Sensors & Transducers, Vol. 235, Issue 7, July 2019, pp. 43-54

www.sensorsportal.com

Sensors & Transducers

Published by IFSA Publishing, S. L., 2019
http://www.sensorsportal.com

Modelling Based Approach to the Assurance of an Airborne Actuation System

J. S. Sagoo
QinetiQ, St Andrews Road, Malvern, Worcestershire WR14 3PS, United Kingdom
Tel.: + 44 1684 895188, fax: + 1684 894034
E-mail: jsagoo@QinetiQ.com

Received: 15 April 2019 /Accepted: 28 May 2019 /Published: 31 July 2019

Abstract: Assurance is a key activity for providing confidence that a system satisfies its requirements, which is most crucial for systems operating in safety related environments. Although techniques such as audits are important for providing assurance, they provide limited support for systems constructed from third party COTS software and programmable electronic hardware. This is because for such systems developmental evidence may not be available. This paper presents an assurance approach that combines safety and formal techniques (such as HAZOP, Fault Trees and Coloured Petri-nets). Specifically, this approach uses each technique to perform its analysis of the system and the results of each analysis are used as the basis of the other constituent techniques. The approach is applied to a case study, which involves an actuation system that is required to automatically deploy parachutes when a skydiver exits an aircraft in flight. Using this case study, the attributes of the assurance approach are demonstrated.

Keywords: Assurance, Petri nets, HAZOP, FTA, Sensor modelling, COTS.

1. Introduction

In the construction of computer based embedded control systems, assurance is a set of planned and systematic activities which are applied to provide confidence that a system development satisfies it's given requirements [1]. For safety applications, assurance also provides an important means of showing that the development complies with agreed standards and that the system contains specified behaviours but excludes known unsafe or undesirable behaviours. In the automotive and aviation sectors, assurance activities are mandated by standards such as [2-4]. Specifically, in aviation, regulatory authorities require the production of system safety cases, for which assurance can provide the necessary evidence to form a robust system safety argument [5].

For the development of aviation software and programmable electronic hardware, assurance approaches such as technical reviews have become commonplace and are well-understood by system developers and independent assessors (acting for the regulatory authorities) [6, 7]. These approaches have become part of best practice [8, 9] and are applied at specific phases in the system development. Although technical reviews provide an important assurance technique, they can provide limited support for systems, for which, developmental evidence is unavailable, such as systems constructed from 3rd party Commercial-Off-The-Shelf (COTS) components.

This paper presents an approach that can be used to provide assurance in systems formed using 3rd party software and programmable electronic hardware COTS components. The aim of this paper is to present a pragmatic approach for assurance, which is based on techniques that are familiar to the professional engineer, as this would most likely produce a more

useable approach. Hence, this approach uses an integrated combination of safety techniques (such as Hazard and Operability Study (HAZOP) and Fault Tree Analysis (FTA) [10]) with formal approaches (such as Coloured Petri nets (CPN) [11]) that can be used to provide systems assurance.

This paper considers the combination of techniques on the basis that the safety techniques possess an 'intuitive' quality that can allow an engineer to explore and understand the system's safety behaviours. Formal techniques, on the other hand, can be used to conduct a detailed investigation of the system safety behaviours within a more rigorous framework. It is intended that this technique would be used during a system's development to perform the safety assessment and guide the design activities rather than to be specifically used at the end of a development phase. This approach is illustrated by showing its application in a case study that involves an automatic actuation control system used in an airborne application.

1.1. Related Work

Safety techniques such as HAZOP and FTA are routinely used within a wide range of engineering sectors. HAZOP is intended to be used by a group of experts (who have a detailed understanding of the system to be assessed) to identify hazards from a system's functional description. Since a system description can be available at any level of abstraction (ranging from top-level system functionality to detailed design), a HAZOP can be performed for different phases within a system's development. HAZOP is applied by using a set of guidewords with the system description to develop a set of scenarios. Each scenario is then assessed for its safety implications and this activity is used to derive hazards.

FTA is a prominent technique used in safety and reliability engineering to understand how a system can cause a hazard and then to determine how to reduce the risk of failure. FTA identifies all possible paths leading to an undesired state and to compute the probability of a particular system-level failure. Due to their intuitive nature, HAZOP and FTA are easily learnt however, to produce an assessment that provides useful safety insights into a system operation, these techniques need to be applied by a group of experts who understand the system and the application of these techniques can be time consuming.

Formal techniques have been well researched and applied within an industrial context [12]. These techniques have the advantages of a formal framework that not only has the ability to precisely specify and model a system but also to exhaustively analyse for properties, by exploring the state-space of the system model. Formal techniques tend to contain mathematical notations that can create issues such as they can be difficult and time-consuming to learn, the notation can introduce initial issues in creating system models and techniques may not be easily scalable to large systems. Hence, approaches that combine formal techniques with the more intuitive semi-formal techniques (such as HAZOP and FTA) tend to produce techniques that are more useable because they can be combined to exploit the advantages of each constituent technique.

The combination of formal and safety techniques has been considered within various research studies. Specifically, approaches such as [13] have focused on endowing fault trees with formal semantics but have not considered application. Approaches such as [14] develop methods that attempt to maintain the semantics between fault trees and formal techniques to provide a conversion of the fault trees into formal representations. Although approach [14] showed that conversion was possible, it did not provide formal proof that the conversion preserved the semantics of the FTA. Approaches such as [15] are based on developing separate models of a system using formal and fault tree techniques. This approach allows for an efficient method of constructing fault trees but has problems in verifying their correctness.

This paper considers that approaches, which create separate system models within formal and safety techniques, can provide a more comprehensive system assessment that can enhance systems assurance. In particular, each technique produces its own unique analysis, which is often complementary to the other constituent techniques. Moreover, the results produced by a technique can be used as the basis for the other constituent techniques, thus providing a holistic view of the system.

2. System

The case study used in this paper considers the assurance of an Automatic Parachute Actuation Device (APAD). The APAD is an electromechanical system that, under defined conditions, automatically opens the main and reserve parachutes for a skydiver. The APAD is distinct from the more commonly available parachute actuation devices (such as used in sports), where the device provides a backup to the skydiver in case the manual parachute fails to deploy. The APAD is intended to be the primary mechanism for opening the parachute, where the device is responsible for activating the opening of the parachute without any intervention from the skydiver.

The components that form the APAD are shown in Figs. 1-2. An examination of Fig. 1 shows that the main components of the APAD are:

- Controller;
- Sensors formed by the Altimeter and the Variometer;
- Main parachute;
- Reserve parachute.

