12th IMEKO TC10 Workshop on Technical Diagnostics
New Perspectives in Measurements, Tools and Techniques for Industrial Applications
June 6-7, 2013, Florence, Italy

Improved FBD and RBD generation for system reliability assessment

M. Venzi[1], S. Rossin[1], C. Michelassi[1], C. Accillaro[1], M. Catelani[2], L. Ciani[2]
[1] *PDSE Department – Auxiliary Systems Engineering, GE Oil & Gas – Nuovo Pignone, Florence (Italy)*
[2] *Department of Information Engineering, University of Florence, via S.Marta 3, Florence (Italy)*

***Abstract*- This paper is focused on Reliability Block Diagram generation with the aim of providing a reliability prediction in the early stages of *Oil&Gas* product development, in particular for gas turbine auxiliary systems. Reliability assessment is achieved with a dedicated tool named *RBDesigner* that semi-automatically generates a RBD starting from the sketch of thermal-hydraulic systems and provides the most important reliability parameters.**
Furthermore this paper shows a new approach to assessing reliability of standby redundancy architectures that are widely used in *Oil&Gas* applications.

Keywords: Reliability assessment, Reliability Block Diagram (RBD), Oil & Gas applications, Gas turbine auxiliary systems, Standby redundancy architecture, Cold standby, Warm standby

I. Introduction

Modern technologies and business requirements lead to a growth in manufacturing product complexity and miniaturization of components: this trend increased number and variety of failures and for this reason the interest in RAMS (Reliability, Availability, Maintainability and Safety) and diagnostics parameters is growing in many different manufacturing fields, in particular for *Oil&Gas* applications where products are forced to endure extreme process and environmental conditions.
This paper is focused on *GE Oil&Gas* gas turbine auxiliary systems with the aim of providing a reliability prediction in the early stages of product development: reliability parameters can help design engineering to compare different solutions, prove system robustness and reduce time for improvements.
Reliability assessment is achieved with a dedicated tool named *RBDesigner* that semi-automatically generates a Reliability Block Diagram (RBD) starting from the *P&ID schemes* (sketch of thermal-hydraulic systems) and provides the most important reliability parameters such as reliability vs. time, hazard rate vs. time and MTTF.

A Reliability Block Diagram is a functional diagram of all the components making up the system that shows how component reliability contributes to failure or success of the whole system.
Each block of the diagram represents a component with specific failure/hazard rate and definite connections with the rest of the system [1].
In contrast with Functional Block Diagrams (FBDs) that are focused on normal operation functionality, in RBDs the attention is shifted onto component failures and their consequences on the system.
The necessary assumptions to build the diagram and calculate the reliability parameters are shown below, in compliance with standards IEC 61078 [2]:

- System components can exist only in two states: working ("up" state) or failed ("down" state); intermediate working state is not allowed.
- A block failure cannot affect the probability of failure of any other block within the system modelled; for example, failure probability of block A is not related with failure probability of block B and vice versa.
$$P(A \mid B) = P(A)\,;\; P(B \mid A) = P(B) \quad (1)$$
- Sequential events are not considered in this method and system analysis is interrupted when the first fault is shown; for this reason RBDs are not suitable for modelling order-dependent or time-dependent events.
- System components are considered in the middle of their life-cycle (or "useful life" period) where failures can be considered random events and failure/hazard rate is constant.
$$\lambda_i(t) = \lambda_i \quad (2)$$
- Failure probability density function f(t) follows an exponential distribution; supposing constant failure rate, f(t) and reliability function R(t) can be written as follows:
$$f(t) = -\frac{dR(t)}{dt} = \lambda e^{-\lambda t} \quad (3)$$
$$R(t) = \exp\{-\int_0^{\infty} \lambda(t)dt\} = e^{-\lambda t} \quad (4)$$

- System is considered not repairable so reliability corresponding parameter is Mean Time To Failure (MTTF) instead of Mean Time Between Failures (MTBF), typically used for repairable systems.

$$MTTF = \int_0^\infty t \cdot f(t)dt = \int_0^\infty R(t)dt \quad (5)$$

II. Fault tolerant design and standby redundancy

Fault tolerant design is a design that enables a system to continue its intended operation, sometimes at a reduced efficiency level, rather than failing completely when some components of the system fail. [3]
Fault tolerant configurations are widely used in *Oil&Gas* 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.
There are two main types of redundancy techniques employed in fault tolerant designs, static and dynamic, in compliance with MIL-HDBK 338B [4].
Static (or "active") redundancy consists of fault masking without proper fault detection: in this kind of structures (e.g. parallel, k-out-of-n, major voting) there isn't a performance/status monitoring so final user is not aware of failure occurrence.
Dynamic (or "standby") redundancy, instead, 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.
There are three dynamic redundancy configurations: hot standby, warm standby and cold standby.
The first architecture is not analysed in this paper because it offers the same results of standard parallel configuration in terms of reliability assessment; the other two architectures are shown below supposing a simple configuration with two items, main and standby.

