Part I: "V-nets, Theory and Applications"

John William Vásquez-Capacho[1]

CAGE -SC3, UIS
Universidad Industrial de Santander
Bucaramanga, Colombia.
john.vasquez@uis.edu.co

Abstract

This paper, the first installment of a two-part series, introduces V-nets as an innovative formal model of Discrete Event Systems designed for the intricate diagnosis of complex systems, with a particular focus on applications in the industrial domain. V-nets offer a novel approach to address the inherent challenges of system diagnosis, including simultaneous occurrences, false positives, and partial recognition of event sequences. The paper establishes a robust theoretical foundation for V-nets by providing a comprehensive formal definition and delineating key properties. A detailed exposition illustrates how V-nets adeptly model dynamic processes, deviating from conventional reliance on state machines. Emphasizing the significance of V-nets in managing discrete events, the paper underscores their robust nature in identifying diverse event sequences. To illustrate practical utility, an industrial application is presented that shows the efficacy of V-nets in diagnosing and analyzing intricate systems.

Keywords: V-nets, System diagnosis, discrete-time systems, formalism, industrial applications

1. Introduction

Discrete event sequence analysis is a method used for diagnosing normal and abnormal situations in discrete event systems. In the context of discrete event

[1]Corresponding author

systems (DES), diagnosis is concerned with identifying system failures based on sequences of observed events. This approach involves modeling the system's operation as a sequence of discrete events in time, allowing for the identification of abnormal patterns or faults based on the observed event sequences. The diagnosis of discrete event systems can be based on techniques such as sequence profiling, timed patterns, and regular language modeling, which enable the identification of abnormal behavior and fault sequences within the system [1]. DES are those whose execution is described by a sequence of discrete events, and the use of discrete event sequence analysis allows for the rigorous diagnosis of these systems [2]. A fault diagnosis process involves determining whether faults have occurred in the system and identifying them. Formally, the model-based diagnosis problem can be expressed as $\langle$SD, COMP, OBS$\rangle$, where SD corresponds to the description of the system, COMP corresponds to the components involved in the system, and OBS corresponds to observations representing its normal or abnormal behavior. This framework establishes connections between each component and a fault or failure [3]. However, detecting abnormal situations arising from faults generated by incorrect procedural actions in the process poses a challenge. In this work, failures are not considered unobservable events, as is common in many approaches. Instead, failures are regarded as erroneous or incorrect event sequences, to be detected by a formal model.

In the realm of industrial applications, the seamless operation of complex systems is based on the integration of control and supervision tools. These tools play distinct yet complementary roles in ensuring the efficiency and reliability of industrial processes. Control tools, characterized by the inclusion of control actions within their structure, govern and regulate the dynamic behavior of the system. In contrast, supervision tools, devoid of inherent control actions, are dedicated to the detection and monitoring of how sequences of discrete events unfold within the system. Among the well-established formalisms employed as control tools, GRAFCET [4], automata [5], and Petri nets [6] have gained widespread usage for their effectiveness in structuring and executing control actions. These formalisms are instrumental in orchestrating the various

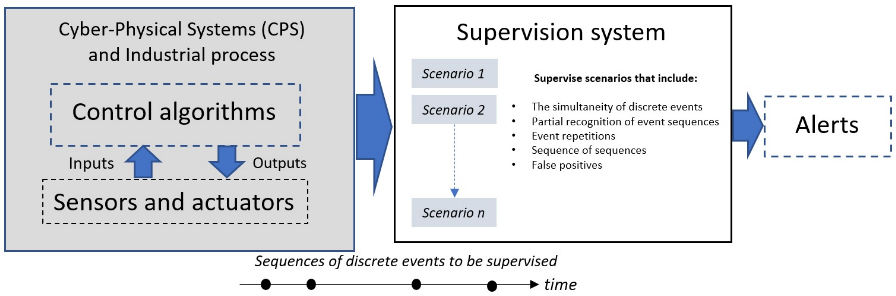


Figure 1: A general framework of the supervision of Cyber-Physical Systems (CPS) [10]

components of industrial processes, ensuring synchronization and coordination. However, when it comes to the supervision of discrete event systems, a different set of formalisms comes into play. While automata and Petri nets can be adapted for supervisory purposes, Chronicles emerges as a distinctive formal framework explicitly designed for the recognition of event sequences. Unlike the control tools that guide the process, Chronicles serves as a monitoring tool, excelling in identifying specific scenarios represented by evolving event sequences [7]. Nevertheless, situations such as simultaneous occurrences, false positives, or partial recognition in event sequences are scenarios that traditional formal DES models cannot detect [8]. On the other hand, Cyber-physical systems (CPS) necessitate the robustness of their supervisory and control systems, particularly in fault detection applications [9]. The overarching framework for the supervision of Cyber-Physical Systems (CPS) and industrial processes is depicted in Fig. 1.

These systems comprise a structure in which sensors and actuators are governed by control algorithms. The information flow generated by these processes can be interpreted as sequences of discrete events, encompassing a wide array of scenarios such as simultaneity, event repetition, false positives, sequences of sequences, and partial recognition. Detecting these diverse situations is crucial to effectively manage system behavior and diagnose potential issues [8], [10].

Simultaneous Occurrences:

Chronicles: Chronicles, while proficient in recognizing specific event sequences, lacks the capability to handle simultaneous occurrences of events. In scenarios where multiple events unfold concurrently, Chronicles may not accurately capture the temporal intricacies, potentially leading to incomplete or inaccurate representations. Petri nets: Traditional Petri Nets face challenges when it comes to modeling and managing simultaneous occurrences of events. The basic structure of Petri nets, with places representing states and transitions representing events, does not inherently support a mechanism for handling events happening simultaneously. Automata: Automata, being state-transition models, are inherently sequential in nature. Simultaneous occurrences pose a challenge as they may not be explicitly represented in the transition structure, leading to potential oversights in system analysis.

False Positives:

Chronicles: While Chronicles are adept at recognizing predefined event sequences, they may be susceptible to false positives. If the system encounters events outside the anticipated sequences due to noise or unexpected behavior, Chronicles may erroneously recognize patterns that do not align with the actual system state. Petri nets: Traditional Petri Nets lack a built-in mechanism for handling false positives. If unexpected events occur, it might disrupt the intended flow, potentially leading to inaccuracies in system representation. Automata: Similarly to Petri nets, automata may struggle with false positives, especially when events not considered in the model unfold. The rigid structure of automata may not easily adapt to unexpected deviations in the event sequence.

Partial Recognition of Event Sequences:

Chronicles: While Chronicles are designed for specific scenario recognition, they may fall short in cases of partial recognition. If an event sequence deviates from the expected pattern, Chronicles may not effectively identify or capture partial matches, limiting its adaptability to diverse system behaviors. Petri nets: Traditional Petri Nets may struggle with partial recognition, as the strict connectivity and firing semantics make it challenging to accommodate variations or partial matches in event sequences. Automata: Automata, being deterministic models, may face difficulties in accommodating partial recognition, especially when the observed event sequence deviates from the predefined transitions. In light of these limitations, there is a need for a more versatile formalism that can address simultaneous occurrences, false positives, and partial recognition of event sequences. Here, the proposed V-nets, as introduced in the previous discussions, aim to fill the gap by offering a formal model that explicitly tackles these challenges in the context of discrete event systems.

This paper is divided into 5 sections. Section 1 is an introduction. Section 2 presents the theoretical foundation of the new formalism "V-nets". Section 3 deals with the key parameters and characteristics. Section 4 presents an example in which simultaneity and repetition are important aspects to detect, and finally, Section 5 is the conclusion and future work.

2. Theoretical foundation

The V-nets formalism serves as a novel theoretical foundation for modeling and analyzing complex systems, particularly in the context of discrete event systems (DES). This formalism is designed to address challenges inherent in traditional formalisms, such as simultaneous occurrences of events, false positives, and partial recognition of event sequences. The theoretical underpinnings are grounded in their ability to provide a robust and flexible framework for representing and managing discrete events in dynamic processes. At its core, a V-net is defined as a tuple comprising sets of events, temporal constraints, and a directed graph. The directed graph visually represents the relationships between events and their temporal constraints. Unlike traditional state machines, V-nets offer a more versatile approach to modeling dynamic processes without the limitations of explicit state representations. The formal definition includes elements such as the initiation and termination events, frequencies of event occurrences, and logical predicates that validate the recognition of V-nets. This formalism introduces a unique perspective on event sequences by allowing the modeling of simultaneous occurrences, partial recognition, and counting the frequency of events in temporal sequences. The elucidation of the following definitions aims at deepening comprehension and shedding light on the practical applications of the V-net formalism. These definitions serve as foundational elements that contribute to a more nuanced understanding of how V-nets can be effectively utilized in various contexts.

Definition 1: An *event type* in the context of discrete event systems is typically denoted by a symbol or label representing a significant occurrence. Let E be the set of all possible events. An event type can be a specific action, observation, or state change in a system. This also can represent a logical combination of two or more event types, for example; the event type A=($a.b$+c); this expression indicates that the evaluation of the event type A is 1 if and only if at the time of evaluation the event type c is active (1) or both event types a and b are active.

Example: Let $a, b, c \in E$ represent event types such as the initiation of a process, the completion of a task, or the occurrence of a particular condition.

The "Time-stamped Observations' Theory" (TOT) is a mathematical theory structured to design artificial cognitive agents, called abstractors, which analyze an input flow of timed messages to produce a minimal but pertinent output flow of timed observations through an Abstraction Problem Solving Method [11]. Le Goc's Timed Observation Theory extends Shannon's Theory of Communication to timed data and offers a unique frame for Markov Chains and Poisson Theories. A dynamic system is assumed as a process $Pr(t) = \{x_1(t), x_2(t), ..., x_n(t)\}$ of time functions $(x_i(t))$. The evolution of these time functions is observed by a program Θ, and the set of variable names are defined as $X = \{x_1, x_2, ..., x_n\}$. A set of constants denoting the possible values for x_i is defined as $\triangle = \bigcup_{\forall x_i \in X} \triangle_{x_i}$ each $\triangle_{x_i} = \{\delta_1^i, \delta_2^i, ...\delta_m^i\}$. Let $\Gamma = \{t_k\}_{t_k \in \Re}$ as a set of arbitrary time instants [12], [13].

Definition 2 & 3: Timed Observation and Event Type Occurrence

A timed observation $o(t_k) \equiv (\delta_j^i, t_k)$, made by a program Θ when observing a time function $x_i(t)$ at time $t_k \in \Gamma$, is the assignment of the values $v = x_i$,

$\delta v = \delta_j^i$, and $t = t_k$ to a predicate $\Theta(v, \delta v, t)$ so that: $\Theta(x_i, \delta_j^i, t_k)$ [12], [13].

The occurrence of an event type is defined as a pair $e = (\sigma, t)$, in which $\sigma \in E$ is an event type, and t is a variable of integer type called the event date. An event type represents some change in the specifications or values of a given domain feature or a set of features. Let us define E as the ordered set of all the types of events involved in one process or industrial application. These events also represent the values δ_j^i in the timed observation.

A flow of activities generated by a system could be referred to as a sequence or trace, with time represented by a discrete set of time points. Points that are completely ordered and have a granularity that is sufficiently thin in comparison to the observed dynamics and the precision that may be obtained from observation are assumed to be accurate. A temporal sequence might thus describe the flow of activity of a system. A temporal sequence (or sequence for short) is a series of events that occur in an orderly fashion, leading to the following definition:

Definition 4: A sequence or trace on E is denoted as an ordered set of timed observations $S = \langle(\delta_j^i, t_k)_m\rangle$ with $m \in N_l$, 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. $l_{(S)} = |S|$ is the size of the temporal sequence, that is, the number of timed observations in S. An example of a sequence or trace representing an activity stream can be given by a sequence $S_x = \{o(t_1), o(t_2), o(t_3), o(t_4), o(t_5)\}$ $= \{(a, 1), (b, 3), (c, 5), (a, 6), (b, 9)\}$ with $l_{(S_x)} = 5$.

