ADVANCED TECHNIQUES FOR SAFETY ANALYSIS APPLIED TO THE GAS TURBINE CONTROL SYSTEM OF ICARO CO GENERATIVE PLANT

Andrea Bobbio[1], Sandro Bologna[2], Ester Ciancamerla[2], Piero Incalcaterra[2], Corrado Kropp[2], Michele Minichino[2], Enrico Tronci[3]

[1]Università del Piemonte Orientale
[2]ENEA CR Casaccia
[3]Università dell'Aquila

ABSTRACT

The paper describes two complementary and integrable approaches, a probabilistic one and a deterministic one, using classic and advanced modeling techniques for safety analysis of complex computer based systems. Such approaches are applied to the gas turbine control system of ICARO co generative plant, in operation at ENEA CR Casaccia. The probabilistic approach addresses the control system by itself, as the set of sensors, processing units and actuators, while the deterministic approach also includes the behaviour of the equipment under control, which interacts with the control system. The final aim of the research, documented in this paper, is to explore an innovative method which put the probabilistic and deterministic approaches in a strong relation, to overcome the drawbacks of their isolated, selective and fragmented use which can lead to inconsistencies in the evaluation results.

1. INTRODUCTION

The main function of ICARO plant is the integration of district heating and electrical power supply of the centre of ENEA CR Casaccia. The plant is based on a small gas turbine and has been specifically designed to facilitate experimental research activities. It is vital that the gas turbine works at optimum efficiency and with high availability. Moreover a protection strategy is needed to protect the engine from over-temperature and over-speed so involving safety aspects. A fault or a deterioration in the gas turbine control system, which performs both control and protection strategies, could result in a reduction of plant efficiency (i.e increasing fuel consumption or nitrogen oxide pollution) in a reduction of plant availability (i.e. decreasing of operating time due to trips or failures) or in a reduction of plant safety (i.e. on failure of a protection function, which could result in a damage of the engine, safety critical to the plant because of its high capital cost). Control and protection functions nowadays rely on computers which, if on one side increase benefits, on the other side increase risks due to their vulnerability to random failures and design errors.

For such reasons the demand of safety for computer based systems is more and more urgent even in conventional application domains, like ICARO co generative plant, as proven by the increasing demand of conformity to IEC 61508 standard. IEC 61508 standard does not address any specific sector. A very important concept in IEC 61508 is that of Safety Integrity Level (SIL). SILs are used as the basis for specifying the safety integrity requirements for the

safety functions to be implemented by the safety related system. As far as it concerns the determination of the appropriate Safety Integrity Level, IEC 61508 is based on the concept of risk and provides a number of different methods, quantitative and qualitative, for determining it. This research is going on by using two complementary approaches, a probabilistic one and a deterministic one, based on different analysis techniques, with the common belief that, at the current state of the art, no single method can be considered sufficient to estimate, with justified confidence, the possible occurrence of undesired states of the plant, due to instrumentation system failures. Another problem is in the current use of the different analysis techniques, which is selective and fragmented and takes place at different stages of the system lifecycle. As a consequence, at the state of the art, the relationship between the different kinds of results of the various analysis often remain vague and unresolved and difficulties arise in relating the results of the various analyses to each other and back to the overall prediction and assessment of not functional properties of the instrumentation system. The final aim of the research is to explore an innovative method which put the probabilistic and deterministic approaches in a strong relation to overcome the drawbacks of their isolated, selective and fragmented use.
The research also intends to use the operational data of the plant in order to calibrate and validate models. Model results will be compared with Safety Integrity Levels of IEC 61508 standard.
The paper is organised in the following sections. We start in section 2 with the description of the gas turbine module of the plant. Section 3 deals with the main requirements of IEC 61508 standard. Section 4 focus on the gas turbine control system, describing its functions and architecture. Section 5 and 6 present the two approaches of analysis, models and first results. In section 7 there are the conclusions.

2. GAS TURBINE MODULE

ICARO co generative plant is based on a small gas turbine (2 Mwe). The plant [1] is composed by two well distinguished modules (figure 1): a gas turbine module for producing electrical power and a module for extract heat from the turbine exhaust. The gas turbine module consists fundamentally of four main parts: the compressor, the combustion chamber, the turbine itself and the generator. The gas turbine is a single shaft engine. The rotor, which rotates at 22500 Rpm, is linked to a reduction gear for coupling with the generator. The compressor feeds air to the combustion chamber where the gas is also fed. Here, the combustion produces high pressure gases and high temperature. The content of NOx can be maintained inside the requested limits by a water injection to reduce the flame temperature. The expansion of these gases in the turbine produces the turbine rotation with a torque that is transmitted to the generator in order to produce the electrical power output. The air flow rate is constant and a control valve regulates the gas fuel in the combustion chamber. The control valve is actuated by the control system and a position sensor reads its position. The exhaust gas temperature, which is the most critical variable for the engine control system, is taken as an average of eight thermocouples, located along the circumference of the turbine exit. Among all variables that participate in the gas turbine only a few are directly measured by the sensors. From these sensors averages are taken by analog circuitry and are used, together with speed of turbine, to protect the engine.

