New concept of safeprocess based on a fault detection methodology: Super Alarms

J.W. Vásquez * **G. Pérez-Zuñiga** ** **J. Sotomayor-Moriano** **
Y. Muñoz *** **A. Ospino** ****

* *GPS, Universidad de Investigación y Desarrollo - UDI,*
Bucaramanga, Colombia (e-mail: jvasquez@udi.edu.co).
** *Engineering Department, Pontificia Universidad Católica del Perú -*
PUPC, Lima, Perú (e-mail: gustavo.perez@pucp.pe,
jsotom@pucp.edu.pe)
*** *GIRES, Universidad Autonoma de Bucaramanga - UNAB,*
Bucaramanga, Colombia (e-mail: ymunoz294@unab.edu.co)
**** *GIOPEN, Universidad de la Costa - CUC, Barranquilla, Colombia*
(e-mail: aospino8@cuc.edu.co)

Abstract: Industrial plants, especially on mining, metal processing, energy and chemical/petrochemical processes require integrated management of all the events that may cause accidents and translate into alarms. Process alarm management can be formulated as an event-based pattern recognition problem in which temporal patterns are used to characterize different typical situations, particularly at startup and shutdown stages. In this paper, a new layer based on a diagnosis process is proposed over the typical layers of protection in industrial processes. Considering the alarms and the actions of the standard operating procedure as discrete events, the diagnosis step relies on situation recognition to provide the operators with relevant information about the failures inducing the alarm flow. The new concept of super alarms is based on a methodology with a diagnosis step that permits generate these types of superior alarms. For example, the Chronicle Based Alarm Management (CBAM) methodology involves different techniques to take the hybrid aspect and the standard operational procedures of the concerned processes into account.

© 2019, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.

Keywords: alarm management, protection layers, safeprocess, diagnosis, super alarms

1. INTRODUCTION

Integrated management of the critical factors in the process ensures an optimum reliability level in the industrial plants (Habibi and Hollifiled, 2006). Factors such as the control of the process variables, procedures, and steps followed in transitional stages try to keep the plants within the operating established "limits" (Garcia et al., 2012). While, on starting or shutdown procedures, the quantity of signals increases, the plant safety needs to involve integrated management of those factors analyzing the causes of the accidents. In other words, these factors must be managed together, and not separately, because if any of them is left outside, unattended or decreased, the security would be threatened (Agudelo, 2015), (Rodrigo et al., 2016). The critical factors of the process work that must be managed together are: facilities safely, control of process variables, safe behaviors, and valid procedures. Safety requirements and the increasing efficiency in monitoring, control, and management of complex systems motivate great interest and efforts devoted to the development of fault detection and isolation techniques. Many popular approaches are available for identifying faults. Among them, methods based on signals are widely used and try to extract useful information from the analysis of specific signals through a comprehensive and rigorous analysis of the main sta-

tistical methods used to detect changes (Magni et al., 2000),(Hollender et al., 2016). The model-based methods, like parity or space-based approaches observers (Patton and Chen, 1997), used a mathematical model of the plant to explore the implicit analytical redundancy relations model to monitor inconsistencies between the model and data measured. However, these methods suggest a big demanding of computational load. Other popular methods as those based on fault trees (Vries, 1990) or causal graphs and propagation (Yang and Xiao, 2012) were based on a qualitative model of the plant. Other approaches have been developed by expert systems based on artificial intelligence techniques (Sarmiento and Isaza, 2012). On the other hand, hierarchical clustering methods were used to carry out pattern matching correlation (Chen and Lee, 2011) in which some frequent patterns multiple alarm correlation may be discovered to have the ability to reflect the sequence of normal operation. Any change in the pattern may indicate abnormal alterations, sensor degradation or malfunctions. Meanwhile, Professor Ali Zolghadri expressed on his conference that currently there is a valley of the death between the diagnosis theory and the industrial process applications (ICONS 2016, Reims France).This raises the need not only of a diagnosis system that helps to maintain safe the process increasing the availability of the installation but also of new alarm management methodolo-
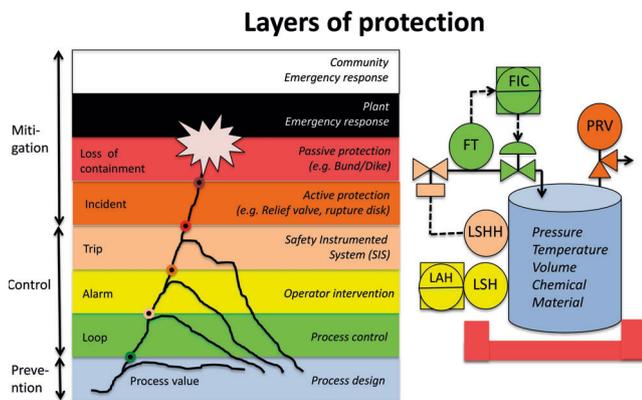
Layers of protection