Definition 5: A simultaneous occurrence refers to a situation in which two or more event types occur at the same time or with such close timing that they can be considered simultaneous. This concept introduces a subset of event types denoted as $E^* \subset E$ to represent simultaneous occurrences. For instance, consider a process with event types a, b, c, however, there could be instances where these events occur simultaneously. Therefore, we define new event types, representing simultaneous occurrences, as follows:

- α: When a and b occur simultaneously

- β: When b and c occur simultaneously
- γ: When c and a occur simultaneously
- δ: When a, b and c occur simultaneously

The new set of event types is denoted as $E^* = \{\alpha, \beta, \gamma, \delta\}$ and the total set of event types is the set $E = \{a, b, c, \alpha, \beta, \gamma, \delta\}$ which partially solves the problem of language theory that does not accept simultaneous occurrence of events.

Definition 6: The sequence of event types, denoted as S^r, represents the sequences of characteristic or learning event sequences of a particular scenario. These sequences serve as a reference for constructing temporal patterns offline.

Definition 7: The sequence of event types, denoted as S^e, represents evaluation sequences used for online validation of a temporal pattern.

Definition 8: The frequency for each event type σ in one sequence S_n is defined as σ^f. For example, when a timed observation of the event type a occurs for a second time, then it can be represented as a^2. The date of occurrence for each type of event is defined as t^{fn} where fn indicates how many times this type of event had occurred. For example, t^3a represents the date of the third occurrence of the type of event a. In addition, the maximal frequency of occurrence for an event type in a temporal sequence is defined as $f^{max}(\sigma)$.

In their seminal works, [8] and [10] introduced a groundbreaking formalism known as V-nets, specifically designed for modeling and analyzing complex systems that evolve over time and are characterized by distinct events. Unlike traditional Petri nets, V-nets employ squares instead of circles to represent events, eliminating the need for places, while arcs connecting these squares incorporate both time constraints and frequency occurrences. This formalism is accompanied by a set of properties that define the behavior of the system, including rules governing transition firing, guidelines for handling simultaneous events, and strategies for analyzing false positives. V-nets offer a more precise and efficient modeling approach for complex systems and fault diagnosis compared to other formalism, particularly within the domains of Cyber-Physical Systems and industrial applications. Furthermore, V-nets demonstrate promising industrial applications in efficiency diagnosis, providing a graphical representation of discrete events and their interconnections within the system; the precise definition of a V-net is as follows.

Definition 9: A V-net (V_N) is defined as the tuple $\langle E, \mathcal{T}, \mathcal{G}$, **INIT, END, Frec,** tl_{eval}**, R** $\rangle$ such that:

- E is the set of event types involved in the V_N,
- $\mathcal{T}$ is the set of temporal constraints of the V-net,
- $\mathcal{G} = (\mathcal{E}, \mathcal{A}, \mathbf{Ev})$ is a directed graph in which:
  - $\mathcal{E}$ is the set of the graphical representations in squares of the event types involved in the V_N,
  - Arcs $\mathcal{A}$ represents the different time constraints between events.
  - **Ev**:(True/false) represents the activation or deactivation function of the arcs $\mathcal{A}$ according to the evolution of the timed observations.
- **INIT** corresponds to the event or events that initiate the event sequence, see Fig. 2
- **END** corresponds to the event or events that end the event sequence, see Fig. 2. In a V-net the initial event and the final event could be the same.
- **Frec** corresponds to the frequencies for each event in the event sequence. Fox example, in the interval or temporal constraint $e_i^{f_{e_i}}[I^-, I^+]^{f_{e_j}} e_j$; in which $f_{e_i(e_j)}$ corresponds to the frequency of the event e_i (e_j) on the interval $[I^-, I^+]$.
- tl_{eval} corresponds to the time of evaluation of the V-net after the occurrence of its first observation.
- **R** contains the set of logical predicates that correspond to the restrictions and warnings that confirm the V-net recognition. Examples:
  - **Frec**(a):5

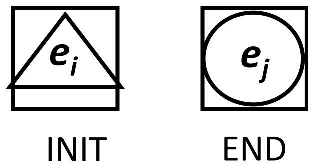


Figure 2: Graphical representation of INIT and END

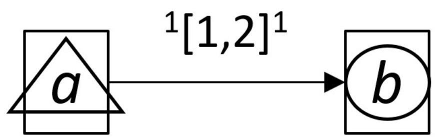


Figure 3: Example 1. Single V-net

- **Frec**(a):1 $\wedge$ **Frec**(b):1
- **Warning:** a=b
- **Warning:** Additional b after a^2

Example 1. Single V-net: Consider the V-net defined by

- $E = \{a, b\}$
- $\mathcal{T}$=$\{\sqcup_1(a^1 \Rightarrow b^1) : [1, 2]\}$
- **Frec** $= \{f^{max}(a) : 1; f^{max}(b) : 1\}$
- tl_{eval}: 2
- $R =$ **Frec**$(b) : 1$

In this simple V-net, the event a is the first event that occurs (INIT), and after of between 1 and 2 time units the event b (END) must occur, then this V-net is recognized. The graph $\mathcal{G}$ for this V-net is presented in Fig. 3

Definition 10: A *V-net event* in the context of the evaluation of V-nets can be assumed to be an object that contains properties and parameters that evolve

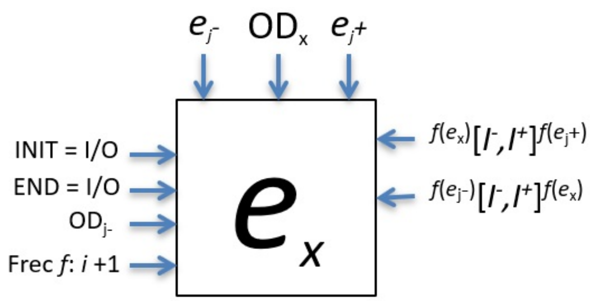


Figure 4: Representation of the event e_x as an object

according to the dynamic of the event occurrences in the evaluation sequence S^e. A graphical representation of this object is presented in Fig. 4

Let's assume that e_x signifies the occurrence of an event type within an event sequence of evaluation S^e.

- OD_x corresponds to the date of occurrences of e_x
- e_{j-} corresponds to the event type that had occurred before of e_x, this not exists if e_x is represented as INIT.
- e_{j+} corresponds to the event type that must occur after of e_x according to the V-net, this will not exists if e_x is represented as END
- INIT is a mark of I or 0 depending of the representation of e_x in the graph
- END is a mark of I or 0 depending of the representation of e_x in the graph
- OD_{j-} is the date of e_{j-} when it had occurred just before of e_x
- Frec f: i+1 corresponds to the frequency of times that event type e_x had occurred. This counter i initiates in zero and goes incrementing each time e_x occurs.
- According to the V-net graph, ${}^{f(e_x)}[I^-, I^+]^{f(e_{j+})}$ corresponds to the time transition between e_x and the next event type occurrence.

- According the V-net graph, ${}^{f_{(e_{j-})}}[I^-, I^+]^{f_{(e_x)}}$ corresponds to the time transition between e_x and event type that had occurred before.

3. Key parameters and characteristics

In V-nets, key parameters and characteristics play pivotal roles in understanding system behavior and dynamics. For example, the concept of time liveness delineates the duration for which a V-net remains operational, providing insight into the system's temporal aspects. In addition, V-net dynamics encapsulate the evolution of the modeled system over time, encompassing state changes, transitions firing, and overall system behavior. Lastly, event sequence analysis within V-nets involves scrutinizing patterns and temporal relationships among events, facilitating the detection of recurring sequences and anomalies. The following parameters collectively contribute to a comprehensive understanding of system dynamics and are vital to optimize performance and diagnose faults in complex systems.

3.1. Bandwidth limits

For the analysis of the event sequences, the time points correspond to a finite set of linearly ordered instants, and the value of the time units depends on the granularity required in the system. The bandwidth limits for each time point can be defined based on the required variability and accuracy. For example, variations of 5% before and 5% after the time point can be permissible for all event-type occurrences within this bandwidth. Fig. 5 presents an example of the bandwidth limit; in this example, the time point tp has two limits, low $tp - \%5$ and high $tp + \%5$. This can help in the computation of the analysis of simultaneous occurrences and the analysis of the date for each occurrence near the time points. Situations that are common in industrial applications.

3.2. Timed language

Similarly to language theory, in the V-nets (V_N) the alphabet corresponds to E. The timed language $L^T(E, \mathcal{T})$ of each V_N will be referenced in the strings

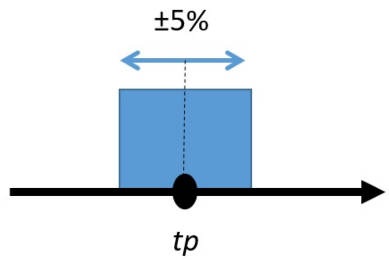


Figure 5: Example of bandwidth limits

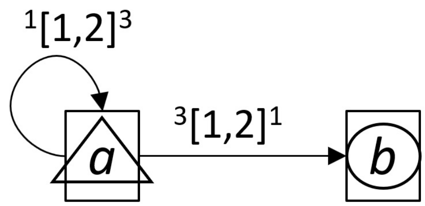


Figure 6: Example 2 of a V-net (V_N)

w that can be generated according to the configuration of the events on the graph. The V-net and the concatenation of the elements in the strings will be restricted by the set of temporal constraints $\mathcal{T}$.

Example 2. V-net with 2 arcs:

Example 2 of V-net presented in Fig. 6 in this case contains:

- $E = \{a, b\}$
- $\mathcal{T}$=$\{\sqcup_1(a^1 \Rightarrow a^3) : [1,2]; \sqcup_2(a^3 \Rightarrow b^1) : [1,2]\}$
- **Frec** $= \{f^{max}(a) : 3; f^{max}(b) : 1\}$
- tl_{eval}: 6
- $R =$ **Frec**$(b) : 1$

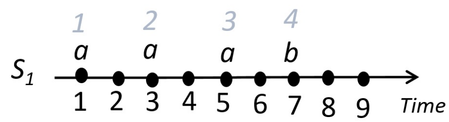


Figure 7: Example of an event sequence

3.3. Event sequences recognized by V-nets

An event sequence S must contain a finite number of timed observations. $S = \langle (e_i, t_i)_j \rangle$, in which $j \in N_l$ is a finite set of linearly ordered time points and $l_{(S)} = |S| = n$. The integration of all the events e_i included in S corresponds to all the events and each from event e_1 to event e_n, n being a finite number, $\bigcap_{e_i \in S} e = \{e | e \in \bigcap_{j=1}^{n} e_i\}$. The example of the sequence of events S_1 (see Fig. 7) has a finite number of events $|E'| = 2$ (a and b) and the number of timed occurrences is $l_{(S_1)} = 4$. The timed language is $L^T = \{(a,t_1), (a,t_2), (a,t_3), (b,t_4)\}$ with $t_1 < t_2 < t_3 < t_4$. Therefore, this sequence of events (S_1) can satisfy the time restrictions and the number of occurrences for Example 2 of V-net.

3.4. Event frequencies in one sequence of events

The frequency of an event type σ in one event sequence is finite. If f^{max} is the maximum number of timed occurrences in a sequence, then the maximal frequency of an event type σ will be $\mathbf{Frec}(\sigma) \leq f^{max}$. For the example in Fig. 6, we have $f_a^{max} = 3$ and $f_b^{max} = 1$. In the process or evaluation of the V-net, when an event frequency appears in parentheses, this indicates that the time observation does not match the frequency indicated on the time restriction of the V-net; at the end of the evaluation, a warning appears indicating the valid event occurrence before the abnormal time observation obtained. For example, the time restriction $a^3[1,2]^{1(1)}b$ and **Warning:** Additional b after a^2 indicates that one additional occurrence of the event type b happened after the second occurrence of the event type a.