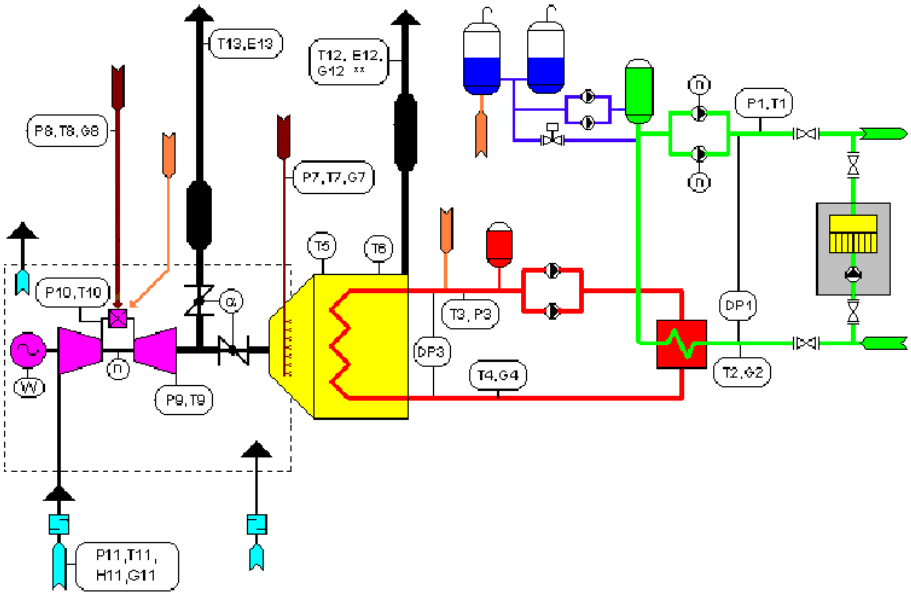


Figure 1 - ICARO plant schema

3. IEC 61508 STANDARD

Process industry requires that well defined safety requirements must be achieved, as hazards may be present in process installations. IEC 61508 introduces a principle referred to with the name As Low As Reasonably Practicable (ALARP). ALARP defines the tolerable risk as that risk where additional spending on risk reduction would be in disproportion to the actually obtainable reduction of risk. The strategy proposed by IEC 61508 takes into account both random as systematic errors, and gives emphasis not only to technical requirements, but also to the management of the safety activities for the whole safety lifecycle [2].

IEC 61508 has introduced the concept of Safety Integrity Level (SIL) attempting to homogenise the concept of safety requirements for the Safety Instrumented Systems. According to IEC 61508 the SIL is defined as *"one of 4 possible discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related systems. SIL 4 has the highest level of safety integrity, SIL 1 has the lowest"*.

The target dependability measures for the 4 SILs are specified in Table 1, for systems with low demand mode of operation and with continuous (or high demand) mode of operation. The determination of the appropriate SIL for a safety-related system is a difficult task, and is largely related to the experience and judgement of the team doing the job. IEC 61508 offers suitable criteria and guidelines for assigning the appropriate SIL as a function of the level of fault-tolerance and of the coverage of the diagnostic.

Table 1 - Safety Integrity Levels: Target Failure Measures

SAFETY INTEGRITY LEVEL	LOW DEMAND MODE OF OPERATION (Probability of failure to perform its design function on demand)	CONTINUOUS/HIGH DEMAND MODE OPERATION (Prob of a dangerous failure per hour)
4	$>=10^{-5}$ to $<10^{-4}$	$>=10^{-9}$ to $<10^{-8}$
3	$>=10^{-4}$ to $<10^{-3}$	$>=10^{-8}$ to $<10^{-7}$
2	$>=10^{-3}$ to $<10^{-2}$	$>=10^{-7}$ to $<10^{-6}$
1	$>=10^{-2}$ to $<10^{-1}$	$>=10^{-6}$ to $<10^{-5}$

4. GAS TURBINE CONTROL SYSTEM

Gas Turbine Control system performs both control functions and protection functions [3,4]. It also performs alarm monitoring and the communication functions, not considered in this paper.