Fig. 1. Safety layers of protection

gies (Vásquez et al., 2013). Industrial plant safety involves the integrated management of all the factors that may cause accidents. Hence alarm management is one aspect of great interest in safety planning for different plants. This article is divided into 5 sections. Section 1 presents the introduction, in Section 2 is a specified description of the traditional layers of protection in an industrial process and the principal concepts of alarm management. Section 3 presents the super alarms, as a new layer of protection. Section 4 indicates the CBAM methodology with a case study. Section 5 corresponds to conclusions and future work.

2. SAFEGUARDS AND ALARMS

In a safe process, a safeguard executes a protection function from the use of hardware, software or human action (through standard procedures or safe practices). These functions must be efficient, this means that it can be able to reduce the probability of occurrence of one risk scenario with its consequences.

2.1 Layers of protection

The operation of many industrial processes, especially in the mineral, energy and petrochemical sector, involves inherent risks due to the presence of dangerous materials like gases and chemicals; which in some conditions can cause emergencies. In these types of industrial processes, safety is supplied by layers of protection.

Layer 1: Process Design (e.g., inherently safer designs). This layer corresponds to the design of the process, for example, the size of the tanks, valves, pipes. In Fig. 1 is presented the tank in cadet blue color as one element of protection in this layer.

Layer 2: Basic controls, process alarms, and operator supervision. A basic process control system (BPCS) is a system that responds to input signals from the process and its associated equipment, other programmable systems, and/or from an operator, and generates output signals causing the process and its associated equipment to operate in the desired manner and within normal production limits (Process Safety Glossary). This layer includes the control elements such as PLCs, industrial controllers, control valves, industrial instrumentation, motors, regulators. In Fig. 1 is presented with the green color elements that

maintain the process variable under control (FT, FIC). In this case, the flow control valve regulates the level in the tank.

Layer 3: Critical alarms, operator supervision, and manual intervention. In this layer, we can find the HMI (Human Machine Interface) and supervisory systems that present to the operator the alarms configured on the system. Always that one alarm occurs, it requires the intervention of the operator, and when flood alarms occur many accidents can happen. Alarm management is an important aspect to have in count currently and it will be described in this section. In Fig. 1 the elements related to this layer are with the color yellow. The level switch of high LSH activates the level alarm of high LAH. The alarms always are assumed as independent variables that not be processed after that they happen, furthermore in many cases, the operator does not check these alarms because for the operators is normally that some alarms occur.

Layer 4: Automatic action (e.g. SIS or ESD); A Safety Instrumented System (SIS) is a new term used in the standards that also has been known by the majority as Emergency stop system (ESD), system of safety stop, the system of interlocks, emergency firing system or security systems. It could also be defined as the ultimate preventive security layer if the control system and operator performance are insufficient. In this case, must exist a system that automatically takes the appropriate actions (partial or total stops of equipment and plants) in order to avoid the risk. These safety instrumented systems are normally separate and independent from control systems, including logic, sensors, and valves on the field. Unlike control systems, which are active and dynamic. SIS is basically passive and "sleepy", it means that the elements of an SIS do not execute some action until a process variable increase without control, so they usually require a high degree of safety and fault diagnosis, as well as to prevent inadvertent changes and manipulations and good maintenance (Fernandez et al., 2012). Therefore, to involve fault diagnosis methodologies is one important aspect of process safety that needs to be developed continuously.