3.5. Events on the directed graph

In the directed graph $\mathcal{G}$, each event is represented only once. From all the representative sequences of events S^r, or in other cases, the event types defined from the automata that manage the control of the system, in the directed graph there exist the initial event e_m:(INIT) and the last event e_k:(END). On the V-net, there could be more of an initial event and more of a final event, $\forall S^r \Rightarrow \mathcal{G}\exists\langle\{e_m : INIT\}, \{e_k : END\}$. In the example of V-net, see Fig. 6, the directed graph represents the events a: INIT and b: END as in its representative event sequences; see Fig. 8.

3.6. Time living of V-net

The time length (tl) corresponds to the time elapsed between the first and final timed observation of an event sequence. For example, if in sequence S its first time observation is (e_i, t_i) and its final timed observation is (e_n, t_n), then the time length for this sequence S is $tl = (t_n - t_i)$. Now, from the set of representative event sequences S^r or from the analysis of the automata that govern the control of the system, the maximum time length of these will be the time length noted tl_{eva} used for the evaluation of any event sequence S in the V-net. After the first timed observation happens, the V-net only will accept the event occurrences that happen before the time-length of evaluation finishes. Fig. 8 indicates that the maximum time length of the representative event sequences (S_1^r and S_2^r) is tl_{eva}=6.

3.7. V-net dynamics

The evolution of the timed observations in the directed graph $\mathcal{G}$ is activated if only congruence is present between the frequency of the event and the frequency indicated in the time interval. Example 2 of the V-net will be evaluated with the evaluation event sequence S_1^e, in which the evolution of the time observation in this V-net is presented from Fig. 9 to Fig. 23.

Fig. 9 presents the possible timed observations to this V_N of Example 2; let's check that the arcs are not activated yet because no event type occurrence has occurred and the first event that must happen is a.

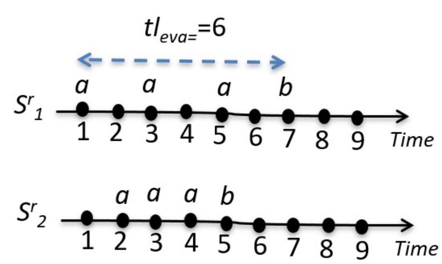


Figure 8: S^r for Example 2 of V-net and its maximal time length

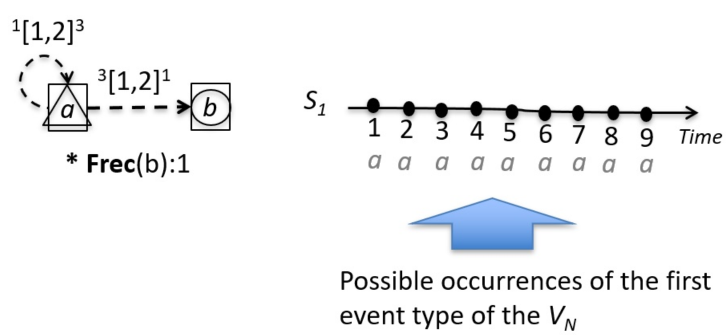


Figure 9: Possible timed observations to this V_N

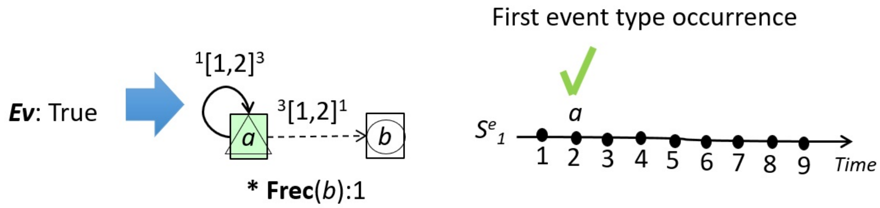


Figure 10: First timed observation (a,2)

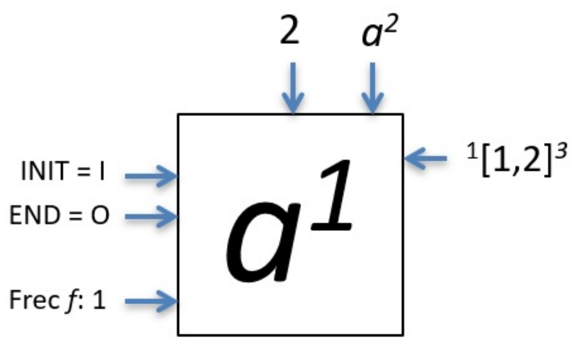


Figure 11: Representation of the event a^1 as an object

Fig. 10 presents the first timed observation to this V_N of Example 2 (a,2); let's check that one arc is active waiting for the next event type occurrence.

Fig. 11 presents the graphical representation of $V - net\ event$: a^1.

Fig. 12 presents the possible second timed observation to this V_N of Example 2.

Fig. 13 presents the second timed observation to this V_N of Example 2 (a,2) satisfying its temporal restriction; let us check that the arc is active and waiting for the next (third) event-type occurrence.

Fig. 14 presents the graphical representation of $V - net\ event$: a^2.

Fig. 15 presents the possible third timed observation of this V_N of Example 2.

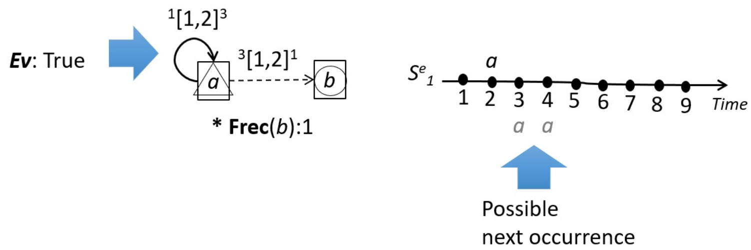


Figure 12: Possible second timed observation

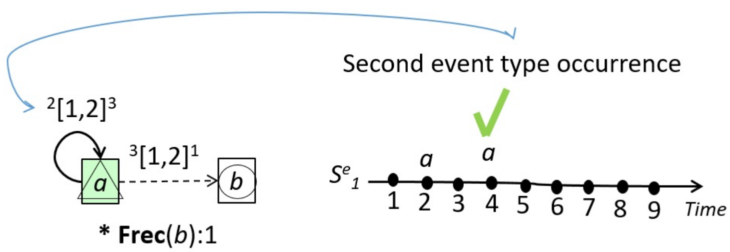


Figure 13: Second timed observation (a,4)

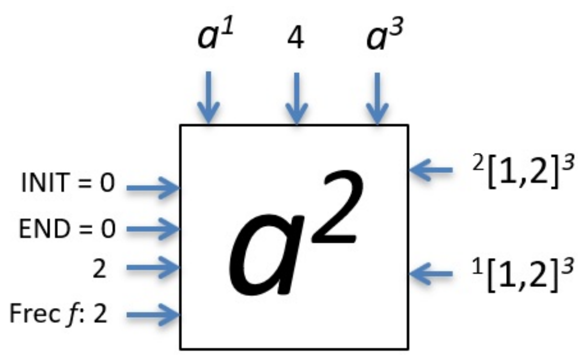


Figure 14: Representation of the event a^2 as an object

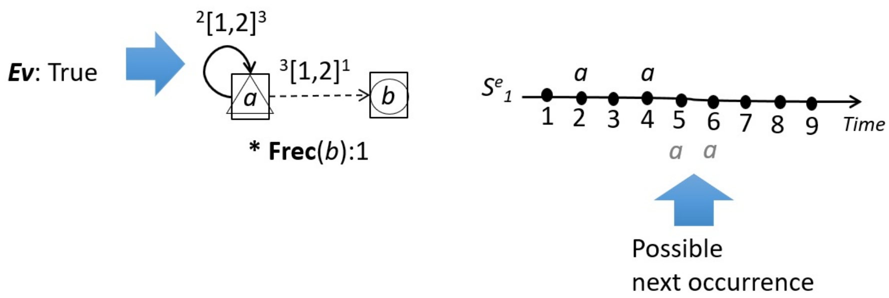


Figure 15: Possible third timed observation

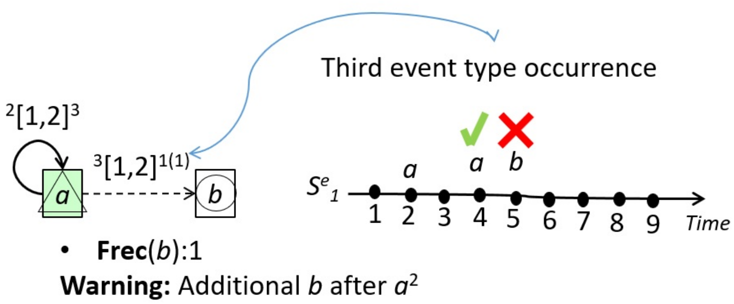


Figure 16: Third timed observation (b,5)

Fig. 16 presents the third timed observation to this V_N of Example 2 (b,5), which does not satisfy its temporal restriction because the arc that connects with b is not active yet. In this case, the frequency of b is in parentheses.

Fig. 17 presents the graphical representation of $V-net\ event$: b^1. Note that the frequency is assumed as (1) because the V-net is waiting for an event type a not for a b. In addition, this time occurrence does not have time restrictions available.

Fig. 18 presents the possible fourth timed observation to this V_N of Example 2, it is waiting for the last a.

Fig. 19 presents the fourth timed observation on this V_N of Example 2 (a,4), which satisfies its temporal restriction.

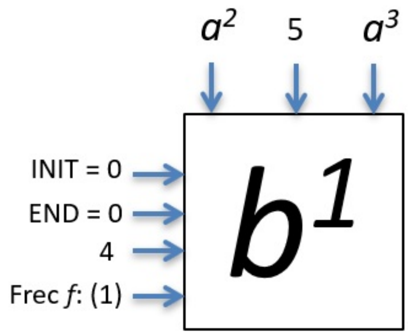


Figure 17: Representation of the event b^1 as an object

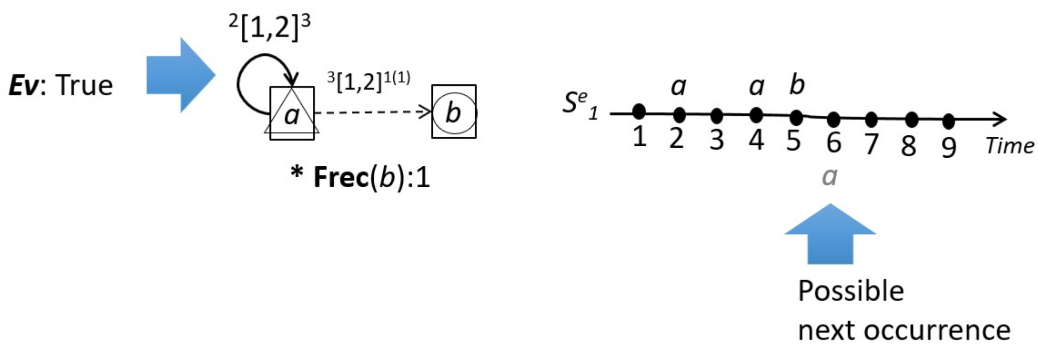


Figure 18: Possible fourth timed observation

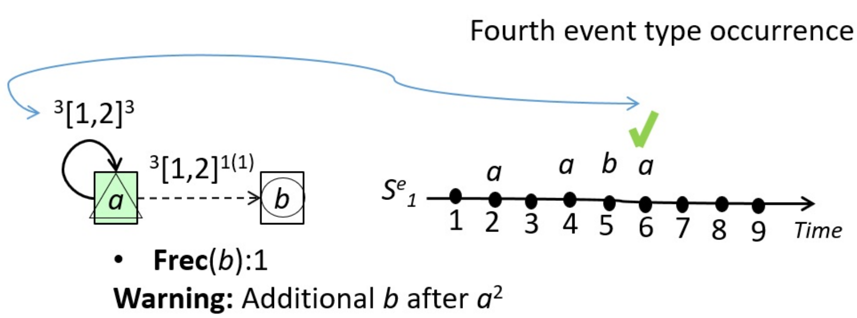


Figure 19: Fourth timed observation (a,6)

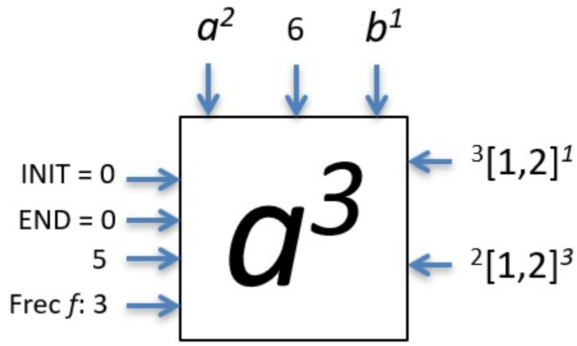


Figure 20: Representation of the event a^3 as an object

Fig. 20 presents the graphical representation of $V - net\ event$: a^3.