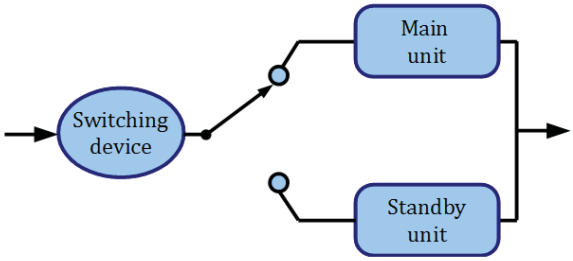

Fig.1 Standby architecture

Cold standby:
In a cold standby architecture only the main unit is operative, the standby unit is inactive and completely disconnected from power source or fuel supply. For this reason quiescent components during the inactive period do not age and cannot fail (this assumption can be done in totally controlled environments where the equipment will be stored, transported, operated and maintained).
In this configuration diagnostics it is necessary to detect main unit failure and switch the load to standby equipment on demand.
In *Oil&Gas* applications standby items are forced to endure severe environmental and process conditions and for this reason they can't be considered failure free by definition; in order to consider a standby unit operative for sure on demand it's necessary to introduce additional procedures to verify standby unit status (e.g. on-line/off-line tests or auto-diagnostics circuits) [4].
In this architecture switching devices can't be considered failure free by definition either because its fault nullifies redundancy advantages; switch failure modes are essentially two, not-required commutation and failure to commute on demand [5].
In these assumptions response-time (necessary to activate and initialize standby unit) and switch failure rate are the residual constrictions of cold standby employment.
Reliability function for cold standby architectures is shown below:

$$R_S(t) = R_1(t) + (1-p) \cdot \int_0^t f_1(x) \cdot R_{2,a}(t-x) \cdot dx \quad (6)$$

Legend:
- R_s: reliability of the system
- R_1: reliability of the active component (main)

- p: failure probability of the switch
- f_1: pdf of the active component
- $R_{2,a}$: reliability of the standby component in active mode
- x: time of main failure and further standby activation

Warm standby:
In a warm standby architecture both units are connected to power source but just one piece of equipment is used for the process (main), the other one (standby) is half operative and ready to run in case of main failure.
An important advantage of this configuration is response-time reduction, in fact it's not necessary to wait for standby unit start-up (equipment is ready to use) so it's sufficient to switch the load from main to standby [6].
Standby units age during quiescent period and can fail before switching the load, for this reason it's necessary to introduce a specific failure rate concerning with the quiescent status [2]. Standby equipment is always described by two different failure rates:

- "λo" when main unit is working properly so standby unit is half-operative;
- "λ" when standby unit is fully operative due to main equipment failure.

Switches can't be considered failure free by definition and the failure modes are the same of cold standby configuration.
Reliability function for cold standby architectures is shown below:

$$R_S(t) = R_1(t) + (1-p)\cdot\int_0^t f_1(x)\cdot R_{2,sb}(x)\cdot R_{2,a}(t-x)\cdot dx \qquad (7)$$

Legend:

- R_s: reliability of the system
- R_1: reliability of the active component (main)
- p: failure probability of the switch
- f_1: pdf of the active component
- $R_{2,sb}$: reliability of the standby component in quiescent mode
- $R_{2,a}$: reliability of the standby component in active mode
- x: time of main failure and further standby activation

Thanks to this broad approach there is no limit to RBD complexity and this feature is essential to achieve reliability prediction of complex systems such as gas turbine auxiliary systems.

III. Reliability assessment

Reliability prediction is one of the most common forms of reliability analysis to evaluate design feasibility, compare design alternatives, identify potential failure areas, trade-off system design factors and track reliability improvement.
RBDesigner tool was developed to achieve reliability prediction in the early product design stages: this tool gives a reliability feedback to design engineers to reduce re-design costs and time for improvements.
Starting from the sketches of the thermal-hydraulic system three steps are required to build a Reliability Block Diagram and calculate reliability parameters: automatic model generator, semi-automatic RBD design and reliability assessment.