The Altimeter detects pressure to provide a measurement of altitude and the Variometer detects changes in pressure to provide a rate of descent. The Controller is constructed from electronic components (such as a processor and programmable electronic

hardware components) and software (which executes the software code that causes the activation of the Main and Reserve parachutes). Since the APAD is constructed from COTS items, the development of these components is not known apart from information on their general functionality.

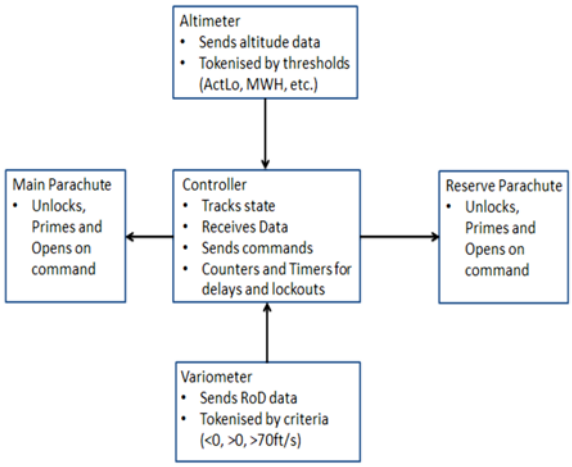

Fig. 1. Functional Composition of the APAD.

2.1. Method of Operation

To activate the APAD, the aircraft must follow a specific trajectory (i.e. during the climb and descent phases of the Aircraft's flight) and the skydiver must operate the APAD at the appropriate points in the Aircraft's trajectory. In particular, when the Aircraft climbs, it must exceed a height at which the APAD is activated (known as the activation lockout (ActLo)) within a certain time, or else the APAD will lockout. The Aircraft must then pass through Main Parachute Wakeup Height (MWH) and Reserve Parachute Wakeup Height (RWH); at these heights the respective circuitry for the Main and Reserve parachutes become operational.

On the Aircraft descent, the APAD's main parachute circuit becomes activated when the Aircraft passes between the heights referred to as the Main Parachute Activation Height (MAH) and the Activation Lockout height 1 (ActLo1). During the Aircraft descent, the MAH marks the highest point at which the Main parachute could be safely opened and the ActLo1 denotes the lowest point at which the Main parachute can be safely opened. Hence, when the Aircraft reaches the MAH, a timer is triggered which allows the main parachute to deploy if the Aircraft's altitude is between MAH and ActLo1, and the Rate of Descent (ROD) is positive. If circumstances occur such that the Aircraft passes the ActLo1 or the timer time-out occurs and the main parachute has not activated, then the main parachute becomes locked out.

If the Aircraft's descent is such that the main parachute does not become activated then the circuitry for the reserve parachute function becomes operational. In particular, similar to the deployment of the main parachute, the reserve parachute can be activated provided the Aircraft height is between Reserve Parachute Activation Height (RAH) and Activation Lockout height 2 (ActLo2). Additionally, between the RAH and ActLo2 heights, the Aircraft's ROD must be greater than a pre-set value (such as 70ft/s). This ROD pre-set value is chosen such that if the main parachute has been deployed, the parachutist will be falling below this value; hence, this condition will not cause the reserve parachute to deploy.

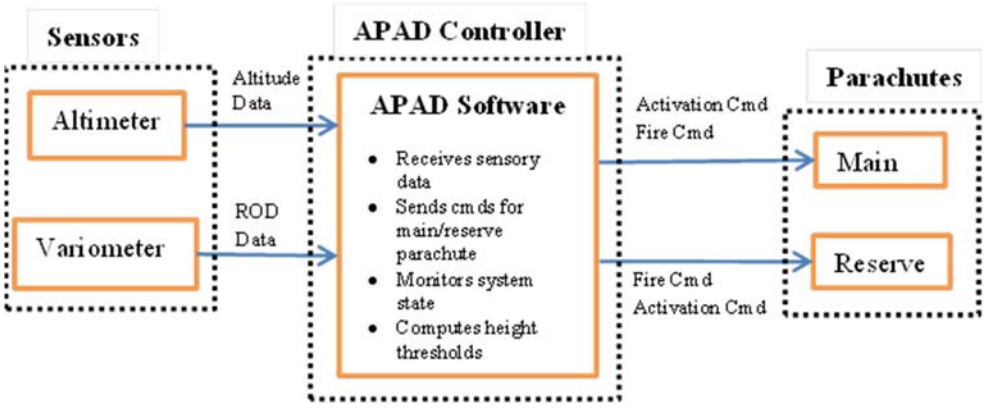

Fig. 2. APAD System used for the HAZOP.

3. Modelling Formalism

The modelling approach was based on identifying the attributes of each constituent technique and combining them in a manner that would exploit these attributes to form an integrated analytical approach. A useful way of integrating these techniques was to determine whether the output of a technique could be used as the basis for an input of another constituent technique.

3.1. CPN Formalism

The formalism of CPN is based on establishing a causal order between conditions (or states) and events

(or transitions). The connection between states and transitions shows 'how' a system functions, which essentially forms a design activity. Moreover, depending on the level of detail available in the system description a high-level or a detailed-level design can be produced.

In creating a CPN model for the APAD, using the available functional description, a very high-level design for the system will essentially be produced. However, it must be understood that the APAD is a COTS-based system, for which a detailed description of its functionality, constituent components and component inter-connectivity is not available. Hence, in producing an APAD CPN Model, it must be recognized that although a high-level design description may have been created, it cannot be used to infer the architecture or the design of the APAD. The APAD CPN model has only been produced to assess the functional behaviour of the APAD system.

Since the CPN allows the state of the system model to change via the enabling and firing of transitions, a CPN model can be executed to produce a sequence of causal ordering of states and transitions. This type of behavior shows a progression of the system in terms of qualitative time, where the occurrence of the next state for a particular state can be identified and thus the set of reachable states can be identified. This type of state description can be used to determine desirable behaviors in the system model (such as whether certain states are reachable) or undesirable behaviors (such as deadlock).

