REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK
34. évfolyam (2022) 1. szám 43–59. • DOI: 10.32560/rk.2022.1.3

László Domán

Overview of Reliability-Based Risk Assessment Methods and their Possible Application to Electronic Warfare Self-Protection Systems for Military Helicopters

There are many uncertainties surrounding electronic warfare self-protection (EWSP) systems for military helicopters, from the design process to the operational management of the equipment. Besides the traditional qualitative analyses, more sophisticated and novel techniques, like the fuzzy theory-based method are coming to the fore. This article aims to show a few possible methods for risk assessment of electronic warfare self-protection systems for military helicopters.

Keywords: *military helicopters, electronic warfare, fuzzy, risk assessment, reliability*

1. Introduction

Safety critical systems are extensively used in military forces. Systems that fall into this category range from software in Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) system to electronic warfare self-protection (EWSP) equipment for helicopters. These systems have a high level of safety and reliability. While safety is defined in MIL-STD-882E, Department of Defense Standard Practice: System Safety [26] as "freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment", reliability is defined in the United States Department of Defense (DoD) [4] as "the probability of an item to perform a required function under stated conditions for a specified period of time", which is often a precondition for safety. Both properties are crucial, and as systems become more complex, their prediction via analysis plays a vital role in the successful design and development of the system; at the same time, with increasing complexity analyses become increasingly difficult [20].

The failure probability of a relatively new component with insufficient historical failure data could, in theory, be estimated based on expert judgement or experience of similar components, if available. However, usually few experts can give useful opinions on the reliability of these systems. In the event of a failure, the survival of the helicopter in both normal and hostile environments is greatly reduced [20].

It can be concluded that different analysis methods are used to evaluate system safety and reliability.

The aim of this paper is to review reliability-based methods for risk assessment and their possible application to electronic warfare self-protection systems for military helicopters.

2. Military helicopter electronic warfare self-protection system

According to research, threat types and probability of occurrence depends on the military helicopter's location relative to the combat area. Table 1 shows an estimation of how various threats relate to different mission stages. The main uncertainty about estimation is the nature of the conflict; armed conflicts of today happen in a fragmented battlefield where there is no clear line of demarcation between friends and enemies [14, p. 51–52].

Table 1
Threat assessment for battlefield helicopters [7], [14]

Weapon	Take-off and landing	Transit	Forward edge of battle area	Beyond forward edge of battle area
Infrared (IR) Man-portable air defence system (MANPAD)	Very Low	Medium	High	High
Laser beam rider MANPAD	Very Low	Medium	High	High
Low-level air defence system	None	Medium	Very high	Medium
Direct fire	None	None	Very Low	Very Low
Third or later generation anti-tank guided missile (ATGM)	None	None	Low	None
Second or earlier generation ATGM	None	None	Very Low	None
Active beyond visual range (BVR) air-to-air missile (AAM)	Very Low	Medium	Low	Medium
Semi-active AAM	Very Low	Medium	Low	Medium
IR BVR AAM	Very Low	Low	Low	Medium
Short-range IR-guided AAM	None	Very Low	Low	Medium
Fixed-wing fighter gun	None	Very Low	Very Low	Medium
Long-range surface-to-air missile (SAM)	None	Low	Low	Low
Medium range SAM	None	Low	Low	Medium

2.1. General requirements of EWSP systems

"Aircraft combat survivability (ACS) is defined as the capability of an aircraft to avoid or withstand a man-made hostile environment" [2]. Thus, combat survivability is distinguished by the fact that only the man-made hostile environment is considered. Hostile environments

that are not man-made, for example: air defence, and the natural hostile environment including bird strike, severe turbulence. In addition, the normal environment includes system failures and operator errors. The system safety discipline attempts to minimise those conditions known as hazards that can lead to a mishap resulting in harm to people and the environment. These hazards can be caused by internal system failures or features or outside influences, such as operator errors or others. The environment, either normal or hostile, causes damage or hazards that could result in accidents or the destruction of the aircraft. The survivability and the system safety and reliability disciplines attempt to maintain safe operation and maximise the survival of the military helicopters and other aircraft in all environments in peacetime and wartime alike [2].

