ARTICLE INFO:
Received : July 17, 2019
Revised : January 24, 2020
Accepted : March 17, 2020
CT&F - Ciencia, Tecnologia y Futuro Vol 10, Num 1 June 2020. pages 45 - 66
DOI : 10.29047/01225383.168

ctyf@ecopetrol.com.co

AN ADDITIONAL LAYER OF PROTECTION THROUGH SUPERALARMS WITH DIAGNOSIS CAPABILITY

UNA NUEVA CAPA DE PROTECCIÓN A TRAVÉS DE SÚPER ALARMAS CON CAPACIDAD DE DIAGNÓSTICO

Vásquez-Capacho, John-William[a]; Perez-Zuñiga, Gustavo[b]; Muñoz, Yecid[c]; Ospino, Adalberto[d]*

ABSTRACT

An alarm management methodology can be proposed as a discrete event sequence recognition problem where time patterns are used to identify the process safe condition, especially in the start-up and shutdown stages. Industrial plants, particularly in the petrochemical, energy, and chemical sectors, require a combined approach of all the events that can result in a catastrophic accident. This document introduces a new layer of protection (super-alarm) for industrial processes based on a diagnostic stage. Alarms and actions of the standard operating procedure are considered discrete events involved in sequences, where the diagnostic stage corresponds to the recognition of a special situation when these sequences occur. This is meant to provide operators with pertinent information regarding the normal or abnormal situations induced by the flow of alarms. Chronicles Based Alarm Management (CBAM) is the methodology used to build the chronicles that will permit to generate the super-alarms furthermore, a case study of the petrochemical sector using CBAM is presented to build the chronicles of the normal start-up, abnormal start-up, and normal shutdown scenarios. Finally, the scenario validation is performed for an abnormal start-up, showing how a super-alarm is generated.

RESUMEN

Se puede formular una metodología de gestión de alarmas como un problema de reconocimiento de secuencia de eventos discretos en el que se utilizan patrones de tiempo para identificar la condición segura del proceso, especialmente en las etapas de arranque y parada de planta. Las plantas industriales, particularmente en las industrias petroquímica, energética y química, requieren una administración combinada de todos los eventos que pueden producir un accidente catastrófico. En este documento, se introduce una nueva capa de protección (súper alarma) a los procesos industriales basados en una etapa de diagnóstico. Las alarmas y las acciones estándar del procedimiento operativo son asumidas como eventos discretos involucrados en las secuencias, luego la etapa de diagnóstico corresponde al reconocimiento de la situación cuando ocurren estas secuencias. Esto proporciona a los operadores información pertinente sobre las situaciones normales o anormales inducidas por el flujo de alarmas. La gestión de alarmas basadas en crónicas (CBAM) es la metodología utilizada en este artículo para construir las crónicas que permitirán generar las super alarmas, además, se presenta un caso de estudio del sector petroquímico que usa CBAM para construir las crónicas de los escenarios de un arranque normal, un arranque anormal y un apagado normal. Finalmente, la validación del escenario se realiza para un arranque anormal, mostrando cómo se genera una súper alarma.

KEYWORDS / PALABRAS CLAVE

Alarm management | Protection layers | Safe process | Diagnosis | Super-alarm.
Gestión de alarmas | Capas de protección | Procesos de seguridad | Diagnóstico | Super-alarma.

AFFILIATION

[a]Grupo de investigación GPS, Universidad de Investigación y Desarrollo - UDI, Bucaramanga, Colombia
[b]Grupo de investigación GECA, Pontificia Universidad Católica del Perú - PUCP, Lima, Perú
[c]Grupo de investigación GIRES, Universidad Autónoma de Bucaramanga - UNAB, Bucaramanga, Colombia
[d]Grupo de investigación GIOPEN, Universidad de la Costa - CUC, Barranquilla, Colombia
**e-mail: jvasquez@udi.edu.co*

1 INTRODUCTION

An automatic reconfiguration on embedded control system is a common requirement on highly automated systems and the fault diagnosis applications are difficult to implement [2]-[3]; consequently, the ultimate goal for a supervisory and control system is to optimize the availability, reliability, and safety of production processes [4]. As regards safety, an integrated management of the critical factors in the process ensures an optimum reliability level at the plant [5]-[6]. Today, the expanding complexity of control systems is caused by the increasing automation of industrial production processes. The use of digital data-based technologies in these systems suggests an increase in the amount of data that must be monitored and processed, including better communication ability among process agents [1]. Factors such as the control of process variables, procedures, and steps followed in transitional stages seek to keep the plants within the operating established "limits" [7] With regard to start up or shutdown procedures, the number of signals increases, the plant safety must have a comprehensive management of factors to analyze accident causes. In other words, these factors must be managed in a comprehensive, rather than separate manner, because if any of them is left outside, unattended or they decrease, this will be a safety threat [8]-[9]. When an industrial process changes its status, for example, start-up or shutdown, the alarm flood spreads, cuasing severe situations that prevent the operator's correct reaction. Furthermore, it is commonly reported that 70% of plant conflicts occur at the start-up/shutdown stages [34]. Due to this alarm flood, dynamic alarm management is necessary. Nowadays, many fault detection and diagnosis methods for multimode processes have been proposed; however, these techniques cannot register the main faults in the basic alarm system [35]. Consequently, the operators need a tool to help them recognize the situation at the plant, especially in transitional stages such as start-up and shutdown. Safety conditions and monitoring, control, and management of complex systems require interest and efforts seeking prompt fault detection and isolation techniques. Many popular approaches are available for identifying faults; for instance, signal-based methods are widely used, seeking to extract useful information from the analysis of specific signals by means of thorough, rigorous analyses of the main statistical methods used to detect changes [10]-[11]. The model-based methods, such as parity or space-based a observers [12], used a mathematical plant model to explore the implicit analytic redundancy relations model to monitor inconsistencies between the model and data measured. However, these methods suggest a large demand of computational load. Other popular methods as those based on fault trees [13] or causal graphs and propagation [14] were based on a qualitative model of the plant. Other approaches have been developed by expert systems based on artificial intelligence techniques [15]. Additionally, hierarchical clustering methods were used to carry out pattern matching correlations [16] in which some frequent patterns of multiple alarm correlation may have the ability to reflect the normal operation sequence, and any pattern change may be a sign of abnormal alteration, sensor degradation or malfunction. Finally, the work [17] included several examples of a model and signal-based fault detection Electrical Flight Control System (EFCS) in aircraft.

This suggests the need not only of a diagnosis system to maintain the process safe by increasing the availability of the installation, but also new alarm management methodologies [18]. Industrial plant safety involves a comprehensive management of all factors that may cause accidents. Hence, alarm management is of great relevance in safety planning for different plants. Any additional support relative to protection of industrial processes will be welcomed by the process safety community.

This article is divided into 7 sections. Section 1 is the introduction; section 2 is a brief description of safeguards, alarm management, and the formal framework of the chronicles; section 3 presents the traditional layers of protection in an industrial process and the super-alarm, as a new layer of protection. Section 4 describes the CBAM methodology; Section 5 and 6 presents the results of a case study and the results analysis. Finally, section 7 corresponds to conclusions and future work.

2. THEORETICAL FRAME

SAFEGUARDS AND ALARM MANAGEMENT

Some years ago (the '60s, the '70s), the combination of a new alarm on the systems had a high cost and required careful studies and analyses before using it. Currently, alarm management is an important aspect of industry processes safety. Each alarm had to be wired given the limited space on the control room panels. New hardware and software improvements have enabled the implementation of alarms at a minimum cost, without space limitation and requiring less inspection. Therefore, quite often unnecessary alarms are triggered, Hence, there has been significant progress related to alarm systems, as alarms are installed and configured considering the number of existing signals (analog and discrete) and the rate of alarms with which an operator can respond efficiently. Alarm systems can induce numerous alarms that cannot be evaluated by the operator, which is a serious threat to process safety [9]. Therefore, the question is: What alarms can be ignored without compromising the integrity of the process? This can lead to sub-alarm systems, which is as bad as having a an over- alarmed system [21]-[22]. Alarm management systems must deal with two main setbacks: A very high rate of alarms, and lack of criteria for assigning the priority of an alarm. The alarm rate indicates the load produced by the alarm system to the operator. If the operator is supposed to respond to all alarms, the system must not produce more alarms than the operator can respond to effectively. The most important factors that affect the rate of alarms are: the number of alarms settled, the dead band analog alarms (pressure, temperature, flow, level, etc.), the analog alarm limits, and the alarms packages equipment (compressors, furnaces, etc) [23]. The alarm priority determines the order in which the operator must respond to the alarm, i.e. it determines the relative importance of the alarms. Often it can be found that all alarms have the same priority, or sometimes a large percentage is assigned to one priority and only a little to other priorities. It is important to have alarms prioritized correctly because, in a setting where the operator receives a sequence of alarms in a short period, the priority is the only factor that the operator has to determine the alarm to which he must respond as priority [24]. Alarm management is a process whereby alarms are designed, monitored and managed to ensure more reliable and safe operations. The first mistake is to assume that alarm management has to do with reducing the number of alarms. The aim of an alarm management system is to improve the quality process acting on the rate of alarms during normal operation, abnormal situations, on the priority of alarms, and on problems related to maintenance and Operation/Control.

The motivation of alarm management is based on improving the work environment for the operator (ergonomics) preventing overload, and unexpected stops, making operations safer and thus achieving improved plant reliability [18]. To define the performance of an alarm system, a set of performance indicators (KPIs) is necessary. The KPI (Key Performance Indicator) should be calculated over a reasonable period of time, e.g. a week. The Engineering Equipment and Materials Users Association EEMUA, through its publication 191, suggests some indicators that can be used when evaluating an alarm system. On the other hand, many operator failures have been registered as incidents that have been the main cause of major accidents. For controlling and mitigating these events, it is necessary to have clear, concise and accurate operating procedures in place. Operating procedures must provide instructions for proper operation of the process plant on aspects such as the Control of Substances Hazardous to Health (COSHH), manual handling, Personal Protective Equipment (PPE) regulations, quality, the Hazard and Operability study (Hazop), and the Safety Health and Environment (SHE) requirements. A Standard Operating Procedure (SOP) is a set of step-by-step instructions structured to help the operators carry out routine operations, and each company or organization defines their SOP as they deem more convenient. The principal objective of the SOPs is to achieve efficiency, quality output and uniformity of performance, reducing delays and failures. Therefore, the standard operating procedures should depict a definition of the best practice that can work at any moment. In addition, alarm management corresponds to determining, documenting, designing, operating, monitoring, and maintaining alarm systems and recently many researchers have focused on themes such as Alarm history visualization and analysis, process data-based alarm system analysis and rationalization, plant connectivity and process variable causality analysis (causal methods) [25]. In sum, the fundamental purpose of an alarm is to alert the operator of deviations of 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 of plant conditions requiring timely assessment or action. As already mentioned, the alarms and operational actions will be treated as discrete events. In each scenario (normal or abnormal behavior), these discrete events will occur. Therefore, these sequences of events will be recognized by the chronicles, which is the formal framework used in the alarm management methodology.

Alarm management implies determining, documenting, designing, operating, monitoring, and maintaining alarm systems and recently the attention of many researchers has been focused on themes such as Alarm history visualization and analysis, Process data-based alarm system analysis and rationalization, and plant connectivity and process variable causality analysis (causal methods).

ALARM HISTORY VISUALIZATION AND ANALYSIS

A combined analysis of plant connectivity and alarm logs to reduce the number of alerts in an automation system is presented in [42]; the aim of this work is to reduce the number of alerts presented to the operator. If alarms are related to one another, those alarms should be grouped and presented as one alarm issue. This process analysis starts with the alarm history, which is a log containing all past alarm messages; therefore, this is combined with the plant topology of the controlled system and a set of rules. Graphical tools for routine assessment of industrial alarm systems are proposed by [43]; they present two new alarm data visualization tools for performance evaluation of the alarm systems, known as the high-density alarm plot (HDAP) and the alarm similarity color map (ASCM).

An alarm message displayed in the operator console has a variety of properties such as tag name, alarm setpoint, tag description, alarm identifier, plant name, timestamp, area, priority, trip value and so on. Most of the information in the alarm message is used by the operator to identify the root cause of the abnormal event. "Timestamp" is the time of occurrence of the alarm. "Tag name" is usually the variable name of the instrument measuring any physical property such as temperature and pressure. Depending on the response time available to the operator, each alarm is assigned a priority (Low, High, and Emergency are commonly used priorities). "Trip value" is the value of the process variable at the time of alarm occurrence and it may be different from the alarm setpoint. Event correlation analysis, and a two-layer cause-effect model, are used to reduce the number of alarms in [44].

The event correlation analysis is a knowledge extraction method that detects statistical similarities among discrete events of alarms and operations. The method uses event data from the plant to quantify the similarity with its time lag between two events by evaluating the cross-correlation function. By grouping correlated alarms and operations in accordance with the degree of similarity, nuisance alarms and operations can be found more easily than by analyzing individual alarms in the top 10 worst alarm methods. A Bayesian method has been introduced for multimode process monitoring in [45]. Conventional methods assume that either the process data are Gaussian in each operation mode, or some process knowledge can be incorporated, thus making the methods supervised.

Table 1. Techniques of alarm history visualization

Technique/Aspect	DES	Time	SOP	Simultaneous	Repetition
Plant connectivity and alarm logs [42]	NO	NO	NO	NO	NO
Graphical tools [43]	YES	YES	NO	NO	NO
Event correlation analysis [44]	YES	YES	NO	YES	NO
Bayesian methods [45]	NO	NO	NO	NO	NO

Source: see references [42], [43], [44] and [45]

A new unsupervised method is developed for multimode process monitoring in this work, which is based on Bayesian inference and two-step independent component analysis, plus a principal component analysis (ICA–PCA) feature extraction strategy. ICA–PCA is introduced for feature extraction and dimension reduction. In addition, by transferring the traditional monitoring statistic to fault probability in each operation mode, monitoring results in different operation modes can be easily combined by the Bayesian inference. Table 1 in these alarm management techniques includes the following aspects: DES (discrete event system), the time between event occurrences, SOP (standard operating procedures), simultaneous occurrences of events and repetition of events in a temporal sequence. This type of technique can help recognize alarm chattering, grouping many alarms or estimating alarm limits in transition stages, but the occurrence date of the alarms related to the procedure actions is not included.

PROCESS DATA-BASED ALARM SYSTEM ANALYSIS AND RATIONALIZATION

The evaluation of plant alarm systems by behavior simulation using a virtual subject was proposed by [46]. An operator model, which mimics the FDI (fault detection and identification) behavior of a human operator with primary cognitive and executive capabilities is developed as a virtual subject for supervising a chemical plant system. Another proposal [47] introduced a technique for the optimal design of alarm limits that analyzes the correlation between process variables and alarm variables. The interrelationship between variables causes the problem of multivariable alarm analysis and rationalization is complex and important for smart alarm management. Visualizing and capturing correlation data, especially from historical alarm data directly, is useful for further analysis. In this work, they suggest that the Gaussian kernel method is applied to generate a pseudo-continuous time series from the original binary alarm data. This can reduce the influence of missing, false and chattering alarms. In 2009, a framework based on the receiver operating characteristic (ROC) curve was proposed for optimal design alarm limits, filters, dead bands, and delay timers; this work was presented in [48]. In industry processes, most of the alarms are false or nuisance alarms and only distract the operator from the normal operation of the process. Filtering process data, adding alarm delay, and using alarm dead band are simple techniques that if used properly can reduce the false and nuisance alarm rate significantly. This paper investigated the effect of these three techniques on the accuracy of the alarm system and detection delay. They also propose a framework for designing optimal filters, time delay, and dead band to reduce false and missed alarm rates.