3.2. HAZOP Formalism

The HAZOP was initially developed for the Chemical Processing Plant industry (in the mid-1960s) as a means of identifying hazards based on a knowledge of previous known accidents and incidents. Currently, a HAZOP is a structured approach that, in its application, brings together domain specialists to examine the system under consideration. In the examination, the domain specialists commence by developing typical scenarios that may affect the safety of the system and then perform an analyses on these scenarios by considering the possibility for the occurrence of safety failures. The approach has three main concepts:

- The safety investigation is always performed as a team activity;
- The HAZOP analysis concentrates on identifying the deviations in the behaviour of the system components in comparison to their expected behaviours;
- The HAZOP analysis uses a set of well-defined guidewords to structure the identification of hazards.

A diagrammatic representation of the HAZOP procedure is given in Fig. 3.

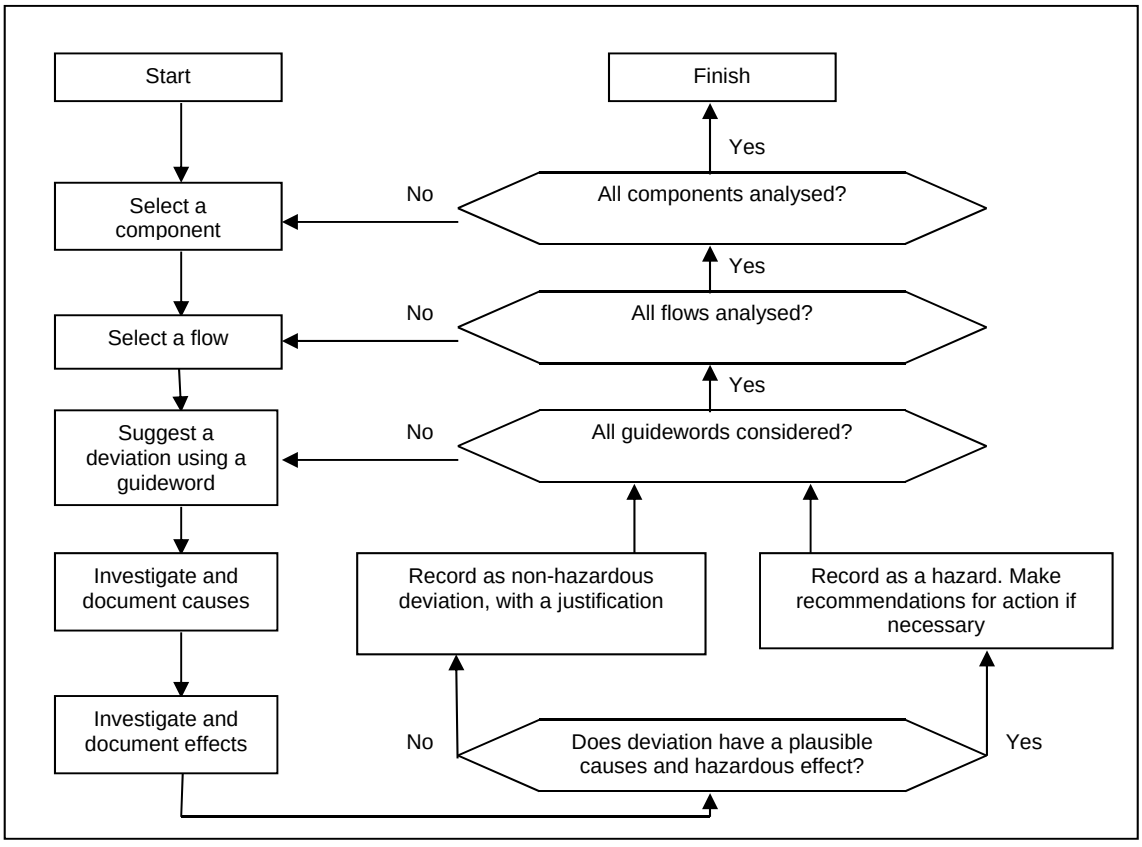

Fig. 3. Diagrammatic representation of the HAZOP process.

As mentioned in the above concepts, the HAZOP requires a system description, which may be in terms of various types of documentation (such as operational manuals or system specifications). Since the CPN model forms a description of the behaviour of the APAD, this formalism can also be used as the basis for the HAZOP.

One of the main results produced from the HAZOP is the identification of hazards. However, these hazards need to be further assessed in order to categorize them in terms of their severity to cause harm (in the intended use of the system) and probability of occurrence. The assessment and categorization of the hazards is an important part of the HAZOP activity because it can identify:

- Those hazards that are tolerable due to a low probability of occurrence, thus representing low risk;
- Those hazards that are intolerable and need to be mitigated (such as by operational means or re-design).

The HAZOP activity typically culminates in a tabulation of the identified hazards supplemented by information such as a description of hazards, hazard causes and hazard mitigation.

3.3. Fault Tree Formalism

When a safety assessment is performed on a system, a fault tree is used to represent every major failure that has been identified. The fault tree shows how the individual fault events in a system combine to result in an undesirable system behavior or catastrophic failure. The fault tree commences from the undesirable event, which forms the root of the tree, and the nodes of the tree represent the specific fault events. Hence, a fault tree represents the undesirable event, in terms of its causal factors (or faults), in a hierarchical manner. The fault tree classifies events into various types such as:

- Primary (or basic failure) events – events that are not further developed on the fault tree;
- Intermediate events - events that are used above a primary event and typically form the output of a gate.

The fault tree comprises nodes, edges and logical gates. The nodes represent events, which are considered as inputs and the edges are used to connect nodes. The logical gates are used to describe the relationship between input and output events. Gates essentially describe Boolean logic functions such as OR, AND, Exclusive OR, Priority AND, and Inhibit.

The analysis of a fault tree can be performed qualitatively or quantitatively. In quantitative analysis, a probability of occurrence is ascribed to the primary events and a computation of probability of occurrence of the root node from the primary nodes is performed. In qualitative analysis, the set of failures that should occur together in order for the root node to occur is determined. Since this paper considers COTS components, for which the probability of component failures would not be available, this paper considers qualitative analysis.