4.1 Control functions

Control functions address the normal run operation and all plant sequencing needed in starting and stopping operations. In performing control function, the control system evolves throughout several states: from starting to no-load states, running on load and shutting down states. From such states shutdown requests override control logic and lead the system to the prior to start state. At any time a shutdown request will cause the control system to enter in its emergency shutdown state and carry out the shutdown actions which include the de-energisation of related relays. There are 79 possible shutdown requests.

The control functions are essentially based on the fuel metering valve position control and provide all the necessary control logic for position of the metering valve, with respect to a demanded fuel flow from the fuel demand control logic. The control valve is commanded by the control system and its position is read by a position sensor. The fuel demand control logic provides overrides for shutdown conditions. The fuel demands are limited by acceleration (maximum fuel) and deceleration (minimum fuel) schedules.

The scope of the analysis is limited to the control functions of the fuel metering valve position control in normal run operation. Figure 2 shows the simplified block diagram of fuel metering valve command, in normal run operation, with the variables that participate to the minimum/maximum selection: Speed governor, Power limiter, Exhaust temperature limiter.

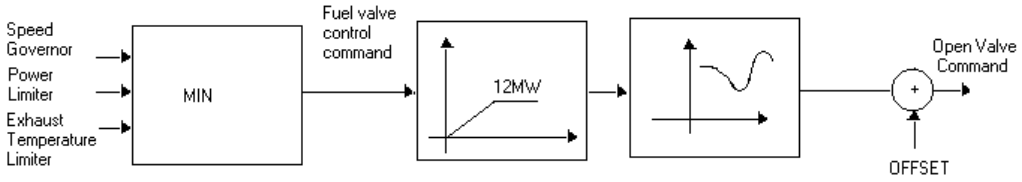


Figure 2 - Simplified block diagram of the fuel metering valve command

As an example, the control strategy of the fuel metering valve, limited to speed governor, is shown in figure 3. The gas turbine speed governor comprises a proportional plus integral control loop demanding a fuel demand control setpoint. The speed error is acted upon both the proportional control and the integral control loops and then summed to provide the final fuel demand into a fuel demand wins selector. Power limiter and Exhaust temperature limiter concur in the fuel metering valve control in a similar way.

4.2 Protection functions

Protection functions simply consist in providing the engine protection by independent overtemperature and overspeed shutdown.

Two thermocouple sensors are used, together with one speed probe as inputs of the protection functions.

