarian Academy Of Sciences**, Institute For Computer Science And Control, Budapest, Hungary
- The Institute of Radioelectronics and Multimedia Technology, **Warsaw University of Technology**, Warsaw, Poland

Research activity

MODELS

Failure rate and repair evaluation

Failure rate prediction, MTTF (Mean Time Between Failure), MTTR (Mean Time to Restore), etc.

Reliability analytical models

Dynamic and static models (Reliability allocation, Rel. Importance, RBD, Fault tolerance)

ASSESSMENT

Failure analysis and risk assessment

Failure Mode Effect and Criticality analysis (FMECA), Fault Tree Analysis (FTA), etc.

Functional safety assessment

SIL evaluation, IEC 61508

MEAS &TESTING

Measurements

Device and components characterization, Automatic Measurement System

Reliability test & lab experiments

Thermal and mechanical stress (i.e. accelerated testing, aging test)

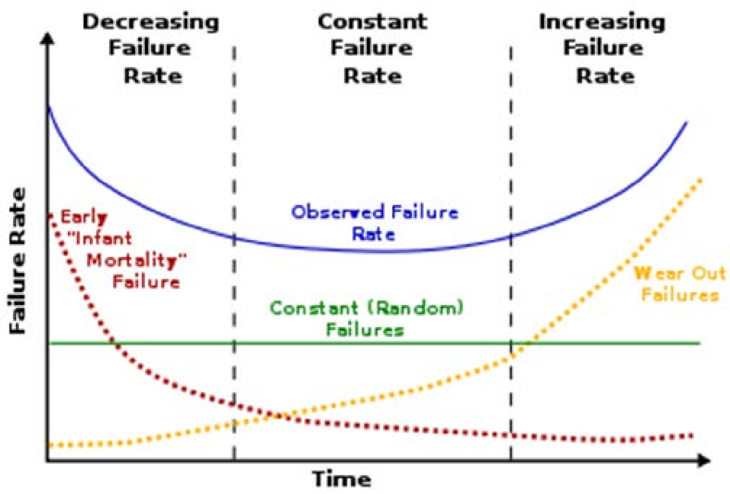
Failure rate and repair evaluation

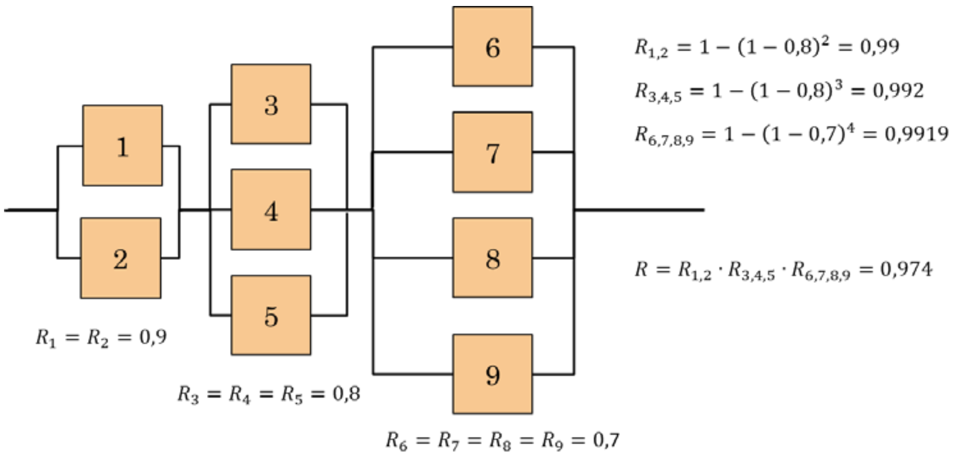
Failure rate prediction, MTTF (Mean Time Between Failure), MTTR (Mean Time to Restore), etc.

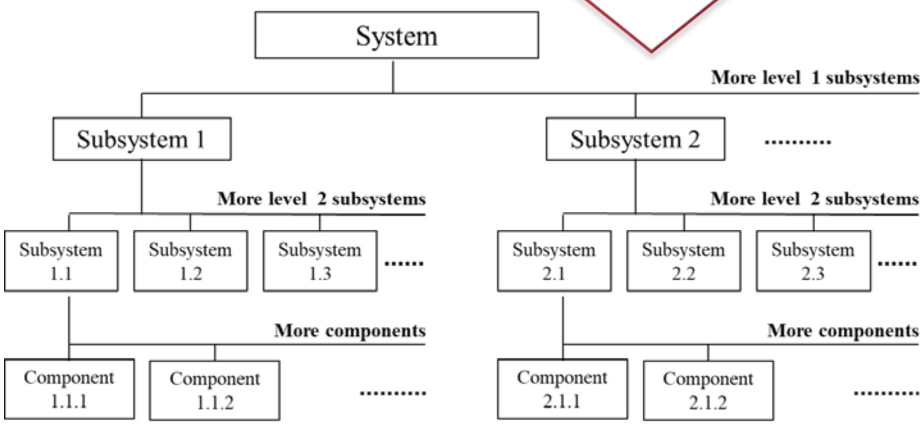
MODELS

Reliability analytical models

Dynamic and static models (Reliability allocation, Rel. Importance, RBD, Fault tolerance)

