Reliability Engineering and System Safety 169 (2018) 166–178

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Application of temporal logic for safety supervisory control and model-based hazard monitoring

Francesca M. Favarò [a,*], Joseph H. Saleh [b]

[a] Department of Aviation and Technology, San Jose State University, San Jose, CA, USA
[b] School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA, USA

ARTICLE INFO

Keywords:
Supervisory control
Hazard monitoring
Temporal logic
Dynamic risk assessment
Verification

ABSTRACT

In this work, we extend a previously introduced framework for safety supervisory control with the ingredient of Temporal Logic (TL) to improve both accident prevention and dynamic risk assessment. We examine the synergies obtained from integrating model-based hazard modeling/monitoring with the verification of safety properties expressed in TL. This expanded framework leverages tools and ideas from Control Theory and Computer Science, and is meant to guide safety intervention both on-line and off-line, either during the design stages or during operation to support operator's situational awareness and decision-making in the face of emerging hazardous situations. We illustrate these capabilities and the insight that results from the integration of the proposed ingredients through a detailed case study. The study involves a runway overrun by a business jet, and it shows how hardware, software, and operators' control actions and responses can be integrated within the proposed framework. The aircraft suffered from a faulty logic in the Full Authority Digital Engine Computer (FADEC), which prevented the pilot from activating the thrust reversers in a particular operational scenario. We examine the accident sequence against three system safety principles expressed in TL: the fail-safe principle, the defense-in-depth principle, and the observability-in-depth principle. The framework is implemented in Simulink and Stateflow, and is shown to provide important feedback for dynamic risk assessment and accident prevention. When applied on-line, it provides warning signs to support the sensemaking of emerging hazardous situations, and identifying adverse conditions that are closer to being released. When applied off-line, it provides diagnostic information regarding missing or inadequate safety features embedded in the system. For the specific case study, we propose a new TL safety constraint (based on speed measurements and the history of pressure sensors from the landing gears) to be incorporated in this and other aircraft FADEC, and that could have prevented the hazardous situation, in this case a rejected takeoff following tire explosion, from turning into a deadly accident. We conclude with some recommendations to prevent similar accident recurrences and to improve accident prevention.

1. Introduction

In this work, we extend the safety supervisory control framework introduced in a companion article [8] with the ingredient of Temporal Logic (TL). Specifically, we examine the synergies obtained from integrating model-based hazard modeling/monitoring with the verification of TL safety constraints to improve both accident prevention and dynamic risk assessment. We present a detailed case study to illustrate the novel insights that result from this integration for improving dynamic risk assessment and accident prevention.

The use of TL in risk assessment offers many possibilities for overcoming some of the limitations associated with traditional Probabilistic Risk Assessment (PRA), for example in accounting for time-related considerations in accident scenarios and in handling software issues. The latter is a serious issue since most engineering systems are increasingly software-intensive, and not having a risk assessment tool (and modeling formalism) that can handle all risk aspects of such systems in an integrated manner is an important gap in the analytical toolset of risk analysts and safety professionals.

In our previous work, we developed a safety supervisory control framework and analytical tools for monitoring emerging hazards in a system, and guiding safety interventions both on-line and off-line [8]. We leveraged state-space formalism and model-based approaches, first to establish hazard levels or danger indices as metrics that measured the "proximity" of the system to adverse events, and second to estimate the times at which critical thresholds for the hazard level are (b)reached. This estimation process provided important prognostic information and produced a proxy for a time-to-accident metric or advance notice for

* Corresponding author.
E-mail address: francesca.favaro@sjsu.edu (F.M. Favarò).

http://dx.doi.org/10.1016/j.ress.2017.08.012
Received 4 August 2016; Received in revised form 4 August 2017; Accepted 11 August 2017
Available online 17 August 2017
0951-8320/

impending adverse events. We also introduced a hazard temporal contingency map as a tool to support operators' situational awareness by providing prognostic information regarding the time windows available to intervene before hazardous situations become unrecoverable, and to help decision-makers prioritize attention and defensive resources for accident prevention.

We now augment the previous safety supervisory framework (anchored in state-space formalism) with the new ingredient of Temporal Logic. Temporal Logic is being adopted in an increasing number of fields, such as robotics and safety-critical systems, and it is used in a variety of ways, as a formal language to express software requirements for example [5,26], or for the expression of specifications for automated motion planning of vehicles such as robots and UAVs [18]. Once a requirement or specification is provided in TL, checks and controls can be implemented to ensure that such behavior is followed. We made the case for the introduction and use of TL in risk assessment in [9], to overcome the static nature of most risk assessment tools which are ill-suited to handle modern applications of cyber-physical systems [20]. Briefly stated, TL allows the explicit inclusion of temporal considerations in the definition of safety requirements, which then act as constraints on the system behavior. Safety features can then be put in place to either ensure compliance with these constraints or to trigger warnings if/when they are violated.

Uses of TL and other timed logics for risk assessment and safety analysis have been proposed and pioneered in the late 1990s early 2000s (notable in particular are the works by Chris Johnson [15–17]; for a survey of the use of timed logics in risk and safety applications see [8]).