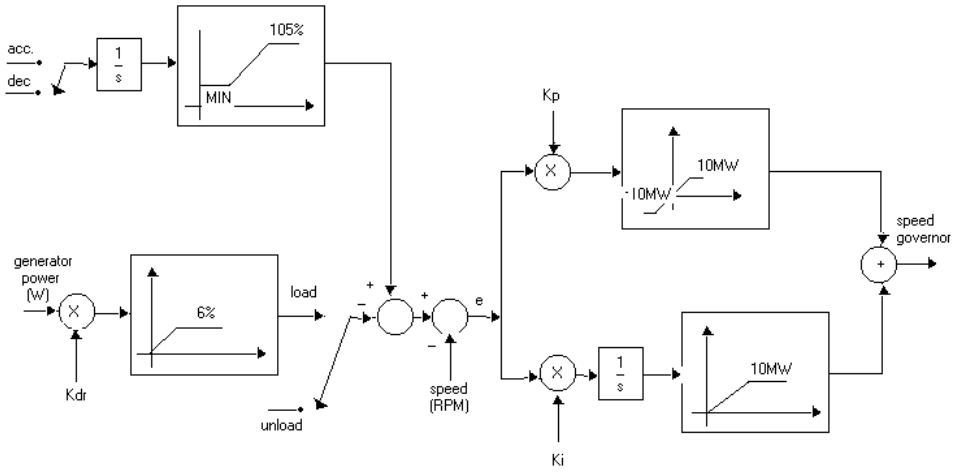


Figure 3 - Gas turbine speed governor

4.3 High level Architecture

Gas turbine control system (figure 4) comprises a Main Controller, which implements the control functions, and a Backup Unit, which implements the protection functions. The Main Controller and the Backup Unit have separate processors and independent power supplies so that the Backup Unit is able to provide independent protection functions. The Main Controller occupies two boards in full: the Baseboard and the Expansion Board, and a portion of the Auxiliary Board that is shared with the Backup Unit. In the Baseboard is located a processor performing the main control functions. The Expansion board provides an additional intelligent I/O Capacity. The Backup Unit occupies one other portion of the Auxiliary Board on which an independent processor performs the protection functions. Main Controller and Backup Unit are composed by the following components: Digital Input, Analog to Digital Converter, Processing Unit, RAM, EPROM, EEPROM, Digital Output, Digital to Analog Converter. Shutdown requests can be generated both from Main controller and Backup Unit: *Shutdown on hardware failures* related to CJC Failure, RAM Failure, EPROM failure, EEPROM Failure, Analog to Digital Converter (ADC) Failure, and *Shutdown on software failures*, a watch dog signal is driven by software via a triggerable monostable every 12.48 msec, if the software fails to trigger the monostable then the relay will be de-energised (Processing timeout). Moreover, for *The Main Controller,* the sensors and the actuators, reported in figure 4, are limited to the ones needed to perform the fuel demand control logic at run state. On such sensor/actuator failures, the Main Controller can perform shutdown requests: *Shutdown on failures of sensors/actuators* (Sensors: Loss of dual Engine Speed signals, Loss of fuel valve feedback signal, Loss of control Exhaust Temperature signals; Actuators: Fuel Metering Valve Actuator failure). The *Backup Unit* shares, through isolation, the following signals with the Main Controller: two Input Thermocouples and one Speed Engine signal. The Backup Unit implements the protection functions of the turbine by providing an independent overtemperature and overspeed shutdown. Figure 5 shows the overtemperature and overspeed shutdown conditions.