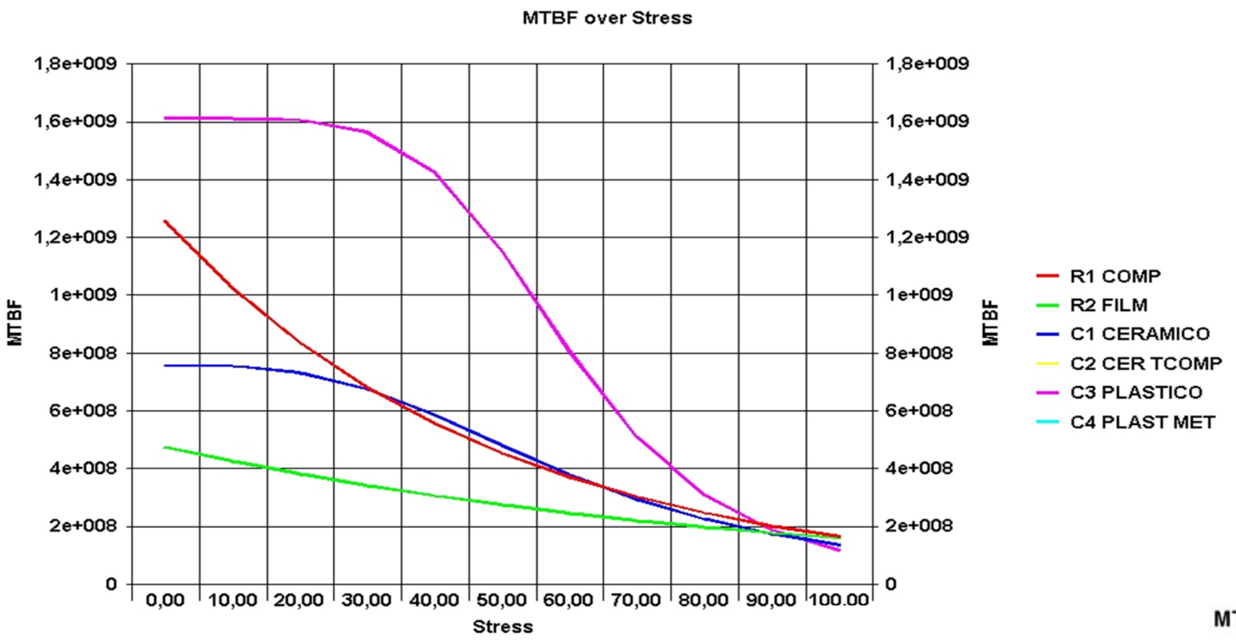


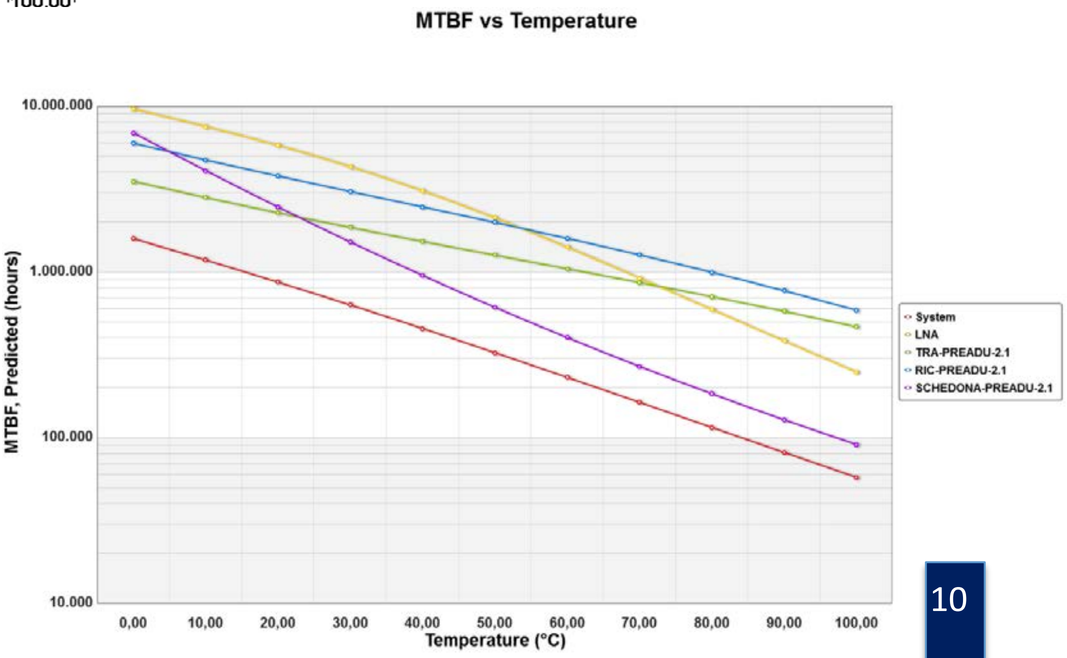




$$\lambda_{System} = f(\lambda_{1.1.1}, \lambda_{1.1.2}, \dots \lambda_{2.1.1}, \dots)$$

- λ, failure rate models
- MTBF Mean Time Beetween Failures
- MTTR Mean Time To Restore
- Reliability allocation
- Reliability importance

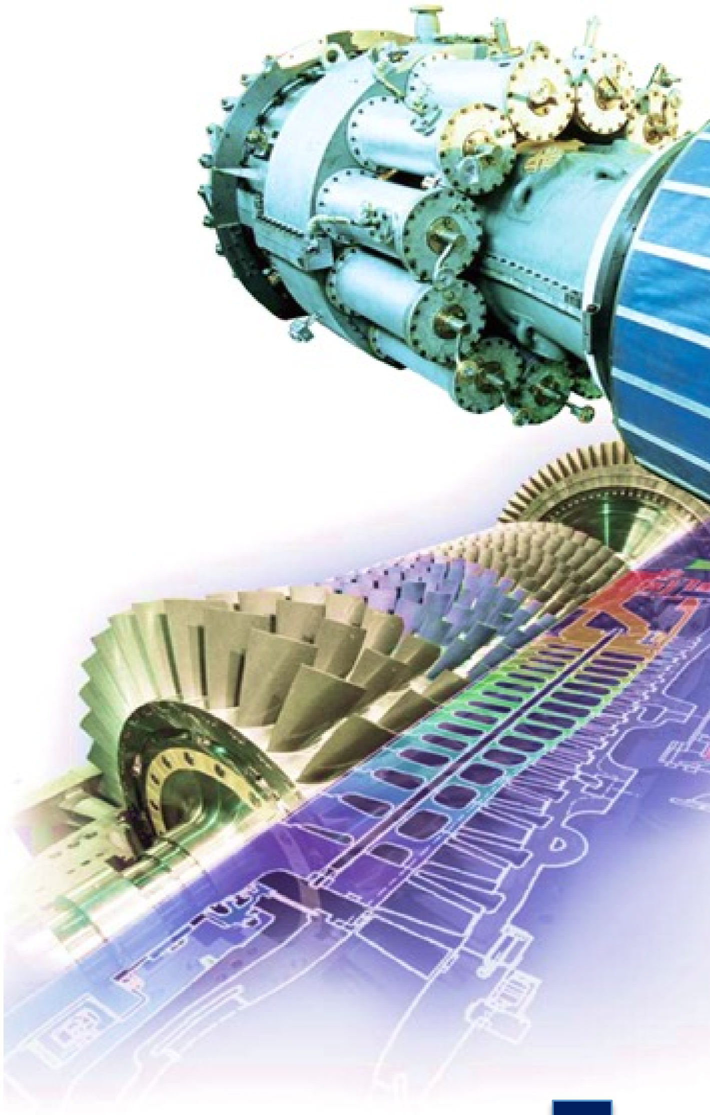




- Most critical components
- Derating
- Temperature effects

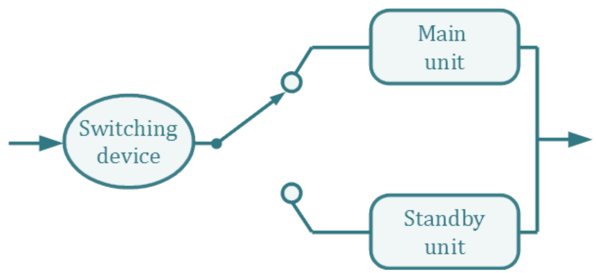
Fault Tolerant Design

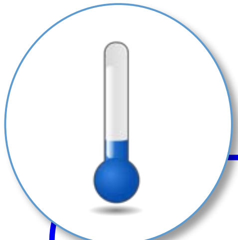
- **Fault tolerance** enables a system to continue its required operation, sometimes at a reduced efficiency level, rather than failing completely when some components of the system fail.
- It is widely used in *Energy* applications **to achieve continuous and successful operations despite extreme process and environmental conditions.**
- The most used fault tolerant technique is **redundancy**: critical components performing the same function are duplicated to increase system reliability and availability.
- A particular effective architecture is "**standby redundancy**": **in case main component failure arises, standby unit is activated to complete the mission.** There are three different redundant configurations: hot standby, warm standby and cold standby.



Standby Redundancy

Dynamic (or "standby") redundancy consists of fault detection and system reconfiguration with a standby unit; in case of main component failure, standby unit is activated to complete the mission.

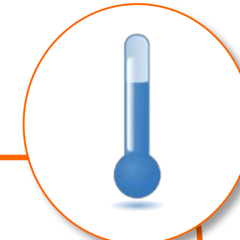




Cold standby

Standby unit is inactive and completely disconnected from power source or fuel supply; quiescent components during the inactive period do not age and cannot fail.

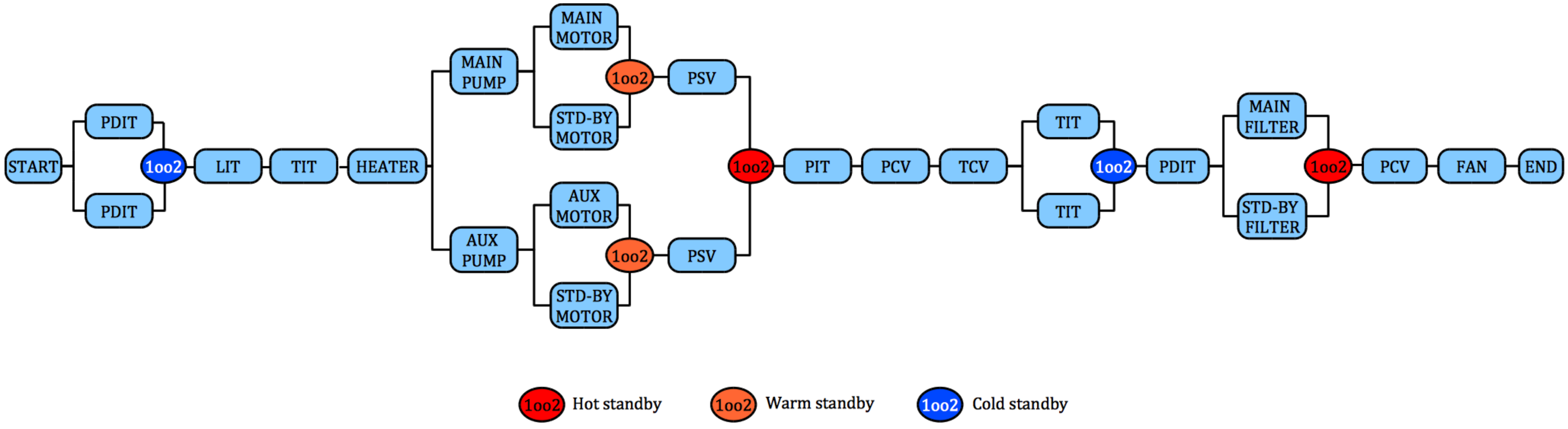
$$R_s(t) = R_1(t) + (1-p) \cdot \int_0^t f_1(x) \cdot R_{2,a}(t-x) \cdot dx$$



