Artigo completo nº 20170614232246

# On the Characterization of Hidden Failures and the Exposure to Risk Scenarios

Heitor Azuma Kagueiama, Acires Dias
*Universidade Federal de Santa Catarina*

Johan Ölvander
*Linköping University*

*Hidden failures may result on the accumulation of events with significant impact on risk and safety. The occurrence of hidden failures is unknown until something else occurs, and the simultaneous occurrence of multiple events can compromise the response capability of the operation or maintenance crew. Once something occurs and the crew is deployed they may find other problems that were not expected and they may not be prepared to act. This paper shows how important the characterization of hidden failures is and how often a system is exposed to them. Hidden failures are usually associated to protective and redundant systems and managed with periodic inspection. However, this paper shows that for systems with strong dynamic characteristics, that constantly demand a component to change the operational state, hidden failures are also common and their definition depend both on failure modes and the operational state (when a component turn on or off, for example). This means that the combination of events involving a failure occurrence should be considered in short periods of time (a component is demanded to turn on from time to time), to identify hidden failures, since the system may be exposed to risk even though the mission time is achieved. Two examples are modeled using Monte Carlo method to get time samples both for failure and operational state, and the simultaneous occurrence of events that define hidden failures is checked. The first example is a problem based on nuclear reactor cooling systems formed by a tank, two pumps, a valve and a controller that should be able to keep the level of fluid stable until the mission time is achieved. If level variation is detected the controller changes the state of the components, making it possible to detect some of the hidden failures. The second example is based on a fighter aircraft fuel tank divided in two compartments linked by a set of check valves that should hold enough fuel on the pump side to allow inverted flight. It is shown that sometimes mission time is achieved only because of redundant valves allowing the system to overcome hidden failures. Both examples consist of holding an amount of fluid in a tank until the mission is completed, but it is showed that even though the mission is successful, hidden failures are constantly occurring and exposing the system to risk scenarios. Therefore, the analysis allows a better understanding of failure occurrences and the identification of possible design changes to the system.*

## 1. INTRODUCTION

A fundamental outcome of risk and safety analysis is the identification of critical scenarios that may result in an incident or accident. Every system that carries a great amount of energy has risks and understanding the sequence of events that may turn a hazardous condition into an incident allows the identification of possible measures to avoid the occurrence of such events, or stop the consequences of any incidents before they cause any damage.

Hidden failures are important in the scenario characterization given that they may result on the accumulation of events that lead to an accident. Techniques such as Fault Trees (FT) and Failure Modes and Effect Analysis (FMEA) are not enough to demonstrate hidden failures because the combination of events depend on the ability to predict all hidden failure scenarios. Their focus is mainly on the cause and effect characterization of functional failures [9]. In order to correctly evaluate the probability of a hidden failure to occur, it is necessary to consider other aspects besides the occurrence of a failure mode itself, since hidden failures are characterized by a combination of component states. Therefore, it is necessary to consider operational aspects of the system that underline what are the component states in a particular moment, besides the traditional cause and effect information in FTs and FMEAs.

This paper presents the first step of a methodology to characterize and evaluate the occurrence probability of hidden failure scenarios in order to provide means for designers to compare concepts and identify possible barriers that to be implemented or procedures to be established to reduce risks and improve safety. This first step consists on the characterization of hidden failures through potential failure modes and operational states. The main objective is to demonstrate hidden failures by Monte Carlo simulation. In order to exemplify that, two cases are shown, using Monte Carlo simulation to obtain time samples to evaluate the probability of simultaneous occurrence of events that characterize hidden failures. It is noticed that even in successful missions, the system is constantly exposed to hidden failures, which is unacceptable given the random aspect of event occurrence probabilities.

## 2. RISK AND SYSTEM SAFETY

A complex engineering system consist of a number of subsystems and components with specific functions (sub-functions in a subsystem level and elementary functions in a component level) that are combined to perform a global function. Subsystem and component functions are connected thru inputs and outputs (matter, energy and information flows) that may be affected by the occurrence of failures. In this sense, failure analysis gives information on how the loss of a function may occur and how it may affect other functions performance.

