System robustness against misuse

Z. Vintr & D. Valis
Faculty of Military Technology, University of Defence, Czech Republic

Abstract

The operation of a number of technical systems is related to the danger of events' occurrence posing threat to human health and life, resulting in material damage or damage to the environment. Methods and procedures used for risk management also take into consideration the failure of a human factor as a possible cause of dangerous events' occurrence, but they do not give us the opportunity to take into account the possible intention of man, who can cause a dangerous event on purpose. In view of the terrorist threat we lack a coherent methodology that would enable us to influence a system's ability so that consequences of a dangerous event could be reduced or the system could be protected against misuse by its design solution. This ability of a system is called security robustness. This article presents fundamental approaches of a new methodology that enables us to specify systems' security robustness, to describe and classify "weak" points of the systems, to analyze and assess security robustness level, and to find and suggest effective ways of increasing the systems' security robustness. The presented methodology is based on the assumption that similarly, as in case of dependability and safety, the assurance of system security robustness should also be an object of systematic attention in all phases of the system life cycle, and that the system security robustness is formed in a crucial manner mainly in the early phases of a life cycle (the so called pre-manufacturing stages – conception, development, design).

Keywords: system robustness against misuse, security robustness, system safety, methodology of security robustness assessment.

1 Introduction

In technical practice there are quite a few different technical systems, the operation of which is related to the threat of an event occurrence that can affect massively health and human life, and can result in huge material damage or

WIT Transactions on the Built Environment, Vol 108, © 2009 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE090261

extensive devastation of the environment. The typical examples of such systems are means of transport (aircraft, rail vehicles, couches, etc.), technological systems in the chemical industry, nuclear installations, weapon systems, etc. The systems of a critical infrastructure of the state, such as power distribution networks, telecommunication networks and so on, are other important representatives. In this proposal such systems will be called critical systems.

Risks related to dangerous events' occurrence are, concerning these systems, systematically controlled using sophisticated approaches and methods. Generally it is required to implement so called safety programme for each system where events with dangerous consequences might occur [1]. The programme determines activities, sources and sequences of activities, which are supposed to be carried out in single phases of a life cycle in order to achieve the required level of the system safety. General procedures and methods used for safety assurance are also standardised very extensively [2].

In particular areas of human activities the principles and procedures for assuring the safety are very well developed, and they are often standardised at the international level (e.g., air transport, rail transport, military equipment, etc.) for a specific area. Dealing with selected types of systems even the safety requirements are determined by international or national standards (e.g., rail transport, nuclear power engineering, chemical industry, etc.).

2 Methods for safety and risk assessment

Generally it can be noted that methods and procedures used for safety assurance of technical systems are carefully worked-out and enable us both to specify safety requirements of systems in a rational way and to verify with analytical methods if the conditions under which the requirements are to be fulfilled, have been followed as early as in the early stages of a life cycle of the system.

The most frequently used methods and procedures are standardised, and the application of them in practice is easier owing to commercial software products of a number of producers. The most frequently used methods how to assess systems' dependability and safety are as follows [2]:

- Preliminary Hazard Analysis - PHA,
- Failure Mode and Effect Analysis – FMEA,
- Failure Mode, Effect and Criticality Analysis - FMECA,
- Fault Tree Analysis – FTA,
- Event Tree Analysis - ETA,
- Reliability Block Diagram - RBD,
- Hazard and Operability Studies – HAZOP studies,
- Operating and Support Hazard Analysis - O&SHA,

and many more.

The outstanding feature of all these methods is the idea that if they deal with a human factor as potential cause of dangerous situations' occurrence, they consider only a human failure as a possible cause of the situation. However, the essential of the introduced methods as well as the principles how to apply them

do not enable us to consider that man could have an intention to cause dangerous event on purpose.