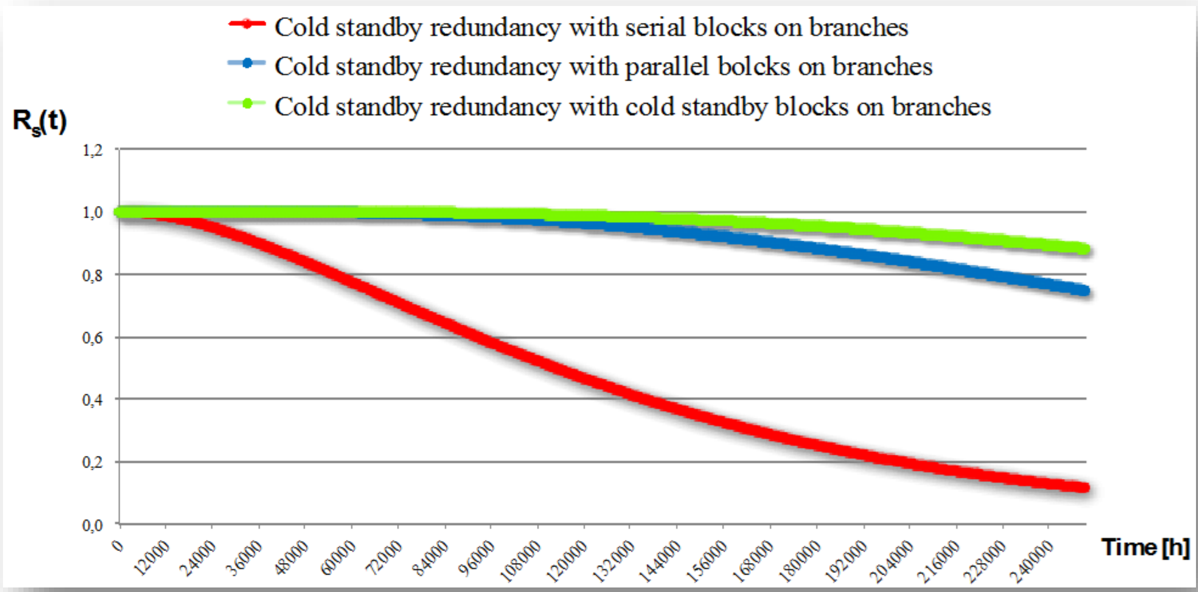
Warm standby

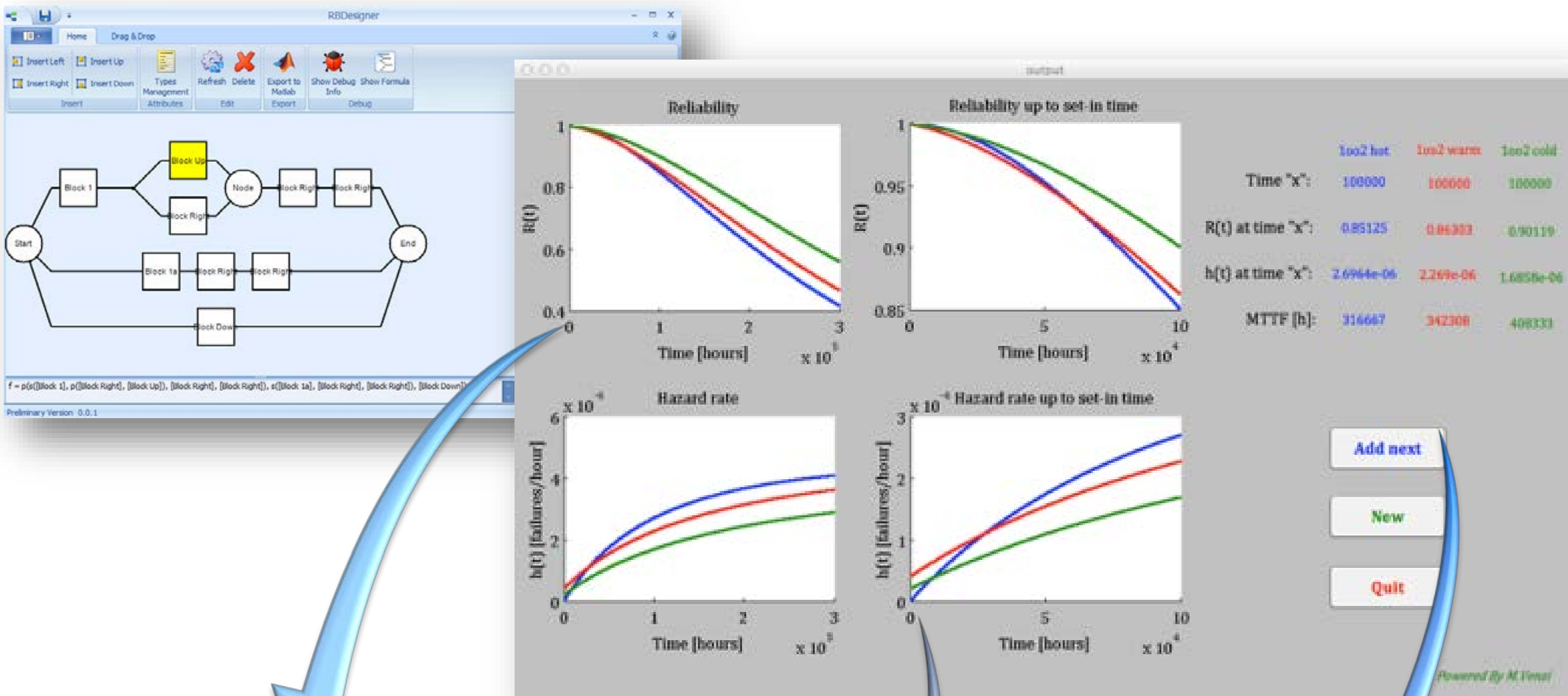
Both units are connected to power source but just one piece of equipment is used for the process, the other one is half operative and ready to run in case of main failure.

$$R_s(t) = R_1(t) + (1-p) \cdot \int_0^t f_1(x) \cdot R_{2,sb}(x) \cdot R_{2,a}(t-x) \cdot dx$$