The objective of this work is to integrate TL with the safety supervisory framework on the one hand, and to demonstrate the practical application of the integrated framework and the novel insights it can provide for improved risk assessment and accident prevention on the other hand. The expanded framework leverages tools and ideas from two disciplines, Control Theory (state-space formalism, feedback, and estimation), and Computer Science (Temporal Logic and requirement specifications/verifications). To illustrate the capabilities and workings of the integrated framework, we present a case study as a "proof-of-concept" involving a Learjet accident during a rejected takeoff. The case study shows how hardware, software, and operators' control actions can be integrated within the framework. Software played a key role in the escalation of the accident sequence, and it is here analyzed in detail. We show among other things that the aircraft suffered in fact from a faulty logic, a lurking accident pathogen, in the Full Authority Digital Engine Computer (FADEC), which prevented the pilot from activating the thrust reversers in particular operational scenarios, and further aggravated the situation by shifting the backward thrust selected by the pilot to a forward thrust schedule. We propose a new TL safety constraint (based on speed measurements and the history of pressure sensors from the landing gears) to be incorporated in this and other aircraft FADEC, and that could have prevented the hazardous situation, in this case a rejected takeoff following tire explosion, from turning into a deadly accident. Moreover, we examine a novel metric for online support of pilots' go/no-go decision-making during critical takeoffs. This metric relates the distance required for the aircraft to stop (in both nominal and worst-case conditions) to the total length available to the aircraft before encountering an obstacle on its path. Its set-up and check against predefined criticality threshold can augment the current (limited) thinking that revolves around the decision speed V_1 as a safety threshold for aborting a takeoff, and can also better inform accident investigation and provide cues for the prevention of similar occurrences in the future.

The remainder of this work is organized as follows. Section 2 provides a brief review of the safety supervisory framework and the necessary background material regarding the notion of hazard level and the TL syntax. Section 3 presents the case study, and analyzes in detail the hazard monitoring process and the verification of compliance of the TL safety principles. Section 4 concludes this work.

2. Setting the stage: a brief review of the safety supervisory control framework and temporal logic

This section provides a brief review of the two main ingredients that are combined in this paper:

1. The safety supervisory control framework, originally presented in [8]
2. The TL logical constraints, whose verification allows the embedding of a quantitative safety assessment both off-line and/or in real-time (details are available in [9]).

2.1. Model-based safety supervisory control framework

The model proposed in [8] is shown in Fig. 1, and the TL components are added to the "Safety supervisory monitoring" block. The objectives of the framework and analytical tools here developed are to guide safety intervention for improved accident prevention by leveraging a novel dynamic approach to risk assessment.

Our previous work sought to shift the emphasis from the pervading probabilistic mindset in risk assessment, which is largely static, toward the notions of danger indices and hazard temporal contingency. The elements in Fig. 1 are grounded in Control Theory, except for the TL ingredients, and they make use of the state-space formalism in modeling dynamical systems.

The approach starts with the creation of a model for the dynamical system under consideration (shown in the lower right part of Fig. 1 in the "System model" block). We showed that the use of state variables enables the definition of metrics for accident escalation, termed hazard levels or danger indices H(t), which measure the "proximity" of the system state to adverse events. State variables (a subset of) are then mapped into danger indices, and their dynamics is captured in a hazard state equation. A notional example of hazard dynamics is shown in Fig. 2.

In order to define the hazard function H(t), we first need to specify what accident we wish to monitor against. The case study of Section 3 analyzes a runway overrun. A simple 1-D H(t) example can be set as

$$H(t) = \frac{x(t)}{\ell_{rw}} \tag{1}$$

where x(t) represents the position of the aircraft along the runway and ℓ_{rw} is the total length of the runway. In this simple example, the value H = 1 would correspond to the situation in which the aircraft has reached the end of the runway. A simple use of Eq. (1) (or a more detailed version of it as shows in Section 3) is that of ensuring a maximum safety threshold in terms of "distance from the end of the runway" before which the aircraft has to have completed rotation for take-off.

One goal is to establish and monitor danger indices such as the one in Eq. (1) to support and help guide safety interventions. These features/functions are shown in the lower part of the "Safety supervisory monitoring" block in Fig. 1. Estimation of the hazard level provides important prognostic information and produces a proxy for a time-to-accident metric or advance notice for impending adverse events. Hazard state equations are used to estimate the times at which critical thresholds for the hazard level are (b)reached. For instance, by setting up a maximum allowable value for H(t) corresponding to an accident occurrence and denoting this value by H_A, we obtain the requirement

$$H(t) < H_A \tag{2}$$

One simple linear estimator of the time at which the critical threshold H_A is reached can be obtained through the hazard equation as

$$\widehat{\Delta T_A}(t_e) = t_A - t_e = \frac{H_A - H(t_e)}{\dot{H}(t_e)}. \tag{3}$$

More involved estimators will be examined in future work; they are not the focus of the present article. When multiple hazards levels are monitored, we proposed a hazard temporal contingency map to displays