A dynamic risk analysis methodology that uses alarm databases to improve process safety and product quality was presented in [49]. Important data about unsafe conditions resides in the large alarm databases of distributed control systems and emergency shutdown systems. These overlooked and underutilized data can be analyzed to identify process near-misses and to determine the probability of serious accidents. Many companies record these alarm occurrences in the distributed control systems (DCS) and emergency shutdown (ESD) databases. Operators, engineers, and managers seek guidance from these databases by recording key indicators and paying special attention when alarm flooding occurs. Most of the time, further analysis is done after process upsets, unexpected trips, and accidents. In another approach [50], the Gaussian mixture model was employed to extract a series of operating modes from the historical process data to then derive the local statistics and its normalized contribution chart for early detection of abnormalities and isolating faulty variables. Fault isolation based on data-driven approaches, in general, presumes that the abnormal event data will be formed in a new operating region, measuring the differences between normal and faulty states to perceive faulty variables. When operators are involved in processes, they are aware of abnormalities occurring and, if the process behavior is non-stationary, the operators try to bring it back to normal state. Therefore, the faulty variables must be located in the first place when the process deviates from its normal operating regions. Table 2 includes in these alarm management techniques the following aspects: DES (discrete event system), the time between event occurrences, SOP (standard operating procedures), simultaneous occurrences of events and repetition of events in a time sequence. The use of virtual subjects could be applied to probe the alarm system added to historical data on alarm behavior for detecting abnormalities. The problem arises when the simulation requires a long time to probe all the possible scenarios and when analyzing new plants lacking historical data.

Table 2. Techniques of process data-based alarm systems

Technique/Aspect	DES	Time	SOP	Simultaneous	Repetition
Virtual subjects [46]	YES	YES	NO	NO	NO
Correlation information [47]	YES	YES	NO	NO	YES
Receiver operating characteristic [48]	NO	NO	NO	NO	NO
Dynamic risk analysis [49]	YES	NO	NO	NO	NO
Gaussian mixture model [50]	NO	NO	NO	NO	NO

Source: see references [46], [47], [48], [49] and [50]

PLANT CONNECTIVITY AND PROCESS VARIABLE CAUSALITY ANALYSIS

In the literature, transition monitoring of chemical processes has been reported by a good number of researchers. In [51] ,a dynamic alarm management strategy for chemical process transitions was presented, in which the artificial immune system-based fault diagnosis (AISFD) method and a Bayesian estimation based dynamic alarm management (BEDAM) method were integrated. However, the traditional alarm management systems configured for a single steady-state cannot handle the problem of alarm flooding during transitions. Therefore, it is necessary to propose a new alarm management strategy for transitions. In this work, the proposed dynamic alarm management strategy uses dynamic alarm limits instead of static upper bound and lower bound values. In the proposal of [52] a fault diagnosis strategy for the startup process based on Standard Operating Procedures (SOP) was presented; this approach proposes a behavior observer combined with dynamic PCA (Principal Component Analysis) to estimate process faults and operator errors at the same time.

The startup/shutdown is a common transition in the chemical process industry. Therefore, a startup/shutdown is normally executed by plant operators who follow predefined standard operating procedures, so that the plant settles down to a different steady state. Operator errors, in addition to process faults, occur frequently during this stage. There is another work [53], which is related to direct causality detection via the transfer entropy approach. An important and challenging problem in root cause and hazard propagation analysis is the detection of direct causality, as opposed to indirect causality. Numerous methods propose alternative solutions to this problem, especially when linear relationships between variables are involved.

Currently, only overall causality analysis can be conducted for nonlinear relationships; however, direct causality cannot be identified for such processes. In this work, the authors describe a direct causality detection approach suitable for both linear and nonlinear connections. In [54], the focus was the work progress in root cause and fault propagation analysis of large-scale industrial processes, in which several causal graphs, rule-based models, and ontological models are summarized. Given the interconnection of material and information flows in large-scale industrial processes, a fault can easily propagate between process units. Therefore, the problem of fault detection and isolation for these processes is concentrated on the root cause and fault propagation before applying quantitative methods in local models.

Reference [55] presented a framework for managing chemical plant transitions, proposing a trend analysis-based approach for locating and characterizing the modes and transitions in historical data. Chemical processes work in different steady states and frequently undergo transitions between them. However, alarm management, fault diagnosis, and other automation systems, are usually configured, supposing a single state of operation. When the plant moves out of that state, these applications signal false alarms even when the desired change is occurring. In this paper, the authors propose a framework that would enable these applications to be state-conscious and reconfigure themselves to remain relevant in any process state. Process states are defined in modes and transitions corresponding to quasi-steady state and transient operations, respectively. Finally, in [56] a hybrid model-based framework was used for alarm anticipation and the user is prepared for the possibility of a single alarm occurrence. The modern chemical plants have many integrated and interlinked process units. When an abnormal situation occurs, the automation system alerts the operators through alarms. The authors introduce a new type of alarm, known as "anticipatory alarms", intended to direct the operators in a holistic way to the abnormal situation. These anticipating alarms were developed based on an alarm anticipation algorithm using dynamic process models to obtain an accurate short-term prediction of the process state.

Table 3. Techniques of plant connectivity and causality analysis

Technique/Aspect	DES	Time	SOP	Simultaneous	Repetition
Dynamic alarm management [51]	NO	NO	NO	NO	NO
SOP strategy [52]	NO	NO	YES	NO	NO
Direct causality [53]	NO	NO	NO	NO	NO
Root cause [54]	NO	NO	NO	NO	NO
Framework plant transition [55]	NO	NO	NO	NO	NO
Hybrid model base framework [56]	NO	NO	NO	NO	NO

Source: see references [51], [52], [53], [54], [55] and [56]

Table 3 includes in these alarm management techniques the following aspects: DES (discrete event system), the time between event occurrences, SOP (standard operating procedures), simultaneous occurrences of events and repetition of events in a temporal sequence. For transition monitoring, these types of techniques are used in industrial processes and the hybrid model-based framework is a possible representation of a petrochemical system. It can be observed that a causal model leads to the identification of the root of the failures and to check the correct evolution in a transitional stage.

In conclusion, a review of alarm management techniques was presented. Techniques that permit the recognition of alarm chattering, grouping many alarms or estimate the alarm limits in transition stages. Other techniques use virtual subjects to probe the alarm system and historical data on alarm behavior for detecting abnormalities. The last techniques presented used the hybrid model-based framework as a possible representation of a petrochemical system and these techniques also rely on standard operating procedures. Although none of these types of techniques use DES, our proposal is closer to this third type of approaches and our work seeks to leverage on the causal relationships between process variables and procedure actions, as will be addressed further below.

The relationship between the field of discrete events and the techniques exposed is summarized in that 31,2 % of these alarm management techniques use DES, 25 % including the time between event occurrences, 12,5 % of these use SOP, 6,25 % include the study of simultaneous occurrence of events, and finally 6,25 % analyze event repetitions. No techniques for alarm management include all these aspects simultaneously in the same approach. In this paper, a dynamic alarm management strategy is proposed to deal with alarm floods occurring during any transition of the chemical processes (start-up, shutdown, slow march, fast march, etc.); consequently, this approach relies on the situation recognition (i.e. chronicle recognition). Chronicle Based Alarm Management (CBAM) [37]-[39] is the methodology used to generate super-alarms as a new protection layer in industrial processes. This methodology has been developed as an alarm management technique, using hybrid models and inspired on fault diagnosis approaches, see Figure 1. As the efficiency of alarm management approaches depends on the operator expertise and process knowledge, this information is used with the methodology (see Section 4), and our goal is to develop a diagnosis approach as a decision tool for operators.

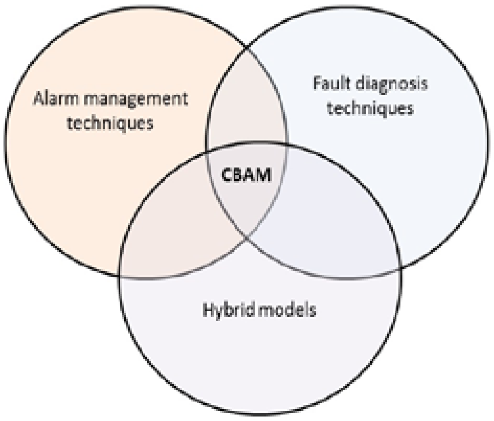


Figure 1. Chronicle Based Alarm Management CBAM

CHRONICLES: A FORMAL FRAMEWORK

A chronicle is a set of events linked by relationships or temporal constraints which occurrence 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. For the time, C. Dousson considers a discrete totally ordered set ***T*** which granularity is fine enough as compared to the environment observed dynamics and to the precision obtained from the means of observation [9],[39]. The notion of event type expresses a change in the value of a given domain feature or set of features, and ***E*** is the set of all types of events. Let us consider time as a linearly ordered discrete set of instants.

Definition 1: An event e is defined as a pair $e = (e_i,t_i\ )$, in which $e_i \in E$ is an event type and t_i is a variable of integer type called the event date. Several events can have the same type of event, but do not necessarily have the same date, for instance $e_1 = (a,3)$ and $e_2=(a,6)$ are two events carrying the same type of event ***a.***

A flow of activity generated by a system is represented by a temporal sequence. In these temporal sequences time is represented by a discrete set of time points, totally ordered which granularity is sufficiently thin compared to the observed dynamics and precision permitted by means of observation, thus considering that there is no inaccuracy. Next, it may refer to an event type as an event for short. A temporal sequence (or sequence for short) consists in several events in an orderly manner, which leads us to the following definition:

Definition 2: A sequence on E is denoted as an ordered set of events $S=\langle(e_i,t_i\ )\_j\ \rangle$ with $j \in N_l$, in which l is the size of the temporal sequence S and N_l is a finite set of linearly ordered instants of cardinal l. l = $|S|$ is the size of the temporal sequence, i.e. the number of event type occurrences in S. An example of sequence representing an activity stream may be given by a sequence $S_1=\{e_1,e_2,e_3,e_4,e_5,e_6\ \} = \{(a,2),(b,4),(c,5),(a,8),(b,9),(a,10)\}$ with $l_1 = 6$.

Definition 3: A chronicle is defined as a triplet $C = \langle\xi,T,G\rangle$ [33] such that:

- $\xi \subseteq E$. In which ξ is called the typology of the chronicle,
- T is the set of temporal constraints of the chronicle,
- $G = (\ \Psi,A)$ is a directed graph in which:
    - ○ Ψ is a set of indexed event types, i.e. a finite indexed family defined by ψ: $H \rightarrow E$, in which $H \sqsubset \mathrm{N}$
    - ○ A is a set of edges between indexed event types; there is an edge $(e_{i\,(h1\,)}\,,\ e_{j\,(h2\,)}\ ) \in \mathrm{A}$ if and only if there is a time constraint between $e_{i(h1\,)}$ and $e_{j(h2\,)}$.

Definition 4: Chronicle instance. A chronicle C = ⟨ ξ, T, G ⟩ is recognized in a temporal sequence S of event types ξ', such that $\xi \subseteq \xi'$, in which all temporal constraints T are satisfied. Then $C_{inst} = \langle\xi\ ,\ T_v\ \rangle$ in which T_v is a valuation of T_v. If the sequence S has finished, and at less, one event that occurs violates some temporal constraint, this chronicle is not recognized. Figure 2 illustrates the above definition: the chronicle on the left is recognized in the first and second sequence. Nevertheless, it is not recognized in the third sequence because the only set of constraints relating a,b,c, and d in this sequence is: $T_v = \{a[5,5]b;\ a[3,3]c;\ c[2,2]b;\ b[2,2]d\}$ and T_v is not a valuation of $T = \{a[3,4]b;\ a[1,2]c;\ c[1,2]b;\ b[1,2]d\}$.

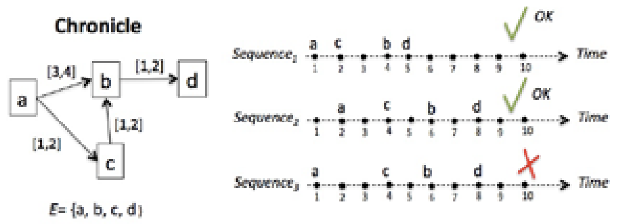


Figure 2. Chronicle instance

Definition 5: Temporal restriction. A temporal restriction for a pair of event types (e_i, e_j) is a given time constraint between their event dates $TR_{ij} = e_i\,[t^-, t^+]\ e_j$.

3. STATE OF THE TECHNIQUE

The operation of many industry processes, especially in the chemical, mineral, energy and petrochemical sector, involves inherent risks due to the presence of hazardous materials like gases and chemicals that in certain conditions can cause an emergency. In these types of industrial processes, safety is managed by layers of protection, starting with a safe design (Process Design Level) and an effective process control (Process Control Level), followed by the manual (Operator Interventions Level) and automatic (Safety Instrumented System Level) prevention layers, and concluded with layers to mitigate the consequences of a critical event (Active protection level, Passive protection level, Plant emergency response level, and Community emergency response level) as shown in Figure 3.

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. Figure 3 presents the tank in cadet blue as one element of protection in this layer.

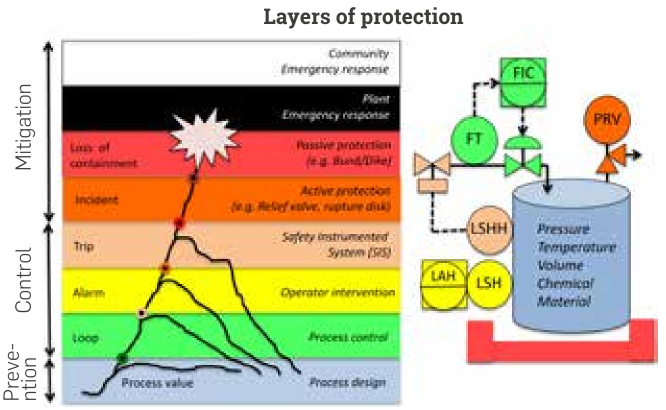


Figure 3. Safety layers of protection

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 control elements such as PLC´s, industrial controllers, control valves, industrial instrumentation, motors, and regulators. **Figure 3** shows in green the elements that maintain the process variable under control (FT, FIC). In this case, the flow control valve regulates the tank level.

Layer 3: Critical alarms, operator supervision, and manual intervention. In this layer, we see HMI (Human Machine Interface) and supervisory systems showing to the operator the alarms configured on the system. Whenever an 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 mind currently, which is described in this section. In **Figure 3** the elements related to this layer are shown in yellow. The level switch of high LSH activates the level alarm of high LAH. The alarms are considered independent variables that are not processed after occurring; furthermore, quite often, these are ignored by operators as as alarms are of normal occurrence.

Layer 4: Automatic action (e.g. SIS or ESD); A Safety Instrumented System (SIS) is a new term used in the standards usually referred to as Emergency Shutdown System (ESD), safety stop system, interlocks system, 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, that must be a system that automatically takes the appropriate action (partial or total stops of equipment and plants) in order to avoid the risk. These safety instrumented systems are normally separate and independent from the control systems, including logic, sensors, and valves at the field.