System Reliability vs. Time

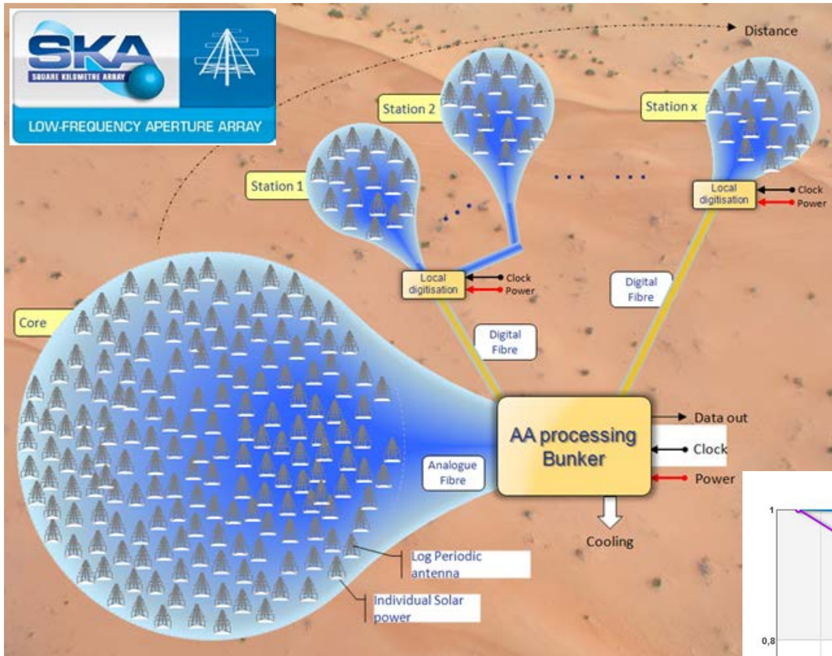




Reliability vs. time

Hazard rate vs. time

System MTTF



512 *Stations* with **16** *tile*

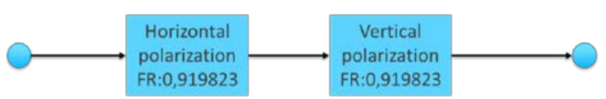
A *tile* is composed by **16** antennas

Total: **131.072** antennas

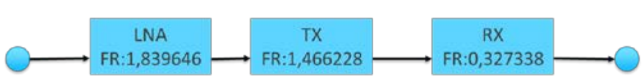
FR: Failure Rate $[10^{-6}h^{-1}]$

Data obtained with Telcordia Issue 3

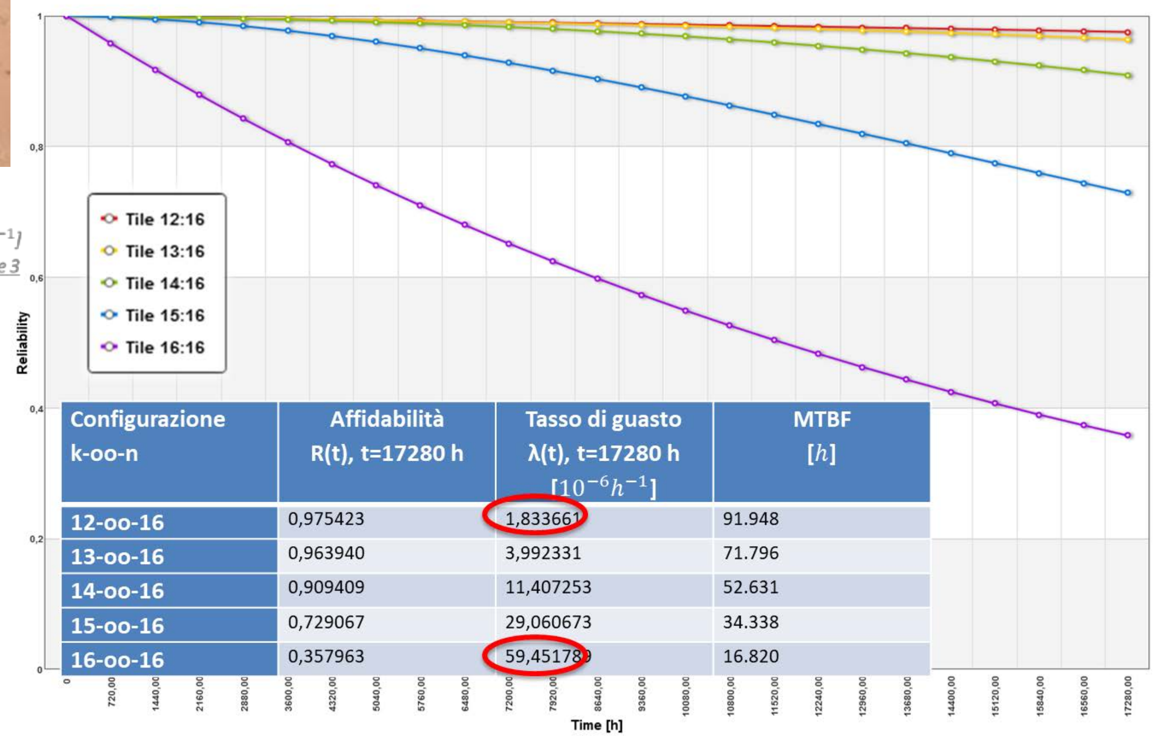
RBD of 2 LNA



Receiver chain



$$R_{Syst}(t) = \prod_{i=1}^{n} R_i(t) \qquad \lambda_{Syst} = \sum_{i=1}^{n} \lambda_i \qquad MTBF = \int_0^{+\infty} R_{Syst}(t)\,dt = \frac{1}{\sum_i \lambda_i}$$



Configurazione k-oo-n	Affidabilità R(t), t=17280 h	Tasso di guasto λ(t), t=17280 h $[10^{-6}h^{-1}]$	MTBF $[h]$
12-oo-16	0,975423	1,833661	91.948
13-oo-16	0,963940	3,992331	71.796
14-oo-16	0,909409	11,407253	52.631
15-oo-16	0,729067	29,060673	34.338
16-oo-16	0,357963	59,451789	16.820

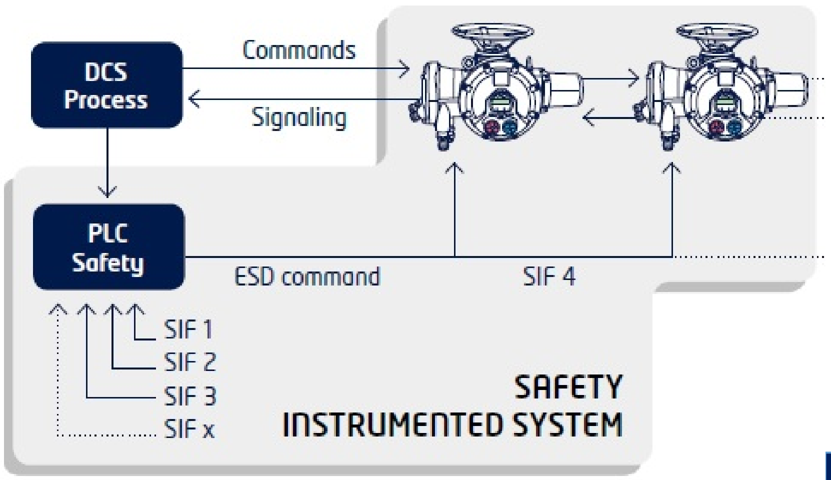
Failure analysis and risk assessment

Failure Mode Effect and Criticality analysis (FMECA), Fault Tree Analysis (FTA), etc.

ASSESSMENT

Functional safety assessment

SIL evaluation, IEC 61508

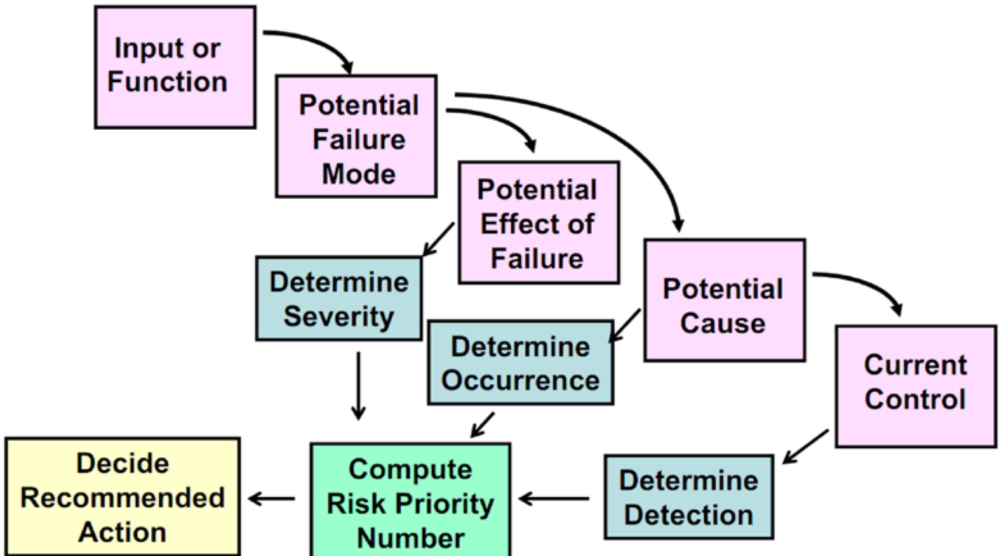


Failure Analysis Methods

- Every product or process has **modes of failure**
- An analysis of potential failures helps designers focus on and **understand the impact of potential process or product risks and failures**
- **Several systematic methodologies** have been develop to quantify the effects and impacts of failures.

