https://doi.org/10.26552/com.C.2004.3.55-60

Tatiana Olejníková *

RELIABILITY OF ELECTRICAL SECURITY SYSTEMS IN EXTERNAL PROTECTION OF THE MILITARY OBJECTS

In this paper electrical security systems used in military objects and areas of the Slovak Republic Armed Forces are described. There is described a method of reliability calculation of the safety system elements as a probability that the system will operate without a failure during the defined time in the given conditions.

1. Introduction

To increase the security of military objects in current practice modern technical safety equipment is being used such as:
- electrical safety signalling,
- electrical fire signalling,
- access systems,
- industrial television.

Security systems using modern technical safety equipment consist of a set of scanning, transmitting and decoding devices which signal a dangerous situation in case of an object or area disturbance or in case of fire etc. An application of this equipment creates active inhibitions and barriers, which result in signalling the object disturbance or an unusual situation. Technical security of military objects supports classic security in the means of insurance and information delivery about its disturbance and attack and it increases the efficiency of physical security. The ammunition and armoury storage places and some regime workstations of the Slovak Republic Armed Forces are only areas where technical electrical safety equipment utilizing optical and sound signalling with outing in an operational centre (e.g. supervisory station) is used. Electrical cam sensors and switches installed at the entrances and points of access as well as signalling centres which signalise the opening or closing of these storage places are used. Another material storage (automobile, joint, equipment and another material) which does not require a level of security as ammunition and equipment storage is equipped with elementary cam mechanisms and seals, i.e. with a form of the classic security. In the last years featuring increase in criminality and loss of material, the significance of military objects security and overall interest in total security of property and persons grow continuously. With an increasing interest in a risk-free service of military objects it is necessary to realize a necessity of the professional systematic solution for security of objects using quality services and techniques, which ensure an effective and reliable exploitation of the equipment mounting and undisturbed usage of guarded areas. In choosing the security and regime systems, three basic principles of object security have to be taken into consideration:

1. The absolute security does not exist. Every security system can be overcome. It is only a question of time and appliances available to a disturber.
2. The only arrangement does not solve the safety of an object. There must be a complex solution.
3. The technical appliances are able to support but not to substitute a human.

2. Electrical safety systems

The technical security of objects is created by a set of scanning, transmitting and decoding devices which signalise the dangerous situation from the aspect of an attack, formation of fire etc. The application of these appliances creates a system of active barriers, which in case of overcoming attempts by a disturber result in alarm declaration or they signalise the disturbance of an object. The technical security supports the classic security and transforms efficiency of physical security. According to the space location the technical security can be classified as:
- external, where detectors decoding an attack of an object are situated outside a safety object and they detect the disturbance before the approach to the object,
- jacketed, where detectors decode the disturbance of a building jacket (entrance door, windows, skylights, ventilation and air-condition),
- space, where detectors decode the presence of entities in the safety space inside the building,
- anvil, where detectors decode the manipulation with safety entities.

3. Electrical safety used in the external military objects security

The external safety of objects is a significant component in monitoring large complexes of military buildings and areas, such as airports, industrial objects, military bases, etc. The mission of external safety is to detect the disturber with technical equipment

* **Tatiana Olejníková**
Technical University of Kosice, Faculty of Civil Engineering, Department of Descriptive Geometry, Vysokoškolská 4, 042 00 Košice,
E-mail: tolejnikova@post.sk

as soon as possible until he still does not make an actionable work in the safety area. By detecting a disturber on the periphery of the monitored object the intervener unit will have sufficient time to approach and execute an intervention in the place of disturbance. It mostly deals with an external guard, which is based on the following components:

- *Warning*
  The existence of a fence is the condition for application of an external safety system, because the disturbance can be defined only in this case. Without barrier or fence mechanical restrictions the disturber would enter the detected system or safety area. The action and right of recovery against a disturber would be problematic and at the same time then ineligible alarms would be raised. The fence construction, warning signals and boards should discourage a potential disturber.

- *Detection*
  The electrical detecting barrier detects impacts in the different physical values, which originate in the process of detecting the barrier disturbance attempts. The different systems are dissimilar in technology of detection by which the specific type of physical effect such as compression, vibrations, motion, thermal, etc are assured and analysed. Cameras are used to verify the presence of a disturber.

