Sensor Integration Verification

Avi Harel https://avi.har-el.com/

Ergolight consulting ergolight@gmail.com

Abstract

The article presents a model based on scoping review of three published accidents, due to sensory setup errors, and a framework for eliminating these errors by design. Two of the accidents were at the system setup, and the third was due to a maintenance error. The framework is based on a simple model of sensory data, which classifies the sensory values as regular, exceptional, or high risk. The underlying model is motivated by the practice of statistical process control (SPC), by splitting the range performance variables according to statistical quantiles. The protection is by notifying about exceptional values and alerting on high risks. Such simple models are easy to implement in the scope of the developing discipline of integration engineering.

Objective

The article addresses the topic of detecting setup errors, demonstrated in three case studies. The goal is to propose a model, including principles and a procedure, for detecting and reporting on sensor integration problems. The model is based on analysis of investigation reports of three well-known accidents.

Case studies

The model was obtained by analysis of investigation reports of three published accidents, attributed to sensor integration errors. Two of the accidents were due to sensor assembly errors, and the third in due to a maintenance error.

MX981 mishap - 1949

MX 981 was a rocket sled, used for the testing of ejection seats for supersonic jets. The system used 24 sensors to measure extreme acceleration. The engineer who built the system was the famous Ed Murphy, the person behind the famous Murphy’s Law. His technician assembled all the acceleration sensors upside down. As a result, the system accelerated abruptly at 40g.

Ed Murphy did not propose ways to avoid this kind of error, or the need for standards intended for this goal. Instead, he chose to blame the technician, arguing that "If there are two or more ways to do something and one of those results in a catastrophe, then someone will do it that way."

This case study was reported by Harel (A, 2024) based on published information.

Proton M – 2013

Proton M was an expendable Russian heavy-lift launch vehicle. In July 2013, a Proton-M carrying three satellites failed shortly after liftoff. The investigation indicated that three of the first stage angular velocity sensors, responsible for yaw control, were installed in an incorrect orientation. In this case, the sensor design protected from integration errors, enabling installation only in one direction, yet the technicians forced them to the wrong orientation. The error was not detected at the setup.

This case study was reported by Harel (B, 2024) based on published information.

AeroPeru PL603 - 1996

Aeroperú Flight 603 was a scheduled passenger flight from Miami International Airport in Miami, Florida, to Arturo Merino Benítez International Airport in Santiago, Chile, with stopovers in Quito, Ecuador, and Lima, Peru. On October 2, 1996, the aircraft flying the final leg of the flight crashed, killing all 70 people aboard. Flying over water, at night, with no visual references, the pilots were unaware of their true altitude, and struggled to control and navigate the aircraft. The investigation determined that the air data computers were unable to show correct airspeed and altitude on cockpit displays because a maintenance worker had failed to remove tape covering the pitot-static system ports on the aircraft exterior. The error was not detected until after takeoff. The airplane designers failed to provide any indication of the setup error.

This case study was reported by Harel (C, 2024) based on published information.

Modeling the sensor integration

Sensory integration may be described in terms of a controller server interaction, in which the server is a sensor, and the controller is the system that utilizes the measurements in a performance-oriented design. To obtain a model of setup failure, we need to analyze how the system may utilize the measurements in a utility-oriented design, in which the system should detect and alert about unexpected activity.

Operational risks

According to the failure model described above, the operational risks may be classified as either expected or unexpected. In the context of sensor integration, the trigger is an assembly error, and the situation component is exceptional measurement. The risks of setup sensor integration may be regarded as expected.

The MX981 and the Proton M mishaps may be attributed to an operator's slip or confusion, and the Aeroperú Flight 603 accident may be attributed to maintenance carelessness. .

Protection challenges

The failure mode of Proton M is very similar to that of MX981. The developers of Proton M could have learned from MX981, should learning was enforced by standards and regulation.

The protection is based on early detection of instances of extreme sensory data, and promptly alerting about them to the controller and/or the supervisor, to enable early recovery. The detection is by risk indicators based on performance variables.

The method of risk indicators addresses the problem of unexpected events. The system may validate any system variable and inform the operators about exceptional values. In particular, the system may examine the validity of any performance variable, as well as the elapsed time of any process and any state transition. This validation may be used to detect situations of unit malfunction, in which a process did not start on time, when it stopped too early, or when the transition between certain states was extremely fast or extremely slow.

Discussion

The problem of sensor failure is a special case of the problem of unexpected events. Besides sensory data, the system may validate any system variable, and inform the operators about exceptional values. In particular, the system may examine the validity of any performance variable, as well as the elapsed time of any process and any state transition. This validation may be used to detect situations of unit malfunction, in which a process did not start on time, when it stopped too early, or when the transition between certain states was extremely fast or extremely slow.

References

Harel, A. 2024 (A), Assembly verification: the MX981 case study,
DOI: 10.13140/RG.2.2.18592.19209

Harel, A. 2024 (B), Assembly verification: the Proton M case study,
DOI: 10.13140/RG.2.2.14397.88808

Harel, A. 2024 (C), Setting verification: the PL603 case study,
DOI: 10.13140/RG.2.2.16075.60966