If a failure occurrence has potentially severe consequences for the system, for example, resulting in human fatalities or loss of continuity, the risks involved in the operation should be managed. [1] define risk as five primitives: outcome, likelihood, significance, causal scenario, and population affected. This means that to analyze and manage risks, a failure occurrence should be evaluated in terms of the sequence of events that may result in an incident, the probability of occurrence of a given scenario, and the effects over the system operation and its surrounding environment.

A common way of managing risks is using multiple layers of defense to control the causes of a hazardous condition, avoiding the occurrence of an incident, or even stop the effects of an incident before it escalades into catastrophic consequences. This concept is called defense-in-depth and is illustrated in Fig. 1.

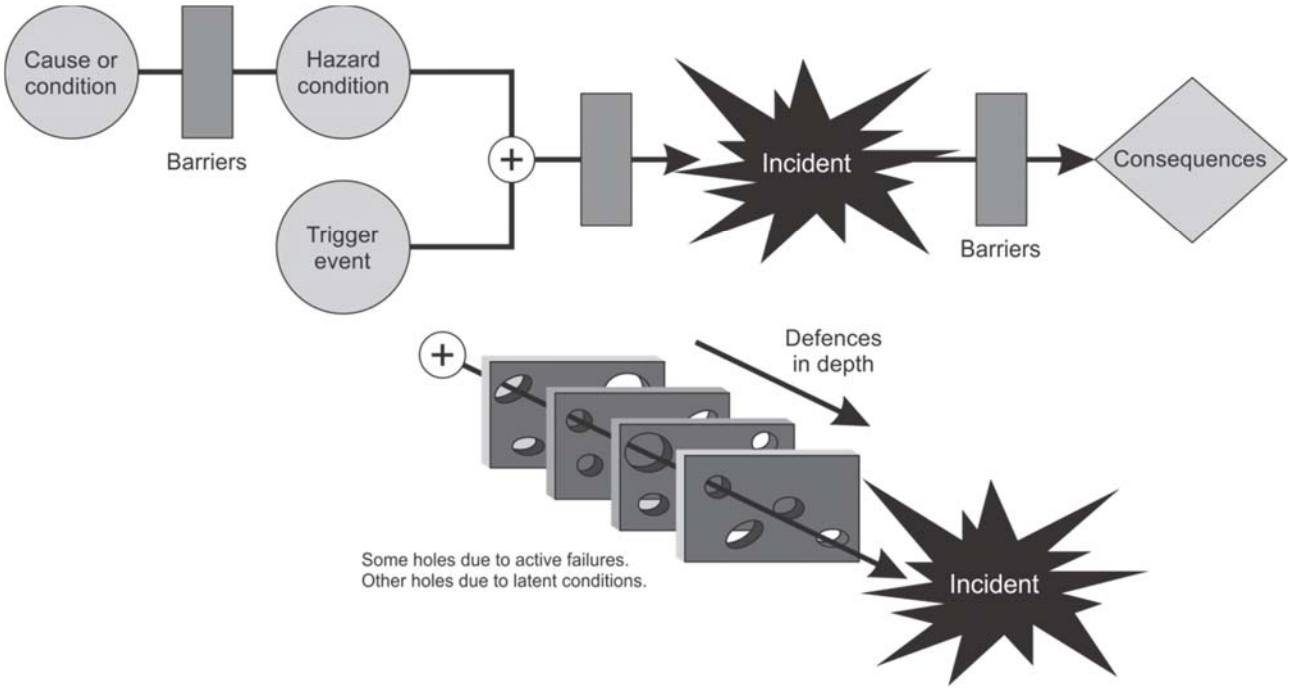


Fig. 1. Defense-in-depth representation [ 2].