The area of information technologies can be regarded as a sort of exception where, on the basis of practical experience (e.g., the first computer virus which spread extensively was made as early as in 1986), the protection of computers, computer networks and information against intentional interference of man has been an object of long term systematic attention [3, 4]. In the area of computer safety we are introduced to a number of sophisticated methods and procedures commonly used in practice and standardised at the international level (e.g., a wide set of standards ISO/IEC used in this field).

Safety applications used for security of property and people are another area which systematically focuses on systems' robustness against the potential interference, and where crime in general has triggered the development of safety applications [5–7]. The assurance of high robustness of the systems is an object of main attention, and it is supposed to prevent from unauthorized entering the protected area. The methods and procedures used in this field are again widely standardised.

However, the methods and procedures used in the area of computer security and applications, which serve for securing the property and people, can be, owing to their special characteristics, used for different technical systems only in a very limited manner. Usually we work only with the term "vulnerability" which specifies weaknesses of the system enabling the attacker to violate integrity of the system and having unauthorized access to information, source codes, finances, property, etc. A matter of priority is not to initiate an event with serious consequences but to get unlawful benefit. Of course there are cases, e.g., using harmful codes (computer viruses), where integrity violation of the computer system resulted in extensive damage.

However, providing the computer technology is a part of technical system (at present it is a common situation), the methods and procedures used in the area of computer safety can be applicable very well to this part of the system.

3 Security robustness as a new system attribute

Generally it can be noted that at present there is no coherent set of methods and procedures which would enable the security requirements of critical systems to be specified in a rational manner, and which would set the conditions for systematic analytical assessment of an achieved level of security with respect to possibility of intentional interference of man in the system in order to initiate an event with serious consequences.

Nowadays a terrorist threat is a global problem and these particular critical systems are supposed to be a logical target of a series of terrorist attacks. As you would expect, besides the attacks made by brute force (using explosives) we will face more sophisticated attacks which would take advantage of the construction knowledge as well as of the information about working of the single systems. A typical example is the hijack and then the misuse of an airliner for the attacks on public buildings in the USA on September 11th (about 3000 casualties).

That is the reason why it would be convenient to deal systematically with the possibility of intentional interference of man in the system in order to affect the system functions the way in which the conditions for event occurrence with serious consequences would be made (hereafter referred to as an intentional interference).

The possibility of intentional interference in each critical system should be considered in the early stages of a system life cycle (conception, development, design), and the system should be designed the way in which the chance of intentional interfering would be adequately limited (regarding seriousness of the consequences of such an interference), or the negative consequences of the interference could be minimized.

In this proposal the systems due to their construction project will be able to prevent the possibility of intentional interference in the system, or to reduce the consequences of this interference termed system robustness against misuse (hereafter referred to as system security robustness).

Broadly speaking, the system security robustness defined this way cannot be regarded as the bare opposite of the vulnerability mentioned above because, by its conception, it shows much more complex attribute of the system than it is in case of the vulnerability.

4 Methodology of system security robustness assessment

The suggested idea is based on the assumption that similarly, as in case of dependability and safety, the assurance of system security robustness should be also an object of systematic attention in all phases of the system life cycle, and that the system security robustness is formed in a crucial manner mainly in the early phases of a life cycle (so called pre-manufacturing stages – conception, development, design).

The essence of the idea then lies in the development of methodology of security robustness systems' assessment, which means searching for methods and procedures that enable the system security robustness to be systematically influenced in the early phases of a life cycle. The suggested methodology creates theoretical fundamentals for engineering of technical systems' robustness against misuse. Primarily it is a matter of research and suggestion of methods and procedures which enable systems' security robustness requirements to be specified, and which allow us to detect, describe and classify weak points of the system, analyse and asses the level of robustness, and find and suggest effective ways of increasing the systems' robustness.

The aim of the methodology is to create and open to the public the assessment methodology of systems' security robustness formed as a set of methods and procedures which logically continue commonly fulfilled activities when assuring dependability and safety of the systems, and which provide important assumptions for achieving required system robustness. The suggested set of methods and procedures will enable us in particular to:

- describe the system security robustness (robustness measures) in a qualitative and quantitative manner,

- perform predictive analyses of the systems' security robustness (to understand possible impact of a human factor on a technical system, to detect weak points of the system and the possibilities of improving robustness, etc.),
- assess the level of the system security robustness (to compare the achieved level of security robustness with the required level).