3.4. Modelling Approach

In order to perform an assessment of the APAD, the formalisms detailed in the above sections were combined in the following manner to form the modelling approach:

1. System Description - Initially, it was important to understand the operation of the APAD in the context of its environment. For this to be achieved it was necessary to know the components that form the APAD and their functionality. Furthermore, the functionality of the APAD needed to be related to the trajectory and phases in the Aircraft's flight (as detailed in Section 2.1). This understanding formed an integrated description of the APAD's functionality, which would be crucial to develop failure scenarios from which to perform the HAZOP activity;
2. CPN Modelling - The understanding of the system's functionality, developed in the System Description, can be used to form the basis of generating a CPN model of the APAD. Specifically, the functionality of the APAD in the context of the Aircraft's flight could be used to determine the causal relationship of events that can show how and when the APAD would become activated;
3. HAZOP – The system description can be used as the basis to perform a HAZOP study from which the APAD system hazards could be identified;
4. Fault Tree Analysis – From the HAZOP the major failures were used as the basis to produce the FTA. This description would use the system description and the APAD component description to understand the failure events;
5. CPN Model Analysis – Once the APAD CPN model was produced, it needed to be analysed to show whether it faithfully models the system. This analysis can be performed by generating all the reachable states from the CPN using state space analysis techniques;
6. Augmentation of CPN Model – The information provided by the FTA in terms of the primary events and causes of faults could be used to augment the APAD CPN to create a safe model.

A preliminary application of the above modelling has been presented in the work of [16].

4. Modelling Approach: CPN Modelling

A CPN model for the APAD was created using CPN Tools [11]. A top-level model for the APAD CPN is shown in Fig. 4 and a detailed model is shown in Fig. 5. An examination of the APAD CPN Model of Figs. 4 and 7 shows that each component of the APAD

system was constructed from distinct CPN structures and they are labelled as follows:

- MAIN – represents the states and events modelled for the main parachute;
- RESERVE – represents the states and events modelled for the reserve parachute;
- ALT1 – represents the states and events modelled for the pressure altimeter. In the APAD CPN model, the states of ALT1 were chosen so that they represent when significant heights in the trajectory of the Aircraft (such as ActLo or MAH) have been reached; these heights are deemed to be significant because they are used an inputs to the APAD Controller's parachute activation logic. Also, although the pressure altimeter derives the Aircraft heights from pressure measurements (by a process of sampling and converting signals from analogue to digital form), this type of detail was considered to be at a low-level of abstraction and not modelled;
- VARIO - represents the states and events modelled for the variometer, which measures the pressure difference to provide a ROD indication. Similarly, to ALT1, the states modelled for the variometer were chosen so that they are useable by the controller;
- CONTROL – represents the states and events modelled for the controller.

The APAD system was partitioned into the above components because they were noted from the system description. Specifically, it was noted that the APAD Controller controls and manages the dataflow and program execution within the APAD system; the pressure altimeter and variometer provide the sensory data to the APAD Controller; the operation of the main and reserve parachutes are actuated based on the control commands produced by the APAD Controller.

Since a detailed description of the APAD was not provided, no information is provided on the architecture or connectivity of the above components. Hence, to form the APAD CPN model certain assumptions needed to be made. For example, the model assumed that the APAD Controller was a centralized controller, given that it seemed to be responsible for coordinating the device operation. In addition, it was not clear on what methods are used by the APAD systems to sample the sensors, i.e. via polling or interrupts-driven mechanisms. Hence, a simple message passing method was assumed in the CPN model.

As the APAD is a "one-shot" system, it was deemed acceptable to model the APAD Controller, the main and reserve parachutes as open chains because physical repacking and re-arming of the parachutes would be required for next operation. In the CPN Model, the "one-shot" function of the APAD is modelled by not allowing the final states of the main and reserve parachutes to form inputs to any other CPN structure. Hence, the state of the APAD CPN Model would need to be reset to its initial state before the commencement of the next flight.

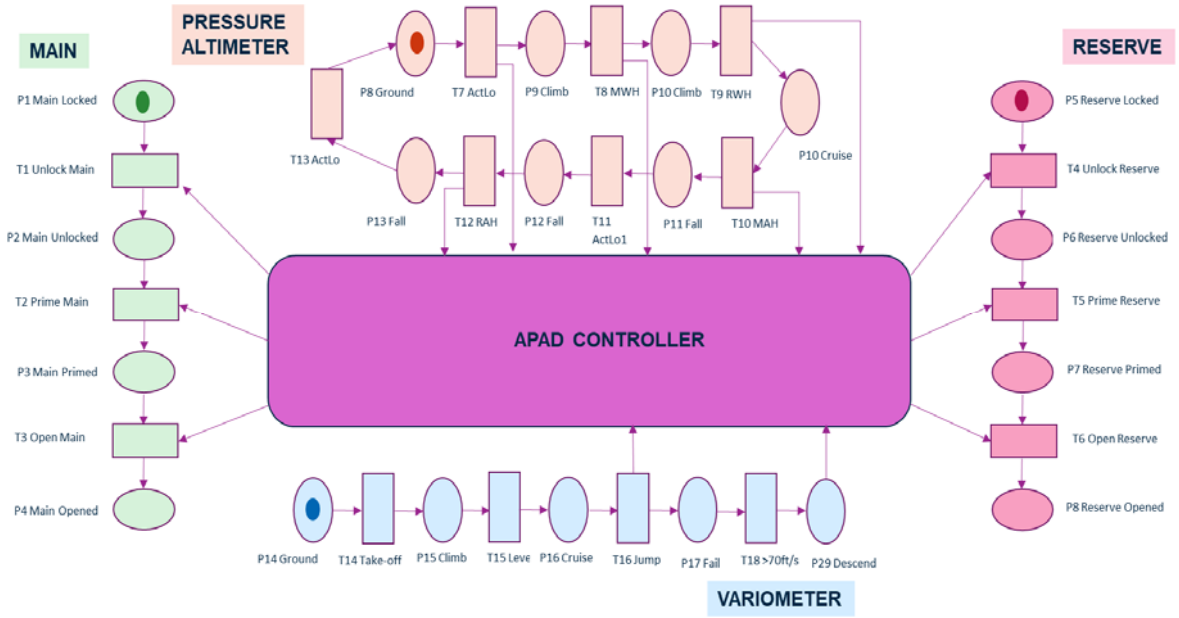

Fig. 4. A Top-level representation of the APAD CPN Model.