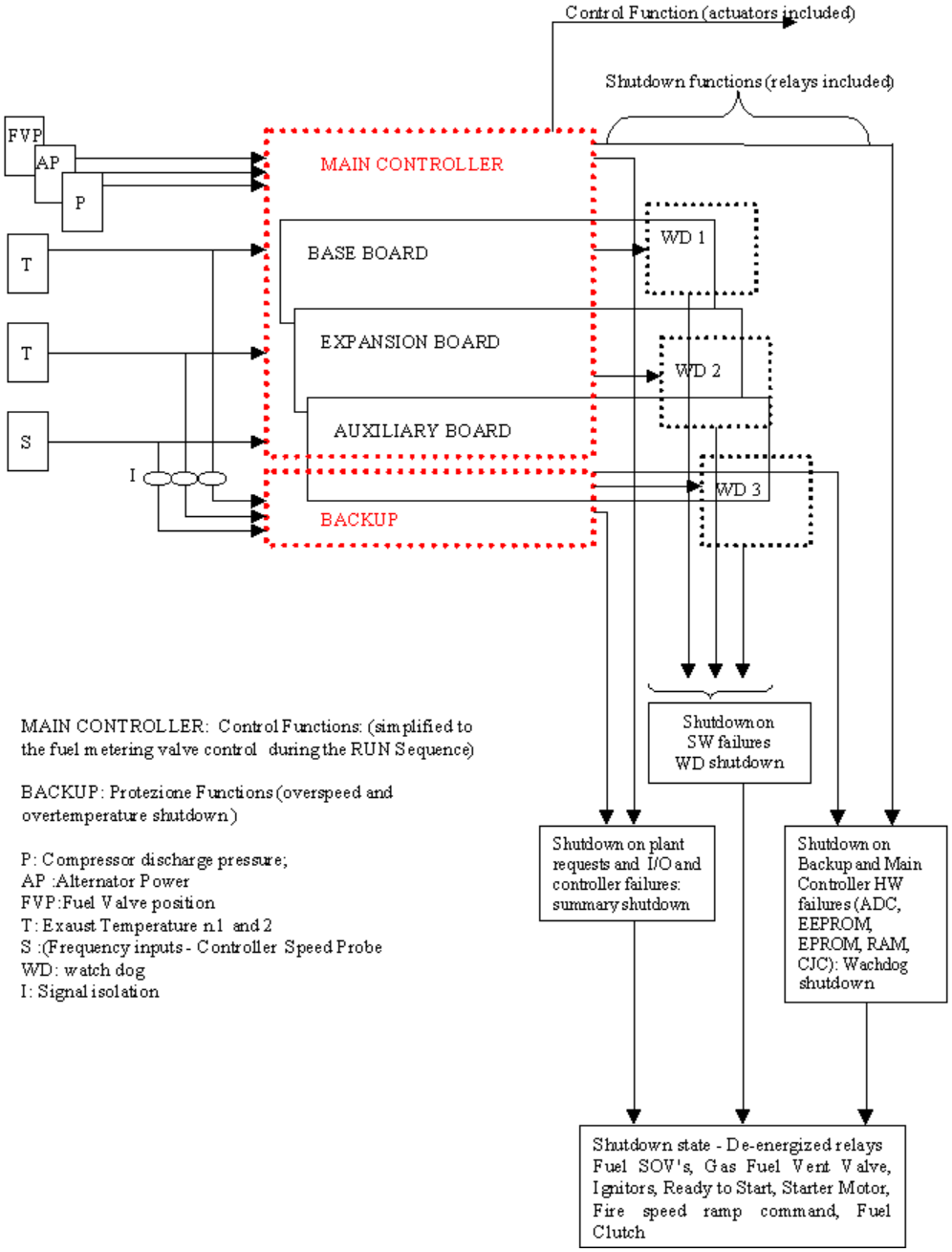


Figure 4 - High level architecture of the Gas Turbine Control System

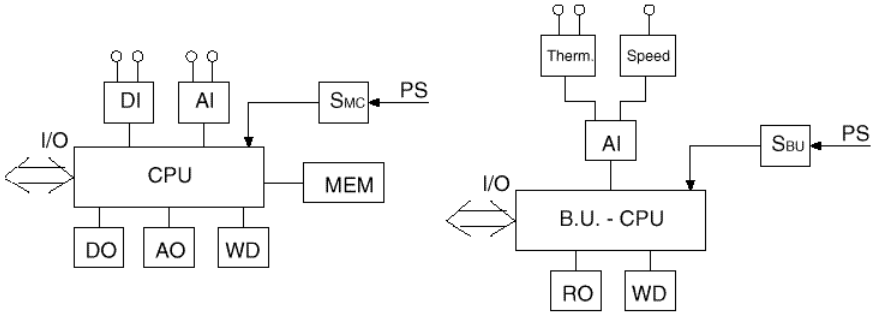
overtemperature shutdown: (failure of both thermocouples) **or** (enginespeed < 50% of full speed **and** exhaust temperature > 560 °C **and** exhaust temperature time > 100 msec) **or** (enginespeed >= 50% of fullspeed **and** exhaust temperature > 560 °C for time >100 msec)

overspeed shutdown: (exhaust temperature > 450 °C **and** enginespeed < 5% of fullspeed **and** Engine speed time > 1 sec) **or** (enginespeed > 110% of full speed **and** Engine speed time > 0 msec)

Figure 5 - The overtemperature and the overspeed shutdown conditions

5. PROBABILISTIC APPROACH

The hardware structure of the control system has been summarised as composed by two subsystems (figure 6), representing the Main Controller that provides control and shut-down functions and the Back-Up unit that provides protection function with respect to the only two critical events of overspeed and overtemperature Each unit has an independent CPU, uses a separate power supply circuit (operating from the same supply inlet) but shares the following transducer signals: 2 thermocouples and 1 speed probe. "Watchdog" relays are associated to each hardware circuit board.



DI - Digital input; AI - Analog input; DO - Digital output; PS - Power Supply inlet;
CPU - 32-bit microprocessor; AO - Analog input; S_{MC} - Supply circuit of the main controller.
MEM - Memory; WD - Watchdog relay; RO - Relay output.
I/O - I/O bus;

Figure 6 - Main Controller and Backup Unit hardware structure

Different techniques, with different levels of modelling power and analytical tractability can be used [5, 6] to characterise safety aspects of the gas turbine control system. As a first step, a Fault-Tree (FT), modelling system basic assumptions (i.e.independent stochastic activities and binary states), has been built. The elementary components of the gas turbine control system are assumed to have constant failure rates (table 2).

Table 2 - Component /Failure Rate (f/h)

Component	Failure rate (f/h)
Iobus	$\lambda_{IO}=2.0\ 10^{-9}$
Therm.	$\lambda_{Th}=2.0\ 10^{-9}$
Speed	$\lambda_{Sp}=2.0\ 10^{-9}$
Memory	$\lambda_{M}=5.0\ 10^{-8}$
DO	$\lambda_{DO}=2.5\ 10^{-7}$
AO	$\lambda_{AO}=2.5\ 10^{-7}$
RO	$\lambda_{RO}=2.5\ 10^{-7}$
DI	$\lambda_{DI}=3.0\ 10^{-7}$
AI	$\lambda_{AI}=3.0\ 10^{-7}$
PS	$\lambda_{PS}=3.0\ 10^{-7}$
S_{MC}	$\lambda_{Smc}=3.0\ 10^{-7}$
S_{BU}	$\lambda_{Sbu}=3.0\ 10^{-7}$
CPU	$\lambda_{CPU}=5.0\ 10^{-7}$
WD	$\lambda_{WD}=2.5\ 10^{-7}$

At the highest level of the analysis we adopt a Fault Tree model (figure 7).