- *Detection - check*
  The check fence decelerates an action of a disturber before entering the safety area and it provides the intervention unit with necessary time between detection and access to the disturbed place for execution of the encroachment. The combination of all components and physical encroachments inhibits the disturber in achieving his goal.

- *Light*
  It affords an exterior illumination of an object. It must be intensive enough for searching of a disturber, but it is oriented outwards to assure that a driveway for a guard, or encroachment unit would be in relative darkness. Where cameras are used, a different type and density of exterior illumination is required.

- *Way for a watch walk*
  It affords a suitable and safety drive for walk execution and for an encroachment unit to access the disturbed place of an object periphery in the shortest time and in adequate weather conditions.

- *Communication system*
  It creates a line or radio connection between a detect security system installed on the object periphery and a main control place.

- *The main control system*
  It enables the control and monitoring of different emergency systems installed in a protected area. It ensures the command of watch service members and encroach units in "normal" or "warning" conditions via communication channels.

4. The reliability of an electrical safety system used in external security of military objects

Quantitavely the reliability can be defined as the probability that the system would carry out its function without a failure during the defined time in the given conditions. Reliability is a criterion of the effective operation probability of a system at the certain time. Estimation of reliability is initially administrated for components which will be used during the system lifetime phase. Reliability of components is directed by the reliable "bath curve".

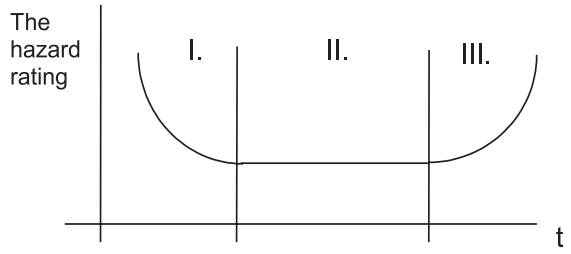

Fig. 1 Reliable bath curve

In the 1st phase the hazard rating is reduced by elimination of weak components.

In the 2nd phase (operation phase) the hazard rating is constant.

In the 3rd phase the components will be worn out and the hazard rating will increase

For a constant value of risk relation may express reliability of a system

$$R(t) = \lambda e^{-\lambda t}$$

- $R(t)$ is the reliability of a successful device operate of the time t
- λ is the grade of failures (constant)

If fault liability of a system can be tolerated and repair can be accomplished, then, the system functionality criterion is the system *availability* expressed by the relation

$$A = \frac{MTBF}{(MTBF + MTTR)},$$

where *MTBF* is the mean time between failures, which is an inverted value of accident intensity: $MTBF = 1/\lambda$, *MTTR* is the mean time of repair – it is the mean time between a system error and its operation.

Availability c*an be defined as an element of the total time in which* in which a system performs the desired function. Availability is marked as A and its complement unavailability as Q and after

$$A + Q = 1.$$

The system failure can be detected if there is a deposit requirement on its performance. Probability that the system will be in

failure status in the instant of time, can be represented by unavailability or proportionate dead time (*PDT*)

$$PDT = \lambda\left(\frac{\Phi}{2} + \tau\right)$$

- *PDT* – proportionate dead time
- Φ – an interval of a test
- τ – mean time for repair.

τ is much shorter than the test interval Φ and therefore *PDT* is often approximated by the relation

$$PDT = \frac{\lambda \cdot \Phi}{2}.$$

Probability of a system safety failure before the risk is the following

$$P_f = PDT \cdot D$$

- it is a product of the proportionate dead time *PDT* and required probability *D*.

Majority of methods for the reliability research is established on these relations.

4.1 Quantitative estimation of reliability and risk

Methods of reliability and risk detecting are included in the studies of different configurations of failure identification, which resulted in decreased system functions.

The study of a system malfunction includes a quantification of failures. The risk of failures can be reduced by money investments, but it is not possible to play for safety absolutely. In the function appraisal of a system it is necessary to define when the system is "functional enough".

The risk or "expected loss of a system malfunction" can be quantitatively defined as a product of the consequence rate of specific accidents and probability of these occurrences:

$$Risk = Effects \cdot Probability$$

The risk can be decreased by reduction of accident consequences or by reduction of probability of their occurrences. The methods for reduction of consecutive losses utilizing more elementary systems are included in different areas. If the risk is identified and evaluated, we can decide if it is acceptable or whether we should make an arrangements for the system upgrade of reliability. We must make decisions concerning realistic goals.

