Diagnostics and Fault Tolerant Sensor Architectures

M. Catelani, L. Ciani, M. Venzi
Department of Information Engineering, University of Florence, via S.Marta 3, Florence (Italy)
E-mail: lorenzo.ciani@unifi.it

Abstract. The focus on diagnostic and fault tolerant architectures is an important subject of the reliability analysis, especially in Oil&Gas application. This paper proposes a new approach for redundant configuration that guarantee the maximum productivity and minimize the possible equipment down-time due to an item failure. Sensors, transmitters and indicators used in this manufacturing field could be connected in 2DA or 3DA redundant configuration in order to obtain this scope.

1. Introduction
Nowadays diagnostics is an essential part of manufacturing performance requirements, and it plays a fundamental role in all modern industrial process. The recent diagnostic techniques are mandatory in several industrial fields, in particular for Oil&Gas applications where products are forced to endure extreme process and environmental conditions. With the introduction of fault diagnosis the designers are allowed to improve standard scheduled maintenance methods based on planned actions and severe timetables: thanks to diagnostics both corrective and predictive maintenance procedures can be put onto practice [1-4].

2. 2DA and 3DA architectures
Redundant architectures and fault diagnosis are key issues in Oil&Gas applications [5-6]. Two new architectures have been developed for this application in order to combine redundancy and diagnostic in the same configuration. 2DA and 3DA architectures differ only for the number of devices involved (two or three respectively). The designer is able to choose the type of redundancy for these new configurations, for example the 3DA architectures could be designed with only one sensor necessary to work (1oo3), with two sensors necessary to work (2oo3) or, in some particular application, with all the sensors necessary to work (3oo3) [7-8].

2DA architecture with on-board diagnostics (see figure 1) is based on two signals: the process measurement and a dedicated boolean variable “unhealthy”. The measurement assumes values inside the 4-20mA range, otherwise it is considered out-of-range. The “UNHEALTHY” signal assumes two values, false or true, and it communicates sensor status (working or fault respectively) to the central processing unit, in some applications called logic solver (table 1).

Table 1. Sensor status accordingly to unhealthy and out-of-range signals

| UNHEALTHY | OUT OF RANGE | STATUS |
|-----------|--------------|--------|
| FALSE     | FALSE        | OK     |
| FALSE     | TRUE         | FAIL   |
| TRUE      | FALSE        | FAIL   |
| TRUE      | TRUE         | FAIL ALL |


The logic solver calculates average, maximum or minimum of the measurements received from field sensors depending on the values assumed by AVGSEL (average) and MAX (maximum) pins. Furthermore, LS checks the spread between the two measurements (Spread=|In1-In2|): “high spread” is a boolean variable that is true in case the difference between input signals exceeds a fixed threshold. High spread signal is “ND – not defined” in case the measurements are not valid and the spread is not achievable. “Default” status produces a pre-set output in case both measurements are not trustworthy.

2DA logic may be used in either 1oo2 or 2oo2 architecture depending on the number of sensors required by the control panel to execute the system functionality. Anyway out-of-range and drift are the most common failure modes of field sensors. Drift is a gradual and incremental signal trend towards the upper (or lower) limit of operative range; in absence of on-board diagnostics and corresponding HEALTY/UNHEALTY signal (only OUT OF RANGE is provided), control logic cannot be aware of failure occurrence until device output goes out of range. Drift can occur very slowly and that period of time is rather critical because control logic is using wrong values coming from a faulty sensor. Obviously drift is more critical in case it develops moving away from the monitored threshold.

3DA architecture with on-board diagnostics is based on three sensors (figure 2); “UNHEALTHY” and “OUT OF RANGE” signals, mode of operation and measurement management are the same used in 2DA. The mode of operation of 3DA architecture without on-board diagnostics is the same of 2DA without diagnostics: in fact both out of calibration and stack in-range are undetectable and in absence of on-board diagnostics only “OUT OF RANGE” signal is provided so control logic cannot be aware of failure occurrence until device output goes out of range.