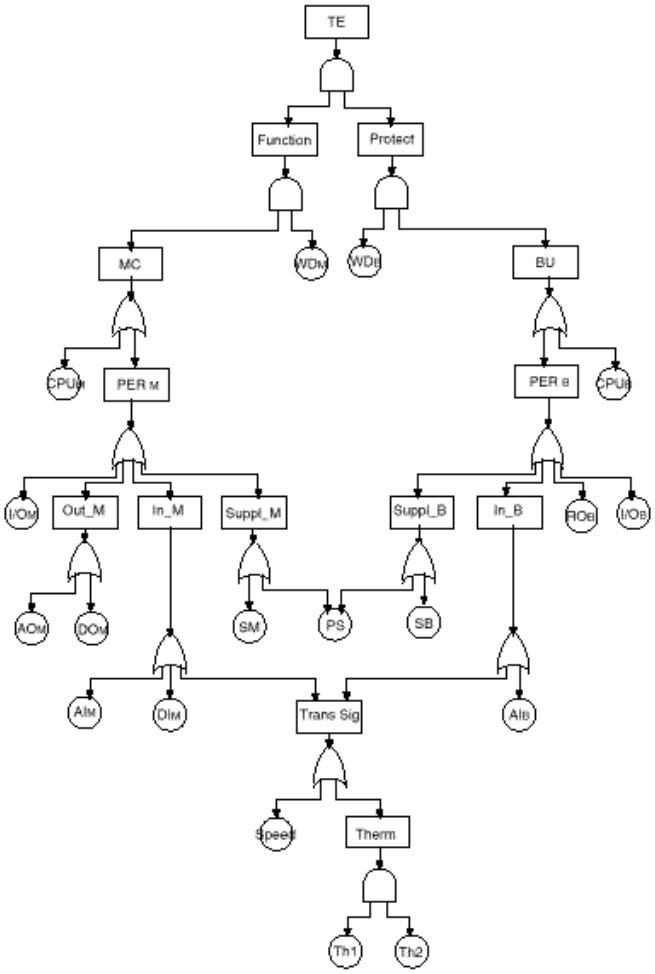


Figure 7 - Fault Tree model for safety critical failures

The fault tree analysis is based on the following simplifying assumptions: components (and the system) have binary behaviour (up or down) and failure events are statistically independent. Qualitative and quantitative analyses of the FT have been carried out. Qualitative analysis was aimed at enucleate the most critical failure paths. Quantitative analysis was aimed at evaluate measures useful to characterise safety. The qualitative analysis was carried on using the ASTRA tool [7]. The quantitative analysis was carried on using the SHARPE tool [8]. The following results have been obtained: order and number of *mcs* and criticality of the *mcs*. The analysis has found 43 mcs, with the characteristics given in the table 3. The most critical *mcs* sorted by order are shown in table 4.

Table 3 - Order and number of mcs

Order	Number of mcs	% on TE Unreliability
4	2	93.09
3	41	6.91

The following measures have been performed:

- Unreliability versus time;
- Safe Mission Time (SMT) computed as the time interval in which the system unreliability is strictly lower than a pre assigned threshold;
- Mean Time To Failure (that we consider a less significant measure with respect to SMT);
- Most critical failure paths;
- SIL evaluation limited to table 1 requirements.

Table 4 - Most critical mcs

	Minimal Cat Set
1	PS WDB WDM
2	CPUB CPUM WDB WDM
3	Speed WDB WDM
4	AIB CPUM WDB WDM
5	DIM CPUB WDB WDM
6	SupM CPUB WDB WDM
7	CPUM SupB WDB WDM
8	AIM CPUB WDB WDM

Unreliability versus time and failure frequency have been computed (table 5) for SIL evaluation according to IEC 61508. Comparing the results for the failure frequency of dangerous failures of the table (third column), and comparing t with the SIL Target Failure requirements (table 1), it is obtained SIL - 3 up to 500,000 h.
Fixing a limit for the Unreliability $U=1.0* 10^{-3}$, the Safe Mission Time is *SMT= 210.000 (h).*
The Mean Time To Failure for the Top Event is: $MTTF(for\ the\ TE) = 3.072 * 10^{6}\ (h)$

Table 5 - Unreliability versus time and failure frequency of dangerous failures

Time t (h)	TE Unreliability	Failure Frequency
10,000	$9.095\ 10^{-9}$	$9.095\ 10^{-13}$
50,000	$5.157\ 10^{-6}$	$1.031\ 10^{-10}$
100,000	$7.317\ 10^{-5}$	$7.317\ 10^{-10}$
150,000	$3.291\ 10^{-4}$	$2.194\ 10^{-9}$
200,000	$9.256\ 10^{-4}$	$4.128\ 10^{-9}$
250,000	$2.014\ 10^{-3}$	$8.056\ 10^{-9}$
300,000	$3.730\ 10^{-3}$	$1.243\ 10^{-8}$
350,000	$6.181\ 10^{-3}$	$1.766\ 10^{-8}$
400,000	$9.447\ 10^{-3}$	$2.372\ 10^{-8}$
450,000	$1.358\ 10^{-2}$	$3.018\ 10^{-8}$
500,000	$1.861\ 10^{-2}$	$3.722\ 10^{-8}$