Quantitative evaluation of risk has four phases:
1. eventual menace identification of a system function
2. estimation consequences of each malfunction
3. estimation of probability of each malfunction occurrences
4. comparison of analysis effects with acceptable criteria.

Eventual menace identification of the system function may be defined using failure statistics from the production or from records about genesis of undesired incidents. Preliminary analysis of failure risk with an arrangement of critical effects in different inadequate conditions can be effectively used for identification of subsystems that can considerably endanger the global function of a system.

4.2 Reliability in the risk evaluation

The electrical security system manufacturers must consistently consider the reliability of a system during different phases of planning, so they can evaluate and be optimal for a failure-free operation of a system. It is often expensive to repair the defect in the later phase, especially directly in the object, where the electrical security system has been installed. The report that is based on the study of spectrum failure effects is the valuable project revise. In the project development, it is more appropriate to study the failure causes in more details and more systematically. The engineers still more and more assist the designers to crack the partial problems that relate to system reliability.

4.3 Quantification of element/system failure probability

Even very well designed systems once definitely fail. The basic task is to guarantee that even the system fails the frequency of its failures or probability to abide in the failure status in time will be acceptable. The acceptability can be evaluated by using either economic, activity, or safety criteria depending on a system type. The best adequate probability formulas for the description of element or system accomplishment are availability and reliability.

We consider a reparable element, which begins its life cycle in the operation status. It continues in this status for the specified time until it aborts and then its status changes from the operation status to the failure status. It stays in the failure status until repair is over and the element functions again. This alternation of failures and repair will continue throughout the element lifetime. Availability is an adequate power rate for these reparable elements. Availability can be considered in the following three meanings:

1. *Availability – probability that the system is functional when required.* This definition is adequate for electrical security systems, which operate when requested. Security systems monitor an occurrence of unacceptable accidents and they prohibit the expansion of a risky situation. If the security system is in the failure status in time when it should operate, it is unavailable. As the request for activity can come in a moment, the longer the system is in the function status, the bigger the chance is that it will operate in the given moment, i.e. its availability is bigger. The back up systems also must function on request. Requests for their operation will rise from the failure of a primary system. The character of these alternative systems is inactive in general, i.e. they do not need to carry out an action in normal condi-

tions. The elements, which fail as inactive, fail, unrecognised. The time of their repair depends on the following factors:
- the time it took to detect that a system failed
- availability of a maintenance team
- character of a failure (reparable or irreparable, in the second case the time of exchange depends on the existence of storage or it needs to be ordered from the contractor)
- the time for a system check before its activation

By decreasing the time of a factor activity the dead time is abbreviated and system availability increases.

2. *Availability in the time t - probability that the system functions in the special time t* is a definition of the availability adequate for constantly operated systems of which a failure is immediately detectable and a repair process can start immediately after the failure.

3. *Availability - fraction of the total time when the system functions.* This definition is important for calculation of the productivity of manufacturing process. In this aspect we can use the fraction of the total time when a system functions, to estimate the aggregate output and also the expected advantages in the given time. Probability that system is non-functional in the time t is unavailability where

$$Unavailability = 1 - Availability.$$

In some systems the failure cannot be tolerated. Especially when the failure represents a catastrophic case which damages the device. In this case the zero presence of failure will be a fundamental indicator of accomplishment during the whole-expected system lifetime. We must consider the system *reliability*. Probability that system fails in the specific conditions is known as its *faithlessness* where

$$Faithlessness = 1 - Reliability.$$

In the situation where the system is irrecoverable, then, if the system functions in the time t, it must have acted also during the period (t_0, t), where t_0 is the beginning of the operation status. For irrecoverable systems the unavailability equals faithlessness.

In the simplest models for derivation of probability that system fails, it is assumed that the system can exist only in two forms of status: in the operation status and in the failure status. It is assumed that a system begins its life in the operation status. After definite time the system fails and it changes its status into the failure status. If the system is unrecoverable this status is definite. The reparable element of the system stays in the failure status until the repair is finished and the element is again in the operation status. Two assumptions were defined for this model:
1. only one alternation can arise in the short moment dt
2. alternation between two discrete forms of status is too short.

The alternation from the operation status to the non-functional status is called the *failure*. The regress process is the *repair*. It is also assumed that after the repair the element functions as well as it was new. The life cycle of an element consists of alternation series between these two stages.