The layers of defense, or barriers, may be for example actual physical barriers (like emergency exit doors in a building in case of fire) or emergency procedures (how the fire brigade should act in case of a fire). [3] present a safety strategy to avoid a few drawbacks that might exist in the defense-in-depth, especially related to non-observable events. According to the authors, sometimes events that are not observable can escalade and compromise the lines of defense. Therefore, to improve the effectiveness of risk management strategies, it is important to pay special attention to hidden failures, since they are not observable and result on the accumulation of events that might not be anticipated when the barriers were established. The authors point out that the fact that an event is not observable leave operators unaware of some hazardous scenarios and as a result their response time and capability are compromised. They present the concept of observability-in-depth, which consists on real-time monitoring and identification of hazardous states, giving the defense-in-depth a dynamic characteristic.

The present research contributes by giving a more detailed definition of hidden failure that considers the combination between state transitions caused both by operation and failure occurrences.

## 3. HIDDEN FAILURES

A function loss may occur due to evident failures and hidden (dormant) failures [4]. Evident failures are linked to the functions that are active throughout the item's life cycle and their occurrence is immediately observable because they change the system behavior. Hidden failures are characterized by one or more events that compose a fault scenario and are not observable until another event occurs. This event may be the failure of another item or system operational changes. These failures are significant in technical systems that carry large amounts of energy: power generation and transmission; petrochemical; oil; aircraft among others, since they reduce the response time of operators and maintainers to return the system back to normal.

Currently, hidden failures are managed with periodic inspections to verify that the hidden failure is present and are mainly attributed to protection and redundant systems [5]. In reliability centered maintenance there is the failure finding task, aiming at the detection of the occurrence of hidden failures, but these tasks must be performed without interference on system operation, avoiding the inclusion of other equipment failures. Thus, most of the efforts are to optimize the periodicity of inspections [6]. It should be point out that, according to [7], it is clear that in certain technical systems around 40% of failures are classified as hidden failures and that around 80% of these depend on fault detection tasks. However, it is evident that for critical systems such as aircraft, nuclear power plants, among others, this traditional approach to hidden failures is not got enough, because any failure in these systems can have catastrophic consequences.

What makes hidden failures critical is the accumulation of events. As previously said, hidden failures are observable once another event occurs. In some cases this event may be another failure or just some change in the system operation. In case of a hidden failure, given the accumulation of events, any recovering measures might be compromised. For example, an operator may identify high pressure and decides to open a relief valve without knowing that it has a hidden failure. This means that his ability to evaluate the situation and properly act to return the pressure back to normal was compromised. Another example could be after an evident failure is identified and maintenance is performed. If a hidden failure has also occurred the maintenance crew might not be prepared to perform all the maintenance tasks required because they expect to find only the evident failure.

If the hidden failure became evident due to a operational change, the system will not behave as expected and if it happens in an emergency situation, the consequences could be severe and lead to an accident. Therefore, it is important to identify the scenarios that might be linked to hidden failure occurrences, so that design improvements and procedures can be identified, tested and implemented. Even though hidden failures do not impact the system immediately after it happens, depending on the system, the simple exposure to the hazardous condition of a hidden failure scenario is unacceptable.

## 4. CASE STUDY

To exemplify how often a system may present hidden failures, two systems are presented. These examples are being used to help develop a more complete method to address hidden failures. It is showed that to classify a

failure occurrence as hidden, it is important to consider the previous state (on and off, for example) and the failure mode to check if the failure cause an immediate impact on the system operation.

In the first example, Monte Carlo simulations were used to get time samples for the failure occurrences and compare them with the combination of component states. In the second example, the time samples were used to see how often many redundant components fail, exposing the system to hazardous conditions.