Unlike control systems, which are active and dynamic, e.g. LSHH in **Figure 3**, SIS is basically passive and "sleepy"; this means that the elements of a SIS do not execute actions 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, manipulation, and good maintenance [20]. Therefore, to involve fault diagnosis methodologies is an important aspect of process safety that needs to be developed continuously.

Layer 5: Physical protection (e.g. relief devices); physical protection in an industry process include relief devices used to reduce the impact from a catastrophic failure of equipment and/or minimize the effects of any unanticipated or uncontrolled event. These relief devices are used as emergency devices and not for normal process control. For individualized equipment, as well as equipment assembled as part of a chemical process, abatement elements are used. Rupture disks, relief valves, and expansion chambers are common elements used as physical protection. **Figure 3** shows the Pressure Relief Valve in orange as a component of this protection layer.

Layer 6: Physical protection (e.g. dikes); the area shut-in with concrete contours or physical barriers 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. Moreover, the total dike area, rather than the storage tanks could be considered the hazard to be protected by a suitable fixed foam fire protection system. A dike is shown in red in **Figure 3** as a physical barrier.

Layer 7: Plant emergency response. Through planning, preparation, mitigation, response and recovery in the event of emergencies and disasters, direct and indirect consequences are expected to be increasingly weak. A plant emergency response seeks to eliminate/diminish vulnerability to threats, implementing the necessary measures to secure 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

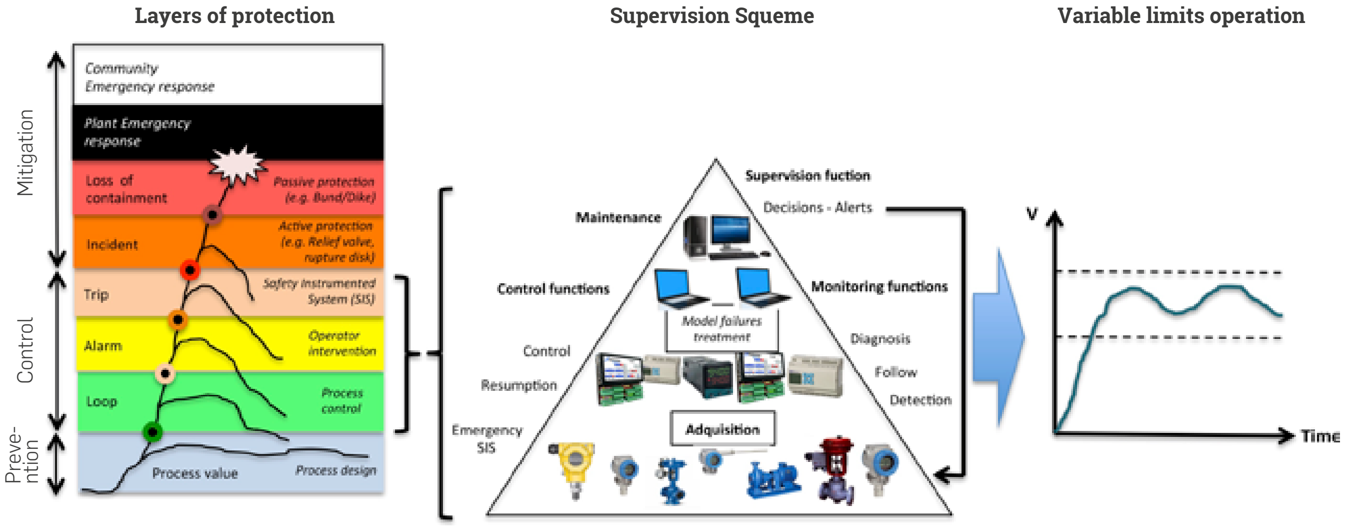


Figure 4. Process safety relationships

with Acts of God or events caused by men. Emergency management includes the following four phases: preparation (before), mitigation (before and after), response (during) and recovery (after). The main objectives of planning for managing emergencies are people, the protection of property, and the protection of operations and standardization of tasks.

Prior to including a new layer on the typical protection layers, diagnosis in industry processes includes procedures, activities, and tools that help operators recognize the actual plant situation, especially during transition stages when the risk of accidents increases. Figure 4 shows process safety relationships, protection layers (Loop, Alarm, and Trip) involving supervision scheme components where the first level includes system instrumentation and actuators, added to the Safety Instrumented System (SIS). The next level contains the acquisition and control equipment followed by the supervision stage, in which the diagnosis tools are implemented.

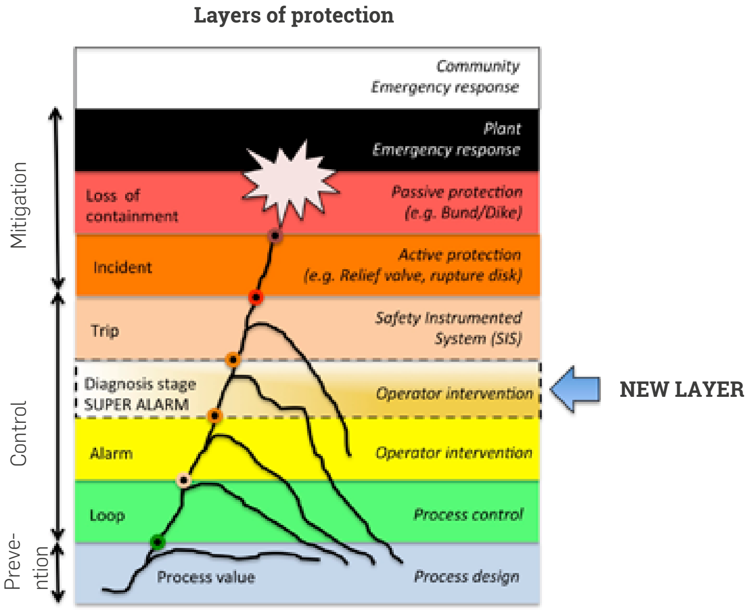


Figure 5. New protection layer (Super-alarm: Diagnosis stage)

To determine the events and signals of a procedure, it is necessary to analyze and consider the initial conditions of the process and to identify potential failure modes. Hence, a complex system requires a division into subsystems for allowing for a reliable analysis. The goal of the technology used maintains the process variables on their limits of operation. In terms of process safety, the principal characteristics of a good protective barrier are specificity, independence, reliability, and audit. 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 associated with the potentially dangerous event and when there is no potential for common cause failures. Furthermore, the protection layer is independent of the triggering event. Reliability: The protection provided by the barrier reduces the risk identified for a specific and known quantity, then determined by its probability of failure. Audit: A barrier must be designed to allow inspections and periodic and regular testing of the protection function [26]-[27].

This article proposes a new protection barrier between the "Alarm" and the "Trip" (SIS) layers, see Figure 5. One additional protection layer could reduce the accident probability by helping the operators take better decisions when alarm floods happen. It has been demonstrated that advanced diagnostic systems for industrial processes, along with the intervention of the operators, may constitute an additional protective safety layer. However, these new elements seem to never have been included as a protection layer because diagnostic systems for industrial processes are not yet extensive as practical tools [28].

The new barrier comes from a diagnosis process and it is specific as it is capable of detecting and preventing a specific (particular) dangerous situation, e.g. wrong operating action in the start-up procedure or failure in a valve. This new barrier is independent because its functionality does not depend on other elements; if some of the signals involved in the diagnosis tool fail, this new tool can detect it. The reliability of this barrier is determined by the reduction of a large number of alarms avoided by the operators. Finally, this new protection layer can be auditable because the diagnosis tools permit checking it from a methodology that includes simulations of scenarios, checking the response. The notion of "super-alarm" corresponds to a new alert to the operators resulting from a diagnosis procedure representing a superior alarm.

Consequently, in automatic control systems, the supervision functions indicate undesirable or not permitted process status and appropriate actions to maintain performance and avoid damage or harm states. A system can be diagnosed if, regardless of the system behavior, it will be able to determine a unique diagnosis, without any ambiguity. When a super-alarm is generated, the supervisory and control system can trigger automatic control actions in addition to operator alerts. The diagnosis capacity of a system is generally computed from its model [31], and in applications using model-based diagnosis, such model is already present, and does not need to be built from scratch. The methodology used to generate super-alarms in this paper is supported by an event-based diagnosis process where from a flow of discrete events, normal and abnormal situations can be detected. The fault diagnosis in general consists in the following three relevant aspects: Fault detection: it consists in discovering the existence of faults in the most useful units in the process; Fault isolation: it is referred to locating (classify) the different faults; and Fault analysis or identification: it consists in determining the type, degree, and origin of the fault [32].

In this paper, a fault is considered as the consequence of a sequence of discrete events representing this faulty scenario, and not a single fault event. In sum, a super-alarm corresponds to a new element resulting 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. A methodology for generating super-alarms is described.

4. EXPERIMENTAL DEVELOPMENT

CHRONICLE BASED ALARM MANAGEMENT – CBAM

The principle of Chronicle Based Alarm Management –CBAM- is to consider several process situations (normal or abnormal) during start-up and shutdown stages and to model each of these situations through a learning chronicle. Thus, given the situation to be modeled, the algorithm HCDAM (Heuristic Chronicle Discovery Algorithm Modified) is fed by a set of event sequences structured from simulations and expert knowledge, giving us the respective chronicle of each situation [36]. Finally, with the chronicle built, a super-alarm can be generated giving to the operator's relevant information and assuming it as a new layer of protection to reduce accident occurrences because in many situations of alarm flood, hazard scenarios exist. The overarching objective of CBAM is to generate a chronicle database on which a diagnosis process based on chronicle recognition is then performed. This new methodology relies on three main steps summarized here in below:

STEP 1: Event type identification: The aim is to determine event types that define the chronicles. Data from the standard operating procedures and the evolution of the continuous variables are used.

STEP 2: Event sequence generation: Based on expertise and on an event abstraction procedure, this step determines the date of occurrence of each event type to build 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 process scenario. The representative event sequences are then verified using the hybrid model of the system and the hybrid causal graphs.

STEP 3: Chronicle database construction: For each scenario, the representative event sequences and temporary restrictions given by experts are considered as learning chronicles. For learning chronicles, this step uses the extended version of the Heuristic Chronicle Discovery Algorithm (HCDAM), which is described in [9],[37]. The set of chronicles learned for each scenario and each process element constitutes the chronicle database. A complex process *Pr* is composed of different units or areas $Pr = \{Ar_1, Ar_2, Ar_3 \ldots\ldots Ar_n\}$ in which each area has φ operational modes (e.g start-up, shutdown, slow march, etc.) noted O_i, $i = 1,2,3 \ldots \varphi$. The process behavior in each operating mode can be either normal or faulty. The set of failure labels are defined as $\Delta_f = \{f_1, f_2, f_3 \ldots f_r\}$ and the complete set of possible labels is $\Delta = N \cup \Delta_f$, where N means normal. To monitor the process and to recognize the different situations (normal or faulty) of the operational modes, we propose building a chronicle base for each area. For a given area, a learned chronicle C_{ij}^{m} is associated to each couple (O_i, L_j) in which $L_j \in \Delta$, see equation (1).

$$C\,Ar_m = \begin{bmatrix} - & N & f_1 & f_2 & \cdots & f_r \\ O_1 & C_{10}^{m} & C_{11}^{m} & C_{12}^{m} & \cdots & C_{1r}^{m} \\ O_2 & C_{20}^{m} & C_{21}^{m} & C_{22}^{m} & \cdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ O_\varphi & C_{\varphi 0}^{m} & C_{\varphi 1}^{m} & C_{\varphi 2}^{m} & \cdots & C_{\varphi r}^{m} \end{bmatrix} \qquad (1)$$

When $L_j = N$, the chronicle is a model of the normal behavior of the system, otherwise $(L_j = f_j)$ the chronicle is a model of the system behavior when threre is occurrence of a fault f_j. This methodology (CBAM) was aimed at addressing the difficulty of alarm management by promoting reliable tools to support the analysis of event streams and identify scenarios that can generate normal or abnormal circumstances in complex flows [38]-[39]. The challenge is then to fit the formal recognition of behaviors in the context of Complex Event Processing. The dynamics of a process can be represented by an approach that depicts the behavior of the process using events occurring during the process evolution. In this context, the chronicle approach [40] has been used in numerous applications to recognize situations and often with a diagnosis objective.

Chronicles are patterns supported by a set of observable events and a set of temporary constraints between pairs of events. One of the main difficulties of situation recognition based on chronicles is to obtain automatically a chronicle base that represents each situation of interest. Diagnosis by situation recognition (chronicle-based diagnosis) in start-up and shutdown stages of mining/mineral/metal/chemical/petrochemical processes as a support to human operators is the principal goal of this new methodology

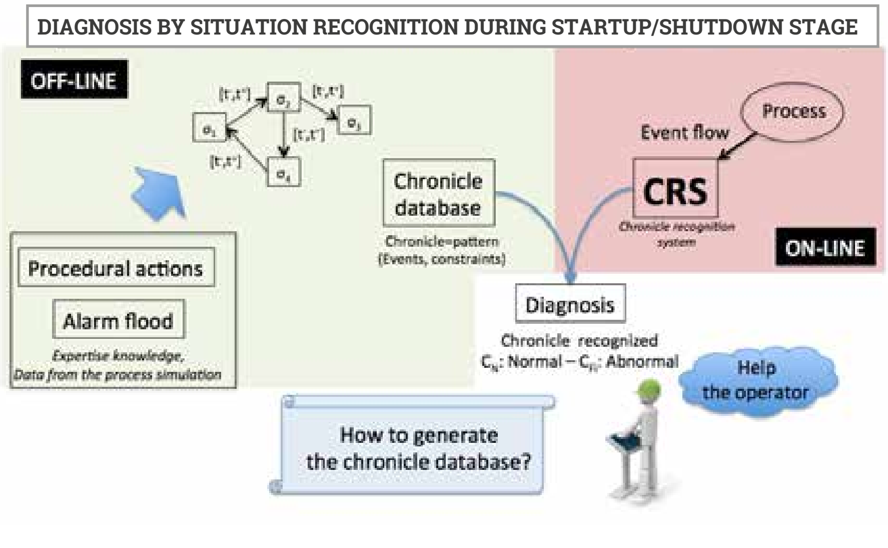

DIAGNOSIS BY SITUATION RECOGNITION DURING STARTUP/SHUTDOWN STAGE
OFF-LINE
[t,t']
o_1
o_2
o_3
o_4
Chronicle database
Chronicle=pattern (Events, constraints)
Process
Event flow
CRS
Chronicle recognition system
ON-LINE
Procedural actions
Alarm flood
Expertise knowledge, Data from the process simulation
Diagnosis
Chronicle recognized
C_N: Normal – C_{fi}: Abnormal
Help the operator
How to generate the chronicle database?

Figure 6. Diagnosis by situation recognition

and it is summarized in Figure 6, in which "super-alarms" can be generated according to the scenarios detected by the chronicles. Note that the chronicle database is created offline, when there are flow events in the process, the chronicle recognition system detects if the events match the chronicle that represents one specific scenario. The chronicle recognition system corresponds to an algorithm that uses the event flow to recognize a specific chronicle according to the evolution of the discrete events in the timeline.

Further, the methodology introduced integrated different techniques to take the hybrid characteristics of the system into account. Data on procedural actions and the behavior of continuous variables are analyzed to extract the representative event sequences. Another important aspect of this work is the dynamic alarm management. Indeed, most of the time the alarm is assumed to be a static indicator, while in this proposal an alarm is an event with an occurrence date and the alarm flow is formally modeled by a chronicle [37]-[39]. The important contribution is the exploitation of chronicle recognition as a super alarm generator providing operators relevant information about the process situation. A new extension of the protection layer of protection corresponding to a diagnosis step based on chronicle recognition should have to be integrated into the global safety structure increasing the reliability of the protection layer related to the operator intervention.