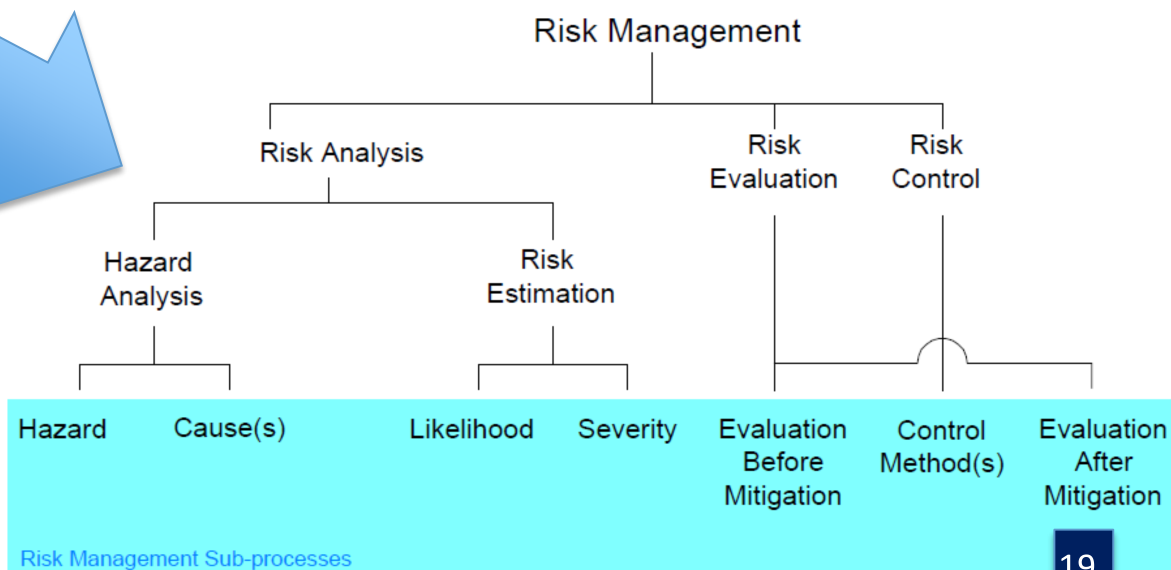
FMEA on Ultracapacitors

Item	Failure Modes	Failure causes	Local effect	Final effect
Ultracapacitor	Capacitance decrease	Overvoltage Overtemperature Ageing	Decrease of component efficiency	Loss of system performance
	Equivalent Series Resistance (ESR) increase	Overvoltage Overtemperature Mechanical stress Ageing	Decrease of component efficiency	Loss of system performance
	Temperature increase	Mechanical stress	Fire	System damage
	Capacitance/ESR out of specific	Overvoltage Overtemperature	Decrease of component efficiency	Loss of system performance
	Cell leakage (solvent vapor release)	Overpressure	Component Explosion	System damage
	Cell opening	Electrochemical decomposition overpressure	Component Explosion	System damage
	Gas pressure	Overvoltage Overtemperature	Component Explosion	System damage



RISK ASSESSMENT MATRIX

SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			



RISK: combination of the probability of occurrence of harm and the severity of that harm

SAFETY:

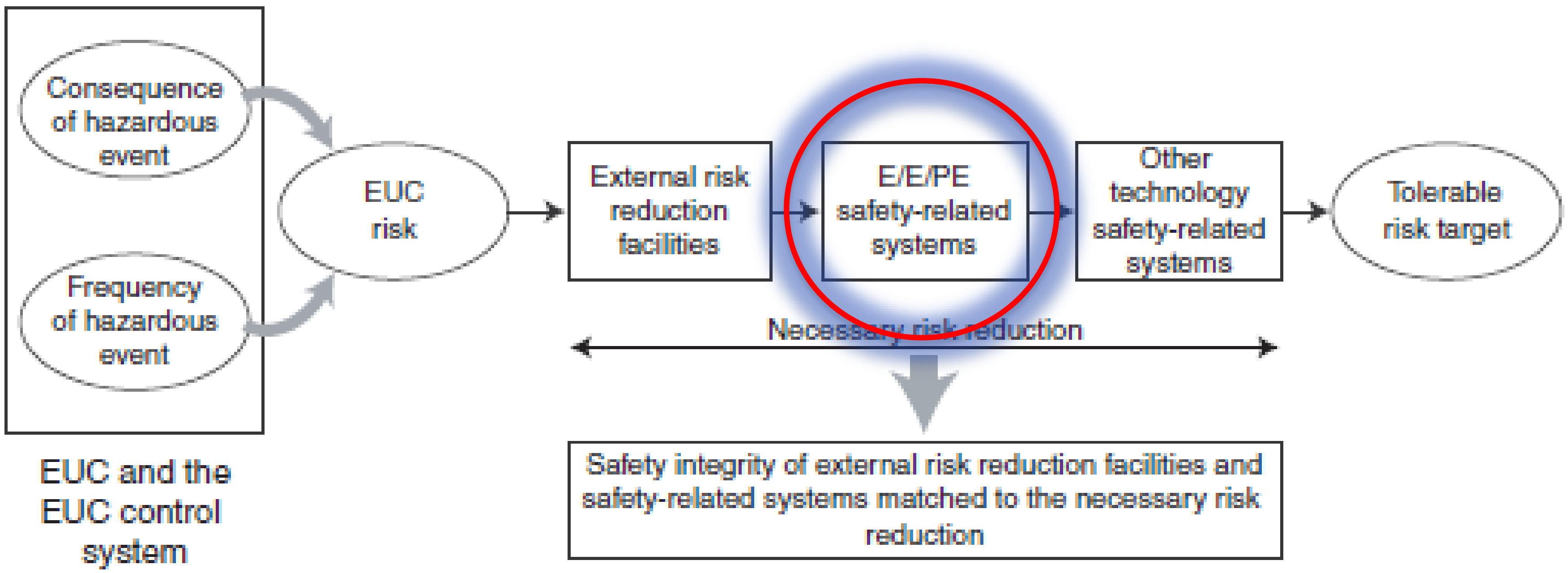
Safety is the freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment

IS IT SAFE?

Certificate

FS Eng (TÜV Rheinland)
Functional Safety Engineer (TÜV Rheinland)

Application Area: Safety Instrumented Systems
ID-No.: # 5062/12
Certificate Owner: Lorenzo Ciani
Italy


Consequence of hazardous event
Frequency of hazardous event
EUC and the EUC control system
EUC risk
External risk reduction facilities
E/E/PE safety-related systems
Other technology safety-related systems
Tolerable risk target
Necessary risk reduction
Safety integrity of external risk reduction facilities and safety-related systems matched to the necessary risk reduction

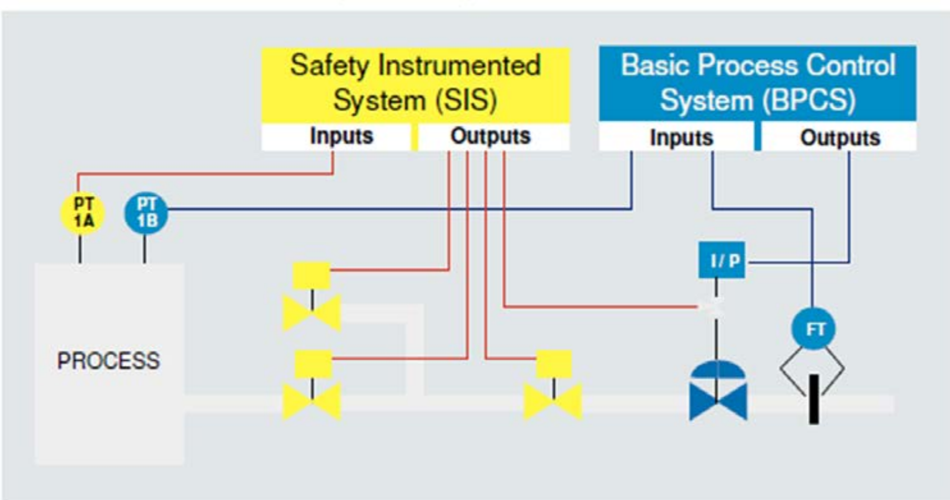
A **safety instrumented system (SIS)** is a designated system that implements the required safety functions necessary to achieve or maintain a safe state for some equipment (an EUC).