Layer 5: Physical protection (e.g. relief devices); Physical protections on an industrial process include relief devices that are used to reduce the impact of a catastrophic failure of equipment and/or minimize the effects of any unanticipated or uncontrolled events. These relief devices are used as emergency devices and they are not used for normal process control.

Layer 6: Physical protection (e.g. dikes); An area shut-in by contours of concrete or a physical barrier that could contain oil, fuel, water or any liquid is defined as a diked area. The flammable liquid storage area could be a number of tanks within a common diked area.

Layer 7: Plant emergency response. Through planning, preparation, mitigation, response and recovery in the face of emergencies and disasters, direct and indirect consequences are expected to be increasingly weak. A plant emergency response seeks to eliminate/diminish vulnerable to threats, through the necessary measures that guarantee the survival of those involved directly or indirectly

and the reduction of costs for damage to furniture, and equipment.

Layer 8: Community emergency response. Nowadays the concept of emergency management refers to the rational process by which society prepares to deal with the consequences associated with natural events or events created by the man. Emergency management includes the following four phases: preparation (before), mitigation (before and after), response (during) and recovery (after).

2.2 Alarm management

Alarm management is an important aspect of the safety of industrial processes. In years past (60's, the 70's) the integration of a new alarm on the systems had a high cost and required a careful study and analysis before deploying. Each alarm had to be wired given the limited space on the panels of the control room. Today, advances in hardware and software have made possible the implementation of alarms at a minimum cost, without limits of space and with less review. Therefore, in many cases, unnecessary alarms arise. Due to this, an important advance has been the appearance of alarm systems, in which alarms are installed and configured considering the number of existing signals (analog and discrete) and the rate of alarms that an operator can respond efficiently. Alarm systems can induce many alarms that cannot be evaluated by the operator which is a serious threat to the safety of the process. Therefore, now, the question is: *Which alarms can be ignored without compromising the integrity of the process?* This at the extreme can lead to sub-alarm systems, which is as bad as having a system over-alarmed (Palomeque, 2005). Alarm management systems must deal with two main difficulties: A very high rate of alarms, and a lack of criteria for assigning the priority of an alarm. The alarming rate indicates the load that produces the alarm system to the operator. If the operator is supposed to respond to all alarms, the system must not produce more alarms that the operator can respond effectively. The most important factors that affect the rate of alarms are The number of alarms settled, the deadband analog alarms (pressure, temperature, flow, level, etc.), the analog alarm limits and the alarms packages equipment (compressors, furnaces, etc.). Summarizing, the fundamental purpose of an *alarm* is to alert the operator of deviations in the process variables from normal operating conditions, i.e. abnormal operating situations. ISA-18.2 defines an alarm as *"An audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response"*. This means that an alarm is more than a message or an event; an alarm indicates a condition requiring the operator's attention towards plant conditions requiring timely assessment or action.

3. SUPER ALARM

Diagnosis in industrial processes corresponds to the procedures, activities, and tools that help operators to recognize the real plant situation, especially at transitional stages in which increases the risk of accidents. In terms of process safety, the principal characteristics of a good protective barrier are specificity, independence, reliability, and audit.
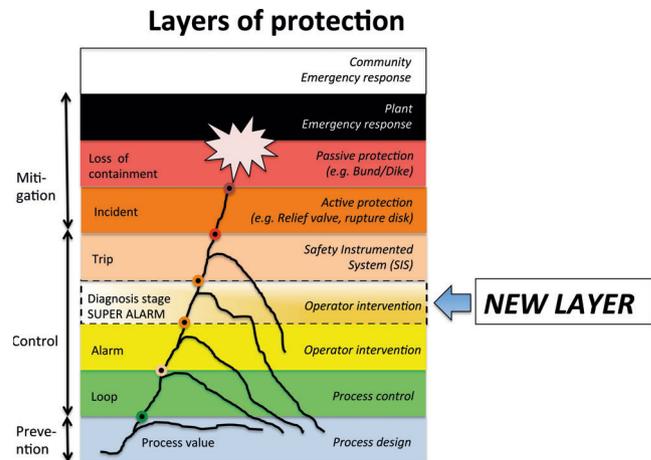

Fig. 2. "Super alarm" layer of protection

Specificity: Barrier capable of detecting and preventing or mitigating consequences of a potentially dangerous specific event (e.g. explosion). Independence: A barrier is independent of all other layers which are associated with the potentially dangerous event, when: There is no potential for common cause failures. And the protection layer is independent of the initiating event. Reliability: The protection provided by the barrier reduces the risk identified by a specific and known quantity. Determined by its probability of failure. Audit: A barrier must be designed to allow inspections and periodic and regular testing of the protection function.