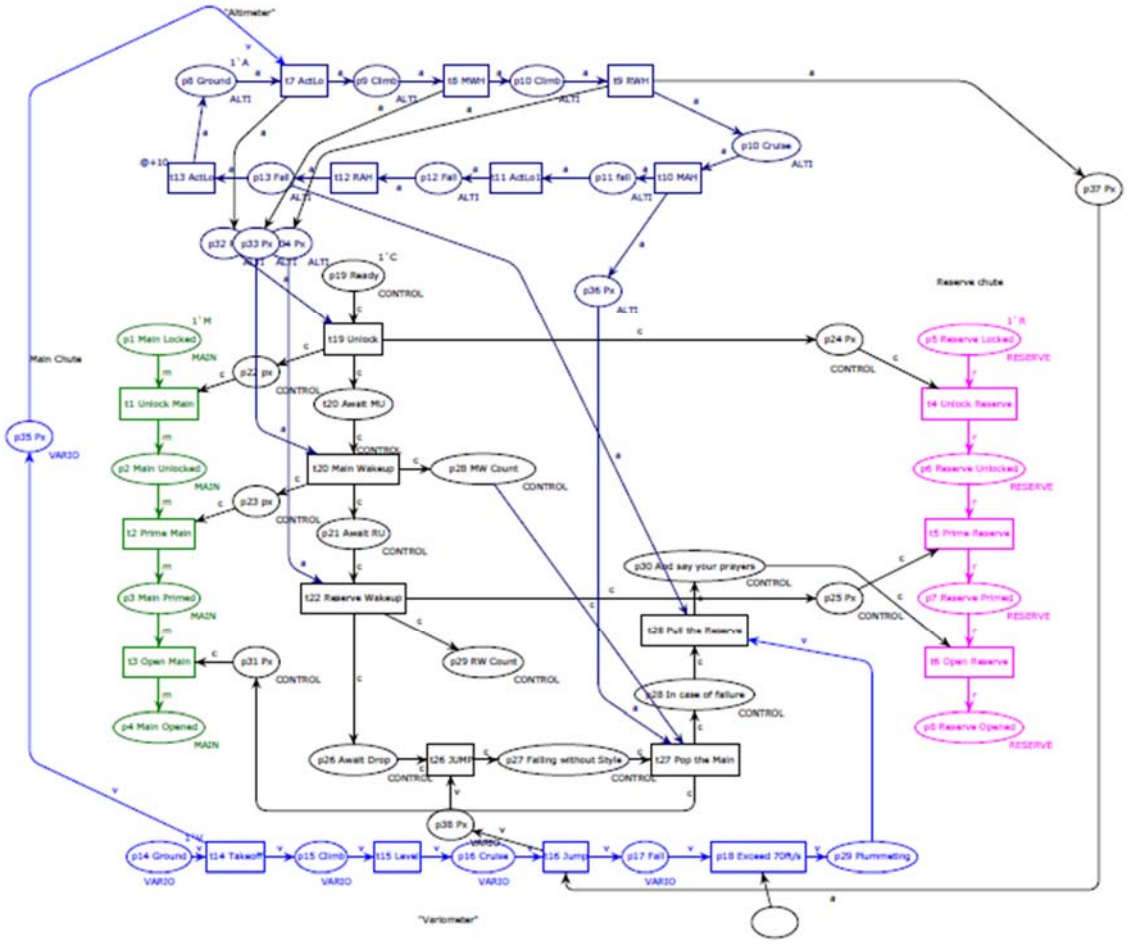

Fig. 5. Initial APAD CPN Model.

5. Modelling Approach: Safety Assessment

5.1. HAZOP

The approach taken to perform the HAZOP process for the APAD system involved the execution of the following steps:

- Define the system under consideration – The domain specialists need to develop an understanding of the system's role, its operational environment and define the functionality that is in scope of the assessment;
- Agree the HAZOP guidewords and attributes – The domain specialists need to determine and agree on the HAZOP guidewords and attributes that they will use to investigate the deviations from expected behaviours connected with the system;
- HAZOP recording – This step tabulates the HAZOP activity and provides a written record of the hazards;
- HAZOP outcome – This step involves identifying the hazards produced by the assessment and classifies their severity.

HAZOP was performed on the APAD system using the available APAD documentation. Specifically, the HAZOP considered a simplified form of the APAD system which shown in Fig. 2; this form shows the basic components and the data flow within the system.

Although a HAZOP analysis uses a standard set of guidewords, their interpretation can vary depending on the type of system that is being assessed and the level of abstraction to which the analysis is being performed. For APAD HAZOP, the guidewords and their meaning are presented in Table 1.

Table 1. Guidewords used for the APAD HAZOP.

Guideword	Data Description
Too much	The data value is too high (exceeds upper limit or bounds)
Too little	The data value is too low (less than lower limit or bounds)
Incorrect	The data value is within limits but has incorrect value

Since the core of the APAD system is the controller, the HAZOP considered the sensory inputs that it receives (i.e. the pressure altimeter (PA) and ROD) and used a set of guidewords (Table 1) to determine the effect of changes in the sensory inputs on the APAD system.

The results of the HAZOP activity are recorded on a table, which typically has information such as:

- Type of input under consideration;
- Guideword used;
- Cause of fault;
- Consequence of implication of fault;
- Indication of fault occurring or mechanism for protecting against a fault;
- Recommendations or questions arising from fault;
- Identification of hazard;

Due to space limitations, the complete tabulation and details of the HAZOP cannot be shown. However, a summary of the HAZOP results is detailed in Table 2, which shows the input sensory data of PA and rate of descent (ROD). For the descent phase of the Aircraft's trajectory, the HAZOP produced the following 3 key hazards (also shown in Table 2):

I. Failure to deploy parachutes when required;
II. Inadvertent opening of the parachutes in the Aircraft;
III. Inadvertent opening of the parachutes before skydiver clears the Aircraft.

For Hazards II-III, it was observed that their occurrence was dependent on the APAD having a breakaway mechanism, which detects whether or not the APAD system is on board the Aircraft. Since it was not clear on what form of breakaway mechanism had been used with the APAD system, this paper focuses on Hazard I. Furthermore, Hazard I (which concerns the failure of the parachutes to open when the skydiver performs an exit from the Aircraft) was considered because it was:

- Better understood by the domain experts, given the description of the APAD system provided;
- More likely to have a severity level of critical or catastrophic.

Examples of the above hazards are shown in Table 2.

Table 2. Extract of the HAZOP for the inputs provided by Pressure Altimeter and Variometer to APAD System.