CASE STUDY - HYDROSTATIC TANK GAUGING SYSTEM

The technological transformation of the Cartagena Refinery in Colombia have incorporated news components such as the atmospheric hot tower, the vacuum tower, the Hydrostatic Tank Gauging (HTG) system, and the vacuum oven between other elements. Our proposal aims to help the operator to recognize dangerous conditions during the start-up stage of the refinery with modified equipment [9]. The unit analyzed in this paper is the water injection unit on its start-up and shutdown stages, see Figure 7.

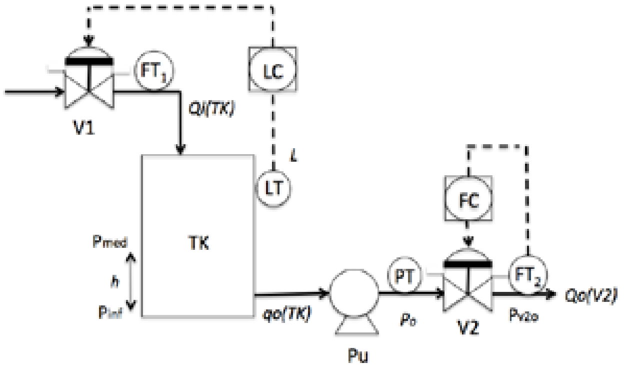


Figure 7. Hydrostatic Tank Gauging

The continuous variables measured are the level of the tank L, the pressure Po in the pump and the outlet flow *Qo*(V2) in the valve **V2**. For the start-up stage in this process, the initial conditions are that tank (**TK**) empty, valves **V1** and **V2** closed and pump Pu is off. In this situation, the alarms for low levels in all the continuous variables (*L, Po,* and *Qo*(V2)) are active. For the shutdown stage in this process, the initial conditions could vary, depending on the situation in each system . For example, one condition is that the outlet pressure (*Po*) has passed its high limit activating the alarm *PAH* (Pressure Alarm High), but the outlet flow (*Qo*(V2)) does not increase over its low limit after a specific number of time units has passed. The standard operating procedure dictates the standard procedural actions for the start-up and shutdown stages. For proper execution of these procedures, the operators must carry out actions according to the correct evolution of the procedure. Abnormal situations are detected when the evolution of the procedural actions and the continuous variables evolution do not match the standard operating procedure and fault events occur. The fluctuations of the inlet flow to the tank, the response time of the pump that affect outlet pressure and other conditions generate uncertainties that can be determined based in expertise as obtaining a complex model to simulate all process uncertainties requires significant time and resources.

HYBRID FEATURES OF THE HTG SYSTEM

In this paper, the hybrid system is represented by an extended transition system, which discrete states represent different operating modes, with continuous dynamics characterized by a qualitative domain [41]. Formally, a hybrid causal system is defined as a tuple $\Gamma = \langle V, D, Tr, E, CSD, Init, COMP, DMC \rangle$.
Where:

- $V = \{ \upsilon_i \}$ is a set of continuous process variables that are a function of time.
- D is a set of discrete variables. $D = Q \cup K \cup V_Q$
    - Q is a set of states q_i of the transition system that represent the system operation modes.
    - The set of auxiliary discrete variables $K = \{K_i\}, i = 1,2,3,....n_c$ represents the system configuration in each mode q_i, in which K_i indicates the discrete state of the active components.
    - V_Q is a set of qualitative variables whose values are obtained from the behavior of each continuous variable υ_i
- $E = \Sigma \cup \Sigma^c$ is a finite set of observable (Σ_o) and unobservable (Σ_{uo}) event types, noted σ, in which:
    - Σ is the set of event type associated to the procedural actions, for example in the start-up or shutdown stages.
    - Σ^c is the set of event type associated to the behavior of the continuous process variables.
- $Tr: Q \times \Sigma \rightarrow Q$ is the transition function. The transition from mode q_i to mode q_j with associated event σ is noted (q_i, σ, q_j).
- $SD \supseteq \cup_i CSD_i$ is the Causal System Description or the causal model used to represent the constraints underlying the continuous dynamics of the hybrid system.

Every CSD_i associated to a mode q_i, is given by a graph $G_c = V \cup K, I$. In which, I is the set of influences in which there is an edge $\epsilon(\upsilon_i, \upsilon_j) \in I$ from $\upsilon_i \in V$ to $\upsilon_j \in V$ if the variable υ_i influences variable υ_j. A dynamic control model DCM_{Ik} is associated to every influence $I_k \in I$. Figure 8 presents the Dynamic Control Model, which relates one procedural action σ_i as an observable event that connects the industrial controller (PID) with the model of the active component (Comp. model). Model that corresponds to a delayed first order transfer function. The event that close the control loop σ_j is assumed as an unobservable event.

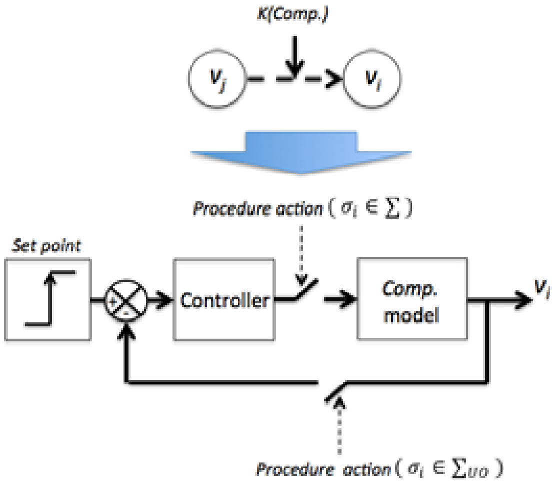

K(Comp.)
V_j
V_i
Procedure action ($\sigma_i \in \Sigma$)
Set point
Controller
Comp. model
V_i
Procedure action ($\sigma_i \in \Sigma_{uo}$)

Figure 8. Dynamic Control Model - *DCM* -

With respect to the case study, this process is an HTG (Hydrostatic Tank Gauging) system comprised by the following items: sensors, passive and active components. The sensors are the level sensor (**LT**), the pressure sensor (**PT**), the inflow sensor (**FT1**), and the outflow sensor (**FT2**). The passive component is the tank (**TK**); in addition, the active components are two normally closed valves (**V1** and **V2**), and one pump (**Pu**). Since there are three active components, the HTG system obviously involves hybrid behavior. Modeling the behavior of this hybrid system involves a set of continuous variables and a set of discrete variables. The continuous variables are level L, pressure Po, and outflow *Qo*(V2), *V = {L, Po, Qo (V2)* }. On the other hand, the discrete variables (*D*) are:

- The states *Q* of the transition system represent the system operating modes. The HTG has thus $2^3 = 8$ configurations and operating modes denoted q_0 to q_7 due to the two valves (**V1** and **V2**) each with two possible modes (opened and closed); and the pump (**Pu**) with two possible modes (ON and OFF), see **Figure 9**, in which the bold lines indicate that the causality relationship between the variables is activated.

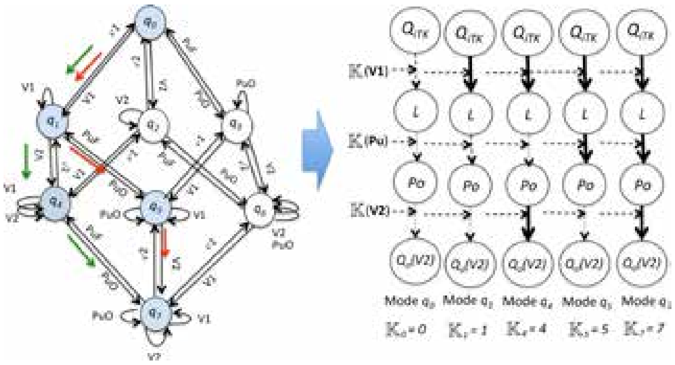


Figure 9. Start-up stage of the HTG System: underlying DES and Causal System Description

- V_Q the set of qualitative variables values (Low, Medium and High) are obtained from the behavior of continuous variables. In this case study, continuous variable domain partitioning has been chosen according to expert knowledge and to limit values specified in standard operating procedures. $V_Q = \{L^L, L^M, L^H\} \cup \{Po^L, Po^M, Po^H\} \cup \{Qo(V2)^L, Qo(V2)^M, Qo(V2)^H\}$.

- The set of auxiliary discrete variables indicating the state of active components is given by: $K = \{K_i\}$, $i = 0,1,\ldots 7$ i.e, the system configuration associated to an operation mode. The configuration is defined by the state (opened or closed) of the two valves and the state of the pump. For a normal start-up, the HTG evolves through the modes q_0, q_1, q_4, q_5, and q_7. In mode q_0, the two valves are closed and the pump OFF, then $K_0 = 0$. When the valve **V1** is opened, the system passes to the mode q_1 and $K_1 = 1$. The system can evolve to q_4 if the valve **V1** is opened, then $K_4 = 4$, or it can evolve to q_5 if the pump **Pu** is turned ON, then $K_5 = 5$. Finally, for q_7, both valves are opened and the pump turned ON, then $K_7 = 7$, see **Figure 8**.

In each operating mode, the variables evolve according to its dynamics. This evolution is represented with qualitative values. The domain $d(V_i)$ of a qualitative variable $V_i \in V_Q$ is obtained through the function $f_{qual}: d(\upsilon_i) \rightarrow d(V_i)$ that maps the continuous values of variable υ_i to ranges defined by limit values (High noted H_i and Low noted L_i), see equation (2).

$$f(v_i)_{qual} = \begin{cases} V_i^H & if \;\; v_i \geq H_i \\ V_i^M & if \;\; L_i < v_i < H_i \\ V_i^L & if \;\; v_i \leq L_i \end{cases} \qquad (2)$$

The behavior of these qualitative variables is represented in **Figure 10** by the automaton $G_{Vi} = (V_Q, \Sigma^c, \gamma)$ where V_Q is the set of the possible qualitative states *(V_i^L: Low, V_i^M: Medium, V_i^H: High)* of the continuous variable υ_i. Σ^c is the finite set of events associated to the transitions, and $\gamma: V_Q \times \Sigma^c \rightarrow V_Q$ is the transition function.

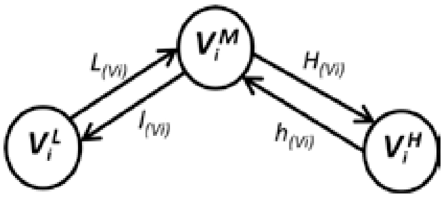


Figure 10. Automaton G_{Vi}

The corresponding event generator is defined by the abstraction function $f_{VQ} \rightarrow \sigma$. See equations (3) and (4).

$$f_{V_Q \rightarrow \sigma}: V_Q \times \gamma(V_Q, \Sigma^c) \rightarrow \Sigma^c$$

$$\forall V_i \in V_Q, (V_i^n, V_i^m) \rightarrow \begin{cases} L_{(v_i)} & \text{if} \;\; V_i^L \rightarrow V_i^M \\ L_{(v_i)} & \text{if} \;\; V_i^M \rightarrow V_i^L \\ H_{(v_i)} & \text{if} \;\; V_i^M \rightarrow V_i^H \\ h_{(v_i)} & \text{if} \;\; V_i^H \rightarrow V_i^M \end{cases} \qquad (3)$$

$$V_i^n, V_i^m \in \{V_i^L, V_i^M, V_i^H\}$$

$$\Sigma^c = \cup_{(v_i \in \mathcal{V})}\{L_{(v_i)}, l_{(v_i)}, H_{(v_i)}, h_{(v_i)}\} \qquad (4)$$

5. RESULTS

This section presents the results achieved using the CBAM methodology with the HTG system. The chronicles obtained are for the following scenarios: normal start-up, abnormal start-up, and normal shutdown; the three steps of this methodology to generate these chronicles are described below.

STEP 1: EVENT TYPE IDENTIFICATION

In the HTG system of the case study, the set of event types **Σ** that represent the procedure actions is:

$$\boldsymbol{\Sigma = \{\mathrm{V1}, \mathrm{V2}, \mathrm{PuO}, \mathrm{v1}, \mathrm{v2}, \mathrm{PuF}, \mathrm{M2A}\}} \tag{5}$$

Where V1 (resp. V2) represents the action that switches the valve **V1** (resp. **V2**) from closed to opened. On the other hand, v1 (v2) represents the action that switches the valve **V1** (resp. **V2**) from opened to closed and PuO (resp. PuF) for the action that turns on (resp. off) the pump. The event M2A corresponds to the transition from "manual" to "automatic", closing the control loops. In the reminder, we assume that this is the only unobservable event of the system, i.e. $\mathbf{M2A} \in \mathbf{\Sigma_{uo}}$. The underlying DES (Discrete Event System) of the HTG represents the sequence of observable procedure actions for a start-up stage (indicated red or green arrows on **Figure 8** corresponding to the evolution of the operating modes (I.e $\boldsymbol{q_0}$,$\boldsymbol{q_1}$,$\boldsymbol{q_4}$,$\boldsymbol{q_5}$,$\boldsymbol{q_7}$) Each operation mode $\boldsymbol{q_i}$ is associated to a causal system description to identify the influences between the variables *L*, Po and Qo(V2), see **Figure 8**. These influences allow to determine the occurrence of events $\mathbf{\Sigma^c}$ (see equation 6). For instance, in the q_1 operating mode, it can be determined that when valve **V1** is opened, the continuous variable Q_{iTK} influences variable *L*, and thus the supervision system will wait to the event $L_{(L)}$, which indicates that after a specific period, the water level in the tank **TK** has passed its low limit.

$$\boldsymbol{\Sigma^c = \begin{matrix} \{L_{(L)}, l_{(L)}, H_{(L)}, h_{(L)}, L_{(Po)}, l_{(Po)}, H_{(Po)}, h_{(Po)}, \\ L_{(Qo(\mathrm{V2}))}, l_{(Qo(\mathrm{V2}))}, H_{(Qo(\mathrm{V2}))}, h_{(Qo(\mathrm{V2}))}\} \end{matrix}} \tag{6}$$

STEP 2: EVENT SEQUENCE GENERATION

The behavior of variables is obtained from simulations, and the learning event sequences are generated according to the evolution of the system in each scenario. Three scenarios are analyzed in this paper: normal start-up, abnormal start-up, and normal shutdown.

SCENARIO 1, NORMAL START-UP:

According to standard procedural actions, the first event type that must occur is V1 (Open **V1**). After this type event occurrence, the system is in the $\boldsymbol{q_1}$ ***operating*** operating mode in which variable L increases and the event type $L_{(L)}$ must occur after that the valve **V1** is opened, indicating that the liquid level of the tank **TK** has passed the low level limit. After $L_{(L)}$, the liquid in the tank must reach the high limit level and event type $H_{(L)}$ must occur. At this point in time, the ordered sequence of event types that has occurred is V1, $L_{(L)}$, $H_{(L)}$. The high limit of the level in the tank is the condition for continuing with the procedure actions "open **V2**" and "turn on **Pu**" (V2 and PuO). If the operator opens valve **V2** first, the system passes from $\boldsymbol{q_1}$ to the operating mode $\boldsymbol{q_4}$, but if the pump Pu is turned on first, then the system passes to $\boldsymbol{q_5}$. The duration between the occurrences of event types V2 and PuO must be 1 time unit, leaving the system in operating mode $\boldsymbol{q_4}$ or $\boldsymbol{q_5}$. At this point in time, the ordered sequence of event types that has occurred must be V1, $L_{(L)}$, $H_{(L)}$, PuO, V2 or V1, $L_{(L)}$, $H_{(L)}$, V2, PuO.