This article proposes a new protection barrier between the layer "Alarm" and the layer "Trip"(SIS), see Figure 2. One additional layer of protection could reduce the accident probability helping the operators to take better decisions when alarm floods happen. It has been demonstrated that advanced diagnostic systems for industrial processes together with the interventions of the operators may constitute an additional protective safety layer. However, these new elements seem that never had been included as a layer of protection because diagnostic systems for industrial processes are not yet extensive in practical tools (Koscielny and Bartys, 2015). The new barrier comes from a diagnosis process and it is **specific** because is capable of to detect and to prevent dangerous situations. This new barrier is **independent** because its functionality does not depend on the other elements, if some of the signals involved in the diagnosis tool fail, this new tool could detect it. The **reliability** of this barrier is determined by the reduction of a large number of alarms avoided by the operators. And finally, this new protection layer can be **auditable** because the diagnosis tools permit its revision from a methodology that includes simulations of scenarios checking the response. The concept of super alarm corresponds to a new alert to the operators resulted from a diagnosis procedure representing a "superior" alarm. Consequently, in automatic control systems, the supervision functions serve to indicate undesirable or not permitted processes states and take appropriate actions that maintain performance and avoid damage or harm states. From supervision we can discriminate the following functions: **Monitoring**: The measurable variables are checked to respect their tolerances and alarms are generated to alert the operators. **Supervision**: Supervision with fault diagnostic: This action

is developed from the analysis of the measurable variables detecting the symptoms of a possible failure (Astolfi and Praly, 2006), (Lew et al., 1994). **Automatic protection**: Actions for counteract the possible damages. A system is said to be diagnosable if whatever the behavior of the system, we will be able to determine without ambiguity a unique diagnosis. When a super alarm is generated, the supervisory and control system can provoke automatic control actions in addition to the alerts to the operators. The diagnosability of a system is generally computed from its model (Bayoudh et al., 2006), and in applications using model-based diagnosis, such a model is already present and does not need to be built from scratch. The fault diagnosis in general consists in the following three important aspects: Fault detection: it consists in to discover the existence of faults in the most useful units in the process, Fault isolation: it is referred to localize (classified) the different faults, and Fault analysis or identification: it consists of determinate the type, degree and origin of the fault (Ding, 2008). Concluding, a super alarm corresponds to a new element resulted from a diagnosis process in which risk and hazard analysis are required. To design and construct super alarms in a supervisory system requires a methodology that gives us relevant information of the process according to the events and procedural actions that had occurred. In the next section, a methodology for generating super alarms is described.