1. Automatic model generator produces a Functional Block Diagram automatically from PidXp™, GE engineering tool for P&ID (piping and instrument diagram) definition.
   The output file of this automatic process is an XML net-list containing all blocks and connections.
   XML format was chosen for its wide applicability to many different purposes and a dedicated tool *XML Drawer* was implemented to display and edit the diagram.
   Exported net-list reproduces the thermal-hydraulic system topology and within this diagram each block keeps all the attributes and features of the starting sketch (e.g. technical information, position within the system and generic block properties).
   This automatic process reduces potential errors introduced by data transcriptions or human mistakes and translates P&ID projects into a universal language.

2. The second step is the semi-automatic RBD design: starting from the exported net-list a Reliability Block Diagram can be created with a drag-and-drop method from XML Drawer to RBDesigner.
   This is the required procedure:
   - Block selection: user selects a block from XML Drawer output window;
   - Drag function: block is dragged to RBDesigner input window;
   - Drop function: block is released in a specific position of the diagram.

In order to avoid mistakes and facilitate improvements, RBD generation is guided with structural restrictions and multi-architecture suggestions. RBDesigner user is not allowed to draw a diagram to his liking because all the RBD rules are fully integrated and only suitable actions are permitted; furthermore, if different achievable solutions are possible (in particular for redundant architectures), alternatives are suggested in order to have a complete overview of design feasibility.
Similarly net-list blocks, RBD components keep all the attributes and the features of the starting sketch too and at this stage some additional information can be included for reliability prediction achievement (e.g. component failure rate, MTTF,…): these records are provided from different databases (NSWC Handbook – *Naval Surface Warfare Center* [7] and OREDA Handbook – *Offshore Reliability Data* [8]).
Thanks to these features diagram generation is extremely intuitive and even users without wide reliability knowledge can enjoy it, otherwise advanced editing procedures are provided for expert users that don't need structural restrictions or architectural suggestions.

3. The last step is Reliability Assessment: once RBD generation is completed, all the information concerning diagram structure and component reliability is used to obtain a reliability prediction.
   Processing phase and output generation are achieved on Matlab® platform and the outputs shown are listed below:
   - Reliability vs. time plot (up to default time, 300000h)
   - Reliability vs. time plot (up to user set-in time)
   - Hazard rate vs. time plot (up to default time, 300000h)
   - Hazard rate vs. time plot (up to user set-in time)
   - Reliability value calculated at user set-in time value
   - Hazard rate value calculated at user set-in time value
   - System MTTF (Mean Time To Failure)

Figure 2 shows the whole reliability assessment loop: P&ID section on PidXp™ platform (2a), exported net-list in XML Drawer (2b), Reliability Block Diagram build with drag-and-drop method (2c) and reliability parameters of the system modeled with two suggested alternatives (2d).
Once reliability parameters are achieved this feedback is useful to take re-design actions or prove system robustness.

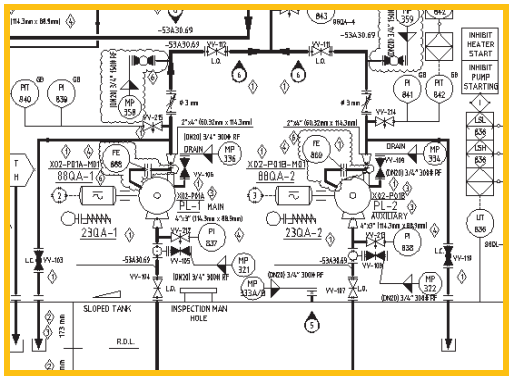

Fig.2a P&ID (PidXp)

Automatic model generator

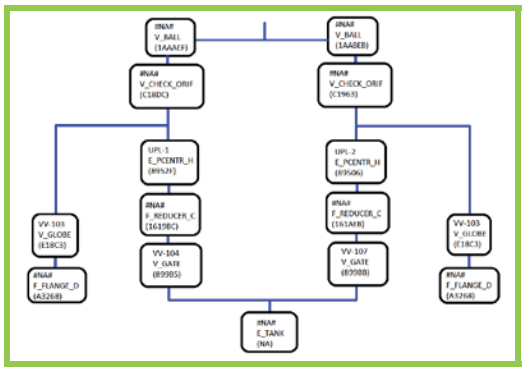

Fig.2b Net-list (XML Drawer)