In scenario1a (V1, $L_{(L)}$, $H_{(L)}$, PuO, V2), the outlet pressure (Po) of the pump **Pu** increases first that the outlet flow (Qo(V2)). Then, after V2, pressure Po has passed its low pressure limitand the event type $L_{(Po)}$ must occur. Passing the high limit of pressure, ($H_{(Po)}$) occurs after $L_{(Po)}$. In scenario1b (V1, $L_{(L)}$, $H_{(L)}$,, V2, PuO), the event type $L_{(Po)}$ occurs after PuO. Now, after $L_{(Po)}$, $L_{(Qo(V2))}$ must occur. Subsequently, the event type $H_{(Po)}$ must occur. At this point, the ordered sequence of event types occurred must be V1, $L_{(L)}$, $H_{(L)}$, PuO, V2, $L_{(Po)}$, $H_{(Po)}$, $L_{(Qo(V2))}$ or V1, $L_{(L)}$, $H_{(L)}$,, V2, PuO, $L_{(Po)}$, $L_{(Qo(V2))}$, $H_{(Po)}$. In this case, the unobservable event type M2A occurs and the control loop is closed, putting the system in a steady state. We assume that the control loops are closed while $L_{(Qo(V2))}$ occurs in scenario1a or $H_{(Po)}$ in scenario1b. Then, event type $h_{(Po)}$ indicates that outlet pressure decreases after the control loops are closed. Similarly, the liquid level in the tank **TK** decreases from the high limit of level $h_{(L)}$ after $h_{(Po)}$ occurs. When this event type ($h_{(L)}$) occurs, it is assumed that the start-up stage ended correctly and the ordered sequences of event types must be V1, $L_{(L)}$, $H_{(L)}$, PuO, V2, $L_{(Po)}$, $H_{(Po)}$, $L_{(Qo(V2))}$, $h_{(Po)}$, $h_{(L)}$ or V1, $L_{(L)}$, V2, PuO, $L_{(Po)}$, $L_{(Qo(V2))}$, $H_{(Po)}$, $h_{(Po)}$, $h_{(L)}$. For this scenario, we opted for representative event sequences (S_1, S_2 and S_3), which represent extreme behaviors with all possible sequence order of event types.

$$\boldsymbol{S_1 = \langle \begin{matrix} (\mathrm{V1}, 1); (L_{(L)}, 20); (H_{(L)}, 48); (PuO, 50); (\mathrm{V2}, 51); (L_{(Po)}, 58); \\ (H_{(Po)}, 71); (L_{(Qo(\mathrm{V2}))}, 80); (h_{(Po)}, 106); (h_{(L)}, 180) \end{matrix} \rangle}$$

$$\boldsymbol{S_2 = \langle \begin{matrix} (\mathrm{V1}, 1); (L_{(L)}, 25); (H_{(L)}, 55); (\mathrm{V2}, 56); (PuO, 57); (L_{(Po)}, 69); \\ (L_{(Qo(\mathrm{V2}))}, 83); (H_{(Po)}, 91); (h_{(Po)}, 115); (h_{(L)}, 188) \end{matrix} \rangle}$$

$$\boldsymbol{S_3 = \langle \begin{matrix} (\mathrm{V1}, 1); (L_{(L)}, 31); (H_{(L)}, 60); (PuO, 61); (\mathrm{V2}, 62); (L_{(Po)}, 71); \\ (H_{(Po)}, 85); (L_{(Qo(\mathrm{V2}))}, 91); (h_{(Po)}, 112); (h_{(L)}, 182) \end{matrix} \rangle}$$

The simulation of a normal start-up is illustrated in **Figure 11**, showing the evolution of variables *L*, *Po*, and Qo(V2). This simulation represents only one possible situation in this scenario related to the pattern sequence S_1. The values of the variables are specified as follows:

- For the variable of level *(L)*, the 0 corresponds to 0 meters, and each 0.5 (vertical axis) increase corresponds to 0.5 meters.
- For the variable of pressure *(Po)*, 0 corresponds to 0 PSI, and each 0.5 (vertical axis) increase corresponds to 10 PSI.
- For the variable of outlet flow (Qo(V2)) variable, the division of 0 corresponds to 0 lts/s (Liters per second), and each 0.5 (vertical axis) increase corresponds to 1 lts/s.
- The time (horizontal axis) in the graph is expressed in seconds.

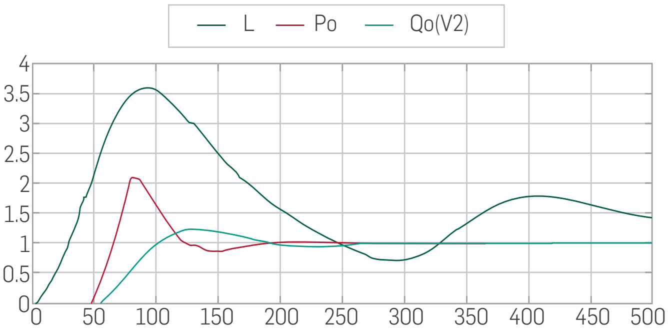


Figure 11. Simulation of a normal start-up in the HTG system

At this point, the representative event sequences must be verified using the hybrid causal model. For example, sequence S1 starts with the event type V1. Then, the system passes to the operating mode $\boldsymbol{q_1}$ and the relationship between Q_{iTK} and L is activated, see **Figure 8**. We wait for the occurrence of two event types, first event type $L_{(L)}$, and second $H_{(L)}$. Then, the standard procedure actions PuO and V2 must occur passing the system from the operating mode $\boldsymbol{q_1}$, in this case, first to the operating mode $\boldsymbol{q_5}$ and then to $\boldsymbol{q_7}$. When the system is in the $\boldsymbol{q_5}$ ***mode,*** the relationship of continuous variables L and Po is activated and we wait for the occurrence of the two event types: first, $L_{(Po)}$, and second $H_{(Po)}$, in this order. Then, when the system is in the mode $\boldsymbol{q_7}$ the relationship of the continuous variables Po and Qo(V2) is activated. After that, the event type $L_{(Qo(V2))}$ and the no observable event M2A is activated and the control loops are closed. >This event sequence concluded with the event types $h_{(Po)}$ and $h_{(L)}$ in this order. For the other sequences, the same procedure is applied.

SCENARIO 2, ABNORMAL START-UP

This abnormal situation is related to a failure in valve V2. In this scenario, the sequences of event types are similar to those of a normal start-up, until it is detected that there is no increase in the system's outlet flow. When the liquid level in the tank TK reached its high limit, the ordered sequence of event types occurred must be V1, $L_{(L)}$, $H_{(L)}$, PuO, V2 or V1, $L_{(L)}$, $H_{(L)}$, V2, PuO. In scenario 2a : (V1, $L_{(L)}$, $H_{(L)}$, PuO, V2) the event type $L_{(Po)}$ occurs after V2. In scenario2b: (V1, $L_{(L)}$, $H_{(L)}$, V2, PuO) the event type $L_{(Po)}$ occurs after PuO. The event type $H_{(Po)}$ occurs after $L_{(Po)}$. So, the ordered sequences of event types must be: V1, $L_{(L)}$, $H_{(L)}$, PuO, V2, $L_{(Po)}$, $H_{(Po)}$) or V1, $L_{(L)}$, $H_{(L)}$, V2, PuO, $L_{(Po)}$, $H_{(Po)}$. For this scenario, we chose the representative event sequences (S_4, S_5 and S_6) showing extreme behaviors with all the possible sequence order of event types.

$$S_4 = \langle (\mathbf{V1},1); (L_{(L)},21); (H_{(L)},48); (PuO,50); (\mathbf{V2},51); (L_{(Po)},60); (H_{(Po)},75) \rangle$$
$$S_5 = \langle (\mathbf{V1},1); (L_{(L)},25); (H_{(L)},55); (\mathbf{V2},56); (PuO,57); (L_{(Po)},63); (H_{(Po)},78) \rangle$$
$$S_6 = \langle (\mathbf{V1},1); (L_{(L)},28); (H_{(L)},60); (PuO,61); (\mathbf{V2},62); (L_{(Po)},71); (H_{(Po)},85) \rangle$$

The simulation of this abnormal start-up is presented in **Figure 12** m showing the evolution of variables *L* and *Po*. Variable Qo(V 2) does not appear because the valve V2 had failed. The values of the variables are specified as follows:

- For the variable of level (L), the value of 0 corresponds to 0 meters, each increase of 2 (vertical axis) corresponds to 2 meters.
- For pressure variable (Po), 0 corresponds to 0 PSI.

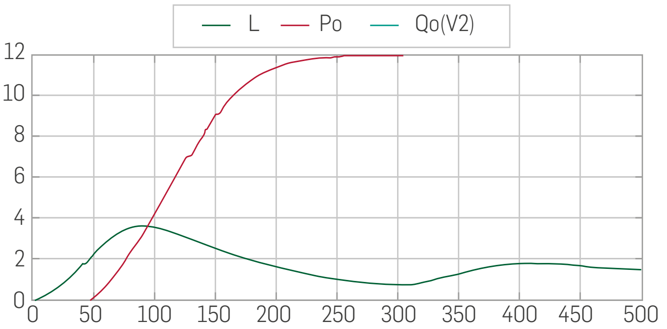


Figure 12. Simulation of an abnormal start-up in the HTG system

SCENARIO 3, NORMAL SHUTDOWN

After detecting an abnormal start-up situation, a shutdown procedure must be executed. According to the foregoing (Scenario 2), it is assumed that after the abnormal start-up is confirmed, standard procedure actions v1, v2, and PuF must be developed. For this scenario, we chose the representative event sequences (S_7, S_8 and S_9) that represent the extreme behaviors with all the possible sequence order of event types.

$$S_7 = \langle \begin{matrix} (\mathbf{V1},1); (L_{(L)},20); (H_{(L)},48); (PuO,50); (\mathbf{V2},51); (L_{(Po)},60); (H_{(Po)},75); \\ (PuF,77); (\mathbf{v1},78); (\mathbf{v2},79); (h_{(L)},190); (h_{(Po)},195); (l_{(Po)},240) \end{matrix} \rangle$$
$$S_8 = \langle \begin{matrix} (\mathbf{V1},1); (L_{(L)},20); (H_{(L)},48); (\mathbf{V2},51); (PuO,52); (L_{(Po)},63); (H_{(Po)},78); \\ (PuF,79); (\mathbf{v2},81); (\mathbf{v1},82); (h_{(Po)},188); (h_{(L)},200); (l_{(Po)},250) \end{matrix} \rangle$$
$$S_9 = \langle \begin{matrix} (\mathbf{V1},1); (L_{(L)},28); (H_{(L)},59); (PuO,61); (\mathbf{V2},63); (L_{(Po)},70); (H_{(Po)},84); \\ (PuF,85); (\mathbf{v1},86); (\mathbf{v2},87); (h_{(Po)},193); (h_{(L)},198); (l_{(Po)},231) \end{matrix} \rangle$$

The simulation of this normal shutdown is presented in **Figure 13**, showing the evolution of variables *L*, *Po,* and Qo(V2). The values of the variables are specified as follows:

- For the level variable (*L*), 0 corresponds to 0 meters, and each increase of 1 (vertical axis) corresponds to 1 meter.
- For the pressure variable (Po), 0 corresponds to 0 PSI, and each increase of 1 (vertical axis) corresponds to 20 PSI.
- For the variable of outlet flow variable (Qo(V2)), the division of 0 corresponds to 0 lts/s (Liters per second), and each increase of 1 (vertical axis) corresponds to 2 lts/s.
- The time (horizontal axis) in the graph is expressed in seconds.

This simulation represents only one possible situation in this scenario related to the representative sequence S_7. The procedure evaluation of this event sequences is similar to the procedure developed in other settings. In this scenario, event types v1, v2, and PuF are involved in the shutdown procedure.

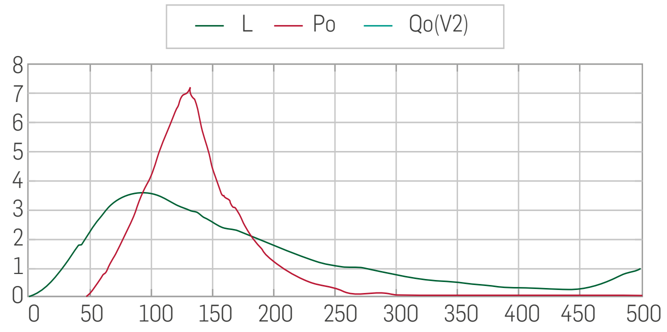


Figure 13. Simulation of a normal shutdown in the HTG system

STEP 3: CHRONICLE DATABASE CONSTRUCTION

This chronicle database is to be submitted to a chronicle recognition system that identifies, in an observable flow of events, all the possible matching with the set of chronicles. Chronicles are used to assess the situation (normal or faulty), by generating a super alarm. The following three chronicles (C^{1}_{10}, C^{1}_{11} and C^{1}_{20}) of the set of chronicles of the HTG (Hydrostatic Tank Gauging) system are presented, i.e those in the area Ar_1 of the whole system. C^{1}_{10} is the chronicle for the normal start-up stage of the HTG, C^{1}_{11} is associated with a failure behavior of type f_1 during a start-up stage, and C^{1}_{20} corresponds to a normal shutdown. In the chronicle figure, the events are specified as follows: $L_{(L)}$ as LL; $l_{(L)}$ as lL; $H_{(L)}$ as HL; $h_{(L)}$ as hL; L(Po) as LP; $L_{(Po)}$ as lP; $H_{(Po)}$ as HP; $h_{(Po)}$ as hP; $L_{(Qo(V\,2))}$ as LQ; $l_{(Qo(V\,2))}$ as lQ; $H_{(Qo(V\,2))}$ as HQ; $h_{(Qo(V\,2))}$ as hQ.

SCENARIO 1, NORMAL START-UP:

For this scenario, the following temporal restrictions represent the expert knowledge used in the extended version of the HCDAM. $TR_{LL,V2}$= LL[30,32]V2, this temporal restriction means that valve V2 is opened between 30 and 32 time-units after reaching the low limit (LL) level in the tank. $TR_{PuO,V2}$=PuO[−2,2]V2, this temporal restriction indicates that valve **V2** can be opened (V2) two time-units before the pump **Pu** is turned on (PuO) or, on the contrary, PuO occurs two time-units before V2. $TR_{HL,V2}$ =HL[1,5]V2, this temporal restriction means that valve V2 is opened between 1 and 5 time-units after reaching the high limit level (HL) in the tank. The chronicle C^{1}_{10} resulting after using the algorithm HCDAM is presented in **Figure 14**. The learning event sequences used are S_1, S_2 and S_3, generated in the event sequence generation section (normal startup).