### *4.1. Benchmark problem*

In a technical system consisting of several components, the characterization of hidden failures should take into consideration the control variables that determine the performance of the system function. For a system like the one shown in Fig. 2 with the main function being to maintain a stable level of fluid, and composed by a tank, two pumps P1 and P2 (P2 in stand by) a valve V and a controller; failure of a component is hidden when it does not cause variation of the level of fluid in the tank. In this particular example, both pumps and the valve have the same flow rate. The original condition of the system is with P1on, P2 off (stand by) and V on. If P1 fails on, for example, the level will not be changed until V fails off or P2 fails on, causing the level to change and the controller to command the components to change states.

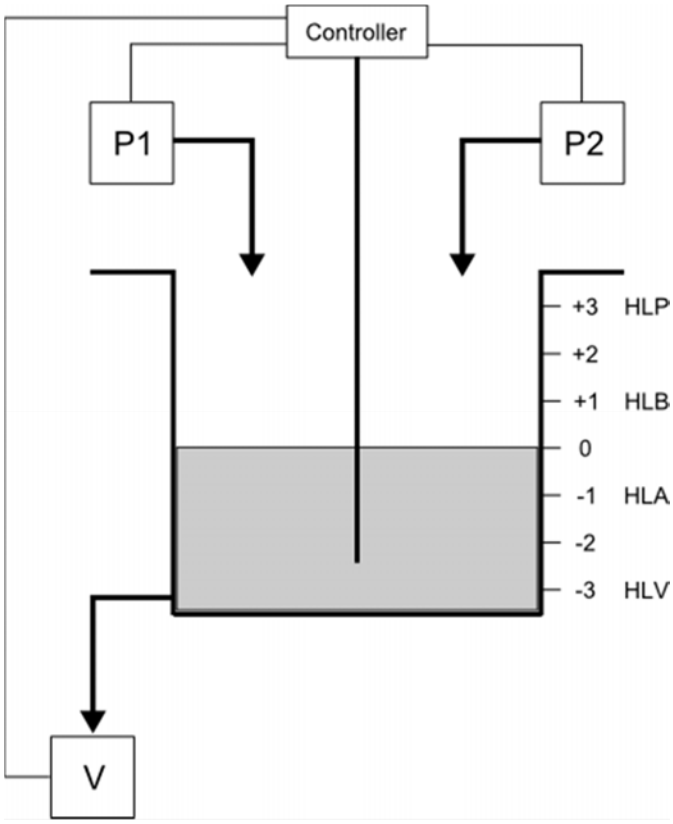


Fig. 2. Benchmark tank problem

The example shown in Fig. 2, is a classic problem used as a reference to compare methods for the analysis of dynamic reliability [8]. In this classic example, the controller is considered a perfect element (not subject to failures) and, if a level variation in the tank is detected (plus or minus 1), it commands the pumps to close and the valve to open, if the level is rising; or turn on both pumps and close the valve if the level is lowering, so the level may return to the original value 0. System failure occurs when the level reaches minus or plus 3. The possible combinations of component states and the consequent flow of fluid into the tank are shown in Table 1.

Table 1. System configuration based on component states

| Configuration | P1 | P2 | V | Flow (m/h) |
|---|---|---|---|---|
| 1 | On | Off | Off | 0,6 m/h |
| 2 | On | On | Off | 1,2 m/h |
| 3 | On | Off | On | 0,0 m/h |
| 4 | On | On | On | 0,6 m/h |
| 5 | Off | Off | Off | 0,0 m/h |
| 6 | Off | On | Off | 0,6 m/h |
| 7 | Off | Off | On | -0,6 m/h |
| 8 | Off | On | On | 0,0 m/h |

The failure rates and flow rates of the pumps and the valve are showed in Table 2. The possible failure modes for all three components are they being stuck on or off. The occurrence probability of the failure modes are 50%, which means that given that a failure has occurred, they have the same probability of being on or off.