3. Case study
In order to test and validate the potentiality of 3DA architecture, a case study on a mineral lube oil console has been analyzed. Figure 3 shows the reliability block diagram (RBD) of the system under test, highlighting the three Pressure Indicator Transmitters (PIT) connected in 3DA architecture.
Considering:

- $R_W(t)$ is the reliability of system without the 3 PIT, that is equivalent to consider the 3DA configuration fault free ($R(t)=1$);
- $R_S(t)$ 3DA 1oo3 is the reliability of the whole system considering 3DA in 1oo3 configuration.
- $R_S(t)$ 3DA 2oo3 is the reliability of the whole system considering 3DA in 2oo3 configuration.
- $R_S(t)$ 3DA 3oo3 is the reliability of the whole system considering 3DA in 3oo3 configuration.

Figure 4 illustrates the reliability trends of the three possible functional configurations of the 3DA architectures.

![Figure 4. Comparison between three PITs in 3DA 1oo3, 3DA 2oo3 and 3DA 3oo3 configuration](image)

Figure 4. Comparison between three PITs in 3DA 1oo3, 3DA 2oo3 and 3DA 3oo3 configuration

Figure 5 shows the reliability trends of the mineral lube oil console, during a 20 years time interval, while figure 6 shows the same trends in a smaller time interval, between 20000h and 40000h. In spite of the mineral lube oil console is a very complex system (as it is possible to see in figure 3), the system reliability is highly influenced by the minimum number of working sensors required to the system functionality (1oo3, 2oo3 or 3oo3).

![Figure 5. Mineral lube oil console reliability](image)

Figure 5. Mineral lube oil console reliability

Considering the reliability point of view, the worst configuration is the 3DA 3oo3: it requires all the sensors working simultaneously. Indeed, the best choice is the 3DA 1oo3 architecture, that requires only
one sensor working. Devices in 3DA 3oo3 configuration reduce the reliability more than the others, and cause several plant interruptions. Therefore, the use of this kind of diagnostic configurations, must be related to the design issue and preliminary and safety requirements.

![Figure 6. Mineral lube oil console reliability (20000h -40000h time interval)](image)

4. Conclusions
For this paper, the 2DA and 3DA architectures have been developed to improve system performances in Oil&Gas plants. In particular, these architectures can be connected in several ways, based on the number of elements (generally sensors) necessary to work, that influence the reliability of these architectures. The analysis shows that the 3DA 1oo3 is the best solution in order to optimize the system reliability. Anyway some particular applications require more sensors to work, therefore 3DA 2oo3 and 3DA 3oo3 could be used.

References
[1] M. Catelani, L. Ciani, M. Venzi 2017 Logic Solver Diagnostics in Safety Applications Proc of 15th IMEKO TC10 Workshop on Technical Diagnostics Technical Diagnostics in Cyber-Physical Era, Budapest, Hungary, June 6-7
[2] M. Catelani, L. Ciani, M. Venzi, 2015 Sensitivity analysis with MC simulation for the failure rate evaluation and reliability assessment Measurement 74 150-158
[3] M. Catelani, L. Ciani, V. Luongo, R. Singuvali 2010 Evaluation of the Safe Failure Fraction for an electromechanical complex system: remarks about the standard IEC61508 Proc. of IEEE Instrumentation & Measurement Technology Conference (I2MTC), Minneapolis, MN, 2013, pp. 686-690
[5] Y. Zhang, C. Bingham, Z. Yang, B. Ling, M. Gallimore 2014 Machine fault detection by signal denoising—with application to industrial gas turbines Measurement 58 230-240
[6] Z. Yang, B. Ling, C. Bingham 2013 Fault detection and signal reconstruction for increasing operational availability of industrial gas turbines Measurement 46 1938-1946
[7] MIL-HDBK-338B 1998 Electronic Reliability Design Handbook U.S. Department of Defense Washington DC
[8] IEC 61078 2017 Reliability block diagrams International Electrotechnical Commission