Survivability is one of the most difficult attributes to establish the operational and technical requirements of performance. Survivability is achieved in so many ways, some of which are associated with the design of the aircraft and some of which are associated with the operation of the aircraft [2].

Research have already found that principles from safety management could be applied to the survivability problem, in particular reducing the risk of survivability to as low as reasonably practicable (ALARP). A survivability assessment process was created that supports the life cycle of military helicopters and establishes the requirements for integrated survivability assessment methods. Moreover, methods were prepared to provide a quantitative assessment of survivability using Quality Function Deployment, (QFD), Analytical Hierarchy Process (AHP) and probabilistic methods [23].

Furthermore, it is very important to know the characteristics influencing the survivability of military helicopters [5]. This is especially important for this system, which are rather complex equipment, with little reliability data and experience available, especially for new systems [6].

According to literature, an EWSP system of military helicopters shall fulfil the following criteria: The warning system shall provide sufficient, timely, accurate and prioritised information on relevant threats to support decisions on further actions. On this level of generalisation, the criteria are applicable to any platform. For the present work, the criteria will act as a guideline, but it should be recognised that they are idealised and cannot be satisfied in a strict sense. Judgement and analysis are required to find practical solutions.

Research have already improved the general understanding of EWSP for military helicopters and united disconnected information on and factors contributing to the EWSP for military helicopters. The advantages and limitations were showed of verification and validation methodologies including modelling and simulation (M&S) or ground tests or open-air range (OAR) flight tests. It can be seen from these that analysing these systems in real conditions like a flight test can be very expensive and does not have many drawbacks [14].

In general, the main task of an EWSP system is to increase aircraft survival and improve their application efficiency by detecting and combating various threats. This includes all activities and operations using the electromagnetic spectrum or controllable energy to attack or prevent attacks by enemy forces [22].

In addition, due to the proliferation of the Man-Portable Air Defence System (MANPADS), since these missiles are already present in any conflict, there is a need for effective electronic support and counteraction against them.

2.2. Configuration for EWSP systems

According to literature, the multilayer methodology for helicopter survival is proposed and summarised in Table 2. Based on these, the conclusion is: "Although implementation of numerous survivability techniques (for Levels II and III) significantly increases the take-off weight, the resultant effectiveness is improved several times" [14, p. 59–60].

Table 2
Matrix of helicopter survivability measures, consistent with the layered survivability concept [6], [13]

Survivability measure		**Level I Flight beyond the reach of enemy fire, no special protection**	**Level II Moderate threat, low weight penalty from protective measures**	**Level III/a Maximum threat, full spectrum of protective measures**	**Level III/b Maximum threat, full spectrum of protective measures**
Vulnerability reduction		Normal design and configuration measures, multiple engines and fire extinguishing system	In addition to Level I: Armour against 7.62 mm bullets for crew and vital units, self-sealing fuel tanks, application of redundant systems	In addition to Level I: Crew and vital units are armour protected against 12.7 mm bullets, self-sealing fuel tanks, application of redundant systems	In addition to Level I: self-sealing fuel tanks and light armour, application of redundant systems
Susceptibility reduction	**EWSP application**	None	Warning systems that can detect threats in various spectral bands, passive countermeasures (limited or extended configuration, Figure 1)	Complete EWSP suite with warning systems, as well as passive and active countermeasures in various spectral bands (full configuration, Figure 1)	Complete EWSP suite with warning systems, as well as passive and active countermeasures in various spectral bands (full configuration, Figure 1)
	IR signature reduction	No reduction measures	Exhaust screens	Exhaust baffles with cool-air mixing, screens on hot engine parts	Additional special design to reduce IR signature
	Manoeuvrability increase	1.5 g	2.5–3 g	2.5–3 g	2.5–3.5 g
	Visual and acoustic character reduction	Camouflage painting	Camouflage painting	Camouflage painting	Small size, camouflage painting, reduce noise signature
	Radar signature reduction	No Radar Cross-Section (RCS) reduction measures	Rotor blades in composite material, radar absorbing fairing on main rotor hub	In addition to Level II: radar absorbing coating on the airframe, tail boom and engine pods	In addition to Level III: Stealth construction (e.g. fenestron tail rotor, weapons in internal bays)

