ZRÍNYI MIKLÓS NATIONAL DEFENSE UNIVERSÍTY
Doctoral Council

NESZVEDA JÓZSEF

RELIABILITY OF APERIODIC OPERATED MILITARY EQUIPMENTS

Author's review of the doctoral (PhD) thesis and formal critiques

- 2011 -

Author's review

Canditate: Neszveda József
Associate Professor, MSc in. electrical engineer, process control engineer

Title of dissertation: Reliability of aperiodic operated military equipments

Supervisor: Dr. Forgon Miklós
Retired engineer Colonel

Doctoral School: Zrínyi Miklós National Defense University
Bolyai János Military engineer Faculty
Military engineer Doctoral School

The scientific problem

Over the past decades there were a growing number of military equipments which were characterized by containing programmable electronics or mechatronic. Within this there are an increasing number of safety-critical devices, which have defined mission time in continuously-run mode. In these cases there is no way or time to repair the operational error during their operation, and any operational mistakes can be fatal. In peace period national armies tend to reduce. The reduced army operates less military devices, which leads to a longer time period between usages (or first use) of a military device. Meanwhile, NATO involved more frequently in UN peacekeeping operations that require military force. These operations require the mobilization of the military equipments, but obviously the mobilization isn't designed several years in advance, so the equipments usage is aperiodic. I call all the military equipments, which can be characterized by the attributes I listed above, aperiodic operated military equipments.

The IEC 61508 and IEC 61511 standards define the safety integrity level (SIL) term and the methods for determining levels. The API 14C and the MIL-STD-882 standards interprets the safety-critical operation concept. The examination of reliability of aperiodic operated military equipments must be assembled from concepts of different standards in the following specifications:

- Number of definitions of the listed standards start from the assumption that the failure rate of equipments or systems is constant in the operational lifecycle. In the case of the aperiodic operated equipments, this assumption is not true.
- The aperiodic operated military equipment has safety-critical nature, but the API 14C and the MIL-STD-882 standards, which describes this nature, were developed for

continuous-run and batch operation. The aperiodic operated military equipment has other type of operation.

- In the case of the aperiodic operated equipments the predictable periodic inspection testing and maintenance carried out in off condition. The continuous-run and batch operation require other types of verification tests and maintenance.

This PhD thesis topic is about the method of the examination of the reliability of aperiodic operated military equipments, which is in line with international standards and takes into account the specificities of these devices.

Research objectives and hypotheses

My first hypothesis is that the reliability of aperiodic operated military equipments can not be investigated by the methods developed so far, and so it is a new group for the reliability calculation. My goal is to create and establish the calculation of the reliability of the aperiodic operated military equipments and defining the classification of MSIL similarly to the SIL of the continuous-run and batch operation by a theoretical elaboration of the calculation of the probability of failure.

According to my second hypothesis, treatment of change between off mode, periodic test mode, and continuous-run mode requires discrete time state description of the probability of failure. My goal is to model the change of modes by converting the profile of the transition probability matrix.

According to my third hypothesis, the influence of the probability of failure of discovered and corrected errors in periodic tests mode can be modeled by the appropriate correction procedures of probability of failure. My goal is to develop an algorithm for the reliability calculations, used in managing operational characteristics of aperiodic operated military equipments. According to my assumptions, the description of the model of operational characteristics of aperiodic operated military equipments needs special definitions of the test coverage factor and the human factor.

The following research methods used

I have studied the reliability and operational safety of the international standards and the methods of calculation of operational safety. I also examine the appropriate hardware architecture design.

Studying, analyzing the literature and publications available on the Internet I expanded my theoretical knowledge in the field. I have collected and systematized the SIL engineering activities related to domestic and foreign research activities and information.

The simulation tests have been run to verify the research results and the set of theses. I analyzed the effect of a certain parameter on the expected probability of failure during the battle task. I have studied the safety-critical hardware structures designed for cost-effective solution and I have developed a simulation model which is taking it into account.