Design improvement

Drag-and-drop procedure

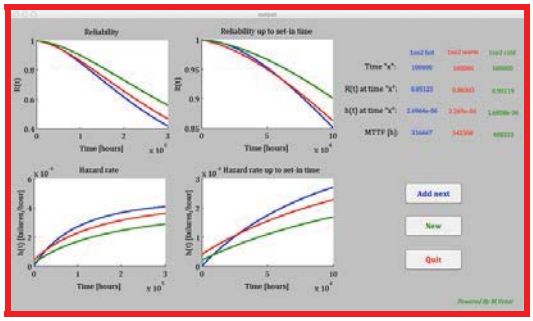

Fig.2d Reliability Assessment

Matlab processing

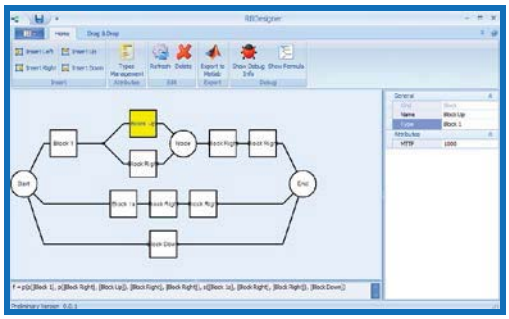

Fig.2c RBD (RBDesigner)

Fig.2 Reliability assessment loop

IV. Conclusions

Reliability prediction in the early stages of product development provides a great support to designing gas turbine auxiliary systems: reliability assessment achieved with RBDesigner allows project engineers to compare different solutions, prove system robustness and reduce time for improvements.
The implemented tool was cross-validated with other commercial software like BlockSim® (ReliaSoft) and Relex® (Reliacore); this comparison was performed considering several plants and architectures and results were always in compliance with expected ones.
The added values of RBDesigner compared with commercial software are listed below:

- Customized architecture library for *Oil&Gas* applications;
- Real-time multi-architecture comparison;
- User-friendly interface and guided RBD generation;
- No limit to RBD architecture complexity (in particular for standby redundancy configurations);
- Multi-database library for component reliability parameters;
- Full-integration with piping and instruments diagram definition.

The data obtained with the proposed approach will be useful also in the safety assessment i.e. in the Failure Modes, Effects and Diagnostic Analysis (FMEDA) technique [9-14].
RBDesigner future developments are the introduction of some parameters for availability/maintainability assessment and reliability importance analysis; this second task will be very important in product design stages because it will identify the weakest components that have the most impact on system performance and prioritize re-design actions to be taken.

References

[1] IEC 50 (191) - Terminology on reliability, maintenainability and quality of service, 1990.
[2] EN 61078. Analysis techniques for dependability -Reliability block diagram and Boolean methods, 2006.
[3] MIL-HDBK 217: Reliability prediction of electronic equipment, Department of defense Washington DC 20301, Notice 1, Notice 2.
[4] Military Handbook 338B (1998) - Electronic Reliability Design Handbook, Department of defense Washington DC 20301.
[5] M.Rausand, A. Høyland, System Reliability Theory, 2nd Edition. New Jersey: J.Wiley & Sons, Inc., Hoboken, 2004.
[6] Tannous, O.; Xing, L.; Rui, P.; Xie, M.; Ng, S.H.; "Redundancy allocation for series-parallel warm-standby systems," Industrial Engineering and Engineering Management (IEEM), 2011 IEEE International Conference, pp.1261-1265, 6-9 Dec. 2011.
[7] NSWC (2010), Naval Surface Warfare Center Carderock Division (January 2010)
[8] OREDA (2009), OREDA Reliability Data. OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway, 4rd edition.
[9] M. Catelani, L. Ciani, V. Luongo, "Safety Analysis in Oil &Gas Industry in compliance with Standards IEC61508 and IEC61511: Methods and Applications" Proc. Of IEEE - International Instrumentation And Measurement Technology Conference (I2MTC) - Minneapolis (USA) - May 2013, pp. 686-690.
[10] M. Catelani, L. Ciani, V. Luongo, "Functional safety assessment: an issue for technical diagnostics", Proc. Of XX IMEKO World Congress - Metrology for Green Growth, Sep. 9 - 14, 2012, Busan, Rep. of Korea
[11] M. Catelani, L. Ciani, V. Luongo, "A new proposal for the analysis of Safety Instrumented Systems" Proc. Of IEEE - International Instrumentation And Measurement Technology Conference (I2MTC) - Graz (Austria) - May 2012, pp. 1612-1616.
[12] 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.
[13] 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, ISSN: 00262714, DOI: 10.1016/j.microrel.2010.07.121.
[14] M. Catelani, L. Ciani, V. Luongo, R. Singuaroli, "Evaluation of the Safe Failure Fraction for an electromechanical complex system: remarks about the standard IEC61508", Proc. Of I2MTC 2010 (IEEE - International Instrumentation And Measurement Technology Conference) - Austin (USA) - May 2010, pp. 949-953.