Table 2. Components failure rates and flow rates

| **Component** | **Failure rate (failure/h)** | **Flow rate (m/h)** |
|---|---|---|
| P1 | 0,004566 | 0,6 |
| P2 | 0,005714 | 0,6 |
| V | 0,003125 | -0,6 |

For dynamic reliability the goal is to evaluate the probability of the dry out or overflow of the tank, considering the dynamic aspects due to the controller's commands to return the level of fluid back to normal. When compared with traditional reliability analysis based on reliability block diagrams (RBD), the dynamic approach is more accurate since it considers the possibility of recovering the system back to its normal condition. With RBD the reliability is defined by the probability of a number of components surviving (depending on the series/parallel configuration), but once a component fails it is not possible to fix it and put back into operation [9]. In dynamic reliability aspects like maintenance, for example, can be incorporated into the models to calculate the reliability [10]. At the same time, the dynamic approach exposes another problem, which is the occurrence of hidden failures.

Dynamic reliability simulations from [11] show that when a component fails and cannot change its state (P1 fails open, for example), the controller command does not have the expected impact and the level of fluid doesn´t go back to normal, but is an event that makes possible to observe the occurrence of a hidden failure, as can be seen in Fig. 3. For this reason it is important to include the state transitions, incorporation information about which are the possible transitions (on and off and with or without failure, for example) in probabilistic models of hidden failures.

Fig. 3 illustrates two examples of the system behavior based on the kind of failure and the moment they occur. In the first example, an evident failure of P1 occurs, causing an immediate change of the fluid level, resulting on the controller command to change the components states in order to return the level back to normal. In the second example, a hidden failure of P2 occurs (the pump fails off) and when the evident failure of P1 happens, the controllers response is not capable of returning the level back to normal since both pumps failed off.

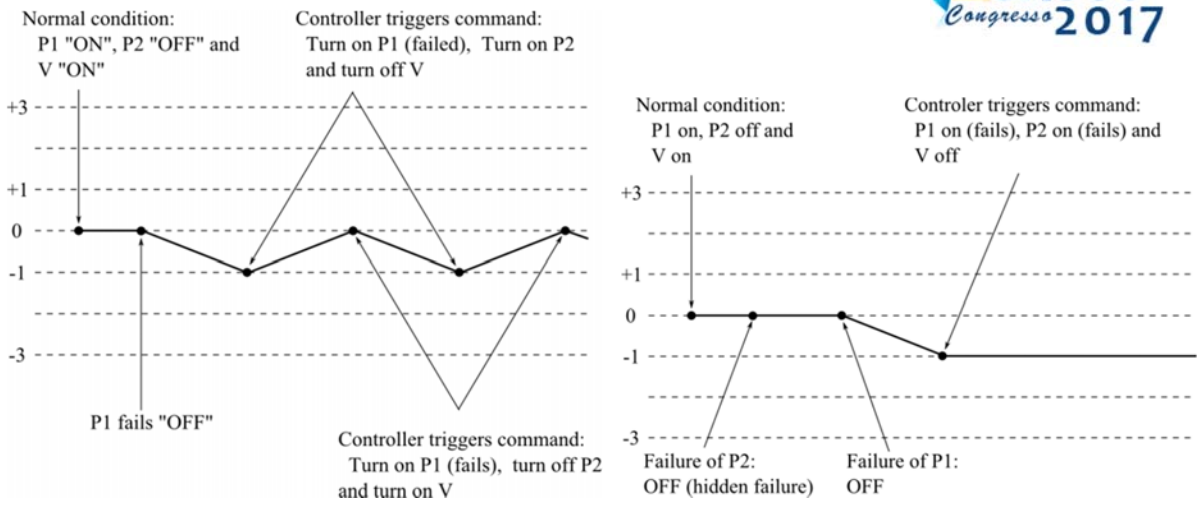


Fig. 3. Examples of evident and hidden failure scenarios (Ref. 7)

Monte Carlo simulation was used to get time samples for the failure of all three components which were then combined with samples for the type of failure (on or off). The time samples for the failure occurrences were obtained considering an exponential distribution for the cumulative probability function [12]. The types of failures were randomly sampled considering they have 50% probability of occurring. 200 time samples were obtained and five of these samples are shown in Table 3, where different failure scenarios can be identified. Sample 1 demonstrates a scenario when V is the first component to fail after 116,57 hours but since it fails on and that it is the valves original state, there is no change on the level of fluid and the failure is hidden. This failure can only be observed once P2 fails on (182,94h) and the controller actuate.