Fig. 21 presents the possible fifth timed observation of this V_N of Example 2, note that a new arc is active, and at this moment it is waiting for END with b.

Fig. 22 presents the fifth timed observation on this V_N of Example 2 (b,8), this is the final event that recognizes the V-net, and restarts it waiting for a new event sequence.

Fig. 23 presents the graphical representation of $V - net\ event$: b^2.

3.8. Connection of the events on graph $\mathcal{G}$

An event is connected with another event in $\mathcal{G}$ if just at least one incidence or precedence of them on the representative event sequences exists. There is an arc $\mathcal{A}$ between e_i and e_j if on the timed observations e_j is successor of e_i or e_j is predecessor of e_i.

Example 3. V-net with 4 events:

Example 3. is presented in Fig. 24, where is indicated its four representative event sequences (S_1^r, S_2^r, S_3^r and S_4^r), and this V-net is defined by.

- $E = \{a, b, c, g\}$

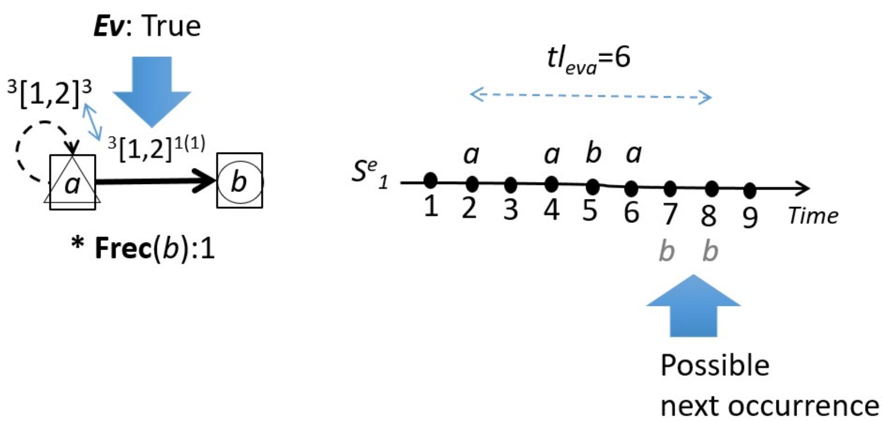


Figure 21: Possible fifth timed observation

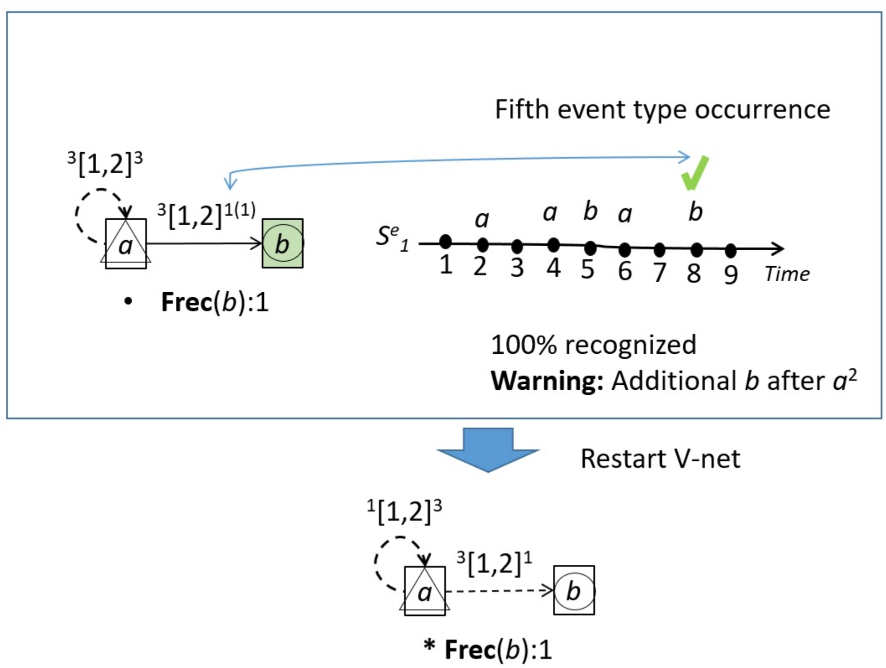


Figure 22: Fifth timed observation (b,8)

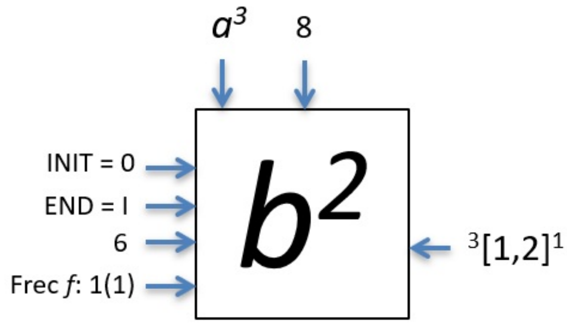


Figure 23: Representation of the event b^2 as an object

- $\mathcal{T}$=$\{\sqcup_1(a^1 \Rightarrow b^1) : [1,1]; \sqcup_2(a^1 \Rightarrow c^1) : [1,1]; \sqcup_3(b^1 \Rightarrow c^1) : [1,1]; \sqcup_4(c^1 \Rightarrow b^1) : [1,1]; \sqcup_5((c^1 \rightarrow b^1) \Rightarrow g^1) : [1,2]; \sqcup_6((b^1 \rightarrow c^1) \Rightarrow g^1) : [1,2]\}$

- **Frec** $= \{f^{max}(a) : 1; f^{max}(b) : 1; f^{max}(c) : 1; f^{max}(g) : 1\}$

- tl_{eval}: 4

- $R =$ **Frec**$(g) : 1$; **Warning**: b=c

In $\mathcal{G}$ the event a is connected to events b and c because in representative event sequences, b and c always follow, after that appearing the event a, and in addition, b and c never happen simultaneously. This is a special situation that generates a warning. The notation ”$b = c$” indicates that these events occur at the same time. Note that the expression $c^1 \rightarrow b^1$ in the time restriction $\sqcup_5$ expresses that activation of the event b^1 is possible only if the event c^1 had occurred before. Similar in $\sqcup_6$ with $b^1 \rightarrow c^1$ but in this case, the activation of the event c^1 only is possible if the event b^1 had occurred before.

3.9. Occurrence matrix

The occurrence matrix is a timeless representation of the event sequences that accept the V-net. The columns of the matrix represent the events of V_N, and the rows represent all ordered occurrences on the possible sequences of

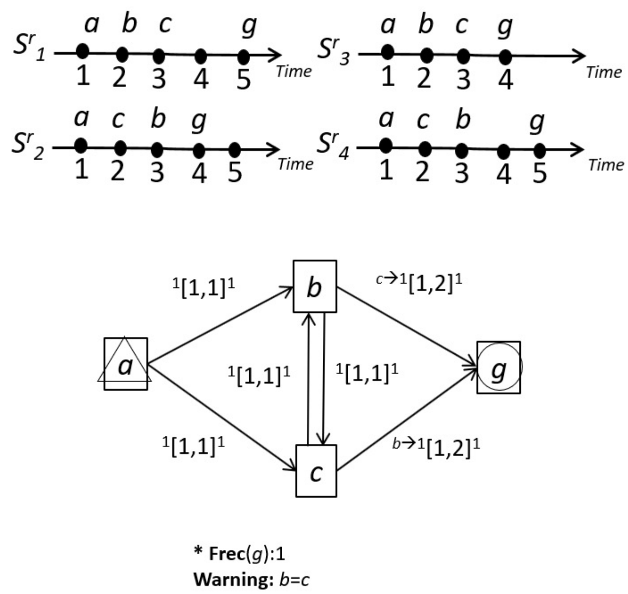


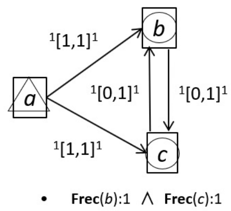
Figure 24: Example 3. V-net with 4 events

events, beginning with INIT and ending with END. This characteristic of the V_N allows for a preliminary review of all the possible order of the event occurrences permitted to evaluate the V-net. Inside these matrices, 1 represents the timed observations of the event types and 0 represents that the event type had not occurred.

Example 4. V-net with 3 events and its occurrence matrices:

Example 4. is presented in Fig. 25, where is indicated its three occurrence matrices, and this V-net is defined by.

- $E = \{a, b, c\}$
- $\mathcal{T}$=$\{\sqcup_1(a^1 \Rightarrow b^1) : [1,1]; \sqcup_2(a^1 \Rightarrow c^1) : [1,1]; \sqcup_3(b^1 \Rightarrow c^1) : [0,1]; \sqcup_4(c^1 \Rightarrow b^1) : [0,1]\}$
- **Frec** $= \{f^{max}(a) : 1; f^{max}(b) : 1; f^{max}(c) : 1; \}$
- tl_{eval}: 3



POSSIBLE OCCURRENCE MATRIX

Matrix 1

	a	*b*	*c*
INIT	1	0	0
END	0	1	1

Matrix 2

	a	*b*	*c*
INIT	1	0	0
Oc1	0	1	0
END	0	0	1

Matrix 3

	a	*b*	*c*
INIT	1	0	0
Oc1	0	0	1
END	0	1	0

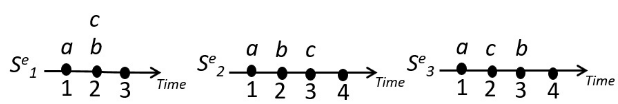


Figure 25: Example 4 of V-net with its occurrence matrices

- $R = \textbf{Frec}(b) : 1 \wedge \textbf{Frec}(c) : 1$

The V-net example depicted in Fig. 25 showcases three potential occurrence matrices. In the first matrix, the initial event (INIT) is labeled a, followed by the simultaneous occurrence of events b and c (END). It is important to note that in this instance, simultaneous occurrences of b and c are permissible, and a specific designation of "simultaneous occurrence" is not necessary to denote this condition. In the second matrix, the sequence begins with event a (INIT), followed by event b (Oc1), and concludes with event c (END). Finally, the third matrix illustrates another scenario where the sequence starts with event a (INIT), proceeds with event c (Oc1), and concludes with event b (END). Note that in the time restrictions from b to c and from c to b it is permitted simultaneous occurrences due to the value of zero 0.

3.10. Partial recognition

Definition 11: V-net instance. A V-net $\langle E, \mathcal{T}, \mathcal{G}$, **INIT, END, Frec,** tl_{eval}**, R** $\rangle$ is recognized when occurs a temporal sequence S of events E', such that $\xi \subseteq E'$ and it satisfies all temporal constraints $\mathcal{T}$.