6. DETERMINISTIC APPROACH

The deterministic approach is based on formulating the system model in terms of concurrently executing finite state machines, and the safety properties in terms of predicates in Computational Tree Logic. A finite state machine consists of a set of states (including the initial state), a set of input events, a set of output events, and a state transition function. Computation Tree Logic (CTL) is a branching-time temporal logic often used by model checking tools. CTL is designed for reasoning about properties of state-transition graphs, and is based on a system description in terms of a set of initial states and a transition relation. The approach to the identification of potentially hazardous paths is to check whether there exists a

path starting from an initial state and leading to a state in which an undesired situation holds (e.g. a requirement is not satisfied). We have selected the model checker SMV [9]. SMV uses CTL as its input language for specifications (requirements) and an automata based language to define the system to be verified.
The system we are considering consists of : a) the controller for the gas turbine together with its sensors (e.g. temperature sensors) and actuators (e.g. valves); b) the gas turbine itself (plant). Here there is a partial list of undesired situations which occurrence we want to inquiry using the deterministic models: overtemperature shutdown, overspeed shutdown, out of range values. We will refer to the *G*as *T*urbine *S*ystem (GTS), figure 8, limited to run sequence state.

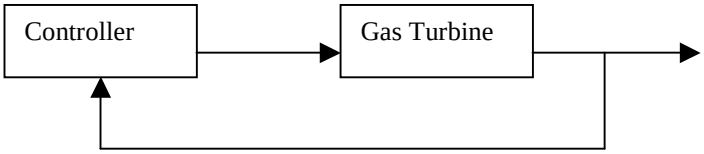


Figure 8 - The functional schema for GTS

GTS must satisfy many safety requirements. Typically such requirements can be stated by saying that certain undesired states are never reached. To answer this question we compute the set REACH of states that the system can reach starting from the initial state and then check if there is any state in REACH that violates any of the given requirements. In figure 9 is an example of a safety requirement for GTS. Such a requirement can be restated by saying that GTS should never reach a state in which the turbine speed is above 110% of full speed.

If the (turbine) speed is greater than or equal to 110% of full speed a shutdown occurs

Figure 9 - A requirement for GTS

Since shutdown are unwanted, the requirement in figure 9 asks the gas turbine control system to keep the turbine speed below 110% of full speed notwithstanding disturbances (e.g. variations in user electric load) or variations in system parameters (e.g. PI's gain).
Given admissible ranges of variations for disturbances and system parameters we can compute the set of reachable states (REACH) and check if any of such states violates any of the given requirements. This, in turn, allows to determine the (most liberal) admissible ranges of disturbances and system parameters that satisfy the given requirements. To carry out the procedure just outlined we need to model the gas turbine control system as well as the gas turbine module of the plant (equipment under control) [10]. We did this by using Finite State Automata (FSA) to model all the building blocks of our system. We used the tool SMV to carry out reachability analysis, that is to compute REACH. Note that using FSA means that we are using a discrete time modeling and state values are quantized to a finite set of values. The input language to SMV allows modeling of systems in an object oriented style. Thus each physical object is represented as an SMV module. In figure 10 we hint at our SMV modeling for a Proportional Integrative controller. Rather than using SMV syntax we just used standard (informal) mathematical notation to define transitions for the FSA modelling a

PI. The GTS model is obtained by gluing together all SMV modules describing the GTS subsystems. The requirement in figure 9 is defined in SMV as shown in figure 11.

```
MODULE PI (u(t), MIN_K, MAX_K, MIN_x, MAX_x, reset, reset_val)
-- u(t): input at time tx(t): state at time t-- reset: when reset  is true PI state reset at value reset_val
-- MIN_K: min PI gain,   MAX_K: max PI gain
-- MIN_x: min allowed value for state, below this underflow
-- MAX_x: max allowed value for state, above this overflow
VAR
-- x can take integer values in the range [0, 150] in this example
INIT
`` initial state: x(0) = MIN_x''
-- TRANS defines possible legal transitions (moves) for PI
TRANS
-``no reset and u(t) >= 0 and overflow and x(t + 1) = MAX_x''
``or''
-``no reset and u(t) >= 0 and no overflow and
x(t) + MIN_K*u(t) <= x(t + 1) <= x(t) + MAX_K*u(t)''
``or''
-``no reset and u(t) < 0 and no underflow and
x(t) + MAX_K*u(t) <= x(t + 1) <= x(t) + MIN_K*u(t)''
``or''
`` no reset and u(t) < 0 and underflow and x(t + 1) = MIN_x''
``or''
-``reset and x(t + 1) = reset  val ''
```