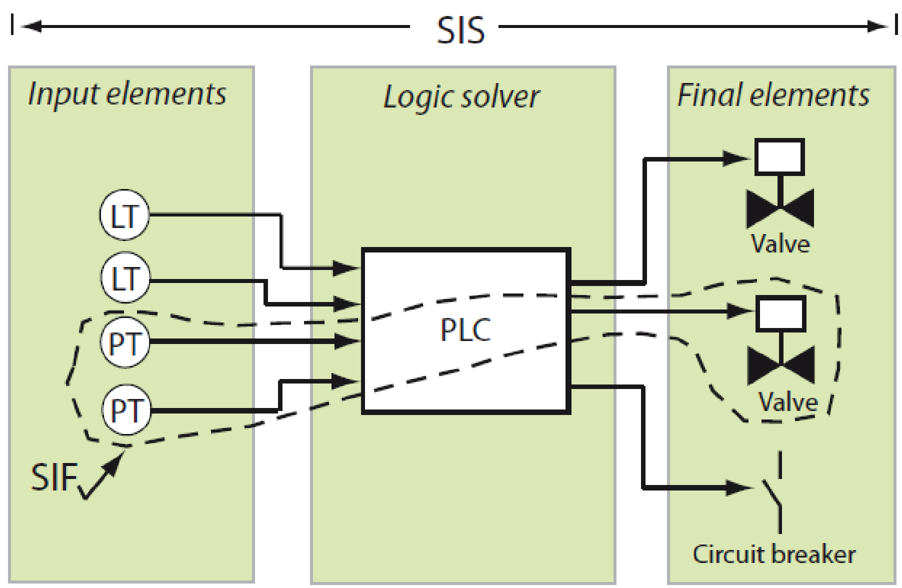
A SIS consists of three types of elements:

- Detectors (or sensors)
- Logic solver (e.g., one or more computers/PLD)
- Actuating items (e.g., valves, brakes)

SIL – PFDav – PFH – modes of operation

Safety Integrity Level (SIL)	Average probability of failure to perform a safety function on demand – PFD_{av} (Low demand mode of operation)	Probability of a dangerous failure per hour – PFH (High demand or continuous mode of operation)
SIL4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
SIL3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
SIL2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
SIL1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$





From the IEC61508-6

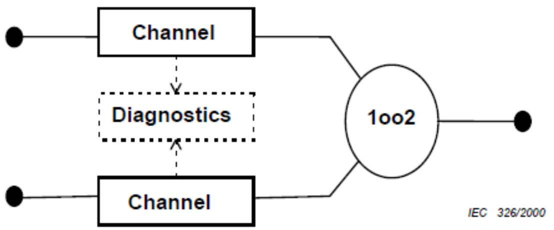


Figure B.6 – 1oo2 physical block diagram

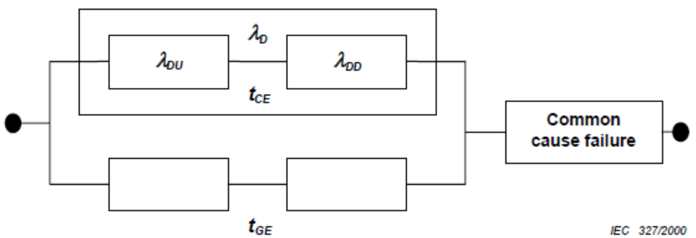


Figure B.7 – 1oo2 reliability block diagram

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

The average probability of failure on demand for the architecture is

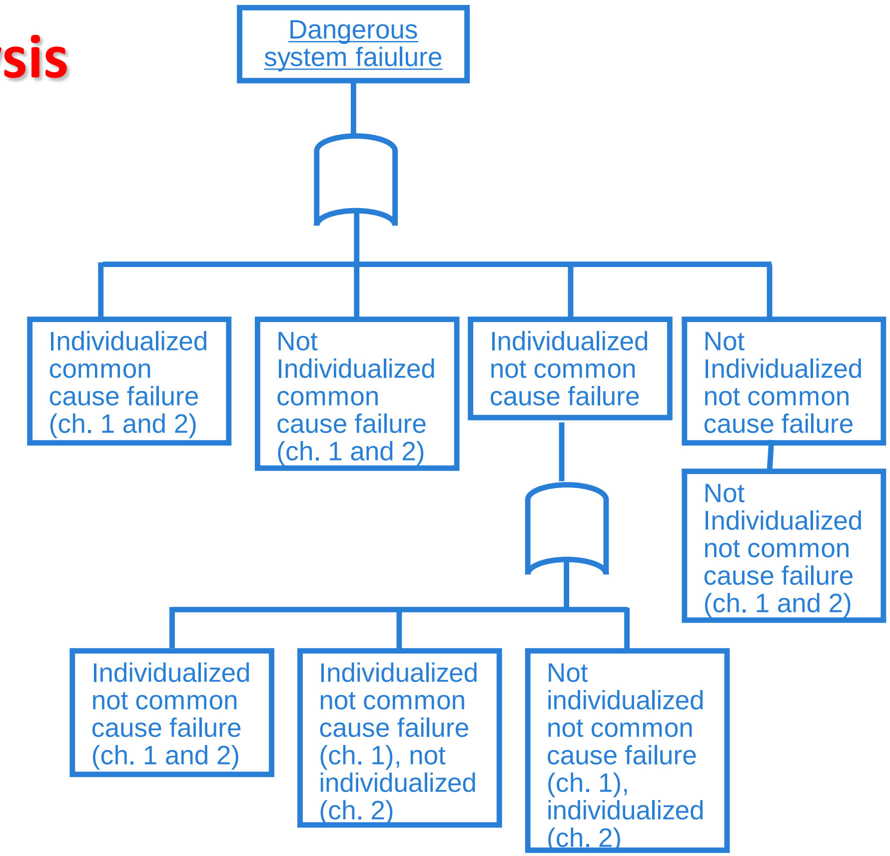
$$PFD_G = 2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$$

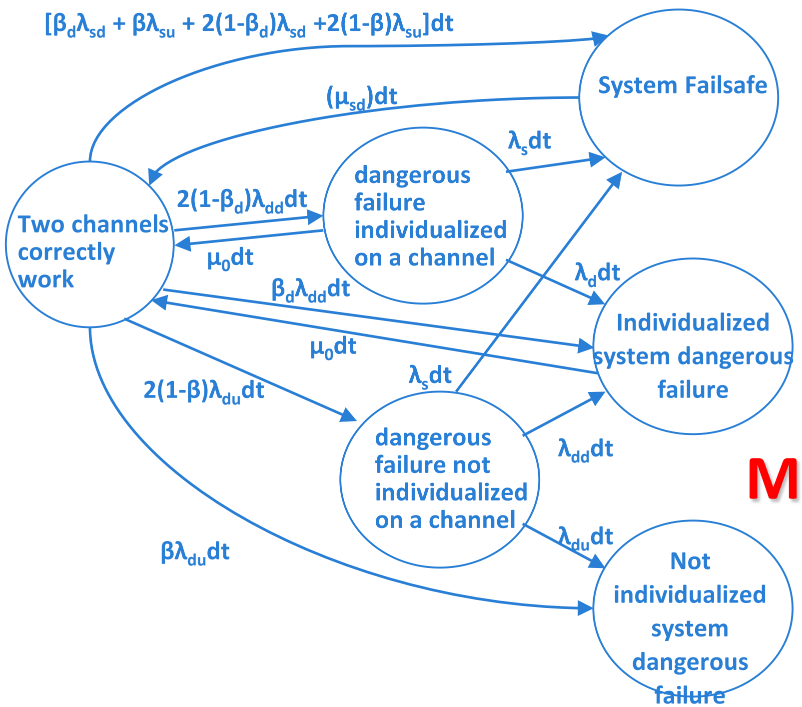
where β denotes the fraction of undetected failures that have a common cause; $β_D$ represents the fraction of detected failures, by the diagnostic test, that have a common cause.