Hazard	Sensor (Guideword)	Consequence/Implication
Parachutes do not open (Hazard I)	PA (Too little)	Immediately after Skydiver jumps from Aircraft
	PA (Too little)	Skydiver has jumped from Aircraft
	PA (Too much)	Skydiver has jumped from Aircraft
	PA (Too much)	Immediately after Skydiver jumps from Aircraft
	PA (Incorrect)	Skydiver has jumped from Aircraft
	PA (Incorrect)	Immediately after Skydiver jumps from Aircraft
	ROD (Too little)	Skydiver has jumped from Aircraft
	ROD (Incorrect)	Skydiver has jumped from Aircraft
	ROD (Incorrect)	Immediately after Skydiver jumps from Aircraft
	ROD (Incorrect)	Immediately after Skydiver jumps from Aircraft
	ROD (Incorrect)	Skydiver has jumped from Aircraft
	ROD (Incorrect)	Immediately after Skydiver jumps from Aircraft
Premature opening of Parachutes (Hazards II-III)	PA (Too little)	Skydiver has jumped from Aircraft
	PA (Too little)	Skydiver is in Aircraft
	PA (Too little)	Immediately after Skydiver jumps from Aircraft
	PA (Incorrect)	Immediately after Skydiver jumps from Aircraft
	ROD (Too much)	Skydiver is in Aircraft
	ROD (Too much)	Immediately after Skydiver jumps from Aircraft
	ROD (Incorrect)	Skydiver is in Aircraft
	ROD (Incorrect)	Immediately after Skydiver jumps from Aircraft
Parachutes open too late (Hazards II-III)	PA (Too little)	Immediately after Skydiver jumps from Aircraft
	PA (Too much)	Skydiver has jumped from Aircraft
	PA (Too much)	Immediately after Skydiver jumps from Aircraft
	PA (Incorrect)	Skydiver has jumped from Aircraft

5.2. Fault Tree

The fault tree for the APAD system (referred to as APAD Fault Tree) was generated by considering each hazard obtained from the HAZOP (see Section 5.1) and establishing the primary events, which are the root causes of the hazard. This activity was performed with the assistance of the APAD architecture (as shown in the APAD CPN Model) and APAD system description. Due to space limitations the complete APAD Fault Tree cannot be shown, however, the APAD Fault Tree for Hazard I is shown in Fig. 6 and the following discusses the key results obtained from the APAD Fault Tree.

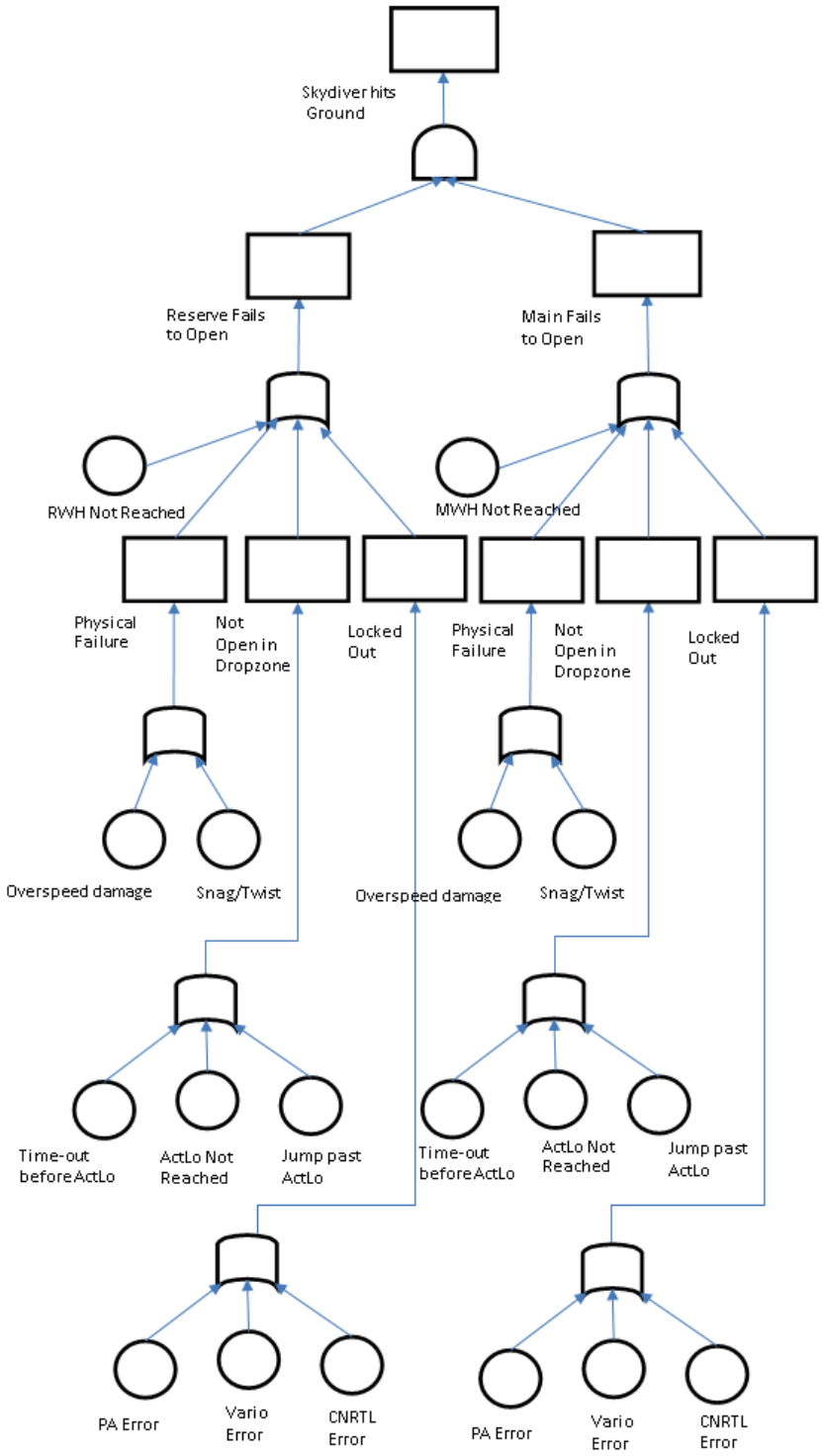

Fig. 6. APAD Fault Tree for Hazard I.

An inspection of the APAD Fault Tree confirmed that the APAD system has built in redundancy due to having two parachutes (i.e. the main and reserve parachutes).

In identifying the root causes for Hazard I, the APAD Fault Tree showed that the first main cause of this hazard, is when the skydiver exits from the Aircraft (referred to as a jump), when the Aircraft is at its appropriate flight phase, and the APAD system is locked out. In this case, both the main and reserve parachutes cannot be activated. This scenario could occur if the skydiver either jumps below ActLo or the APAD timer reaches maximum count before the Aircraft reaches ActLo. The former is unlikely as the APAD system is intended for use by trained skydivers but the latter is likely. Specifically, the APAD timer may exceed its count in scenarios such as the jump being delayed. This situation could be mitigated by installing a manual lockout/disable system for use in the event of the jump being cancelled or delayed.