4. CHRONICLE BASED ALARM MANAGEMENT

In process state transitions such as startup and shutdown stages, the alarm flood increases and it generates critical conditions in which the operator does not respond efficiently; moreover, it is commonly reported that 70% of plant incidents occur at startup or shutdown stages (Beebe et al., 2013). Due to this alarm flood, dynamic alarm management is required. Currently, many fault detection and diagnosis techniques for multimode processes have been proposed; however, these techniques cannot indicate fundamental faults in the basic alarm system (Zhu et al., 2013). On the other hand, the technical report Advance Alarm System Requirements EPRI (The Electric Power Research Institute) suggests both cause-consequence and event-based processing. Therefore, the operators need a tool that helps them recognize the plant situation, especially in the transitional stages such as startup and shutdown. In (Vásquez, 2017) was proposed to use *chronicles* to represent the plant situations under interest and to integrate a diagnosis step based on chronicle recognition in the global schema of alarm management. A chronicle is a set of events linked by relationships or temporal constraints and the occurrence of which will be subject to a certain context. Chronicles can also be expressed as constraint graphs where events are represented by nodes, and the time constraints are the labels of arcs. This approach of alarm management was called the *Chronicle Based Alarm Management* (CBAM). The principle of CBAM is to consider several process situations (normal or abnormal) during startup and shutdown stages and to model each of these situations through a learned chronicle. For this, given a situation one wants to model, an algorithm is fed by a set of event sequences issued from the process and associated with the situation. Then a super alarm can be generated giving to the operators relevant information assumed as
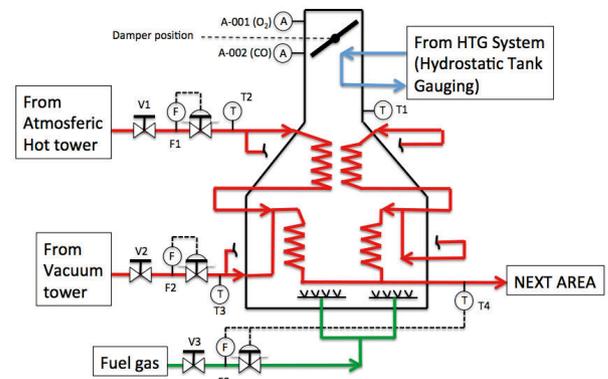

Fig. 3. Vacuum oven

a new layer of protection from which actions can reduce the accident occurrences because, in many situations of alarm flood, hazard scenarios happen. The global objective of CBAM is to generate a chronicle database on which a diagnosis process based on chronicle recognition is then performed, (Vasquez et al., 2015), (Vasquez et al., 2016).

The Chronicle Based Alarm Management (CBAM) relies then on three main steps resumed as below:

STEP 1: Event type identification: The aim is to determine the event types that define the chronicles. For this step, information from the standard operating procedures and from the evolution of the continuous variables are exploited.

STEP 2: Event sequence generation: From the expertise and an event abstraction procedure this step determines the date of occurrence of each event type for constructing the representative event sequences used by a learning algorithm. A representative event sequence is the set of event types with their dates of occurrence that can be associated with a specific scenario of the process. The representative event sequences are then verified using the hybrid modeling of the system and the hybrid causal graphs.

STEP 3: Chronicle database construction: For each scenario, the representative event sequences and temporal restrictions are given by experts are considered to learn chronicles. The set of chronicles learned for each scenario and each processing element constitutes the Chronicle database.

Case study - Vacuum oven

A case study from the Cartagena Refinery in Colombia is presented. This proposal aims at helping the operator (with super alarms) to recognize specific operations (i.e normal and/or faulty operation) during the startup and shutdown stages of the vacuum oven unit, see Figure 3. This section illustrates then the learning of the chronicle base that will be considered by a recognition system to recognize these normal or faulty situations when they occur, and the CBAM methodology is applied with its three steps: 1. *Event type identification*, 2. *Learning event sequences generation* and 3. *Construction of the chronicle database*, (Vasquez et al., 2017).

Event type identification: The set of event types E considered in the chronicles is defined by $E = \Sigma \cup \Sigma^c$ where:

- Σ is the set of procedural actions performed during standard operating procedures
- Σ^c is the set of event types associated to the behavior of the continuous variables .

Procedural actions concern mainly the valves of the oven and $\Sigma = \{V1, V2, V3, v1, v2, v3, M2A\}$. where $V1$ (resp. $V2, V3$) denotes the switch of the valve **V1** (resp. **V2**,**V3**) from closed to opened. $v1$ (resp $v2, v3$) the switch of the valve **V1** (resp. **V2**,**V3**) from opened to closed. The event $M2A$ corresponds to the change from *manual* to *automatic* operating, closing the control loops. In the reminder we assume that this event is the only unobservable event of the system i.e. $\Sigma_{uo} = \{M2A\}$.

