Configuration verification: the Cheongung case study

Avi Harel, Ergolight

ergolight@gmail.com

Situational consistency

During the operation, various states in various components need to change to fit the functional needs. A situation that complies with the functional needs may be regarded as consistent with respect to the supported function.

Operational reliability relies on situational consistency. The operation might fail when the situation is not consistent with a function.

The Cheongung case study

Cheongung is a medium-range, anti-aircraft guided missile, intended to strike a hostile aircraft at an altitude of around 40 kilometers. In March 2019, one of these missiles was launched unintentionally during a routine maintenance check, after the mechanics failed to replace an operational cable with a test cable. The missile was unintentionally launched when the operational cable received a mock launch signal for a testing purpose.

https://www.koreaherald.com/view.php?ud=20190321000476

This case study demonstrates the need to verify the compliance of the information flowing in the system with the operative scenario, each time the scenario changes.

Root Cause Analysis (RCA)

The system consistency depends not only on the function, but also on the operational scenario. If different components assume different scenarios, then the situation might not be consistent (cf. Harel, 2021).

In this case, the system configuration is not the same for all scenarios. Notably, two cables are used there, one for functional operation, and the other for testing during maintenance check.

The accident is due to failure to maintain situation compliance following a change of the operational scenario from operational to maintenance. This kind of accident is typical of systems that do not maintain the primary scenario variable. In such cases, the scenarios are fuzzy, and consequently different system components might assume different scenarios. In such cases, the situation is not consistent.

Operational errors

Analysis of many accidents has shown that the term human error is just a name for operational failure that the human operator was not able to prevent (cf. Dekker, 2007). To eliminate human errors, we need to understand how the operation fails. The challenge is to get enough evidence to understand how errors are generated.

In the Cheongung example, a lapse of changing the cable is often regarded as an operator's error, but it should be regarded instead as a design mistake, namely, lack of warning about the lapse.

RCA conclusions

The system consistency depends not only on the function, but also on the operational scenario. If different interacting components assume different scenarios, then the situation might not be consistent.

The accident of this case study is due to failure to maintain situation compliance following a change of the operational scenario from operational to testing. This kind of accident is typical of systems that do not maintain the primary scenario variable. In such cases, the scenarios are fuzzy, and consequently different system components might assume different scenarios. In such cases, the situation is not consistent.

Enforcing situational consistency

To enforce situational consistency, the system should adapt to scenario changes. We may distinguish between two types of situational variables: controllable variables, such as state variables, and uncontrollable variables, typically continuous variables, obtained by measurements. In this case study the problem was with the physical cable connection, which we cannot enforce by software. However, we can enforce verification, by alerting the operators to violation of the situational rules.

Situational rules

To enable the situation adaptation, the scenario should be defined explicitly, and implemented as a primary system variable. Otherwise, different system components might assume different scenarios, and the corresponding situations might be different. The scenarios should be defined such that a scenario change involves:

- Enforcing consistent change of the adaptable variables
- Verification of the consistency of unadaptable variables.

In this case study, the scenario change was from functional to testing. The scenario implies several mode variables, one of them, the configured cable, is relevant to this event. The rules for scenario-mode compliance should be:

- During functional operation, the system components should be connected by an operational cable.
- During testing, the system components should be connected by a test cable.

The operation in the incident involved violation of the second rule, namely, the system was connected by an operational cable even after changing to a testing scenario. Apparently, the design of the Cheongung missile did not include such tests.

Enforcing the situational rules

To enable the situation verification, the system requirement should specify the operational scenarios, the system design should manage the scenarios, and the software program should verify that the implementation complies with the design. The focus of situation verification is on the mode compliance with the scenario according to the rules and on disabling the operation when they do not comply with the scenario. The design challenge is to specify the rules defining the scenario-mode compliance and the reaction to violating these rules.

Activity rules

Activity may be defined in terms of changes in the system situation. Accordingly, activity rules are about situational changes. The activity rule applicable to this case study is:

- On change to the testing scenario, the system should prompt the operators to disconnect the operational cable and to replace it with a testing cable.

Error proofing

To be on the safe side, we should protect the system from all risky situations, because we cannot tell when one of them might be disastrous. Practically, this implies that error proofing ought to be a key topic of systems engineering.

Enforcing situation awareness

To enforce the operator’s awareness of the rule violation we need to apply two mechanisms:

- Situational verification: ongoing notification, as long as the configuration does not comply with the rules
- Activity verification: an alarm on changing from normal to exceptional configuration.

Conclusion

The Cheongung accident demonstrates a need for early detection of configuration errors in cable connection, and also a method for detecting configuration errors. The method demonstrated here is based on rules for associating the configurations with the scenarios.

The vision proposed here is that system engineering standards may include a chapter on when and how to apply the method for rule-based configuration verification.

References

Dekker, S 2007. Just Culture: Balancing Justice with Accountability.

Harel, A 2021. Scenario-based modelling DOI: 10.13140/RG.2.2.12834.35523