The second cause of Hazard I, identified from the APAD Fault Tree, can occur in the following conditions:

- If the skydiver jumps without the Aircraft having reached the MWH. In this case, both the main and reserve parachutes will not be operational, thus leading to a catastrophic situation;
- If the skydiver jumps without the Aircraft having reached the RWH, the reserve parachute will not be operational. However, this situation poses less risk than the above situation because the Main parachute circuitry will be operational.

The third cause of Hazard I, identified from the APAD Fault Tree, is faults occurring in the pressure altimeter or variometer sensors causing incorrect sensory data values being sent to the APAD Controller. This situation introduces a single point of failure in the APAD system. Given the limited detail available in the APAD system's functionality, it is not clear what mitigations on this scenario have been placed in the design of the APAD system. Typically, safety related systems are likely to be developed to provide mechanisms for failure detection and performing corrective action or to use sensors that are robust to measurement failures. However, such mechanisms cannot be assumed in this situation. From an assurance perspective, in order to mitigate against erroneous readings from these sensors being used by the APAD software, several measures can be used such as:

- A checkable readout (or error alert) can be implemented to ensure that the skydiver does not jump when the APAD Controller either receives no or faulty data from the sensors;
- Additional integrity checks can be implemented on the data provided by the sensors to the APAD Controller.

6. APAD CPN Model Analysis

The APAD documentation and APAD system description (shown in Section 2.0) formed the basis for the construction of the APAD model. In addition, the APAD system was modelled in CPN (see Fig. 5), using CPN Tools. Since the components of the APAD could be easily identified and an understanding on their functionality was obtained, the APAD CPN model could be partitioned into:

- APAD Controller.
- Sensors – as represented by the PA and variometer.
- Parachutes – which contained the main and reserve parachutes.

Since the pressure altimeter provided sensory data, consisting of altitude and ROD data, as an input into the APAD Controller, this data could be modelled as a flow of tokens from the sensory CPN to the APAD Controller CPN. Specifically, the sensory data received from the altimeter and variometer could be modelled in the form of message passing, where a place (which is a Petri net structure representing a state and shown as an 'oval' shape in Figs. 5 and 7) was used to represent the arrival of 'new' data. The existing data in a place would leave the place by firing a transition (shown as a rectangular structure in Figs. 5 and 7) and moving the data to its connecting place.

The APAD Controller contained the software algorithms that processed the sensory data and determined whether the various heights (i.e. ActLo, MWH, RWH, MAH, ActLo1, RAH or ActLo2) had been reached and determined whether conditions had been satisfied to fire the Main or Reserve parachutes. The CPN model for the APAD Controller could be modelled as receiving tokens from the Sensory CPNs, processing these tokens and communicating fire commands to the Main and Reserve Parachute CPNs. The CPN structures for the APAD Controller, Sensory and Parachutes functionality was represented by different colorsets.

6.1. Initial APAD CPN Model

The initial APAD CPN model was constructed and shown in Fig. 5. The initial APAD CPN contained the causal ordering of events detailed in the APAD documentation and this could be easily verified by performing a step-by-step simulation of the model, using CPN Tools. However, when CPN Tools was used to simulate the complete model, it produced some undesirable behaviours that could have safety implications. Specifically, these behaviours includes situations such as the parachutes being ready to deploy whilst the MWH and RWH had not been reached. This scenario was undesirable because the APAD was not in synchrony with the external environment; the Aircraft had not fully achieved its climb (which was the initial stage of Aircraft's flight) but the APAD had set the parachutes to deploy, as required during Aircraft descent.

In terms of CPN modelling, a process of trial and improvement could have been used to remove the above undesirable behaviours by re-modelling and using mechanisms such as interlocks in the CPN model. However, in this paper, the results obtained from the APAD Fault Tree were used to inform the process of improving the CPN model.

6.2. Improved APAD CPN Model

The results from the APAD Fault Tree were used to modify the APAD CPN model to improve its safety functionality; the resulting CPN is shown in Fig. 7. The improvements made to the APAD CPN were as follows:

Firstly, the inclusion of a "status" place, which receives tokens from the APAD Controller to display on the APAD; this allows the skydiver to have a display of the state of readiness of the APAD. This status report can prevent the skydiver from

inadvertently performing a jump with the APAD being in a state of having locked out of both the parachutes. Secondly, additional CPN structures were added to Fig. 7 (such as 'MW count', 'RW count', 'max' and 'not max' places) to indicate lockout states. These modifications provide mitigation to the first and second causes shown by the APAD Fault Tree (detailed in Section 5.2).
Thirdly, timings were added to the APAD CPN model for the altimeter and variometer, as this would allow:

1. APAD Controller to be in synchrony with Aircraft passing through the various phases of its trajectory (such as MWH, RWH, MAH and RAH). This would prevent situations such as parachutes being ready to deploy when Aircraft flight trajectory had not reached that stage;
2. Modelling of the process of sensor sampling and storage of measured data values.