Continuous variables are associated to the different flows ($F1$, $F2$, $F3$) and different temperatures ($T1$, $T2$, $T3$ and $T4$) (see Figure 3). For each evolution of a continuous variable (obtained by simulation) upper and lower bounds are defined from experience feedback. Then the continuous values of the variable are mapped to ranges defined by these limits. We propose to define three ranges: *High* when the value of the continuous variable is higher than the upper bound, *Medium* when the value is between the upper and lower bounds, and *Low* when the value is under the lower limit bound. Form this qualitative abstraction of the continuous variable evolution we consider that an event is generated each time a transition between qualitative domains (i.e ranges) occurs. So, for a continuous variable noted v_i four event types can be considered: L_{v_i} (resp. l_{v_i}) for a transition from the range L to the range M (resp. M to L). H_{v_i} (resp h_{v_i}) for a transition from the range M to the range H (resp. H to M) (Vasquez et al., 2016). For the vacuum oven, the set of event types associated with the behavior of the continuous variables is then defined by:

$$\Sigma^c = \begin{cases} L_{F1}, l_{F1}, H_{F1}, h_{F1}, L_{F2}, l_{F2}, H_{F2}, h_{F2}, L_{F3}, \\ l_{F3}, H_{F3}, h_{F3}, L_{T1}, l_{T1}, H_{T1}, h_{T1}, L_{T2}, l_{T2}, \\ H_{T2}, h_{T2}, L_{T3}, l_{T3}, H_{T3}, h_{T3}, L_{T4}, l_{T4}, H_{T4}, \\ h_{T4} \end{cases}$$

(1)

Learning event sequences generation: The learning event sequences are generated according to the behavior of the system in a given scenario (scenario of normal operating, faulty scenario with a fault on valve, etc...). In this section we consider a scenario of normal behavior during the start up of the oven. By simulation we have obtained three different event sequences (S_1, S_2 and S_3) all of them associated with the same scenario.

$S_1 = \langle (V3, 1), (L_{T1}, 3), (L_{F3}, 5), (V1, 6), (L_{T4}, 7),$
$(L_{F1}, 8), (H_{F1}, 12), (v1, 13), (V2, 14), (H_{T1}, 15),$
$(h_{F1}, 16), (L_{F2}, 17), (H_{T4}, 19), (H_{F2}, 22), (l_{F1}, 24),$
$(h_{T1}, 25), (h_{T4}, 26), (h_{F2}, 27), (V1, 42), (L_{F1}, 45) \rangle$

The two others sequences S_2 and S_3 are identical to S_1 in term of sequence of event types but differ to S_1 in term of event occurrence dates.

$S_2 = \langle (V3, 1), (L_{T1}, 7), (L_{F3}, 13), (V1, 18), (L_{T4}, 21),$
$(L_{F1}, 24), (H_{F1}, 32), (v1, 35), (V2, 37), (H_{T1}, 40),$
$(h_{F1}, 45), (L_{F2}, 48), (H_{T4}, 54), (H_{F2}, 61), (l_{F1}, 65),$
$(h_{T1}, 68), (h_{T4}, 72), (h_{F2}, 76), (V1, 96), (L_{F1}, 101) \rangle$

$S_3 = \langle (V3, 2), (L_{T1}, 6), (L_{F3}, 9), (V1, 12), (L_{T4}, 14),$
$(L_{F1}, 16), (H_{F1}, 22), (v1, 24), (V2, 25), (H_{T1}, 27),$
$(h_{F1}, 30), (L_{F2}, 32), (H_{T4}, 36), (H_{F2}, 41), (l_{F1}, 43),$
$(h_{T1}, 45), (h_{T4}, 48), (h_{F2}, 50), (V1, 68), (L_{F1}, 71) \rangle$

Construction of the chronicle database: A complex process (Pr) such the Cartagena Refinery is composed of $n \in N$ different units or areas $Pr = \{Ar_1, Ar_2, ...Ar_n\}$ where each area Ar_m, $m = 1, ..., n$ has $K \in N$ operational modes (e.g startup, shutdown ..) noted O_i, $i = 1, ..., K$. The process behavior in each operating mode can be either normal or faulty. We define the set of failure labels $\Delta_f = f_1, f_2, ..., f_r$ and the complete set of possible labels is $\Delta = N \cup \Delta_f$, here N means normal.

