Agile Error Proofing

A framework for adaptive resilience assurance

Abstract submitted to the EuroControl Flight Safety Forum, 2018

Avi Harel, Ergolight, Haifa, Israel

ergolight@gmail.com

Most flight accidents are typically attributed to human errors. The article proposes a framework for agile error-proofing of the interaction between the machine and its operators. The framework was evaluated by a working group of Israeli systems engineers, using a database of 67 events.

It is commonly agreed that it is better to prevent accidents than to investigate them. To prevent accidents, we need to prevent operator errors and to apply lessons learnt from low-cost incidences, called near-misses. A recently developed methodology for resilience assurance recommends on a model of system resilience, used to describe common patterns of the system behavior when under hazard. According to this model, incidences are defined as instances of risky operation in exceptional situations.

The resilience model describes common ways in which disruptions are transformed to hazards, conditions for hazard detection, indication and recognition, for alarming and reporting about threats, etc. Following the STAMP paradigm , exceptional situations are instrumented by regarding them as instances of violation of operational rules. The model contains standard definition of critical operational rules about the interaction with the operators. Typically, operational rules may be expressed in terms of various thresholds of system variables based on manipulation of sensory data, defined as system parameters. These thresholds may be used for the alarm control.

Often, operational rules conflict each other. An important example of conflicting rules is of the rules affecting the helm control, namely, the allocation of various control functions to the machine and the operators. If the machine takes over the operator, it may be the case that the machine was not designed to control the particular exceptional situation. On the other hand, if the machine transfers the control to the operators, the operators might fail to recognize the exceptional situation and thereof to act as expected. A way to work around the conflicting rules is by tradeoff rules. For example, helm control may be assigned by default to either the machine or the operators, depending on the task requirements about the particular situation. Also, the other party (the one not in control) may sometimes (depending on the particular situation) be allowed to override the default allocation. Another example of conflicting rules is of those defining the rate of missed alarms vs. those defining the rate of nuisance alarms. The alarming model enables reducing both the rate of nuisance alarm and that of missed alarms.

During the operation it may become evident that the rate of nuisance or missed alarms is too high. This might be due to suboptimal setting of the alarm thresholds. To enable agile, adaptive changing of the system parameters we need to collect data about the system variables, to analyze the data and to recalculate the system parameters. The article proposes to adopt a standard resilience-oriented architecture, which integrates these concepts.

The article will demonstrate the potential benefit of applying the framework by analysis of celebrated accidents.