4.4 The process of a failure

The time of the failure cannot be predicted accurately for an element. The elements of the same type will fail in different time. The time until the element fails can be applied for probability separation, which states the probability that the element will fail before the defined time t. Different elements will have different separation time until they fail. The separations can be estimated by the element testing in the control conditions or by collecting and analysing data about elements in the operation.

The faithlessness of the element $F(t)$ in the failure status represents the probability that the element will fail some time before the time t

$$F(t) = P[\textit{The element will fail in the time interval } (0,t)].$$

The function of probability density $f(t)$ is

$$f(t) = \frac{dF(t)}{dt}$$

that $f(t)dt = P[\textit{The element will fail in the time interval } (t, t + dt)]$,

$$F(t) = \int_0^t f(t)dt.$$

The change into the failure status can be characterised by the conditional failure rate $h(t)$. Sometimes it is described as a risk rate (risk function). It is a criterion of the failure origination rate with regard to the number of elements with the potential to fail, i.e. elements which operate in the time t has the form:

$$h(t)dt = P[\textit{The element will fail in the time interval } (t, t + dt) \,|\, \textit{does not fail in the time interval } (0,t)],$$

that $h(t)dt$ is conditional probability.

From the conditional probability formula

$$P[A \,|\, B] = \frac{P[A \cap B]}{P[B]}$$

where cases A,B can be characterized as follows:

A – the element will fail between t and $t + dt$

B – the element does not fail in the time interval $(0,t)$, follow

$$h(t)dt = \frac{P[A]}{P[B]} = \frac{f(t)dt}{1 - F(t)},$$

because $P[A \cap B] = P[A]$, if an element fails in the time $(t, t + dt)$, it means that it could not fail before the time t. It means that

$$\int_0^t h(t')dt' = \int_0^t \frac{f(t')}{1 - F(t')} = \ln |\, 1 - F(t) \,|,$$

therefore

$$F(t) = 1 - \exp\left(-\int_0^t h(t')dt'\right),$$

where $h(t)$ is the rate of the failure.

If we draw this function depending on time, we will get the graph in the shape of the known "bath curve". This curve is characterised by a declining failure rate in the 1st phase, in the middle it is nearly constant and by a rising failure rate in the 3rd phase. There are these arguments for it:

1st phase is the phase of the element launch where some manufacturing errors can occur
2nd phase is the phase where the failure is accidental
3rd phase is the phase of abrasion where the failure rate rises.

If we consider only the 2nd phase of the element service, the failure rate can be considered as constant.

$$h(t) = \lambda,$$

then

$$F(t) = 1 - e^{-\lambda t}.$$

Then the reliability $R(t) = \lambda e^{-\lambda t}$ is the probability that the element operates continuously in the time $(0, t)$ and it is given by the exponential function. As the failure rate is constant, this function is named "random failure distribution". The function of probability for $F(t)$ is $f(t) = \lambda e^{-\lambda t}$. The mean value of the distribution presents a mean time of a failure:

$$\mu = \int_0^\infty t\, f(t)dt = \int_0^\infty t\, \lambda\, e^{-\lambda t}\, dt = \frac{1}{\lambda}.$$

If we have the constant failure rate then the mean time to a failure is the reciprocal value.

4.5 The process of repair

The parameters, which represent the process of repair, can be given by the following procedures:

Let $G(t) = P[$*The given failure element will be repaired in the time interval* $(0, t)]$ if $g(t)$ is a function of the density, then for the intensity of the conditional repair $m(t)$ is:

$$m(t) = \frac{g(t)}{1 - G(t)}.$$

From this, after the integration, we will get

$$G(t) = 1 - \exp\left(-\int_0^t m(t')dt'\right).$$

If we assume that the repair rate is constant

$$m(t) = v,$$

then

$$G(t) = 1 - e^{-vt}.$$

If the repair rate is constant then the mean time to the repair τ is a reciprocal value of the repair rate:

$$\tau = \frac{1}{v}.$$

If we want to determine the unavailability of the element, we must simulate the all life cycle of the element and we must consider the process of a failure and the process of repair concurrently.