Sample 3 is a good example because two hidden failure occur simultaneously for a period of time. Since P1 fails on and P2 fails off, there is no change on the fluid level. These failures can only be observed once V fails off and the controller tries to shutdown both pumps. Even then the failure of P2 remains hidden since it failed off.

Table 3. Time and failure mode samples of P1, P2 and V

| Sample | P1 | | P2 | | V | |
|---|---|---|---|---|---|---|
| | Failure time (h) | Failure mode | Failure time (h) | Failure mode | Failure time (h) | Failure mode |
| 1 | 421,30 | Off | 182,94 | On | 116,57 | On |
| 2 | 278,54 | On | 179,89 | On | 19,82 | Off |
| 3 | 7,77 | On | 376,07 | Off | 398,91 | Off |
| 4 | 230,89 | Off | 332,71 | Off | 333,62 | On |
| 5 | 240,72 | Off | 257,82 | On | 51,87 | Off |

In sample 1, V is the first component to fail, but since the failure is on it is hidden. Once P2 fails on, the level of fluid starts to rise until it reaches +1 and the controller commands both pumps to turn off and the valve to turn on. At this point, the failure of V becomes evident. The level remains stable at +1 because the controller was able to turn off P1 but P2 and V remain on because they are in a failure condition. Since the level never gets lower, all components stay in the same state until the failure of P1 occurs. This failure has absolutely no impact on the fluid level, because the pump was already off, and the level will keep steady at +1 until the system reaches the mission time. In this example it is clear that even though the mission was successful, different hidden failures happened. If P1 failed on, the level of fluid would rise again and the controller would not be able to command the components and control the level, leading to overflow.

Table 4. Complete description of failure scenarios in sample 1

| Time (h) | Fluid level (m) | Event description |
|---|---|---|
| 0,00 | 0 | Original condition, P1 on, P2 off, V on |
| 116,57 | 0 | Hidden failure of V, on |
| 182,94 | 0 | Evident failure of P2, on |
| 184,61 | +1 | Controller actuates, P1 off, P2 on, V on; level stable |
| 421,30 | +1 | Evident failure of P1 off |

### *4.2. Aircraft collector tank*

The collector tank should ensure that the pump is always submerged to avoid fuel gas suction (which could cause cavitation and problems with the engine) and that the fuel can cool the pump. The collector tank is divided in two sections with check valves (flapper valves) used to connect both sections, allowing fuel to flow inside the section where the pump is, but not allowing the fuel to flow back. The section where the pump is has 1/3 of the total volume of the collector tank. The pump has two intake sections so that fuel suction is guaranteed either under inverted or normal flight. The check valves should guarantee enough fuel to sustain a 10s inverted flight with after burner. The aircraft cannot fly inverted with half tank.

To avoid the possibility of adding failures to the collector tank due to mistakes during maintenance procedures, the collector tank is sealed and only goes under inspection when it reaches the end of life, which is 2000 flight hours. The design solution to guarantee that the tank have enough fuel in the pump section was to add redundant valves. In this particular example it is considered that there are five valves in the tank and that the failure criteria once the tank reaches the end of life and is inspected is three out of five valves still working. The valves are the same and the failure rate is 0,00041 failures/flight hour and represents the case of the valve failing open. Since the failure rate for the valves failing closed are much smaller, this failure mode will not be considered. An schematic representation of the collector tank is shown in Fig. 4.