SCENARIO 2, ABNORMAL START-UP:

For this abnormal start-up scenario, the following temporal restrictions are used in the extended version of the HCDAM. $TR_{PuO,V2}$=PuO[−2,2]V2, this temporal restriction means that valve **V2** can be opened (V2) two time units before the pump **Pu** is turned on (PuO) or, on the contrary, that PuO occurs 2 time units before V2. $TR_{HL,PuO}$ =HL[1,4]PuO, this temporal restriction expresses that the pump **Pu** is turned on (PuO) between 1 and 5 time-units after reaching the high limit level in the tank (HL). The chronicle C^{1}_{11} that resulting after using the algorithm HCDAM is presented in **Figure 15**. The learning event sequences used are S_4, S_5 and S_6, generated in the event sequence generation section (abnormal startup).

SCENARIO 3, NORMAL SHUTDOWN:

In this normal shutdown scenario the following temporal restrictions were used, which represent the expert knowledge used in the

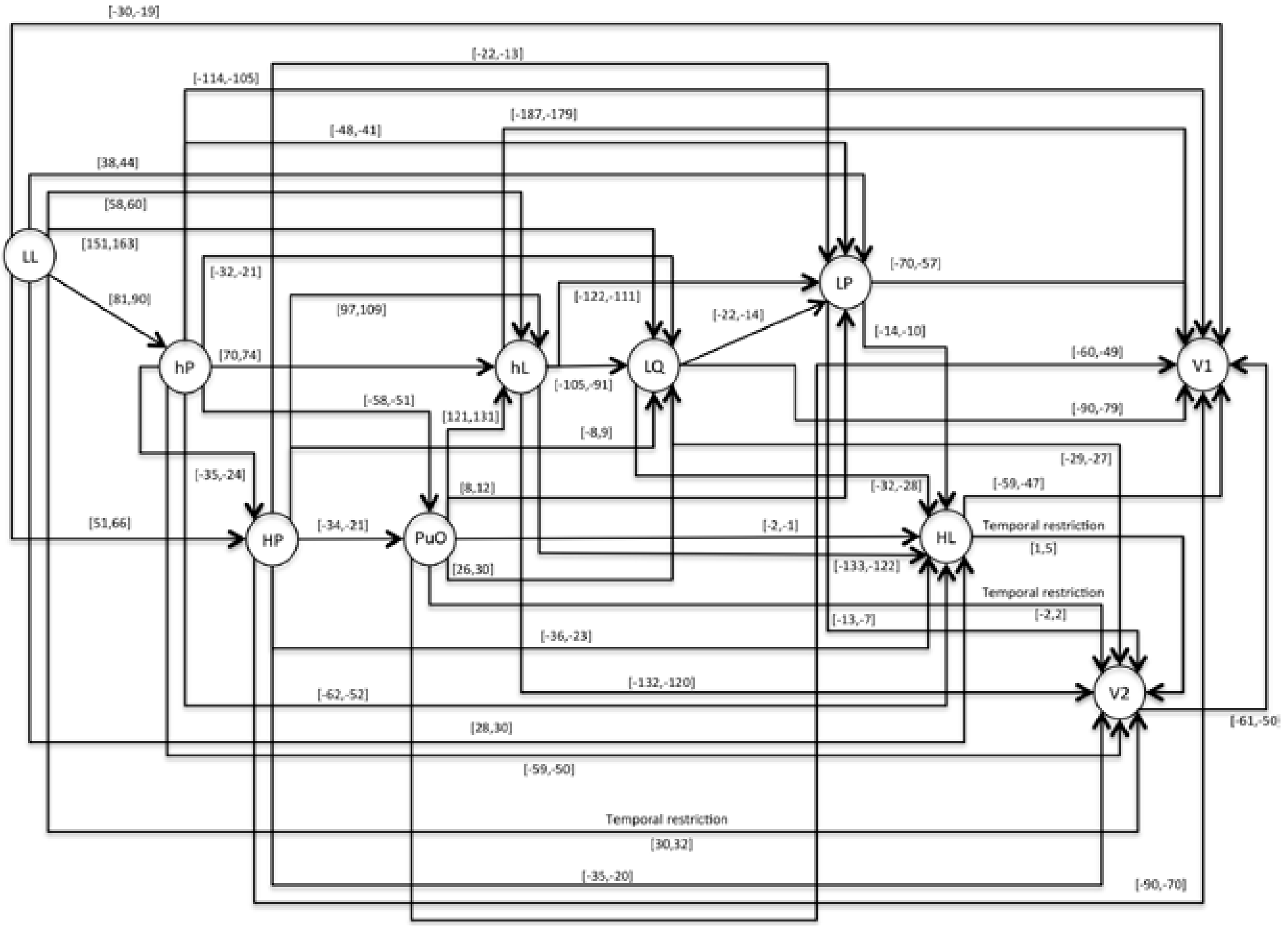


Figure 14. Directed graph (G) of the chronicle C^{1}_{10}

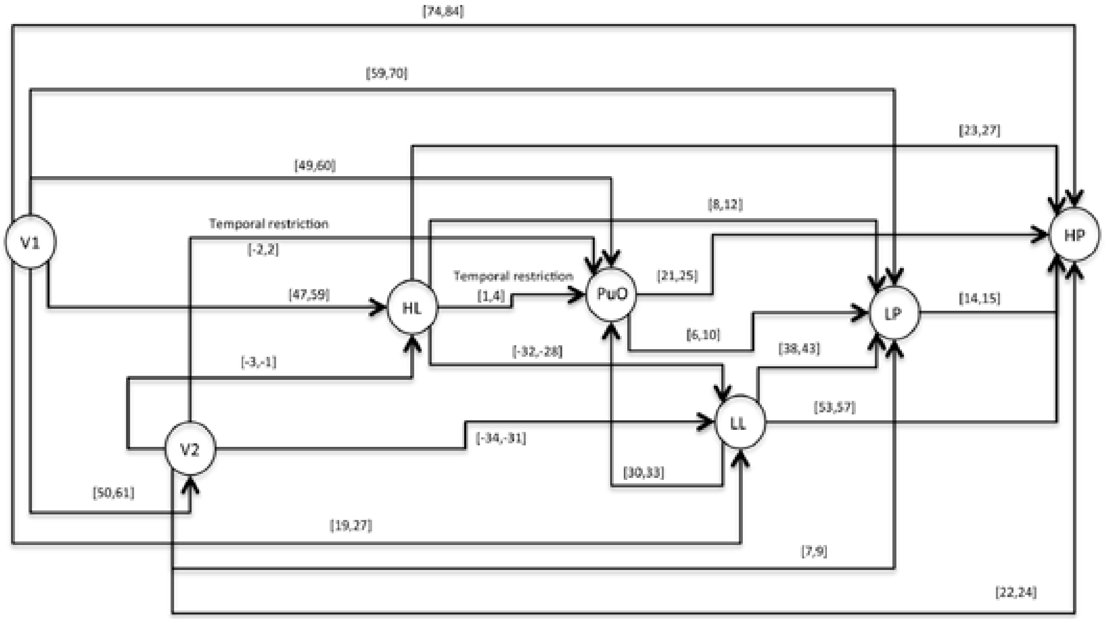


Figure 15. Directed graph (G) of the chronicle C^1_{11}

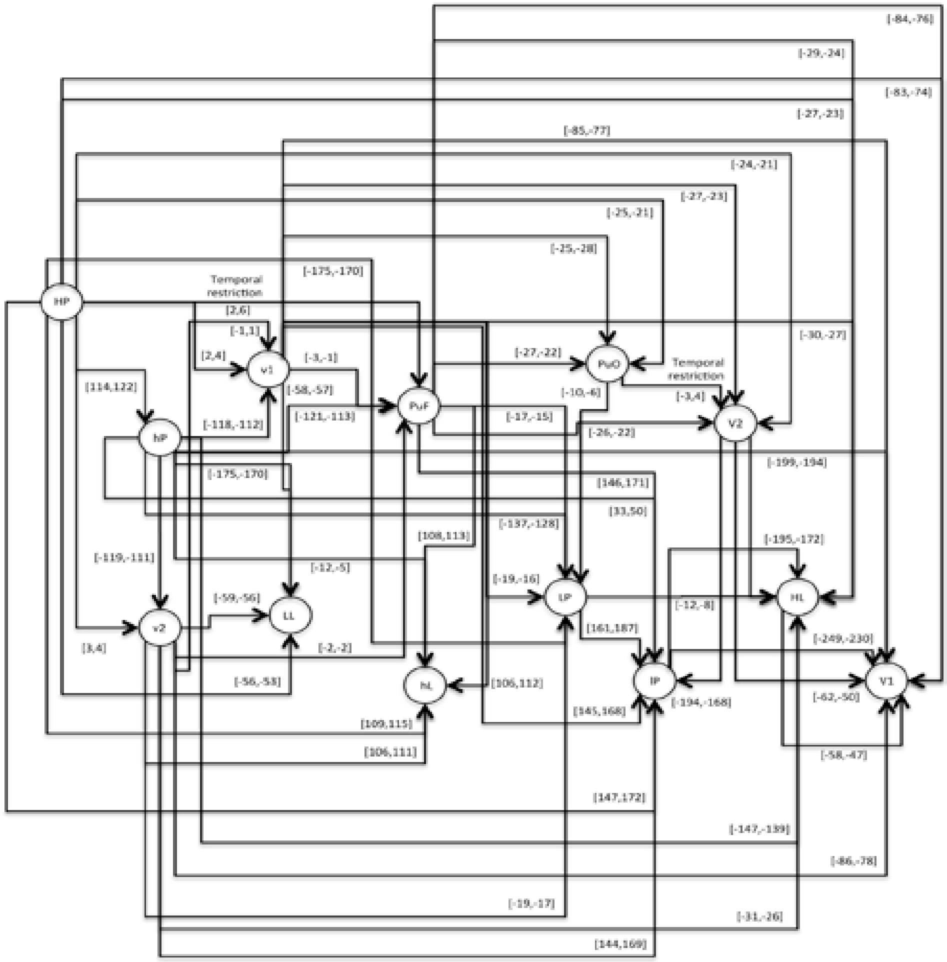


Figure 16. Directed graph (G) of the chronicle C^1_{20}

extended version of the HCDAM. $TR_{PuO,V2}$ =PuO[−3,4]V2, this temporal restriction means that valve **V2** can be opened (V2) 3 time-units before the pump Pu is turned on (PuO) or, on the contrary, PuO occurs 4 time-units before V2. $TR_{HP,Pu}$F=HP[2,6]PuF, this temporal restriction means that the pump **Pu** is turned off (PuF) between 2 and 6 time-units after reaching the high limit (HP) of the pressure Po. The chronicle C^{1}_{20} resulting after using the algorithm HCDAM is presented in **Figure 16**. The learning event sequences used is S_7, S_8 and S_9, generated in the event sequence generation section (normal shutdown).

6. RESULTS ANALYSIS

This section presents the evaluation of chronicle C1 11 that represents the temporal pattern for an abnormal start-up in the HTG system. One sequence of evaluation that belongs to this abnormal scenario is described below: S_{eval}=⟨(V1,1);(LL,26);(HL,58) ;(PuO,60);(V2,62);(LP,70) ;(HP,85)⟩. **Figure 17** to **Figure 23** present the recognition process of the chronicle and the generation of one super alarm. We can see that in **Figure 17** the first occurrence is (V1, 1), the next occurrence must be that of event LL between 20 and 28 time-units. Now, in **Figure 18** the activation of LL at 26 is shown, indicating also that the next occurrence must be HL. The following events occur (PuO, V2, LP and HP) until the chronicle is recognized and the super alarm is generated. Therefore, this new element (super-alarm) corresponds to one superior alarm that provides the operators with relevant data after a diagnosis process, thus increasing the reliability of this protective layer.

Advantage of the system using super-alarms:

Without this super-alarm, the risk that the operator will not detect an abnormal situation is high because, for them, it is normal that the typical alarms occur (high limits, low limits) during transition stages. Now, when one super-alarm occurs, the operators can determine, according to the type of super-alarm generated, what the problem is exactly. Then, they execute the operations determined for this abnormal situation and mitigate potential hazards in the process.