5. Conclusion

The next parameters affect capacity of the element:

The availability $A(t)$ – the probability that a system is in operation in the time t
The unavailability $Q(t)$ – the probability that a system failures in the time t
The intensity of an unconditional failure $w(t)$ – the probability that the element fails in the unit time in the time t, and it operated in $t = 0$. It is the probability that the element fails in $(t, t + dt)$, and it operates in $t = 0$.
The expected number of the failures $W(t_0, t_1)$

$W(t , t + dt) =$ *the expected number of the failures in the time interval* $(t, t+dt) = \sum_{i=1}^{\infty} P[i$ *failures during the* $(t, t + dt)]$.

As during the short time interval dt there is one failure

$W(t, t + dt) = P[$*one failure during the* $(t, t + dt)] = w(t)\, dt.$

Then

$$W(t_0, t_1) = \int_{t_0}^{t_1} w(t')dt'.$$

If the element is not repairable then

$$W(0, t) = F(t).$$

The intensity of the unconditional repair $v(t)$ – the probability that the failed element will be repaired in the unit time in the time t, if it operated in $t = 0$.

The expected number of the repairs $V(t_0, t_1)$ – the expected number of the repairs of a failure element in the time (t_0, t_1)

$$V(t, t + dt) = v(t)dt.$$

After the integration

$$\mathrm{V}(t_0, t_1) = \int_{t_0}^{t_1} v(t)dt.$$

The intensity of the conditional failure $\lambda(t)$ – the probability that the element fails in the unit time in the time t, and it operated in the time $t = 0$. The difference between conditional and unconditional intensity of the failure w is that λ is the failure rate which is established on the elements which operate in the time t and $t = 0$.

$\lambda(t)dt$ is the probability that the element fails during the $(t, t + dt)$ and it operated in the time t and $t = 0$.

$w(t)dt$ is the probability that the element fails during the $(t, t + dt)$ and it operates continuously from $t = 0$ to t. The relation between the intensity of the conditional failure $\lambda(t)$ and the intensity of the unconditional failure $w(t)$ can be derived by the conditional probabilities:

$$\lambda(t)dt = P[\textit{the element fails in the time interval } (t, t + dt),$$

$$\textit{and it operated in time } t = 0] =$$

$$= \frac{P[\textit{the element fails in time interval } (t + dt)]}{P[\textit{the element operated in time } t]} =$$

$$= \frac{w(t)dt}{A(t)} = \frac{w(t)dt}{1 - Q(t)}$$

then

$$w(t) = \lambda(t)[1 - Q(t)].$$

The intensity of the conditional repair $\mu(t)$ – the probability that the element will be repaired in the unit time and in the time t it did not operate and in the time $t = 0$ it operated.

References

[1] KOSTKA, V.: *Information Safety in the Security System* (in Czech), The lecture on the Exposition PRAGOALARM 1996.
[2] FALISOVÁ, B.: *Equipment of Technical Security of Objects* (in Slovak), Academy PZ SR, Bratislava, 1997.
[3] MESÁROŠ, M., LOŠONCZI, P.: *Active Security of Protected Objects as a Component of Security Management* (in Slovak), Acta Avionica, Scientific Magazine of VLA in Košice, vol. IV, num. 5, ISSN 1335-9479, pp. 38–41.
[4] OLEJNÍKOVÁ, T.: *The Disturb Warning Devices of the safety Actives* (in Slovak), Acta Avionica, Scientific Magazine of VLA MRŠ in Košice, 2003, vol. V, num. 7, ISSN 1335-9479, pp. 49–53.
[5] OLEJNÍKOVÁ, T.: *The Integrated System of the Object Security* (in Slovak), Crisis Management, Scientific-Technical Magazine of Faculty of Special Engineering at University of Žilina in Žilina, 2003, vol. 2 , num. 2, ISSN 1336-0019, pp. 43-47.
[6] KOLESÁR, J.: *Simulation of the system Optimization of Safety and Security of a Military Airport* (in Slovak), Dissertation, Košice 2002.
[7] SIVÁK, J.: *The Pilot Project of Integrated Security Systems in the Implementation of the Slovak Republic Armed Forces* (in Slovak), KelcomInfo, Technical Magazine of the Association KELCOM International Liptovský Mikuláš s.r.o., vol. IV, num. 1, Liptovský Mikuláš 2002, pp. 4–7.
[8] PIVKO, D.: *The Equipment of the Jacketed Security* (in Slovak), KelcomInfo, Technical Magazine of the Association KELKOM International Liptovský Mikuláš s.r.o., vol. IV, num. 1, Liptovský Mikuláš 2002, pp. 13–18.