A detailed analysis of general factors which affect the practical human ability to interfere in the system is a starting point for the methodology performance. Continuing the results of this analysis, categories of intentional interference are specified and then optimized regarding the simplicity of its realization and seriousness of the consequences

These categories are a starting point for introducing a general model used for describing the system robustness in a quantitative and qualitative manner. Introducing the measures describing the system robustness is the final step of this part of the methodology.

The next step of the methodology is to examine the possibilities of analytical assessment, both inductive and deductive, of system robustness. The aim of the inductive analytical methods is to examine the way of intentional interference in the function of system single elements, and the methodology is focused on the identification of the final impact it will have on a whole system. Concerning the deductive methods we examine the procedures that enable us to search out possible events' causes with serious consequences. The causes are identified at a system level as a whole.

Practical applicability of the suggested methods and procedures is believed to be verified by a practical analysis of security robustness of a selected real critical system, and by assessment of its robustness level.

5 Proposed methodology benefits

Despite extensive activities of the international community, we still fail to eliminate the terrorist threat. It is typical that terrorist groups do not limit their activities to selected countries but the terrorist attacks or attempts might be experienced by us almost everywhere.

It is also typical that in view of large-scale countermeasures struggling for reduction of the threat, attackers use more and more sophisticated methods to overcome the precautions. In this situation the critical systems themselves, that is, the systems the operation of which is related to the risk of an event occurrence with serious consequences, are logically becoming an object of great interest of terrorist groups. In many cases terrorists can reach the goal, e.g., numerous casualties, huge material damage or large-scale devastation of the environment, in a relatively easy manner misusing the critical system, damaging it or changing its function.

We cannot eliminate in advance the possibility that a particular critical system is not going to be misused in the way described above. Therefore, while designing and developing the critical systems, it is highly advisable to take into account the possibilities of misuse, and to carry out the construction solution the

way in which the likelihood of the intentional interference in the system would be reduced to an acceptable level, or the consequences of such interference could be minimized. The methodology then is focused on the design solution of critical systems, considering the assurance of the systems against misuse, but it is not intended to develop the procedures and instructions which are aimed at the detection and elimination of the people who pose a threat.

Because at present there are no adequate theories and methods as well as procedures which could be used in practice, this procedure is hard to apply systematically and purposefully when designing and developing the critical systems.

6 Description of suggested methods and procedures

The first part of the methodology deals especially with a critical analysis of the latest knowledge in the particular area, and handles complex assessment of the methods and procedures used in the field of computer safety and security applications for securing people and property where the possibility of intentional interference is considered as early as in the phase of designing and developing. An object of particular attention is the information which can be widely applied to all technical systems.

This is followed by a synthesis of the analyst' knowledge and experience they have in the area of dependability assurance, focusing on identifying the most effective ways of achieving the methodology goals

In the next step we identify and analyze in detail general factors which describe simplicity (difficulty) of performing the intentional interference. These factors define the attributes of the assessed system but at the same time they determine requirements for a person who would intend to interfere intentionally in the system (knowledge, skills, necessity of overcoming obstacles, etc.). Using the factors identified this way the categories of intentional interference is suggested and then optimised concerning both the "simplicity" of its performance and the seriousness of its potential consequences.

The suggested categories are a starting point for introducing a general model used for describing system security robustness in a quantitative and qualitative manner, and which will enable the system security robustness to be assessed in a basic way. The model is based on the following assumption: the more serious consequences the intentional interference has, the more difficult it is to be performed.