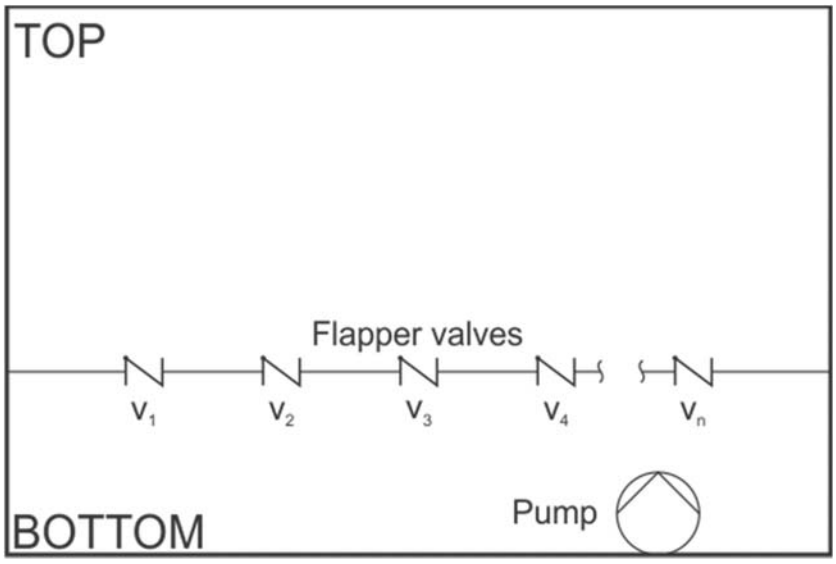


Fig. 4. Schematic of a collector tank

With this example, it is intended to show how exposed the system might be even when the overall reliability is high, and how important is the operation characteristics to avoid accidents. For that, Monte Carlo was used to

get sample times considering that the cumulative density function for the failure probability follows an exponential distribution [12]. 200 time samples were obtained and Table 5 shows a few time samples for failure occurrences of the valves.

As it can be seen by the highlighted numbers, many valves fail before the end of the tank´s lifecycle. In some cases, like the second sample, shown in Table 5, four out of five valves failed. This means that the collector tank reached the end of the lifecycle without accidents just because the flight profiles of the aircraft allowed enough fuel flowing into the collector tank, even though the design criteria of three out of five was not reached. In fact, the sample showed that in 60% of the cases there were three or more failed valves.

In this particular example, the fact is that the aircraft is not able to complete 2000 flight hours without accidents is entirely dependent of the flight profiles. In a one-hour flight, a fighter aircraft could fly inverted during normal maneuvers with different fuel consumption characteristics. The percentage of time the aircraft performs these kind of flights will impact the capability of the remaining valves to keep enough fuel in the collector tank to ensure the possibility of the aircraft to keep performing these maneuvers. Also, the fuel consumption varies depending, for example, if the after burner is on or not.

All these facts should be taken under consideration when analyzing this system and maybe the number of valves or their size could be changed to avoid exposing the aircraft to hazardous conditions.

Table 5. Time samples of the valves in a collector tank

| Valve 1 | Valve 2 | Valve 3 | Valve 4 | Valve 5 |
|---|---|---|---|---|
| **1337,657** | 4693,384 | 4758,62 | 2149,207 | 5824,808 |
| **510,4211** | **32,54911** | **330,275** | **34,1169** | 2325,654 |
| **1295,788** | **218,9954** | 620,7311 | 5050,027 | **645,7642** |
| **1583,626** | 2173,602 | 2316,444 | **1028,652** | **163,7426** |
| 2912,654 | **642,4081** | 2353,823 | **1214,379** | 5490,805 |

## 5. CONCLUSION

Considering the technical system lifecycle, the study of hidden failures has great influence both in the design phase and in the use phase. During the design phase, the conclusions obtained from the characterization of the occurrence of hidden failures in the reliability analysis can directly influence the redesign or the selection of new product solution principles, such as the option to add redundant components, add components for monitoring the causes of a fault or, for example, to opt for more complex or more simple components less susceptible to the occurrence of hidden failures. In the use phase, the analysis results have direct influence on the adopted maintenance procedures, it helps the maintainer in making decisions as to prioritize the maintenance of components, development of procedures to identify component hidden failures and establish barriers to prevent failure to spread.