A V-net is partially recognized (**%Rec**) when occurs a temporal sequence S of events E', such that $|E'| = |\xi|$ and it partially satisfies all temporal constraints $\mathcal{T}$. Also, it is partially recognized, if the quantity of the timed occurrences in S is less than the quantity indicated in the V-net. This guarantees that the exact number of events that will occur will satisfy all temporal constraints. If there are additional event occurrences, although the V-net could be recognized in 100%, warnings may be generated for each additional timed observation that does not match the V-net.

Example 5. V-net with 4 events and its partial recognition:

Example 5. is presented in Fig. 26, where is indicated its partial recognition, and this V-net is defined by.

- $E = \{a, b, c, d\}$
- $\mathcal{T}$=$\{\sqcup_1(a^1 \Rightarrow b^1) : [3,4]; \sqcup_2(a^1 \Rightarrow c^1) : [0,0]; \sqcup_3(b^1 \Rightarrow d^1) : [1,2]; \sqcup_4(c^1 \Rightarrow b^1) : [3,4]\}$
- **Frec** $= \{f^{max}(a) : 1; f^{max}(b) : 1; f^{max}(c) : 1; f^{max}(d) : 1\}$
- tl_{eval}: 6
- $R = \mathbf{Frec}(d) : 1$

The example presented in Fig. 26, indicates that the sequence S_3^e recognized the V-net in 75%, because **%Rec**=(3/4)*100.

$$\%\mathbf{Rec} = \frac{Number \quad of \quad events \quad recognized}{Number \quad of \quad timed \quad observations} * 100 \qquad (1)$$

The example of V-net in Fig. 26 has the following set of events $E = \{a, b, c, d\}$, and S_1^e and S_2^e had recognize 100% the V-net; on contrary S_3^e does not, because event c occurs after event a, and both must happen simultaneously.

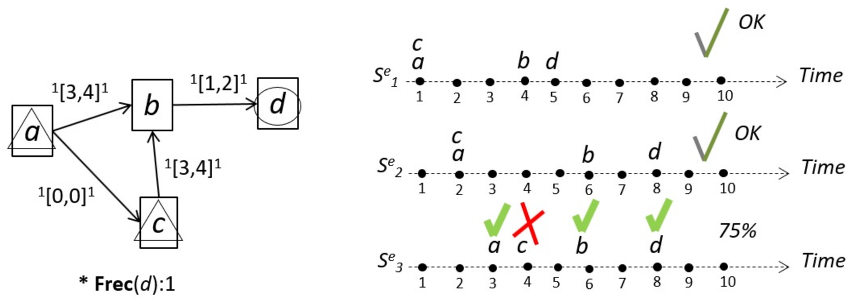


Figure 26: Example 5 of V-net and its partial recognition of a V-net

4. Case study: Reactor Startup Sequence for a Pressurized Water Reactor (PWR)

The launch sequence of a Pressurized Water Reactor (PWR) is a crucial phase in the operation of nuclear power generation plants, marking the transition from shutdown to full power production. This process entails a meticulously planned series of steps aimed at initiating and controlling the nuclear fission process within the reactor core while ensuring the safety and stability of the entire system. The PWR design, renowned for its widespread use in commercial nuclear power plants, relies on a closed-loop cooling system where pressurized water serves as both a coolant and a moderator. In this case study, we dive into the intricate details of the reactor startup sequence for a PWR, focusing on the initiation of the start procedures and the systematic activation of key reactor components. We explore the essential steps involved in control rod manipulation, neutron flux stabilization, coolant system activation, steam generation, turbine synchronization, and grid connection. Through a comprehensive examination of the startup sequence, we gain insights into the operational challenges, safety considerations, and regulatory compliance inherent in the startup process of a PWR. Additionally, we highlight the significance of leveraging advanced modeling and analysis techniques, such as V-nets, to enhance the supervision and monitoring of reactor startup procedures, thereby

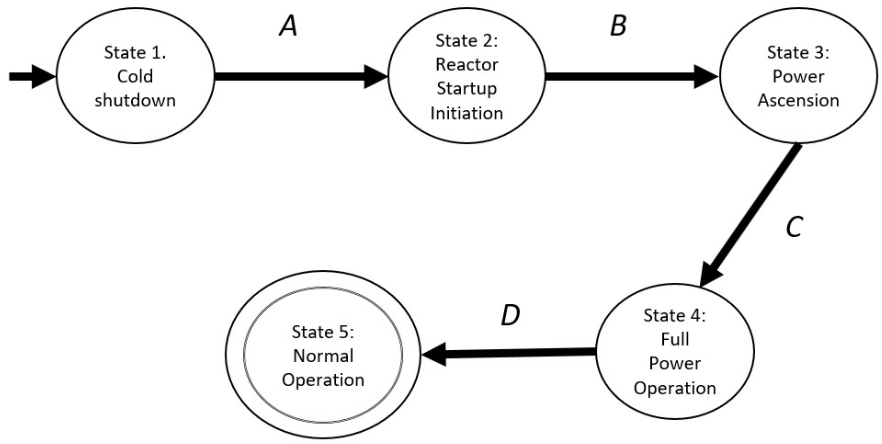


Figure 27: Automata for a Reactor Startup

ensuring the safe and efficient operation of nuclear power generation plants.

4.1. Automata definition

Automata play a crucial role in modeling and supervising the Reactor Startup Sequence for a Pressurized Water Reactor (PWR). These finite-state machines provide a structured framework for representing the sequential progression of events and states during the startup process, ensuring safe and efficient initiation of reactor operations. In this detailed description, we will outline each step of the Reactor Startup Sequence, highlighting the primary industrial components involved, the event sequences required, and the response of process variables such as temperature, pressure, etc., categorized into high, medium, or low levels. The example of this automata is presented in Fig. 27 in which can be observed its five states with its four transition events.

4.1.1. State 1: Cold shutdown

Primary Industrial Component: Reactor Core The primary industrial component involved in the Cold Shutdown state is the reactor core, which houses the nuclear fuel assemblies and controls the fission reaction.

Event Sequence:

- Initialization of Reactor Systems: This event involves the activation and initialization of various reactor systems, including coolant pumps, control systems, and safety mechanisms.
- Pre-Startup Checks: Pre-startup checks are conducted to ensure that all systems are functioning correctly and that safety protocols are in place before initiating the reactor startup process.

Response of Process Variables:

- Temperature: During cold shutdown, the reactor core temperature is maintained at a low level, as the nuclear fission reaction is not active.
- Pressure: The pressure within the reactor vessel is also kept low during cold shutdown, as there is no generation of steam or circulation of coolant.
- Neutron Flux: In a cold shutdown state, the neutron flux within the reactor core is absent since there is no ongoing nuclear fission reaction.

Transition Conditions: The transition from the Cold Shutdown state to the next state is contingent upon the successful completion of pre-startup checks. These checks ensure that all necessary systems are operational, safety measures are in place, and conditions are suitable for proceeding with the reactor startup process. If any anomalies or issues are detected during the pre-startup checks, corrective actions must be taken before advancing to the next state.

4.1.2. State 2: Initiation of reactor startup

Primary Industrial Component: Control rods in the startup stage of the reactor; the primary industrial component involved is the control rods. These rods are instrumental in controlling the nuclear fission reaction within the reactor core by absorbing neutrons and regulating the rate of reaction.

Event Sequence:

- Control Rod Withdrawal: This event involves the gradual withdrawal of control rods from the reactor core, allowing for the initiation of the nuclear fission reaction.

- Neutron Flux Measurement: Following control rod withdrawal, neutron flux measurements are taken to monitor the rate of the nuclear reaction and ensure it remains within safe and controlled limits.

- Coolant System Activation: The coolant system is activated to facilitate the circulation of coolant (usually water) through the reactor core, helping to transfer heat away from the fuel assemblies.

Response of Process Variables:

- Temperature: As the nuclear fission reaction begins and heat is generated within the reactor core, the temperature of the coolant and reactor components starts to rise. The temperature increase is moderate (medium) during this phase.

- Pressure: With the activation of the coolant system and the initiation of the nuclear reaction, the pressure within the reactor vessel also begins to rise as steam is generated. The pressure increase is moderate (medium) at this stage.

- Neutron Flux: The neutron flux, which represents the rate of neutron flow within the reactor core, transitions from a low to a medium level as control rods are withdrawn and the nuclear reaction commences.

Transition Conditions: The transition from the Reactor Startup Initiation state to the next state is contingent upon several conditions:

- Neutron Flux Stabilization: The neutron flux must stabilize within predetermined limits, indicating that the nuclear reaction is proceeding at a controlled and sustainable rate.

- Coolant Temperature and Pressure: Coolant temperature and pressure must reach operational levels, ensuring that the reactor core is adequately cooled and pressurized for stable operation.

4.1.3. State 3: Power Ascension

Primary Industrial Components: Reactor Core and Turbine During the Power Ascension state, the primary industrial components involved are the reactor core and the turbine. The reactor core continues to generate heat through the nuclear fission reaction, while the turbine converts this thermal energy into mechanical energy to generate electricity.

Event Sequence:

- Increase in Reactor Power Output: In this event, the reactor power output is gradually increased by adjusting control rod positions or altering the flow rate of coolant through the core. This increase in power output drives the subsequent processes.
- Steam Generation: As the reactor generates heat, the coolant water circulating through the core absorbs this heat and is converted into steam. This steam is then directed to the turbine for power generation.
- Turbine Activation: The steam produced by the heat from the reactor is supplied to the turbine, causing it to spin. The spinning turbine is connected to a generator, which converts mechanical energy into electrical energy for distribution.

Response of Process Variables:

- Temperature: With the reactor operating at higher power levels, the temperature of both the coolant and reactor core rises significantly. This increase in temperature is characterized by being high.
- Pressure: The generation of steam within the reactor vessel results in a substantial increase in pressure. The pressure within the reactor vessel and associated systems is also high during this phase.

- Neutron Flux: As reactor power output increases, the neutron flux within the reactor core also increases, reaching medium to high levels. This flux is indicative of the intensity of the nuclear reaction occurring within the core.

Transition Conditions: The transition from the Power Ascension state to subsequent states is contingent upon meeting specific conditions:

- Stable Reactor Power Output: The reactor must achieve a stable power output level within predefined parameters, indicating that the nuclear reaction is being controlled and sustained effectively.

- Steam Supply to Turbine: Steam generated must be supplied to the turbine within specified parameters, ensuring optimal turbine performance and electricity generation.

4.1.4. State 4: Full Power Operation

Primary Industrial Component: Power Grid Connection During Full Power Operation, the primary industrial component involved is the connection to the power grid. This state signifies that the nuclear power plant is operating at its maximum power output and is ready to supply electricity to the grid.

Event Sequence:

- Grid Connection: The nuclear power plant synchronizes its output with the electrical grid, ensuring that the generated electricity matches the grid's frequency and phase.

- Full Power Generation: Once synchronized, the reactor continues to operate at full power, generating electricity at its maximum capacity.

- Continuous monitoring: Throughout this state, the plant's systems and processes are continuously monitored to ensure safe and efficient operation. This includes monitoring reactor parameters, coolant flow rates, and safety systems.

Response of Process Variables:

- Temperature: The temperature within the reactor vessel and associated systems remains high during full power operation, reflecting sustained nuclear fission reactions and heat generation.
- Pressure: The pressure within the reactor vessel and associated systems remains high to maintain the integrity of the coolant system and ensure efficient power generation.
- Neutron Flux: The neutron flux within the reactor core remains high during full power operation, indicating the sustained nuclear chain reaction necessary for power generation.

Transition Conditions: The transition from the full-power operation state to subsequent states is contingent upon meeting specific conditions:

- Grid Synchronization Successful: The connection to the power grid must be established successfully, with the plant output synchronized with the frequency and phase of the grid.
- Full Power Generation Sustained: The plant must maintain full power generation within operational limits, ensuring stable and reliable electricity supply to the grid.