Figure 10 - Model of a Proportional Integrative controller

The output of SMV can be YES when the requirement is satisfied or a counter example (a possible system evolution) when the requirement is not satisfied. Currently we have a preliminary version of the model for GTS and have formalized some of the requirements. More work is needed on the model in order to avoid state explosion. Also formalization of requirements is to be completed. At the end of our work we expect a (formal) model of GTS, a set of formal requirements and a corresponding set of SMV runs showing the requirements met by GTS and giving counterexamples for the requirements that are not met by GTS.

```
SPEC
--For all computation paths (system evolutions),
--   speed < 110*MAX_SPEED
AG (speed <= ((110*MAX_SPEED)/10))
```

Figure 11 - GTK requirement in SMV language

7. CONCLUSIONS

To evaluate safety of the Gas Turbine Control System considering both the control and protection strategy is not a trivial matter. In fact, the modelling efforts have to take into account the failure process of sensors and actuators, of hardware and software components of the system, and the timeout conditions. Each of the above events and their combination could

lead to undesired (i.e. hazardous) conditions which occurrences need to be evaluated. Two complementary and integrable approaches, a probabilistic one and a deterministic one, have been used. The probabilistic approach has mainly focused on the safety aspects, modelling the combined effect of the main controller and the backup unit devoted to execute a protective shutdown with respect to two critical parameters: the temperature and rotational speed. Some modelling and analysis problems, related to the use of a combinatorial technique like the FT, have been evidenced. Also for the gas turbine control system SIL evaluation according to IEC 61508 has been performed on simplified basic assumptions. Other more sophisticated modelling assumptions, such as dependencies among stochastic activities of the system, diagnostic and repair activities and the coexistence of deterministic time with stochastic activities, needed to model the actual system could be taken into account in a second step [5,6]. The deterministic approach, consisting in Reachability Analysis by Model Checking, appears to be feasible for plants like ICARO. This is cost and time effective versus manual analysis and offers a better quality of analysis in terms of quite precise bounds on critical parameters and disturbances. Counterexample sequences, other than safety evaluations, can also be used as input for simulation and/or training.
The final aim of the research is to explore an innovative method which will put the probabilistic and deterministic approaches in a strong relation, using the results of the deterministic approach to feed the probabilistic one. That could allow to partially overcome the drawbacks of their isolated, selective and fragmented use, which can lead to inconsistencies in the evaluation results of safety analysis.

9. References

[1] P. Incalcaterra - Impianto di cogenerazione del centro ricerche Casaccia dell'ENEA- Rapporto interno ENEA- 18 gennaio 1999

[2] S. Bologna - Safety applications of programmable electronic systems in the process industry: impact of emerging standards -16th International System Conference, Seattle, Washington, USA - Sept. 14-18, 1998

[3] System manual of gas turbine governor controller of ICARO plant - September1992

[4] Hardware and Software design specification for a controller of ICARO plant gas turbine - October 1997

[5] A. Bobbio, E. Ciancamerla, M. Minichino, L. Portinale, M. Sereno - Comparing different methodologies of Probabilistic Structured Modelling by the analysis of typical industrial dependable systems - CENELEC WGA10 Workshop: Bridging the Gap to Railway Interoperability Systematic Approach to Safety Integrity – Munich, Germany - May 11, 1999

[6] A. Bobbio, L. Portinale, M. Minichino, E. Ciancamerla - Improving the Analysis of Dependable Systems by Mapping Fault Trees into Bayesian Networks- Reliability Engineering and System Safety Journal - vol. 71 N.3 March 2001 pages 249-260 -ISSN 0951 - 8320

[7] S. Contini - ASTRA, Adavanced Software Toolset for System Dependability Analysis - Joint Research Centre - Ispra (VA), Italy

[8] R. Sahner, K. S. Trivedi, A. Puliafito - "Performance and Reliability Analysis of Computer Systems: An Example-based Approach Using the SHARPE Software Package", Kluwer Academic Publisher, 1996

[9] K.L. McMillan -Symbolic Model Checking: An Approach to the State Explosion Problem - Kluwer Academic Publishers, 1993

[10] H. Valisuo - Model based reasoning and control of process plants - VTT Publications 178, ISBN 951-38-4416-1, 1994