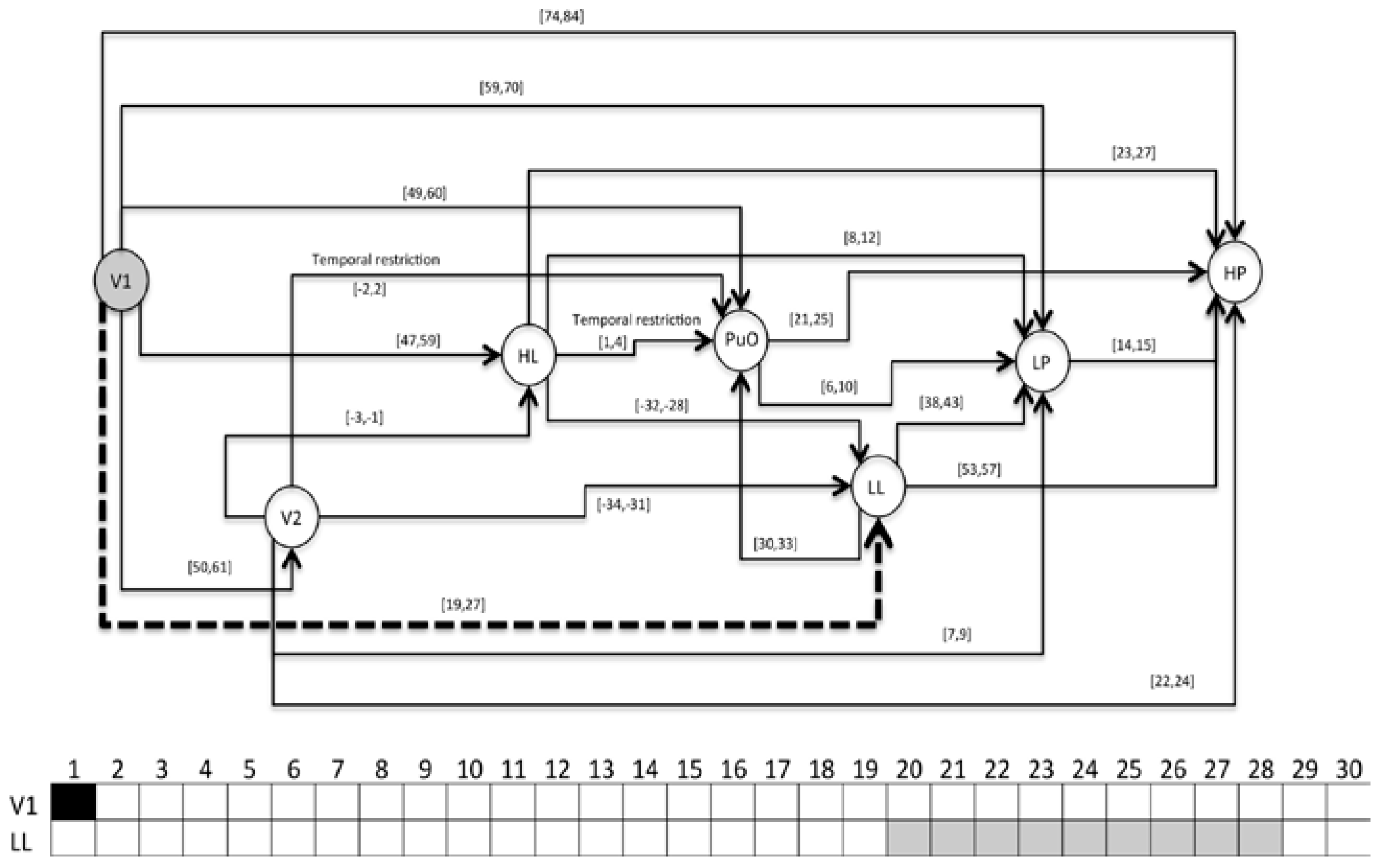
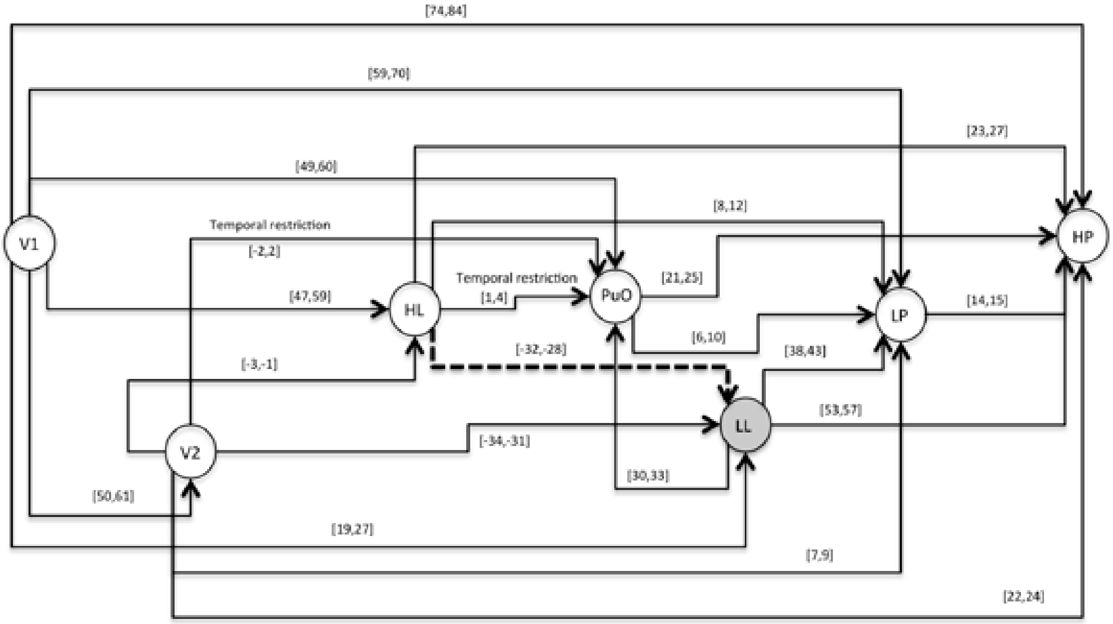
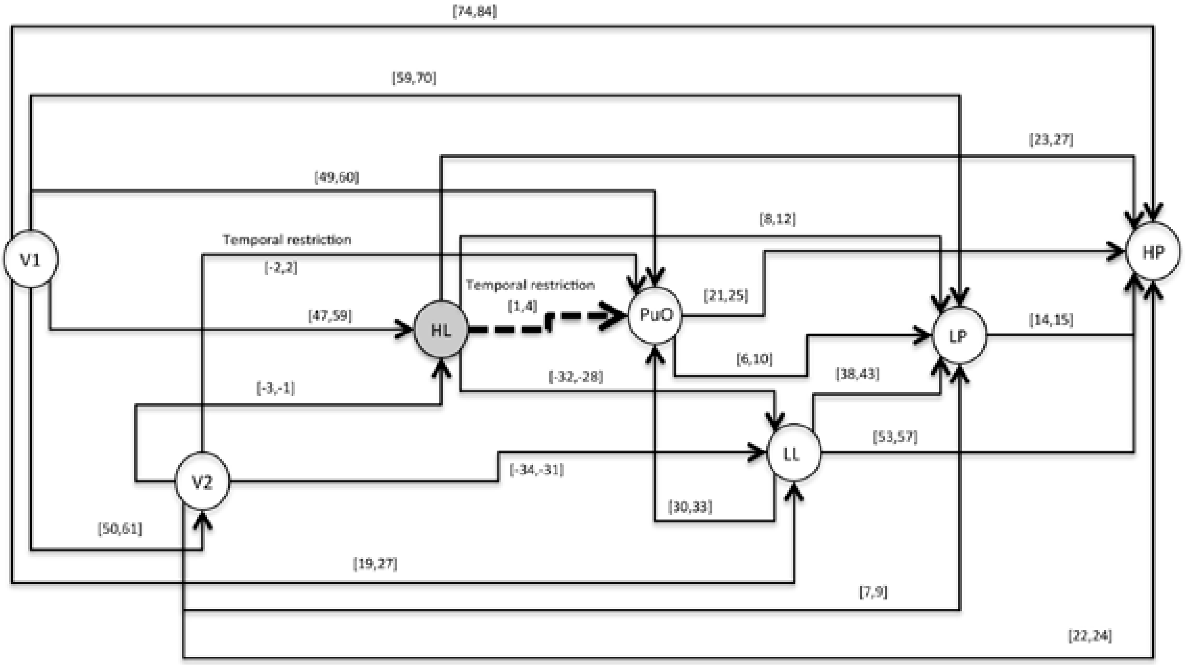


Figure 17. Activation of V1 at 1



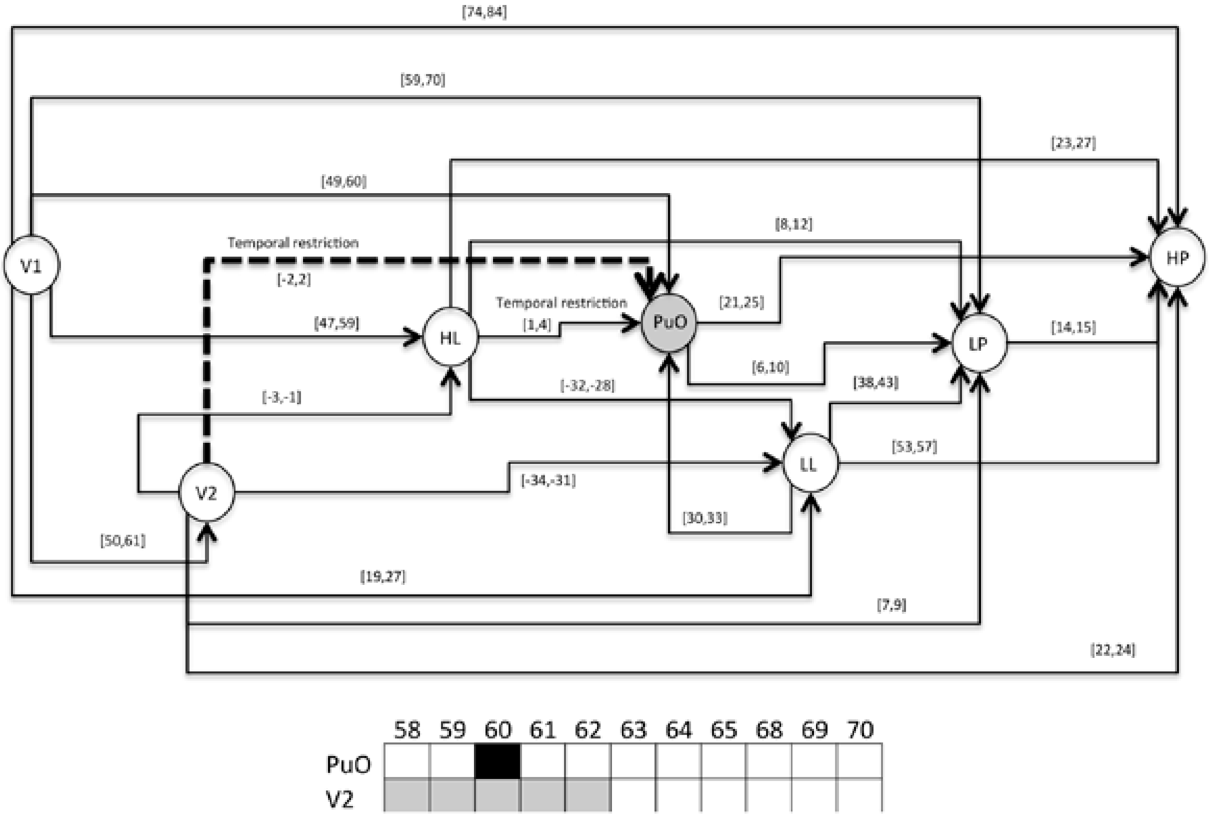
	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
LL	■																																		
HL																													▨	▨	▨	▨	▨		

Figure 18. Activation of LL at 26



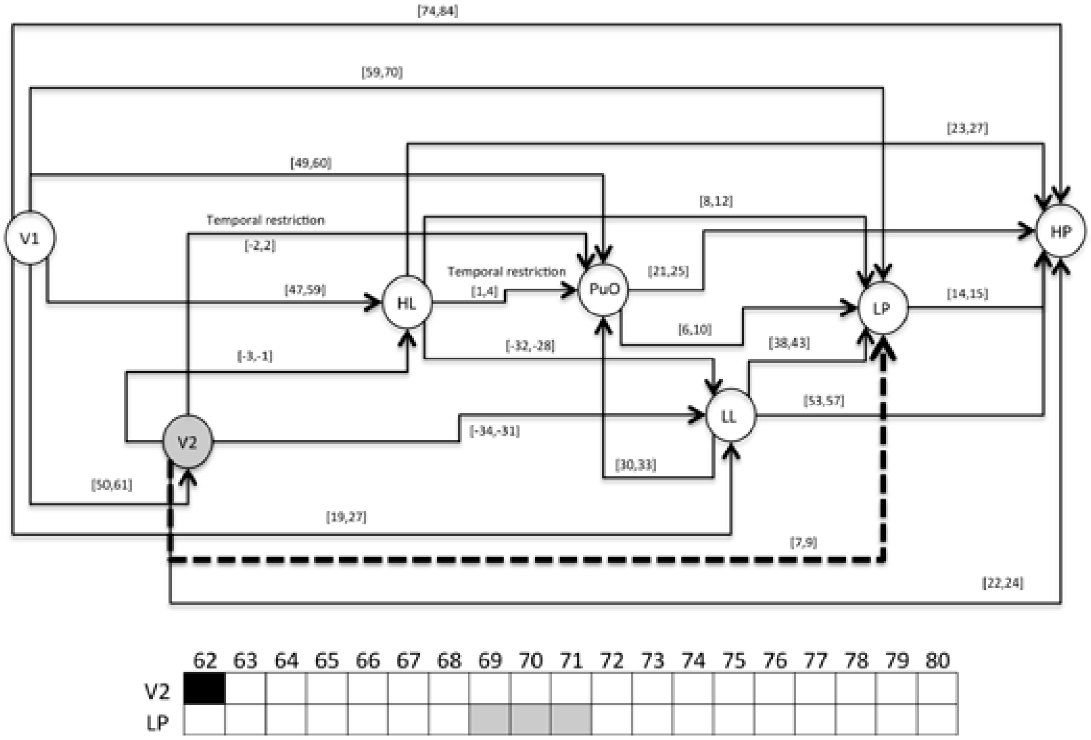
	58	59	60	61	62	63	64	65	34	35
HL	■									
PuO		▨	▨	▨	▨					

Figure 19. Activation of HL at 58



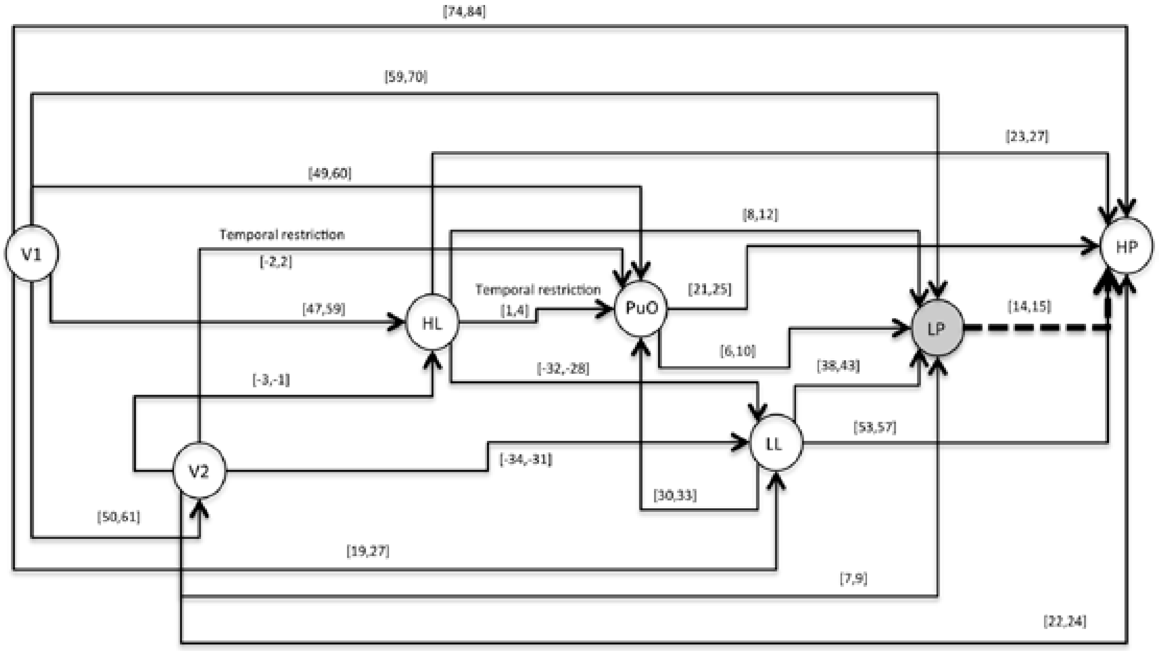
	58	59	60	61	62	63	64	65	68	69	70
PuO			■								
V2	▨	▨	▨	▨	▨						

Figure 20. Activation of PuO at 60



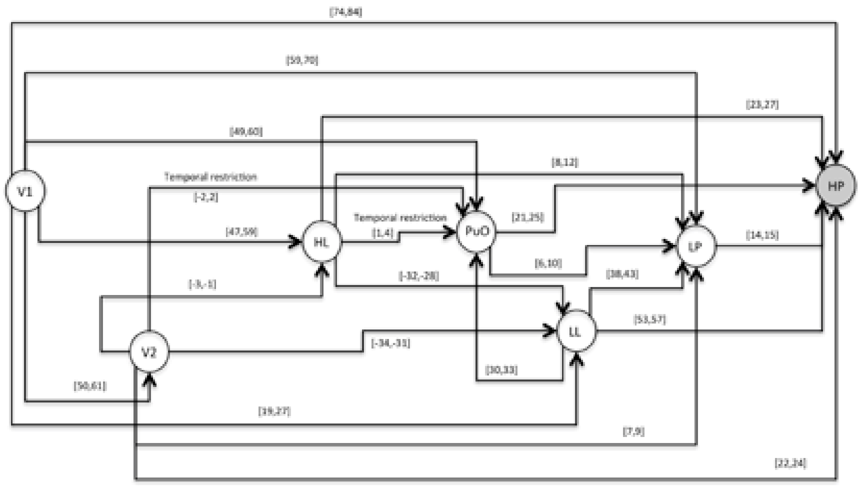
	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
V2	■																		
LP								▨	▨	▨									

Figure 21. Activation of V2 at 62



	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
LP	■																				
HP															▨	▨					

Figure 22. Activation of LP at 70



	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
HP																■					

SUPER ALARM

Figure 22. Activation of HP at 85, abnormal situation recognized generating a super-alarm

CONCLUSIONS

A new layer of protection in industrial processes has been proposed. This new layer is called super-alarm, which corresponds to a new alert to the operators, resulting from a diagnosis procedure for 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 tool to the operators during transitional stages based on recognition of the situation. Situations to be recognized correspond to normal and/or abnormal process behaviors modeled by temporal patterns called Chronicles. Any additional protection layer that increases the reliability of the industrial processes is welcomed as the risk of accidents and failures affecting human lives can be reduced. Therefore, this proposal could increase the tools and components that help the operators with early detection of hazards, and with risk analyses such as fault trees, bow tie, etc. that can be used to build failure scenario models in a supervision system. Future work will be related to the implementation of this new concept in supervision tools of an industrial process (energy, chemical, mining) and the validation of model chronicles, guaranteeing the reliability of the diagnosis tool.