4.1.5. State 5: Normal Operation

Primary Industrial Component: Reactor core and safety systems In the normal operation state, the primary industrial components involved are the reactor core and various safety systems. This state represents the routine operational phase of the nuclear power plant, where the reactor operates within normal parameters, and safety measures are actively maintained.

Event Sequence:

- Routine Maintenance: Scheduled maintenance activities are performed on various plant components to ensure their continued functionality and reliability. This includes tasks such as equipment inspections, lubrication, and minor repairs.

- Periodic Inspections: Regular inspections are conducted to assess the condition of critical plant systems, including the reactor core, coolant systems, and safety features. These inspections help identify any potential issues or degradation that may require corrective action.
- Emergency response preparation: The plant remains prepared to respond to any emergency situations that may arise, such as equipment failures, natural disasters, or external threats. Emergency response drills and training exercises are conducted to ensure that staff are adequately trained and equipped to handle emergencies effectively.

Response of Process Variables:

- Temperature: The temperature within the reactor core and associated systems remain stable at medium levels during normal operation, indicating steady-state conditions and controlled heat generation.
- Pressure: Pressure within the reactor vessel and coolant systems remains stable at medium levels, ensuring the integrity and efficiency of the plant's operations.
- Neutron Flux: The neutron flux within the reactor core remains stable at medium levels, reflecting the consistent nuclear reactions occurring within the reactor.

Transition Conditions: The transition from the Normal Operation state to subsequent states is contingent upon meeting specific conditions:

- No Anomalies Detected: Routine inspections and maintenance activities do not reveal anomalies or problems that require immediate attention. Plant systems continue to operate within established safety and performance criteria.

- Operational of Emergency Response Systems: The plant's emergency response systems remain fully operational and capable of responding effectively to any unforeseen events or emergencies. This ensures that the plant is ready to address any potential safety concerns or disruptions to normal operations.

4.2. V-net construction

This section delves into the construction of V-nets tailored specifically for the Reactor Startup Sequence of a Pressurized Water Reactor (PWR). V-nets, a novel formalism for modeling and analyzing dynamic systems characterized by discrete events, offer a powerful toolset for capturing the intricate dynamics of complex industrial processes. The Reactor Startup Sequence of a PWR represents a critical phase in the operation of nuclear power plants, encompassing a series of meticulously orchestrated steps aimed at safely initiating and ramping up reactor power output. Each stage of this sequence is marked by discrete events, ranging from the initiation of reactor start procedures to the achievement of full power operation and subsequent transition to normal operational mode. To construct effective V-nets for the Reactor Startup Sequence, researchers must first identify and define the discrete events associated with each stage of the process. These events are informed by the expertise of nuclear engineers, plant operators, and safety specialists who have a deep understanding of the operational nuances and safety protocols inherent to nuclear power plant operations. Furthermore, researchers will explore three or more plausible event sequences representative of typical operational scenarios encountered during the Reactor Startup Sequence. These event sequences serve as the building blocks for V-nets, providing concrete examples of how different combinations of events unfold over time and influence the behavior of the system. Through collaborative efforts between domain experts and modeling specialists, the aim is to construct V-nets that not only accurately represent the Reactor Startup Sequence but also offer valuable insights into system dynamics, performance metrics, and potential areas of improvement. Using the rich contextual information provided by experts, V-nets will serve as invaluable tools to enhance the safety, efficiency, and reliability of nuclear power plant operations.

4.2.1. V-net for State 1

The Cold Shutdown phase typically unfolds with the following event sequence, each event occurring within specified time restrictions:

Event a (Initialization of Reactor Systems) occurs first, initializing the primary and secondary coolant systems. Following Event a, Event A (Pre-Startup Checks) takes place, involving safety checks and system verifications. This event should occur within a time frame of 5 to 10 minutes after the start of the shutdown phase. These time restrictions ensure that the reactor systems are initialized promptly and that safety checks are conducted without undue delay, laying the groundwork for the subsequent stages of the reactor startup process. On the other hand, the discrete events defined for the variables will be:

- Temperature
  - Low: T_l
  - Medium: T_m
  - High: T_h
- Pressure
  - Low: P_l
  - Medium: P_m
  - High: P_h
- Neutron Flux
  - Absent: N_l
  - Medium: N_m
  - High: N_h

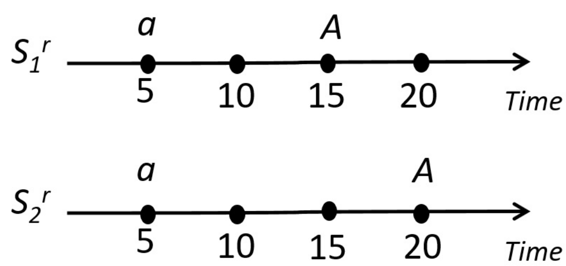


Figure 28: Representative event sequences for State 1

In this case, the event A represents the following expression A: $T_l.P_l.N_l$ which indicates that at the activation of the event A, the evaluation of the process variables will determine that the events T_l, P_l, and N_l must be active representing the correct value of the process variables.

Fig. 28 presents the representative sequences of events in this state. Furthermore, Fig. 29 presents the graphical representation of the V-net to supervise this State 1. Note that the event A is the final event of the V-net and the transition event to the next state.

V_{N1} is defined by

- $E = \{a, A\}$
- $\mathcal{T}$=$\{\sqcup_1(a^1 \Rightarrow A^1) : [10, 15]\}$
- $\mathbf{Frec} = \{f^{max}(a) : 1; f^{max}(A) : 1\}$
- tl_{eval}: 15
- $R = \mathbf{Frec}(A) : 1,\ A = T_l \wedge P_l \wedge N_l$

The condition $A = T_l \wedge P_l \wedge N_l$ must be arranged after a between 10 and 15 minutes.

4.2.2. V-net for State 2

During State 2: Initiation of the reactor startup, the startup sequence involves a series of operational actions and responses of process variables. The

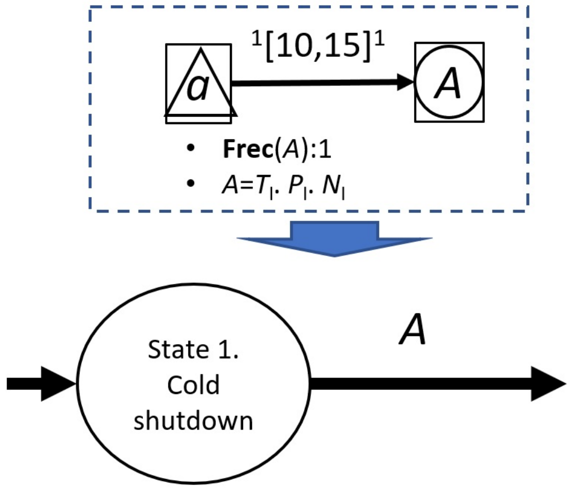


Figure 29: V-net V_{N1} that supervises State 1

sequence begins with the Control Rod Withdrawal (CRW) (event b), where operators initiate the withdrawal of control rods to facilitate the increase in neutron flux. This action leads to a transition of neutron flux from low (N_l) to medium (N_m) levels between 10 and 15 minutes. Subsequently, the Coolant System Activation (CSA) (event c) occurs, where the operators activate the components of the coolant system to manage the reactor temperature. This action leads to the onset of an increase in temperature and pressure from their low levels (T_l, P_l). The activation of the coolant system should be completed within 20 to 30 minutes after the neutron flux measurement to maintain operational safety. These discrete events, marked by their respective operational actions and transitions in the process variables, ensure a systematic and controlled startup process for the pressurized water reactor (PWR).

Fig. 30 presents the representative sequences of events in this state. Furthermore, Fig. 31 presents the graphical representation of the V-net to supervise this State 2. Note that in this case, event B is the final event of the V-net and the transition event to the next state.

V_{N2} is defined by

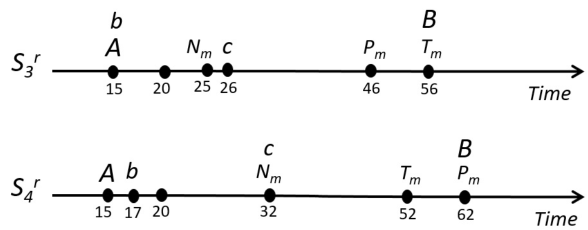


Figure 30: Representative event sequences for State 2

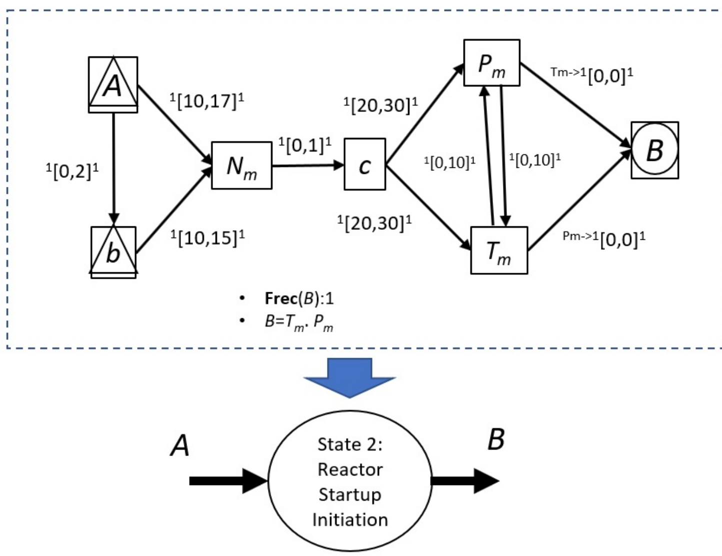


Figure 31: V-net V_{N2} that supervises State 2

- $E = \{A, b, N_m, c, P_m, T_m, B\}$
- $\mathcal{T}$=$\{\sqcup_1(A^1 \Rightarrow b^1) : [0,2], \sqcup_2(A^1 \Rightarrow N_m^1) : [10,17]; \sqcup_3(b^1 \Rightarrow N_m^1) : [10,15]; \sqcup_4(N_m^1 \Rightarrow c^1) : [0,1]; \sqcup_5(c^1 \Rightarrow P_m^1) : [20,30]; \sqcup_6(c^1 \Rightarrow T_m^1) : [20,30]; \sqcup_7(P_m^1 \Rightarrow T_m^1) : [0,1]; \sqcup_8(T_m^1 \Rightarrow P_m^1) : [0,1]; \sqcup_9((P_m^1 \rightarrow T_m^1) \Rightarrow B^1) : [0,0]; \sqcup_{10}((T_m^1 \rightarrow P_m^1) \Rightarrow B^1) : [0,0]\}$
- **Frec** $= \{f^{max}(c) : 1; f^{max}(B) : 1\}$
- tl_{eval}: 58
- $R =$ **Frec**$(B) : 1,\ A = T_m \wedge P_m \wedge N_m$

4.2.3. V-net for State 3

In State 3: The ascendance of the power, which orchestrates the transition to higher power levels, involves a meticulous sequence of operational actions and concurrent changes in the process variables. First, immediately or at least 1 minute after state 2 ends, the Reactor Power Increase (RPI) is initiated (discrete event RPI_i), marking a deliberate adjustment of the reactor parameters to gradually increase the power output until the full power is arranged (discrete event RPI_f). Operators fine-tune control rods and other critical parameters to modulate nuclear fission rates, with a time restriction of 5 to 10 minutes between successive RPI events (summarizing from RPI_i to RPI_f). Subsequently, the Steam Generation Initiation (SGI) starts (event SGI), harnessing thermal energy through heat transfer processes, commencing within 10 to 15 minutes after RPI_f. Following this, Turbine Activation (TA) comes into play (event TA), converting steam's thermal energy into mechanical power to generate electricity, typically within 15 to 20 minutes post-SGI. Concurrently to TA or within a maximum of 1 minute afterward, significant changes unfold in process variables: Temperature (T) surges above $500C$ as reactor power and steam generation intensify (from T_m to T_h), Pressure (P) climbs beyond 150 bar with mounting steam pressure (from P_m to P_h). The last process variable to transition to high levels (T_h, P_h, N_h) is typically the neutron flux (N), this Neutron Flux (N)

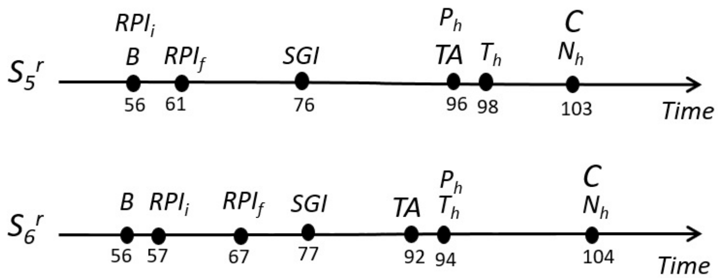


Figure 32: Representative event sequences for State 3

transition from moderate to high level exceeds $5x10^{15} neutrons/cm^2/s$. Therefore, the time restriction after the temperature (T_h) or pressure (P_h) variables reach high levels to arrange the neutron flux (N_h) typically ranges from 5 to 10 minutes. These evolutions, unfolding within designated timeframes, guarantee a meticulously controlled and steady progression toward elevated power levels, thereby enhancing both efficiency and safety in reactor operations.