To monitor the process and to recognize the different situations (normal or faulty) of the operational modes, we propose to build a chronicle base for each area. For a given area, a learned chronicle C_{ij}^m is associated to each couple $(\mathcal{O}_i, l_j)$ where $l_j \in \Delta$:

$$CAr_m = \begin{array}{c} \\ O_1 \\ O_2 \\ ... \\ O_k \end{array} \begin{array}{cccccc} N & f_1 & f_2 \cdots & & f_r \\ \begin{bmatrix} C_{10}^m & C_{11}^m & C_{12}^m & \dots C_{1r}^m \\ C_{20}^m & C_{21}^m & C_{22}^m & \dots C_{2r}^m \\ \dots\dots\dots\dots\dots\dots\dots \\ C_{k0}^m & C_{k1}^m & C_{k2j}^m & \dots C_{kr}^m \end{bmatrix} \end{array}$$

(2)

When $l_j = N$, the chronicle is a model of the normal behavior of the considered system, otherwise ($l_j = f_i$) the chronicle is a model of the behavior of the system under the occurrence of the fault f_i. For the vacuum oven we have considered a normal startup, a normal shutdown and several faulty cases. For instance, a startup stage during which a fault occurs on the control valve **V3**. We present in this section only the chronicle C_{10}^2 learned from the input sequences S_1, S_2 and S_3 capturing a normal startup operating mode of the vacuum oven (area number 2 of the Cartagena Refinery). The output of the extended $HCDAM$ (Heuristic Chronicle Discovery Algorithm Modified) in this case is a chronicle that represents the behavior of the system taking as reference the representative event sequences obtained by simulation and the *temporal runs* obtained from the expertise knowledge. When an alarm flood happens and this chronicle is recognized, then one super alarm is generated informing the operators the final situation of the startup stage of this vacuum oven. The Heuristic Chronicle Discovery Algorithm Modified ($HCDAM$) uses representative event sequences and temporal runs to generate automatically the chronicles for the scenario that these elements (event sequences and temporal runs) represent (Vasquez et al., 2017).

5. CONCLUSION

A new layer of protection in the industrial process had been proposed. This new layer is called a super alarm which corresponds to a new alert to the operators resulted from a diagnosis procedure representing a "superior" alarm. Furthermore, a new methodology for alarm management of complex processes has been proposed to

generate super alarms. This methodology proposes a diagnosis process as a support to the operators during startup and shutdown stages based on situation recognition. Situations to recognize correspond to normal and/or abnormal process behaviors modeled by temporal patterns called *Chronicles*. Any additional protection layer that increases the reliability on the industrial process is well received because the risk of accidents and failures in which human lives are involved. Therefore, this proposal could increase the tools and components that help to the operators to detect early hazard situations and the risk analysis such as fault trees, bow tie, etc. can be used for construct models of failure scenarios in a supervision system. The future work will be related to the implementation of this new concept in industrial projects (energy, chemical, mining) and validate the model of chronicles guaranteeing the reliability of the diagnosis tool.

REFERENCES

Agudelo, C. (2015). Integración de técnicas y las secuencias de alarmas para la detección y el diagnostico de fallos. *Doctoral Thesis, Universidad Politecnica De Valencia - Spain.*

Astolfi, A. and Praly, L. (2006). Global complete observability and output- to-state stability imply the existence of a globally convergent observer. *Mathematics of Control Signals and Systems, Vol:18, ISSN:0932-4194, Pages:32-65.*

Bayoudh, M., Travé-Massuyès, L., and Olive, X. (2006). Hybrid systems diagnosability by abstracting faulty continuous dynamics. *In Proc. of the 17th International Workshop on Principles of Diagnosis, pages 915, 2006.*

Beebe, D., Ferrer, S., and Logerot, D. (2013). The connection of peak alarm rates to plant incidents and what you can do to minimize. *Process Safety Progress.*

Chen, Y. and Lee, J. (2011). Autonomous mining for alarm correlation patterns based on time-shift similarity clustering in manufacturing system. *2011 IEEE International Conference on Prognostics and Health Management.*

Ding, S. (2008). Model-based fault diagnosis techniques design schemes, algorithms, and tools. *ISBN 978-3-540-76303-1. Springer 2008.*

Fernandez, I., Camacho, A., Gasco, C., Macias, A., and M.A. Martin, G. Reyes, J.R. (2012). *Seguridad funcional en instalaciones de proceso: sistemas, instrumentados de seguridad y análisis SIL.* Ediciones Díaz de Santos, S.A.