MTTR : Mean Time To Restore

T_i : Proof Test interval, **periodic test performed to detect failure in a safety related system**

Fault Tree Analysis





Markov diagram 1oo2 configuration

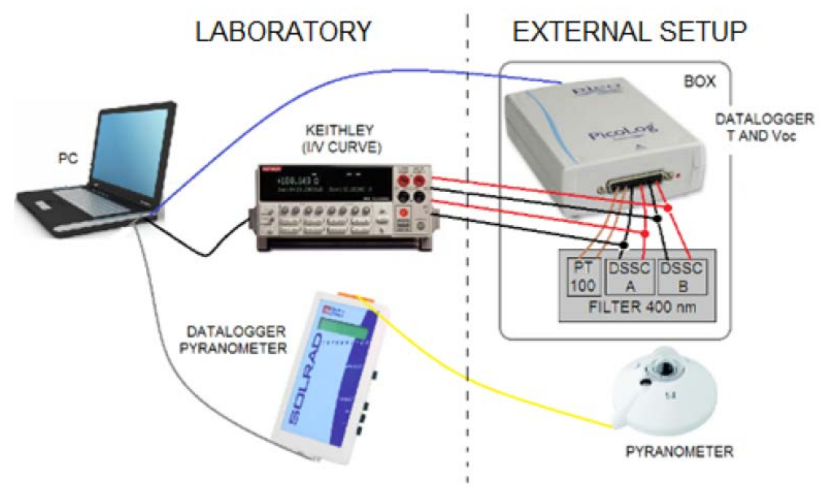
Measurements

Device and components characterization, Automatic Measurement System

MEAS &TESTING

Reliability test & lab experiments

Thermal and mechanical stress (i.e. accelerated testing, aging test)



Thermal tests: planning

Thermal test #1 — **Analysis of critical components behavior @$T_{operating}$=45°C**

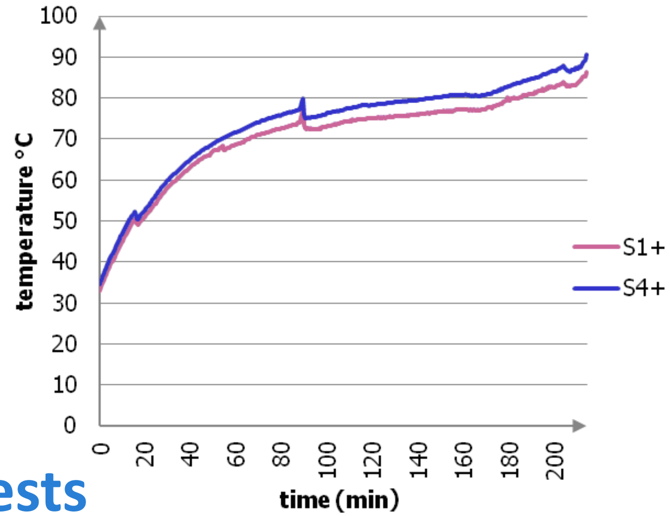
Thermal test #2 — **Replacing the critical components and increasing their temperature range**

Thermal test #3 — **Study of the inverter thermal behavior with increasing operating temperature**

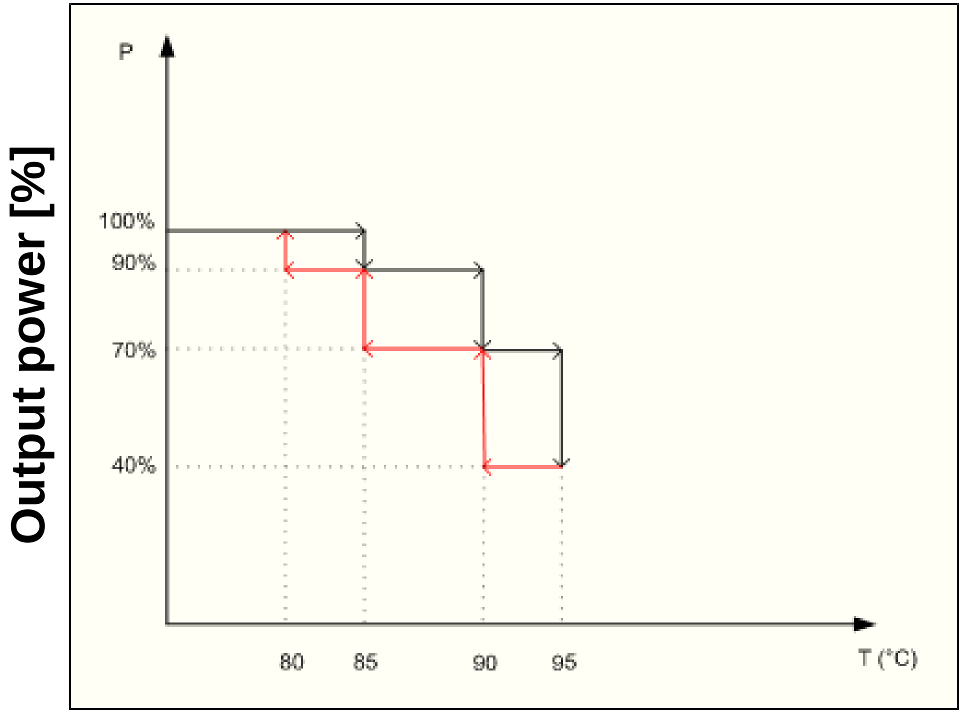
Thermal test #3

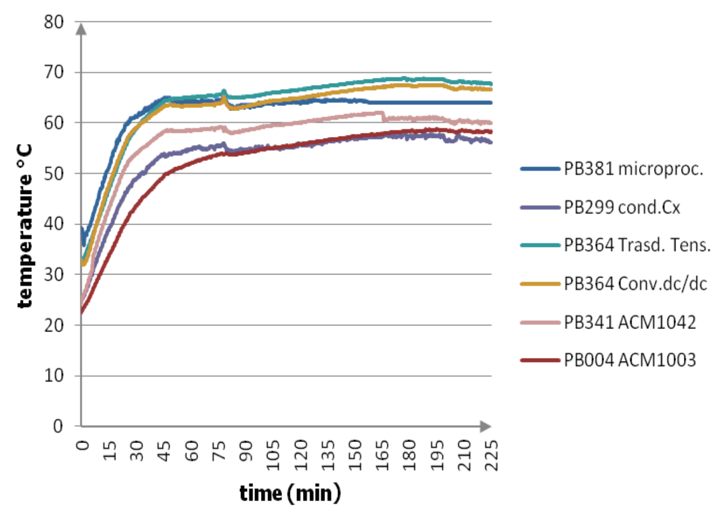
Inverter thermal behavior

- T_{oper}= 45°C
- T_{oper}= 50°C
- T_{oper}= 55°C

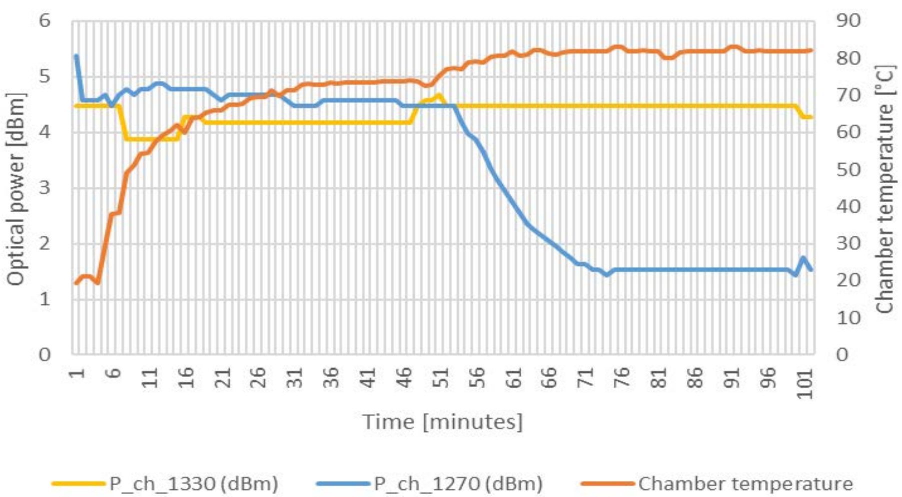


Derating strategy based on thermal tests





Aging Test*



$$k = Ae^{-\frac{E_A}{RT}}$$

- activation energy (E_A)
- rate constant (k)
- kelvin temperature (T)
- the gas consant (R)
- frequency factor or pre-exponential factor (A)
- mathematical quantity, e

Test duration: 800 hours

Severity (T_{max}) = 80°C

*prove in collaborazione con il Lab. Congiunto Analytical - CETACE

Journal with peer review

1. M. Catelani; L. Ciani; G. Patrizi; M. Venzi, "Reliability Allocation Procedures in Complex Redundant Systems," *IEEE Systems Journal*, *in press*, pp.1-11, doi: 10.1109/JSYST.2017.2651161

2. Urko Leturiondo, Oscar Salgado, Lorenzo Ciani, Diego Galar, Marcantonio Catelani, Architecture for hybrid modelling and its application to diagnosis and prognosis with missing data, *Measurement*, *(2017) 108, pp. 152-162*, ISSN 0263-2241, http://doi.org/10.1016/j.measurement.2017.02.003.