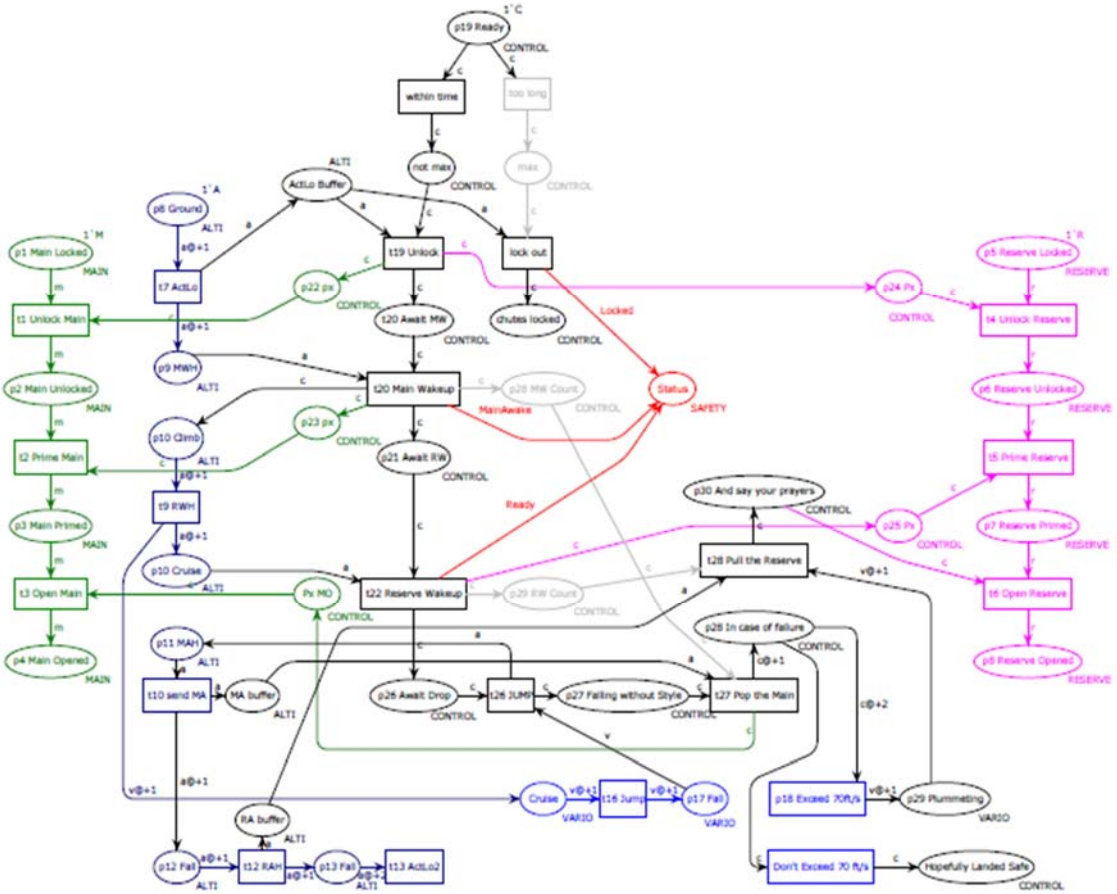

Fig. 7. Improved APAD CPN Model.

6.3. AAD CPN State Space

A state space analysis of the improved APAD CPN model was performed using CPN Tools, which produced a large simulation graph comprising 280 nodes and 710 arcs. Although the simulation graph was difficult to analyse, sections of the graph were examined incrementally. The state space analysis showed that a dead marking (which represents the state of activation lockout having occurred, main parachute not deployed and reserve parachute not deployed) could occur. This marking represented an unsafe state at which a deadlock was reached if ActLo is not reached in time. This state was entirely predicted by the FTA. Since state space analysis did not show any other deadlock conditions, the improved APAD CPN model provided greater assurance in the APAD design.

7. Conclusions

This paper considered the issue of providing assurance for systems that are constructed from 3rd party software and programmable electronic hardware components. Providing assurance for such systems using standard methods (such as technical reviews) presents issues due to the lack of the availability of developmental evidence. Hence, this paper proposed an approach, which used a combination of safety and formal techniques to provide systems assurance.

The motivation of combining safety techniques of HAZOP and FTA and formal techniques of CPN is that these techniques can produce useful assessments, which can be used for assurance, when limited information (or developmental evidence) exists for a system. Specifically, the application of the above techniques to a case study (presented in this paper, which involves a real-time safety related control system) has shown that:

1. The intuitive nature of HAZOP and FTA allows a number of scenarios to be explored and can identify areas of known and unknown system behaviours.
2. Each technique can be used to perform its own unique analysis, without the need to introduce any complexities of ensuring whether the semantics of each technique has been preserved.
3. The results produced by each technique can be effectively used by the other constituent techniques. Specifically, in this case study, the hazards derived from the HAZOP can be used as the primary events for the FTA. The fault causes from the FTA can be used to assess the behavioural sequences that are produced by the CPN model. This can be used to modify the CPN model and constrain its behaviour.

The application of the overall approach shows that it allows a better understanding to be gained of the system behaviour. This understanding can inform on the risk posed by the system: high risk (if too many unknown behaviours), low risk (if most behaviours are known). This understanding can provide greater assurance in the overall system.

References

[1]. D. Raheja, M. Allocco, Assurance Technologies Principles and Practices, *Wiley*, 2006.

[2] Design Assurance Guidance for Airborne Electronic Hardware, DO-254 Training, *EUROCAE/RTCA*, 2000.

[3]. Software Considerations in Airborne Systems and Equipment Certification, DO 178C Training, *EUROCAE/RTCA*, 2012.

[4]. Road Vehicles – Functional Safety, *BS ISO 26262*, 2011.

[5]. D. Jackson, M. Thomas, L. Millett (Eds.), Software for Dependable Systems: Sufficient Evidence ?, *National Academies Press*, 2007.

[6]. FAA Job Aid: Conducting Airborne Electronic Hardware Reviews, *Aircraft Certification Service Rev.*, February 28, 2008, https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/media/CEH-JobAidRev022808.pdf

[7]. FAA Job Aid: Conducting Software Reviews Prior to Certification, *Aircraft Certification Service*, 16th January 2004.

[8]. L. Rierson, Developing Safety-Critical Software, *CRC Press*, 2013.

[9]. R. Fulton, R. Vandermolen, Airborne Electronic Hardware Design Assurance, *CRC Press*, 2015.

[10]. C. Ericson, Hazard Analysis Techniques for System Safety, *Wiley*, 2016.

[11]. CPN Tools (http://cpntools.org/)

[12]. J. S. Fitzgerald, J. Bicarregui, P. G. Larsen, J. Woodcock, Industrial Deployment of Formal Methods: Trends and Challenges, in Industrial Deployment of System Engineering Methods, A. Romanovsky, M. Thomas (Eds.), *Springer*, 2013.

[13]. G. Schellhorn, A. Thums, W. Reif, Formal Fault Tree Semantics, in *Proceedings of the 6th World Conference on Integrated Design and Process Technology*, Pasadena, CA, 2002.

[14]. O. Ariss, D. Xu, W. Wong, Integrating Safety Analysis with Functional Modeling, *IEEE Transactions on Systems, Man and Cybernetics*, Vol. 41, No. 4, July 2010, pp 610-624.

[15]. G. Schellhorn, A. Thums, W. Reif, Safety Analysis of a Radio-Based Crossing Control Systems using formal methods, in *Proceedings of the 9th IFAC Symposium Control in Transportation Systems 2000*, Braunschweig, Germany, June 2000, pp. 289-294.

[15]. J. S. Sagoo, Design Assurance of COTS based Electronic Systems, in *Proceedings of the 2nd International Conference on Microelectronic Devices and Technologies (MicDAT 2019)*, Amsterdam, The Netherlands, 22-24 May 2019, pp.43-50.