Examinations

I. Chapter

The group of the aperiodic operated military equipment was defined. I define the test coverage and the human factor of the Safety Integrity Level for the characteristics of the aperiodic operated military equipment. Defining the interpretation of average failure probability of operation-blocking of aperiodic operated equipments and defining the formula (PFM_{Bavg}) for calculating it. Giving the interpretation of the military safety integrity level (MSIL) of aperiodic and safety-critical operated military equipment.

II. Chapter

This chapter contains: investigation of the different behaviour of the save and the dangerous failures in redundant hardware structures; analysis of the relationship between the diagnostics and the hardware redundancy; overview of the requirements of the control chain and the hardware structure of the aperiodic operated military equipment; justification for choice of 1002D hardware structure.

III. Chapter

Overview of the methodology for calculating reliability of the aperiodic operated military equipment. Deducing the transition-probability matrices of the operation modes and deducing the management of the mode changes. Interpret the effects of periodic inspection test in off mode as correction of probability in the Markov model’s states. Deduce the calculation algorithm of the average value of probability of failure in continuous-run mode.

IV. Section describes the proposed calculating method for the small-range air defense missile TZM equipment control system.

Conclusion

The aperiodic operated military equipments are a new group characterized by their operational characteristics. I have defined it the following way: the aperiodic operated military equipment has defined mission time and safety-critical design, contains programmable electronic and must be handled together all types of its failures.

I found that, the changes between off mode, periodic test mode, and continuous-run mode cause step changes of the actual probability of failures, and so step changes in the λ failure rate too, during the life cycle of these equipments. I've worked out the transition matrix conversion rule to treat it. This rule defined the factors of the operating conditions. I have proved that my transition matrix conversion rule is suitable to enforce the sudden change in λ failure rate.

I created the followings for my investigations: a Markov graph which contains seven state and relates to the control system's hardware structure designed 1002D; the criteria system for determining of the transition probabilities; and the expression which define the aggregated transition probabilities of the transition matrix related to Markov graph.

I pointed out that the definitions of PF_{Davg} and PFD_{avg} of IEC 61508, IEC 61511, and ANSI/ISA 84 standards aren't suitable to determine the reliability of aperiodic operated military equipments for the following reasons:

- in the control system of the aperiodic operated military equipment must be considered together: (PF_{Davg}) the average probability of dangerous failures of the basic control, (PFD_{avg}) average probability of failure on demand of safety control, and ($PF_{avg}^{spurious}$) average spurious probability of failure;
- the reliability of all operation must be jointly determined and not independently, like international standards makes it;
- the concept of test coverage of international standards isn't suitable to determine the effectiveness of investigation test, which break the off mode of the aperiodic operated equipments.

I introduced the term of PFM_{Bavg} – which is the average probability of all fatal failures in the mission's time of aperiodic operated military equipment - the following features:

- the PFM_{Bavg} include the probability of all save, dangerous, and false failures together, which may prevent the successful execution of battle task of these equipments;

- Mission time must be considered as the time period between the last investigation test and the mission time start and the continuously-run time together of the calculation of average probability;
- I have created and defined a test coverage factor which should be applied to calculate the effectiveness of investigation test, which break the off mode.

I gave a formula to calculate the PFM_{Bavg}.

I've interpreted the effects of periodic inspection test in off mode as a correction of probability in the developed Markov model's states, and deduced the algorithm of the correction in fault-vector.

I gave the term of the military safety integrity level (MSIL), which can be calculated by PFM_{Bavg} and can be used the classification of the reliability of aperiodic operated military equipments.

Case study demonstrated that the developed algorithms are suitable for optimization of the frequency of investigation tests, the test coverage levels, and the stuff qualifications.

Scientific results

1. I have defined the term of aperiodic operated military equipment and the term of military safety integrity level (MSIL), and I gave its classification method.
2. For calculating the average probability of failures of aperiodic operated military equipments in the mission period I have introduced the concept of PFM_{Bavg} and I have created and defined test coverage factor and human error factor, which are related to this calculation.
3. For the management of the mode changes of aperiodic operated equipments I have elaborated the conversion rule of probability transition matrix.
4. I have elaborated the correction method for handling the effects of periodic inspection test in off mode and for this and I gave the correction rule of probability transition matrix.