REFERENCES

[1] R. W. Brennan, Toward real-time distributed intelligent control: A survey of research themes and applications, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 37 (5) (2007) 744–765. doi:10.1109/TSMCC.2007.900670.

[2] M. Khalgui, O. Mosbahi, Z. Li, H. Hanisch, Reconfiguration of distributed embedded-control systems, IEEE/ASME Transactions on Mechatronics 16 (4) (2011) 684–694. doi:10.1109/TMECH.2010.2050697.

[3] D. J. Reifer, Software failure modes and effects analysis, IEEE Transactions on Reliability R-28 (3) (1979) 247–249. doi:10.1109/TR.1979.5220578.

[4] M. G. Mehrabi, A. G. Ulsoy, Y. Koren, Reconfigurable manufacturing systems: Key to future manufacturing, Journal of Intelligent Manufacturing 11 (4) (2000) 403–419. doi:10.1023/A:1008930403506. URL https://doi.org/10.1023/A:1008930403506

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

[6] L. Bodsberg, P. Hokstad, Alarm and shutdown frequencies in offshore production, IFAC Proceedings Volumes 21 (15) (1988) 19 – 25, Ifac Workshop on Industrial Process Control Systems, Bruges, Belgium, 28 30 September. doi:https://doi.org/10.1016/S1474-6670(17)54672-8.

[7] C. Agudelo, F. Morant Anglada, E. Quiles Cucarella, E. Garca Moreno, Secuencias de alarmas para detecci´on y diagno´stico de fallos, Revista Colombiana de Computaci´on 12 (2) (2011) 31–44. doi:10.29375/25392115.1798.

[8] C. Agudelo, Integracio´n de t´ecnicas y las secuencias de alarmas para la deteccio´n y el diagnostico de fallos, Ph.D. thesis, Universidad Politecnica de Valencia (2016). doi:doi:10.4995/Thesis/10251/63450. URL https://riunet.upv.es/handle/10251/63450

[9] J. W. Vásquez Capacho, Chronicle Based Alarm Management, These, INSA Toulouse, these en cotutelle avec l'Universidad de los Andes, Colombie (Oct. 2017). URL https://hal.laas.fr/tel-02059631

[10] L. Magni, R. Scattolini, C. Rossi, A fault detection and isolation method for complex industrial systems, IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 30 (6) (2000) 860–865. doi:10.1109/3468.895922.

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

[12] R. Patton, J. Chen, Observer-based fault detection and isolation: Robustness and applications, Control Engineering Practice 5 (5) (1997) 671 – 682. doi:https://doi.org/10.1016/S0967-0661(97)00049-X.

[13] R. C. de Vries, An automated methodology for generating a fault tree, IEEE Transactions on Reliability 39 (1) (1990) 76–86. doi:10.1109/24.52615.

[14] F. Yang, D. Xiao, Progress in root cause and fault propagation analysis of large-scale industrial processes, Journal of Control Science and Engineering, 2012doi:https://doi.org/10.1155/2012/478373.

[15] M. H. Sarmiento, N. C. Isaza, Identification and estimation of functional states in drinking water plant based on fuzzy clustering, in: I. D. L. Bogle, M. Fairweather (Eds.), 22nd European Symposium on Computer Aided Process Engineering, Vol. 30 of Computer Aided Chemical Engineering, Elsevier, 2012, pp. 1317 – 1321. doi:https://doi.org/10.1016/B978-0-444-59520-1.50122-6.

[16] Y. Chen, J. Lee, Autonomous mining for alarm correlation patterns based on time-shift similarity clustering in manufacturing system, in: 2011 IEEE Conference on Prognostics and Health Management, 2011, pp. 1–8. doi:10.1109/ICPHM.2011.6024351.

[17] A. Zolghadri, J. Cieslak, D. Efimov, D. Henry, P. Goupil, R. Dayre, A. Gheorghe, H. Leberre, Signal and model-based fault detection for aircraft systems, IFAC-PapersOnLine 48 (21) (2015) 1096 – 1101, 9th IFAC Symposium on Fault Detection, Super vision and Safety for Technical Processes SAFEPROCESS 2015. doi:https://doi.org/10.1016/j.ifacol.2015.09.673.

[18] V. John, P. Jorge, A. Carlos, J. Jos, Analysis of alarm management in startups and shutdowns for oil refining processes, in: 2013 II International Congress of Engineering Mechatronics and Automation (CIIMA), 2013, pp. 1–6. doi:10.1109/CIIMA.2013.6682784.

[19] P. Mishra, D. R. Samartha, N. Pathak, S. K Jain, S. Banerjee, K. K Maudar, Bhopal gas tragedy: Review of clinical and experimental findings after 25 years, International journal of occupational medicine and environmental health 22 (2009) 193–202. doi:10.2478/v10001-009 0028-1.

[20] P. Hokstad, K. Corneliussen, Loss of safety assessment and the iec 61508 standard, Reliability Engineering System Safety 83 (1) (2004) 111 – 120. doi:https://doi.org/10.1016/j.ress.2003.09.017.

[21] R. Brooks, R. Thorpe, J. Wilson, A new method for defining and managing process alarms and for correcting process operation when an alarm occurs, Journal of Hazardous Materials 115 (1) (2004) 169 – 174, a Collection of Papers Presented at the Annual Symposium of the Mary Kay O'Connor Process Safety Centre, Texas A and M University, College Statis, TX, United States, 28-29 October, 2003. doi:https://doi.org/10.1016/j.jhazmat.2004.05.040.

[22] I. Izadi, S. L. Shah, D. S. Shook, T. Chen, An introduction to alarm analysis and design, IFAC Proceedings Volumes 42 (8) (2009) 645 – 650, 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes. doi:https://doi.org/10.3182/20090630-4-ES-2003.00107.

[23] S. R. Kondaveeti, I. Izadi, S. L. Shah, D. S. Shook, R. Kadali, T. Chen, Quantification of alarm chatter based on run length distributions, Chemical Engineering Research and Design 91 (12) (2013) 2550 – 2558. doi:https://doi.org/10.1016/j.cherd.2013.02.028.

[24] P. Urban, L. Landryov, Identification and evaluation of alarm logs from the alarm management system, in: 2016 17th International Carpathian Control Conference (ICCC), 2016, pp. 769–774. doi:10.1109/CarpathianCC.2016.7501199.

[25] S. D. Treville, J. Antonakis, N. M. Edelson, Can standard operating procedures be motivating? reconciling process variability issues and behavioural outcomes, Total Quality Management & Business Excellence 16 (2) (2005) 231–241. arXiv:https://doi.org/10.1080/14783360500054236, doi: 10.1080/14783360500054236. URL https://doi.org/10.1080/14783360500054236

[26] S. Sklet, Safety barriers: Definition, classification, and performance, Journal of Loss Prevention in the Process Industries 19 (5) (2006) 494 – 506. doi:https://doi.org/10.1016/j.jlp.2005.12.004.

[27] A. M. Dowell III, Layer of protection analysis and inherently safer processes, Process Safety Progress 18 (4) 214–220. arXiv:https://aiche.onlinelibrary.wiley.com/doi/pdf/10.1002/prs.680180409, doi:10.1002/prs.680180409.

[28] J. M. Koscielny, M. Bartys, The requirements for a new layer in the industrial safety systems, IFAC-PapersOnLine 48 (21) (2015) 1333 – 1338, 9th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes SAFEPROCESS 2015. doi:https://doi.org/10.1016/j.ifacol.2015.09.710.

[29] R. Isermann, Model-based fault-detection and diagnosis status and applications, Annual Reviews in Control 29 (1) (2005) 71 – 85. doi:https://doi.org/10.1016/j.arcontrol.2004.12.002.

[30] R. Isermann, On the applicability of model-based fault detection for technical processes, Control Engineering Practice 2 (3) (1994) 439 – 450. doi:https://doi.org/10.1016/0967-0661(94)90781-1.

[31] M. Bayoudh, L. Trav´e-Massuy`es, X. Olive, Hybrid systems diagnosis by coupling continuous and discrete event techniques, IFAC Proceedings Volumes 41 (2) (2008) 7265 – 7270, 17th IFAC World Congress. doi:https://doi.org/10.3182/20080706-5-KR-1001.01229.

[32] Z. Gao, C. Cecati, S. X. Ding, A survey of fault diagnosis and fault tolerant techniquespart i: Fault diagnosis with model-based and signal based approaches, IEEE Transactions on Industrial Electronics 62 (6) (2015) 3757–3767. doi:10.1109/TIE.2015.2417501.

[33] A. Subias, L. Travé-Massuyès, E. L. Corronc, Learning chronicles signing multiple scenario instances, IFAC Proceedings Volumes 47 (3) (2014) 10397 – 10402, 19th IFAC World Congress. doi:https://doi.org/10.3182/20140824-6-ZA-1003.02579.

[34] D. Beebe, S. Ferrer, D. Logerot, The connection of peak alarm rates to plant incidents and what you can do to minimize, Process Safety Progress 32 (1) 72–77. arXiv:https://aiche.onlinelibrary.wiley.com/doi/pdf/10.1002/prs.11539, doi:10.1002/prs.11539.

[35] J. Zhu, Y. Shu, J. Zhao, F. Yang, A dynamic alarm management strategy for chemical process transitions, Journal of Loss Prevention in the Process Industries 30 (2014) 207 – 218. doi:https://doi.org/10.1016/j.jlp.2013.07.008.

[36] J. Vásquez, A. Subias, L. Travé-Massuyès, F. Jimenez, Alarm management via temporal pattern learning, Engineering Applications of Artificial Intelligence 65 (2017) 506 – 516. doi:https://doi.org/10.1016/j.engappai.2017.07.008.

[37] J. Vásquez, L. Travé-Massuyès, A. Subias, F. Jimenez, Enhanced chronicle learning for process supervision, IFAC-PapersOnLine 50 (1) (2017) 5035 – 5040, 20th IFAC World Congress. doi:https://doi.org/10.1016/j.ifacol.2017.08.924.

[38] J. W. Vásquez, L. Travé-Massuyès, A. Subias, F. Jiménez, C. Agudelo, Chronicle based alarm management in startup and shutdown stages, in: 26th International Workshop on Principles of Diagnosis, Paris, France, 2015, pp. 277–280. URL https://hal.laas.fr/hal-01847469

[39] J. Vásquez, L. Travé-Massuyès, A. Subias, F. Jimenez, C. Agudelo, Alarm management based on diagnosis, IFAC PapersOnLine 49 (5) (2016) 126 – 131, 4th IFAC Conference on Intelligent Control and Automation SciencesICONS 2016. doi:https://doi.org/10.1016/j.ifacol.2016.07.101.

[40] M. odile Cordier, C. Dousson, Alarm driven monitoring based on chronicles, IFAC Proceedings Volumes 33 (11) (2000) 291 – 296, 4th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes 2000 (SAFEPROCESS 2000), Budapest, Hungary, 14-16 June 2000. doi: https://doi.org/10.1016/S1474-6670(17)37375-5.

[41] R. Pons, A. Subias, L. Travé-Massuyes, Iterative hybrid causal model based diagnosis: Application to automotive embedded functions, Engineering Applications of Artificial Intelligence 37 (2015) 319 – 335. doi:https://doi.org/10.1016/j.engappai.2014.09.016.

[42] Schleburg, M., Christiansen, L., Thornhill, N. F., and Fay, A. (2014). A combined anal-ysis of plant connectivity and alarm logs to reduce the number of alerts in an automation system. Journal of Process Control, Vol 23, pp. 839–851.

[43]Sandeep, R., Kondaveeti, R., Izadi, I., Shaha, S. L., Black, T., and Chen, T. (2014). Graphical tools for routine assessment of industrial alarm systems. Computers & Chemical Engineering,Vol 46, pp. 39–47.

[44] Higuchi, F., Yamamoto, I., T. Takai, M. N., and Nishitani, H. (2014). Use of event correlation analysis to reduce number of alarms. Computers & Chemical Engineering, Vol 27, pp. 1521–1526.

[45] Ge, Z. and Song, Z. (2009). Multimode process monitoring based on Bayesian method. Journal of Chemometrics, Vol 23, pp. 636–650.

[46]Liu, X., Noda, M., and Nishitani, H. (2010). Evaluation of plant alarm systems by behavior simulation using a virtual subject. Computers & Chemical Engineering, Vol 34, pp. 374–386.

[47]Yang, F., Shah, S. L., Xiao, D., and Chen, T. (2011). Improved correlation analysis and visualization of industrial alarm data. 18th IFAC World Congress Milano, Italy.

[48]Izadi, I., S.L. Shah, a. D. S., Kondaveeti, S., and Chen, T. (2009). A framework for optimal design of alarm systems. 7th IFAC Symposium on fault detection, supervision and safety of technical processes, Barcelona, Spain.

[49]Pariyani, A., Seider, W., Oktem, U., and Soroush, M. (2012). Dynamic risk analysis using alarm databases to improve process safety and product quality: Part ii bayesian analysis. AIChE Journal, Vol. 58, pp. 826–841.

[50]Liu, J. and Chen, D. (2010). Non stationary fault detection and diagnosis for multimode processes. AIChE Journal, Vol. 56, pp. 207–219.

[51]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.

[52]Jing, Z., Boang, L., and Hao, Y. (2013). Fault diagnosis strategy for startup process based on standard operating procedures. 25th Chinese Control and Decision Conference (CCDC).

[53]Duan, P., Yang, F., Chen, T., and Shah., S. (2013). Direct causality detection via the transfer entropy approach. IEEE Transactions of control system technology, Vol. 21, No. 6.

[54]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.

[55]Srinivasan, R., Viswanathan, P., Vedam, H., and Nochur, A. (2005). A framework for managing transitions in chemical plants. Computers & Chemical Engineering, Vol. 29, pp. 305–322.

[56]Xu, S., Adhitya, A., and Srinivasan, R. (2013). Hybrid model-based framework for alarm anticipation. Industrial & Engineering Chemistry Research, Vol. 53, pp. 5182–5193

Towards **ENERGY** transition and decarbonization

- Optimal use of water (re-utilization, agro-industrial use, optimal quality).
- Abatement of fugitive emissions, zero flaring and capture and use of CO_2.
- Energy diversification (solar, geothermal and hydrogen).
- Petrochemical of oil residues (asphalt binders, fossil charcoal, carbon fiber, graphene).

Hacia la transición **ENERGÉTICA** y la **descarbonización**

- Óptima utilización del agua (re-uso, aprovechamiento agroindustrial, óptima calidad).
- Abatimiento de emisiones fugitivas, cero quemas en teas y captura y utilización de CO_2.
- Diversificación energética (solar, geotermia e hidrógeno).
- Petroquímica de residuos del petróleo (ligantes asfálticos, charcoal fósil, fibra de carbono, grafeno).