Fig. 32 presents this state's representative sequences of events. Furthermore, Fig. 33 presents the graphical representation of the V-net to supervise this State 3. Note that now, event C is the final event of the V-net and the transition event to the next state.

V_{N3} is defined by

- $E = \{B, RPI_i, RPI_f, SGI, TA, P_h, T_h, N_h, C\}$
- $\mathcal{T}$=$\{\sqcup_1(B^1 \Rightarrow RPI_i^1) : [0,1]; \sqcup_2(B^1 \Rightarrow RPI_f^1) : [5,11]; \sqcup_3(RPI_i^1 \Rightarrow RPI_f^1) : [5,10]; \sqcup_4(RPI_f^1 \Rightarrow SGI^1) : [10,15]; \sqcup_5(SGI^1 \Rightarrow TA^1) : [15,20]; \sqcup_6(TA^1 \Rightarrow P_h^1) : [0,2]; \sqcup_7(TA^1 \Rightarrow T_h^1) : [0,2]; \sqcup_8(P_h^1 \Rightarrow T_h^1) : [0,2]; \sqcup_9(T_h^1 \Rightarrow P_h^1) : [0,2]; \sqcup_{10}((P_h^1 \rightarrow T_h^1) \Rightarrow N_h^1) : [5,10]; \sqcup_{11}((T_h^1 \rightarrow P_h^1) \Rightarrow N_h^1) : [5,10]; \sqcup_{12}(N_h^1 \Rightarrow C^1) : [0,0]\}$
- **Frec** $= \{f^{max}(SGI) : 1; f^{max}(C) : 1\}$
- tl_{eval}: 59

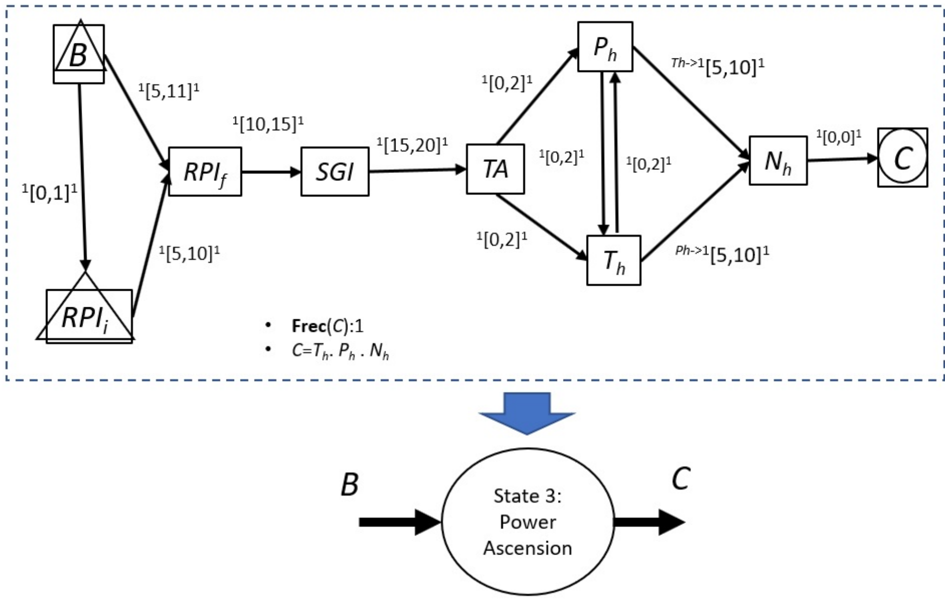


Figure 33: V-net V_{N3} that supervises State 3

- $R = \mathbf{Frec}(C) : 1$, $C = T_h \wedge P_h \wedge N_h$

4.2.4. V-net for State 4

In State 4: Full Power Operation, the event sequence encompasses crucial operational actions and corresponding transitions in process variables, ensuring sustained power generation while upholding operational safety. The time restriction between the finalization of State 3 and the initiation of Grid Connection typically ranges from 30 to 45 minutes.

Firstly, the connection to the grid (event GC) is initiated, marking the synchronization of the nuclear power plant with the electrical grid for full power generation. This pivotal event typically occurs as the initial step in the sequence, signifying the plant's readiness to supply electricity to the grid. The time restriction between Grid Connection and subsequent events depends on plant-specific protocols and grid synchronization requirements, ensuring a seamless transition to full power operation. Following Grid Connection, Full Power Generation (event FPG) ensues, as the reactor ramps up to its maximum power output capacity. This event represents the culmination of the reactor startup process, with the plant operating at optimal power levels to meet electricity demand. The time restriction between Grid Connection and Full Power Generation typically ranges from 5 to 10 minutes, allowing for reactor stabilization and power escalation. Continuous Monitoring (event CM) is then initiated, enabling plant operators to oversee and manage reactor operations in real-time. This event ensures ongoing monitoring of process variables and operational parameters to maintain system integrity and respond promptly to any deviations or anomalies. The time restriction between Full Power Generation and Continuous Monitoring typically ranges from 1 to 5 minutes, ensuring immediate monitoring and assessment of reactor performance.

During State 4, the transition from high levels (T_h, P_h, N_h) to medium levels (T_m^2, P_m^2, N_m^2) in temperature, pressure, and neutron flux occurs gradually as the reactor stabilizes at full power operation. This transition reflects the equilibrium reached in reactor operations, with process variables stabilizing within operational parameters. The time restriction for this transition typically occurs concurrently with the initiation of Continuous Monitoring, ensuring synchronized monitoring and adjustment of process variables during full power operation. After temperature (T) and pressure (P) have reached medium levels, neutron flux (N) follows suit, typically stabilizing at medium level within 5 to 10 minutes, although specific timeframes may vary depending on reactor dynamics and control strategies. Fig. 34 presents the representative sequences of events of this state. Furthermore, Fig. 35 presents the graphical representation of the V-net to supervise this State 4. Note that D is the final event of the V-net and the transition event to the final state (5), and the events T_m^2, P_m^2, N_m^2 express that these have occurred for the second time at reactor startup.

V_{N4} is defined by

- $E = \{C, GC, FPG, CM, P_m, T_m, N_m, D\}$
- $\mathcal{T}$=$\{\sqcup_1(C^1 \Rightarrow GC^1) : [30, 45]; \sqcup_2(GC^1 \Rightarrow FPG^1) : [5, 10]; \sqcup_3(FPG^1 \Rightarrow$

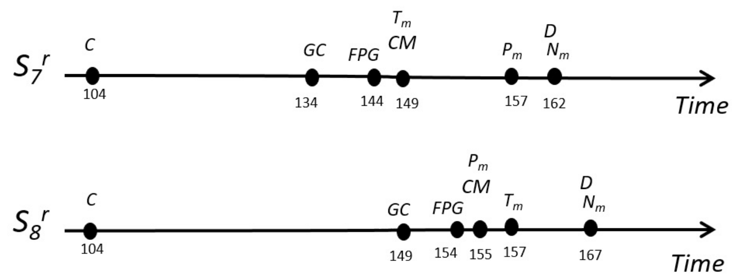


Figure 34: Representative event sequences for State 4

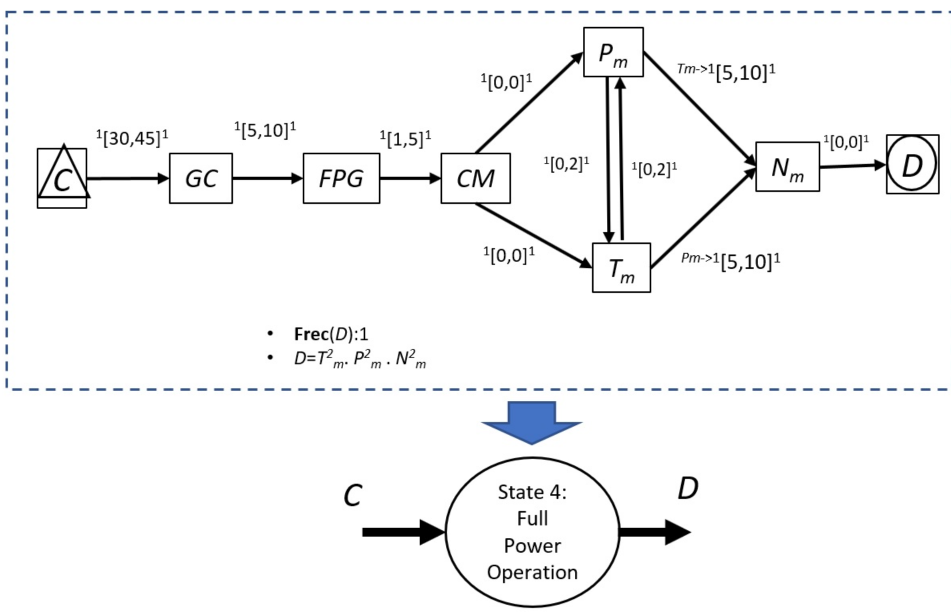


Figure 35: V-net V_{N4} that supervises State 4

$CM^1) : [1,5]; \sqcup_4(CM^1 \Rightarrow P_m^2) : [0,0]; \sqcup_5(CM^1 \Rightarrow T_m^2) : [0,0]; \sqcup_6(P_m^2 \Rightarrow T_m^2) : [0,2]; \sqcup_7(T_m^2 \Rightarrow P_m^2) : [0,2]; \sqcup_8((P_m^2 \rightarrow T_m^2) \Rightarrow N_m^2) : [5,10]; \sqcup_9((T_m^2 \rightarrow P_m^2) \Rightarrow N_m^2) : [5,10]; \sqcup_{10}(N_m^2 \Rightarrow D^1) : [0,0]\}$

- **Frec** $= \{f^{max}(P_m) : 2; f^{max}(T_m) : 2; f^{max}(N_m) : 2; f^{max}(D) : 1\}$
- tl_{eval}: 72
- $R = \mathbf{Frec}(D) : 1,\ D = T_m^2 \wedge P_m^2 \wedge N_m^2$