3. A. Reatti, M.K. Kazimierczuk, M. Catelani, L. Ciani, Monitoring and field data acquisition system for hybrid static concentrator plant, *Measurement*, Volume 98, February 2017, Pages 384-392, ISSN 0263-2241, http://dx.doi.org/10.1016/j.measurement.2015.06.022.

4. Marcantonio Catelani, Lorenzo Ciani, Matteo Venzi, Component Reliability Importance assessment on complex systems using Credible Improvement Potential, *Microelectronics Reliability*, Volume 64, September 2016, Pages 113-119, ISSN 0026-2714, http://dx.doi.org/10.1016/j.microrel.2016.07.055.

5. A. Cappelletti, M. Catelani, L. Ciani, M. K. Kazimierczuk and A. Reatti, "Practical Issues and Characterization of a Photovoltaic/Thermal Linear Focus 20\times Solar Concentrator," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 11, pp. 2464-2475, Nov. 2016, doi: 10.1109/TIM.2016.2588638

6. Catelani, M., Ciani, L., Kazimierczuk, M.K., Reatti, A., "Matlab PV solar concentrator performance prediction based on triple junction solar cell model", (2016) *Measurement*, 88, pp. 310-317, DOI: 10.1016/j.measurement.2016.03.046

7. Zanobini, A., Sereni, B., Catelani, M., Ciani, L., "Repeatability and Reproducibility techniques for the analysis of measurement systems", (2016) *Measurement*, 86, pp. 125-132, DOI: 10.1016/j.measurement.2016.02.041

8. M. Catelani, L. Ciani, M. Venzi, G. Barile, Custom TFT-LCD for avionics applications: Environmental tests and optical measurements, *Measurement*, Volume 80, February 2016, Pages 179-189, ISSN 0263-2241, http://dx.doi.org/10.1016/j.measurement.2015.11.021.

9. M. Catelani, L. Ciani, M. Venzi, Sensitivity analysis with MC simulation for the failure rate evaluation and reliability assessment, *Measurement*, Volume 74, October 2015, Pages 150-158, ISSN 0263-2241, http://dx.doi.org/10.1016/j.measurement.2015.07.003.

10. Marracci, M.; Tellini, B.; Catelani, M.; Ciani, L., "Ultracapacitor Degradation State Diagnosis via Electrochemical Impedance Spectroscopy", *IEEE Transactions on Instrumentation and Measurement*, vol.64, no.7, pp.1916,1921, July 2015, doi: 10.1109/TIM.2014.2367772

11. Lorenzo Ciani, Marcantonio Catelani, Ennio Antonio Carnevale, Lorenzo Donati and Mara Bruzzi, "Evaluation of the ageing process of Dye-Sensitized Solar Cells under different stress conditions", *IEEE Transactions on Instrumentation and Measurement*, vol.64, no.5, pp.1179,1187, May 2015, doi: 10.1109/TIM.2014.2381352

12. Loredana Cristaldi, Marco Faifer, Massimo Lazzaroni, Mohamed Mahmoud Abdel Fattah Khalil, Marcantonio Catelani, Lorenzo Ciani, Diagnostic architecture: A procedure based on the analysis of the failure causes applied to photovoltaic plants, *Measurement*, Volume 67, May 2015, Pages 99-107, ISSN 0263-2241, http://dx.doi.org/10.1016/j.measurement.2015.02.023.

13. Diego Galar, Adithya Thaduri, Marcantonio Catelani, Lorenzo Ciani, Context awareness for maintenance decision making: A diagnosis and prognosis approach, *Measurement*, Volume 67, May 2015, Pages 137-150, ISSN 0263-2241, http://dx.doi.org/10.1016/j.measurement.2015.01.015.

Journal with peer review

14. Marcantonio Catelani, Lorenzo Ciani, Giorgio Graditi, Giovanna Adinolfi, "Measurement and comparison of reliability performance of photovoltaic power optimizers for energy production", ***Metrology and Measurement Systems***, Volume 22, Issue 1, Pages 139–152, ISSN (Online) 2300-1941, DOI: 10.1515/mms-2015-0012, February 2015.

15. Lorenzo Ciani, Marcantonio Catelani, A fault tolerant architecture to avoid the effects of Single Event Upset (SEU) in avionics applications, ***Measurement***, Volume 54, August 2014, Pages 256-263, ISSN 0263-2241, http://dx.doi.org/10.1016/j.measurement.2014.02.018.

16. Loredana Cristaldi, Marco Faifer, Marco Rossi, Sergio Toscani, Marcantonio Catelani, Lorenzo Ciani, Massimo Lazzaroni, Simplified method for evaluating the effects of dust and aging on photovoltaic panels, ***Measurement***, Volume 54, August 2014, Pages 207-214, ISSN 0263-2241, http://dx.doi.org/10.1016/j.measurement.2014.03.001.

17. Marcantonio Catelani, Lorenzo Ciani, Loredana Cristaldi, Marco Faifer, Massimo Lazzaroni, Electrical performances optimization of Photovoltaic Modules with FMECA approach, ***Measurement***, Volume 46, Issue 10, December 2013, Pages 3898-3909, ISSN 0263-2241, http://dx.doi.org/10.1016/j.measurement.2013.08.003.

18. M. Catelani, L. Ciani, M. Marracci, B. Tellini, Analysis of ultracapacitors ageing in automotive application, ***Microelectronics Reliability***, Volume 53, Issues 9–11, September–November 2013, Pages 1676-1680, ISSN 0026-2714, http://dx.doi.org/10.1016/j.microrel.2013.07.051.

19. E. Balestrieri, M. Catelani, L. Ciani, S. Rapuano, A. Zanobini, "Word Error Rate measurement uncertainty estimation in Digitizing Waveform Recorders", ***Measurement*** 46 (2013), pp. 572-581, DOI 10.1016/j.measurement.2012.08.016.

20. M. Catelani, L. Ciani, G. Barile, "A new design technique of TFT–LCD display for avionics application", ***Microelectronics Reliability***, Volume 52, Issues 9–10, September–October 2012, Pages 1776-1780, ISSN 0026-2714, 10.1016/j.microrel.2012.06.034

21. M. Catelani, L. Ciani, "Experimental tests and reliability assessment of electronic ballast system", ***Microelectronics Reliability***, Volume 52, Issues 9–10, September–October 2012, Pages 1833-1836, ISSN 0026-2714, 10.1016/j.microrel.2012.06.077

22. E. Balestrieri, M. Catelani, L. Ciani, S. Rapuano, A. Zanobini, "The Student's t distribution to measure the word error rate in analog-to-digital converters", ***Measurement***, Volume 45, Issue 2, February 2012, Pages 148-154, ISSN 0263-2241, DOI 10.1016/j.measurement.2011.03.002.

23. M. Catelani, L. Ciani, V. Luongo, "A simplified procedure for the analysis of Safety Instrumented Systems in the process industry application", ***Microelectronics Reliability***, Volume 51, Issues 9-11, September-November 2011, Pages 1503-1507, ISSN 0026-2714, 10.1016/j.microrel.2011.07.044.

24. M.Catelani, L.Ciani, V.L. Scarano, A.Bacioccola, "Software automated testing: a solution to maximize the test plan coverage and to increase software reliability and quality in use", ***Computer Standards & Interfaces***, Volume 33, Issue 2, February 2011, Pages 152-158.

25. M. Catelani, L. Ciani, V. Luongo, "The FMEDA approach to improve the safety assessment according to the IEC61508", ***Microelectronics Reliability***, Issue 50, Vol. 9-11 (2010), pp. 1230–1235.

26. M.Catelani, L.Ciani, A.Zanobini, "Uncertainty Interval Evaluation Using The Chi-Square And Fisher Distributions In The Measurement Process", Journal of ***Metrology and Measurement Systems***, Vol. XVII (2010), No. 2, pp. 195-204.

27. M.Catelani, A. Zanobini, L.Ciani, "Introduction to the t and chi-square distribution for a more accurate evaluation of the measure of the Word Error Rate in Analog-to-Digital Converters", Journal of ***Metrology and Measurement System***, Issue 4/2008, vol. XV, , pp. 483-488.

Grazie per l'attenzione!