The possibilities of a quantitative description of systems' robustness is analysed in the next phase. In view of the fact that probability estimation of a particular intentional interference is in effect impossible (no valid and verified data is available), the probability is not included in the assessment and a quantitative system security robustness assessment is based only on the categories showing intentional interference as well as other system properties. A particular way of a quantitative robustness assessment is chosen on account of the results of the previous analyses (regarding the single areas of interest it can be completed with quantification in accordance with the practices common in the

particular area). Generally speaking we use the principles applied when assuming the failures' criticality (used, e.g. within the FMECA, PHA, O&SHA application and the others), or a fuzzy sets theory. In view of the selected way to assess the robustness in a quantitative manner the basic measures describing the level of system robustness is also suggested.

The possibilities of analytical assessment of system security robustness that can be applied mostly in the pre-manufacturing stages of a system life-cycle are examined in the next phase of the life cycle. The methodology is heading for the suggestion of two types of analytical procedures, the inductive and deductive.

The inductive analytical methods are based on the systematic observation of individual elements of the system (components and subsystems). The methods are suggested the way that for each element they are enable us to detect possible ways of intentional attacks, and when using the suggested categories, we are able to assess the difficulty of the interference as well as the seriousness of the consequences. While summarizing the information achieved this way we are able to assess the system security robustness as a whole as well as to detect critical elements of the system. These methods are adequate especially while analysing conceptually new systems where the possibilities of intentional affection of the system are not known enough. However, the methods can be fully used for the systems already existing so that they could assess their robustness and suggest measures leading to improvement of the system properties.

The deductive analytical methods are based on the systematic observation of system functions in order to detect potential events in the system operation which might lead to serious consequences. The suggested methods enable us to detect whether the intentional interference might cause the events and what the interference is like. These methods are adequate especially while analysing security robustness of the systems built according to the verified design principles where potentially dangerous events occurring during the operation of the system are well known and described.

All the methods and procedures are suggested the way in which they can logically continue the methods already established and used while analysing and assessing dependability and safety of technical systems. They are supposed to have minimum requirements for extending analytical procedures commonly performed within design and development of systems, thereby setting conditions under which they can be implemented in practice easier.

Practical applicability of all suggested methods and procedures will be verified when applied to a particular technical system within integrated analysis of the system dependability, safety and security robustness. We assume to perform preliminary the system analysis in the area of rail applications.

7 Conclusions

Social importance of the suggested methodology is to answer to the current terrorist threat, to which is exposed all the international community. In the long-term perspective the methodology solution could contribute greatly to the

reduction of terrorist-related risks and increase security of critical systems in general.

The outcome of the methodology will be widely applicable in industrial companies, especially in the branches where the design and development of critical systems is performed. The application of suggested methods and procedures may also contribute to increasing the competitiveness of products on international markets which are still short of the products with deliberately assured resistance against misuse – security robustness.

Practical experience of research workers working in the area of products' security assurance shows that systematic activity in the phase of design and development can contribute in many cases to great improvement in systems' security robustness with minimum additional expenses, no additional requests for staff training and no increase of a number of existing employees.

Acknowledgements

Preparation of this paper was supported by the Grant Agency of the Czech Republic (project number 101/08/P020) and the Ministry of Defence of the Czech Republic (Institutional Research Plan No. MO0FVT0000401).

References

[1] Vincoli, J.W., *Basic Guide to System Safety,* John Wiley & Sons: Hoboken, 2006.
[2] Ericson, C.A., *Hazard analysis techniques for system safety,* John Wiley & Sons: Hoboken, 2005.
[3] Bishop, M., *Computer Security: Art and Science,* Addison-Wesley: Boston, 2002.
[4] Dowd, M., McDonald, J. & Schuh, J., *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities,* Addison-Wesley: Boston, 2006.
[5] Jaquith, A., *Security Metrics: Replacing Fear, Uncertainty, and Doubt,* Addison-Wesley: Boston 2007.
[6] Norman, T., *Integrated Security System Design: Concepts, Specifications, and Implementation*, Elsevier: Oxford, 2007.
[7] Douglas, J.L., *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, Taylor & Francis: New York, 2006.