4.2.5. V-net for State 5

In this case study, State 5 could not necessitate a V-net for the final of this startup, as it signifies a stable operational phase where the system has reached a state of equilibrium and routine functionality. The reactor system operates within established parameters in this state, with no significant changes or transitions occurring. Therefore, there is no need for continuous monitoring or dynamic analysis, which is typically facilitated by V-nets, as the system remains stable and predictable. Instead, State 5 primarily involves routine maintenance, periodic inspections, and preparedness for emergency responses to ensure ongoing operational integrity and safety. However, V-nets could be used to analyze the sequence of alarms and determine whether a hazardous situation is active. An additional V-net will be developed to monitor possible alarms generated by high levels of process variables $(T_h, P_h, N_h,\ T_l, P_l, N_l)$. Fig. 36 presents the graphical representation of the V-net to supervise this state 5. Note that after the event D appears a divergence of six possible events that could occur $(T_h^2, P_h^2, N_h^2,\ T_l^2, P_l^2, N_l^2)$. This indicates that an increase or decrease in the process variables is assumed as a possible failure or abnormal situation to be managed. Now, the time restriction ${}^1[5,\infty]^2$ indicates that after the reactor is in a stable state, 5 (five) minutes after this process could present some variation in any of the variables. The symbol ∞ (infinity) indicates that there is no time restriction for these events to occur. V_{N5} is defined by

- $E = \{D, P_h, T_h, N_h, P_l, T_l, N_l\}$

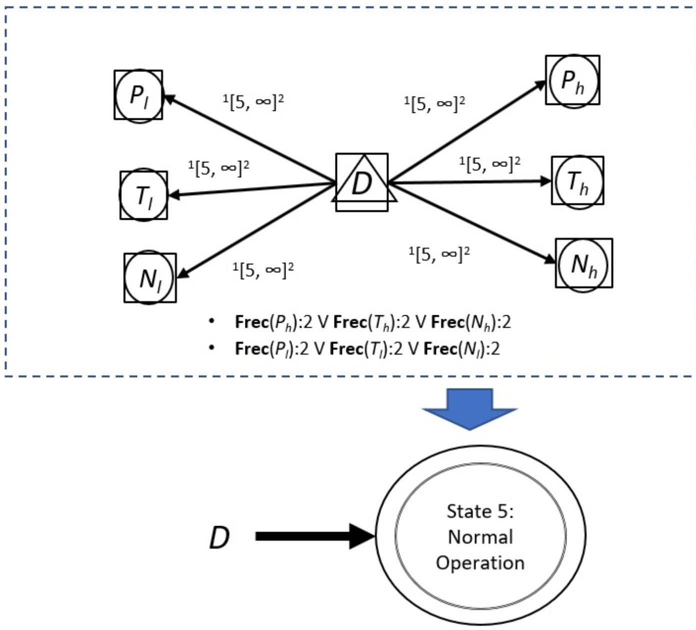


Figure 36: V-net V_{N5} that supervises State 5

- $\mathcal{T}$=$\{\sqcup_1(D^1 \Rightarrow P_h^2) : [5,\infty]; \sqcup_2(D^1 \Rightarrow T_h^2) : [5,\infty]; \sqcup_3(D^1 \Rightarrow N_h^2) : [5,\infty]; \sqcup_4(D^1 \Rightarrow P_l^2) : [5,\infty]; \sqcup_5(D^1 \Rightarrow T_l^2) : [5,\infty]; \sqcup_1(D^1 \Rightarrow N_l^2) : [5,\infty]\}$
- **Frec** $= \{f^{max}(P_h) : 2 \vee f^{max}(T_h) : 2 \vee f^{max}(N_h) : 2 \vee f^{max}(P_l) : 2 \vee f^{max}(T_l) : 2 \vee f^{max}(N_l) : 2\}$
- tl_{eval}: ∞
- $R = T_h^2 \vee P_h^2 \vee N_h^2 \vee T_l^2 \vee P_l^2 \vee N_l^2$

The expression $R = T_h^2 \vee P_h^2 \vee N_h^2 \vee T_l^2 \vee P_l^2 \vee N_l^2$ indicates that if any of the process variables goes to high or low values, the V-net is recognized, giving an alert to the operators. In the start-up process, it is normal that the high or low level appears in the variables, but after the startup procedure, these levels are abnormal.

4.3. Result analysis

Three evaluation event sequences were employed to evaluate the performance of the V-net, and the results are visualized in Fig. 37. The figure illustrates the V-net at the top, with the events and their occurrence dates depicted in the timeline in the middle. The percentage of matching between the evaluation event sequences and the V-nets is indicated at the bottom of the figure, providing a comprehensive overview of the alignment between the observed data and the modeled V-nets.

The first sequence, denoted as S_1^e, originates from the process and exhibits a flawless match with the V-net, achieving an accuracy rate of 100%. For example, in V_{n1}, the initial event a is followed by A, satisfying the prescribed time restriction $a^1[10,15]^1A$. Similarly, the timing observations (SGI,85) and $(TA, 100)$ adhere to the time constraint $SGI^1[15,20]^1TA$ within V_{n3}, concluding the sequence with D and the transition of neutron flux to the medium level for the second occurrence (N_m^2).

S_2^e assesses the compatibility of V-nets at a rate of 60%, as certain temporal observations deviate from the specified time constraints of the V-net model. For

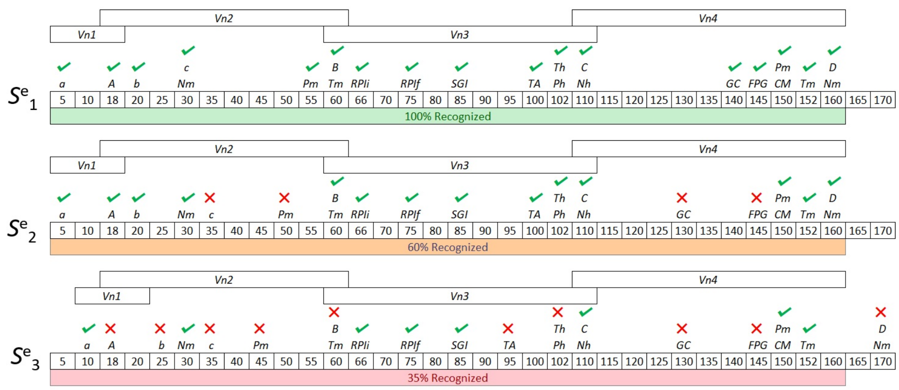


Figure 37: Evaluation of the V-nets with S_1^e, S_2^e, and S_3^e

instance, in V_{n2}, event $(c, 35)$ fails to meet the time restriction stipulated in the arc $\sqcup 4(N_m^1 \Rightarrow c^1) : [0, 1]$, as N_m occurred 5 minutes earlier $(N_m, 30)$. This early occurrence also affects the timing of P_m. Similarly, in V_{n4}, the event GC transpires 10 minutes before its designated time, while FPG occurs 5 minutes late. Of the 23 occurrences of events, only 19 are deemed satisfactory, resulting in a matching rate of 60%.

In the final assessment, S_3^e demonstrates a mere 35% match, with only 8 events conforming to the time constraints specified by the V-nets. In particular, the event A occurs prematurely, while the event b experiences a delay. Furthermore, among other errors, events such as D and N_m occur late, exceeding the allocated timeframe for the evaluation of V_{n4}.

5. Conclusion

In this paper, the foundational theory of V-nets is introduced, which sheds light on key parameters essential for a comprehensive understanding of this formalism. By delving into the theoretical underpinnings of V-nets, the significance of this modeling and analysis tool for complex systems characterized by discrete events has been elucidated. Furthermore, through an industrial example centered on a nuclear power generation plant, the practical utility of V-nets in monitoring and supervising intricate processes has been demonstrated.

Analysis of the reactor startup sequence exemplifies how V-nets offer a nuanced perspective beyond traditional automata or state machines. Leveraging V-nets enables the effective monitoring of procedure evolution, pinpointing simultaneous occurrences, identifying false positives, and detecting partial recognition of event sequences. This case study underscores the invaluable role of V-nets in enhancing the efficiency, safety, and reliability of industrial operations, paving the way for their broader application in diverse domains.

In the subsequent paper, further properties of V-nets will be elucidated, encompassing features such as the inclusion of multiple arcs within a single event. This capability enhances the model's capacity to represent intricate relationships and interactions within the system. Moreover, the paper will explore the concepts of divergence in "or" and convergence in "and," enabling more nuanced modeling of system behaviors and decision-making processes. In addition, the paper will introduce the concept of macro nets, which enable the encapsulation of complex subsystems within a larger network. This enhances the modularity and scalability of V-nets, facilitating the modeling of complex systems in a more organized manner. These properties, among others, will be discussed comprehensively, shedding light on the diverse capabilities of V-nets as a versatile tool for modeling and analyzing complex systems.

Looking ahead, future endeavors will focus on further refining and applying this innovative model in research projects aimed at enhancing the diagnosis and supervision of industrial processes. Key objectives include developing an algorithm for constructing V-nets, leveraging representative event sequences for model structuring, and creating a comprehensive tool for V-net modeling, simulation, and validation. These advancements will contribute to more accurate and efficient analysis in complex system engineering.

References

References

[1] D. Lefebvre, Z. Li, Y. Liang, Diagnosis of timed patterns for discrete event systems by means of state isolation, Automatica 153 (2023) 111045. doi:https://doi.org/10.1016/j.automatica.2023.111045. URL https://www.sciencedirect.com/science/article/pii/S0005109823002005

[2] A. Kampa, G. Gołda, I. Paprocka, Discrete event simulation method as a tool for improvement of manufacturing systems, Computers 6 (1). doi:10.3390/computers6010010. URL https://www.mdpi.com/2073-431X/6/1/10

[3] A. Ignatiev, A. Morgado, G. Weissenbacher, J. Marques-Silva, I. S. RAS, Model-based diagnosis with multiple observations., in: IJCAI, 2019, pp. 1108–1115.

[4] R. David, Grafcet: a powerful tool for specification of logic controllers, IEEE Transactions on Control Systems Technology 3 (3) (1995) 253–268. doi:10.1109/87.406973.

[5] C. I. Chesñevar, M. L. Cobo, W. Yurcik, Using theoretical computer simulators for formal languages and automata theory, SIGCSE Bull. 35 (2) (2003) 33–37. doi:10.1145/782941.782975. URL http://doi.acm.org/10.1145/782941.782975

[6] M. C. Zhou, E. Twiss, Design of industrial automated systems via relay ladder logic programming and petri nets, IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 28 (1) (1998) 137–150. doi:10.1109/5326.661096.

[7] J. W. Vásquez, Chronicle based alarm management, Doctoral thesis of Automatic Control Engineering. INSA Toulouse.

[8] J. W. Vasquez Capacho, C. G. Perez Zuñiga, Y. A. Muñoz Maldonado, A. Ospino Castro, Simultaneous occurrences and false-positives analysis in discrete event dynamic systems, Journal of Computational Science 44 (2020) 101162. doi:https://doi.org/10.1016/j.jocs.2020.101162. URL https://www.sciencedirect.com/science/article/pii/S1877750320304634

[9] O. Niggemann, V. Lohweg, On the diagnosis of cyber-physical production systems, in: AAAI, 2015.

[10] J. Vasquez-Capacho, V-nets, new formalism to manage diagnosis problems in cyber-physical systems (cps) and industrial applications, IFAC-PapersOnLine 53 (5) (2020) 197–202, 3rd IFAC Workshop on Cyber-Physical & Human Systems CPHS 2020. doi:https://doi.org/10.1016/j.ifacol.2021.04.224. URL https://www.sciencedirect.com/science/article/pii/S2405896321004080

[11] M. Le Goc, Notion d'observation pour le diagnostic des processus dynamiques : Application à sachem et à la découverte de connaissances temporelles, Ph.D. thesis (11 2006). doi:10.13140/RG.2.1.5048.2800.

[12] L. Pomponio, M. L. Goc, Reducing the gap between experts' knowledge and data: The tom4d methodology, Data Knowledge Engineering 94 (2014) 1 – 37. doi:https://doi.org/10.1016/j.datak.2014.07.006. URL http://www.sciencedirect.com/science/article/pii/S0169023X14000652

[13] C. Curt, M. L. Goc, L. Torres, I. Fakhfakh, Multimodel-based diagnosis of hydraulic dams, Journal of Computing in Civil Engineering 31 (5) (2017) 04017024. doi:10.1061/(ASCE)CP.1943-5487.0000670.