Garcia, E., Agudelo, C., and Morant, F. (2012). Secuencias de alarmas para detección y diagnóstico de fallos. *Universidad Politcnica de Valencia, 460022 Spain. 3er Congreso internacional de ingeniera mecatrnica. UNAB 2012.*

Habibi, E. and Hollifiled, B. (2006). Alarm systems greatly affect offshore facilities amid high oil prices. *World Oil, septiembre de 2006, pgs. 101-105.*

Hollender, M., Skovholt, T., and Evans, J. (2016). Holistic alarm management throughout the plant lifecycle. In *2016 Petroleum and Chemical Industry Conference Europe (PCIC Europe)*, 1–6. doi: 10.1109/PCICEurope.2016.7604645.

Koscielny, J.M. and Bartys, M. (2015). The requirements for a new layer in the industrial safety systems. *IFAC-PapersOnLine*, 48(21), 1333 – 1338. doi:

https://doi.org/10.1016/j.ifacol.2015.09.710. 9th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes SAFEPROCESS 2015.

Lew, J., Juang, J., and Keel, H. (1994). Quantification of parametric uncertainty via an interval model. *Journal of Guidance Control and Dynamics - J GUID CONTROL DYNAM. 01/1994; 17(6):1212-1218.*

Magni, L., Scattolini, R., and Rossi, C. (2000). A fault detection and isolation method for complex industrial systems. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans (Volume: 30, Issue: 6, Nov 2000).*

Palomeque, D. (2005). Enfoque integral y herramientas de gestin. *Petrotecnia, Vol 46, pp. 42-48.*

Patton, R.J. and Chen, J. (1997). Observer-based fault detection and isolation: robustness and applications. *Control Engineering Practice, vol. 5, no. 5, pp. 671682.*

Rodrigo, V., Chioua, M., Hagglund, T., and Hollender, M. (2016). Causal analysis for alarm flood reduction. *IFAC-PapersOnLine*, 49(7), 723 – 728. doi: https://doi.org/10.1016/j.ifacol.2016.07.269. 11th IFAC Symposium on Dynamics and Control of Process SystemsIncluding Biosystems DYCOPS-CAB 2016.

Sarmiento, H. and Isaza, C. (2012). Identification and estimation of functional states in drinking water plant based on fuzzy clustering. *22st European Symposium on Computer Aided Process Engineering. pp 1317 to 1327.*

Vásquez, J.W. (2017). Chronicle based alarm management. *Doctoral thesis of Automatic Control Engineering. INSA Toulouse.*

Vásquez, J., Prada, J., Agudelo, C., and Jimenez, F. (2013). Analysis of alarm management in startups and shutdowns for oil refining processes. *IEEE Explorer. Engineering Mechatronics and Automation (CIIMA), 2013 II International Congress, Bogota.*

Vasquez, J., Travé-Massuyès, L., Subias, A., Jimenez, F., and Agudelo, C. (2015). Chronicle based alarm management in startup and shutdown stages. *International Workshop on Principles of Diagnosis (DX-2015), Paris.*

Vasquez, J., Travé-Massuyès, L., Subias, A., Jimenez, F., and Agudelo, C. (2016). Alarm management based on diagnosis. *4th IFAC International Conference on Intelligent Control and Automation Sciences (ICONS 2016), Reims.*

Vasquez, J., Travé-Massuyès, L., Subias, A., Jimenez, F., and Agudelo, C. (2017). Enhanced chronicle learning for process supervision. *20th IFAC World Congress, IFAC-PapersOnLine. Volume 50, Issue 1, July 2017, Pages 5035-5040.*

Vries, R. (1990). An automated methodology for generating a fault tree. *IEEE Transactions on Reliability.*

Yang, F. and Xiao, D. (2012). Progress in root cause and fault propagation analysis of large scale industrial processes. *Journal of Control Science and Engineering. Volume 2012 (2012), Article ID 478373, 10 pages.*

Zhu, J., Shu, Y., Zhao, J., and Yang, F. (2013). A dynamic alarm management strategy for chemical process transitions. *Journal of Loss Prevention in the Process Industries. Volume 30, July 2014, Pages 207-218.*