In the first case presented it was showed that the dynamic aspects of the system are extremely relevant for the definition of hidden failures. For example, if the controller commanded both pumps to change their states from time to time, turning P1 into the redundant pump and P2 into the active one, the system behavior would turn completely different not because of the command itself but because hidden failures would be identified more often and failure accumulation would happen more frequently.

If maintenance is incorporated to the benchmark problem, more aspects should be taken under consideration and the detection of hidden failure would change. It would be possible to evaluate the maintenance crew performance and see if they are capable of recovering the system with the accumulation of failures. This could help establishing maintenance performance goals. In the next steps of the ongoing research, all these aspects should be incorporated.

In the collector tank example, it became evident that the flight profile is extremely relevant to keep a sufficient level of fluid in the tank. Therefore, it is important to combine models that represent different flight profiles and combine them with the time samples to check the simultaneous occurrence of event that could result on not enough fuel flowing into the collector tank in time for the aircraft to perform maneuvers under specific conditions.

The study contributes to a better understanding of hidden failures because it helps identifying different hidden failure scenarios besides the ones related to redundant and protection systems, which are the cases found in the literature and currently methods that basically try to optimize inspection times. The method allows the combination of events that may not be anticipated and could have catastrophic impacts on the system.

## ACKNOWLEDGMENTS

This research was supported by Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Swedish-Brazilian Innovation and Research Centre (CISB) and Saab AB in the Call CNPq/CISB/SAAB Nº 42/2014 (sandwich PhD), making possible the collaboration between Brazilian and Swedish researchers.

## REFERENCES

1. E. J. Henley and H. Kumamoto, *Probabilistic Risk Assessment*. NY: IEEE Press. (1992)
2. Mosleh, a. Et al. An Integrated Framework for Identification, Classification, And Assessment Of Aviation Systems Hazards. *International Conference on Probabilistic Safety Assessment and Management (PSAM)*, 7., Berlin, (2004).
3. F. M. Favarò, J. H. Saleh, “Towards the development of the Observability-in-Depth Safety Principle in the Nuclear Industry”, *International Conference on Probabilistic Safety Assessment and Management (PSAM),12.*, Honolulu, (2014).
4. F. S. Nowlan; H. F. Heap, H. F. *Reliability Centered Maintenance*. National Technical Information Center. USA. Report Nº AD/A066-579. 1978.
5. B. Lienhardt; E. Hugues, C. Bes; D. Noll, Failure-finding Frequency for a Repairable System Subject to Hidden Failures. *AIAA Journal of Aircraft*, 45, 5, p. 1804-1809. (2008)
6. S. Taghipour; D. Banjevic, JARDINE A. K. S. "Periodic Inspection Optimization Model for a Complex Repairable System", *Reliability Engineering and System Safety***.** 95, 944, (2010).
7. J. Moubray, *Reliability Centered Maintenance*, pp. 423p, 2, Industrial Press Inc., New York, (1997).
8. A. Bobbio and D. Codetta-Raiteri, A Benchmark on Dynamic Reliability: An approach based on Generalized Stochastic Petri Nets, *Affidabilità Dinamica*, 3ASI, Milan, (2004).
9. B. Bertsche, *Reliability in automotive and mechanical engineering*, Berlin, Springer-Verlag, (2008)
10. G. Manno, F. Chiacchio, L. Compagno, D. D'Urso, N. Trapani, Conception of Repairable Dynamic Fault Trees and resolution by the use of RAATSS, a Matlab toolbox based on the ATS formalism, *Reliability Engineering and System Safety*, 121, 250, (2014).
11. E. Y. Sakurada, *Metodologia para a análise de confiabilidade dinâmica*. (Unpublished doctoral thesis), Universidade Federal de Santa Catarina, Florianópolis, Brazil, (2013).
12. E. Zio, *The Monte Carlo Simulation Method for System Reliability and Risk Analysis*