The requirements for EWSP systems are determined by the increasingly complex electromagnetic environment in which they should operate. These devices are affected not only by electromagnetic radiation for military use, but also for civilian use, so EWSP systems should be able to manage this environment without increasing the rate of false alarms.

Figure 1 shows the functional diagram of an integrated EWSP system in three different configurations [14].

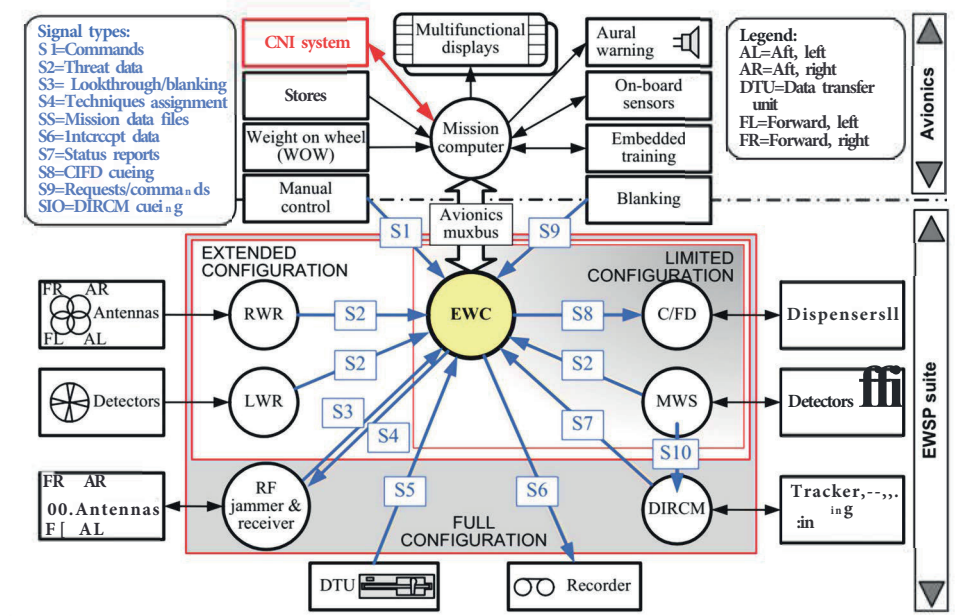

Figure 1
Functional diagram of an integrated EWSP suite in three different configurations [14]

A short summary of the systems is given below:

Chaff and Flare dispensers (C/FD), where the chaff is a radar countermeasure in which the aircraft (helicopter) spreads a cloud of small, thin pieces of aluminium, metallised glass fibre or plastic, which either appears as a cluster of primary targets on radar screens or swamps the screen with multiple returns, in order to confuse and distract. Flare is an aerial infrared countermeasure used by helicopters to counter an infrared homing surface-to-air missile or air-to-air missile.

Missile Warning System (MWS) is a passive defence warning system aiming at detecting, tracking and giving warning of missile threats approaching the protected flying platform.

MWS detects incoming missile threat(s) and automatically takes countermeasures such as the application of Directed Infrared Counter Measure (DIRCM) and/or C/FD system. MWS are based on passive sensor technology operating in solar blind Ultraviolet (UV) spectral band (0.2–0.3 μm) or Mid Infra-Red (MIR) bands (3–5 μm).

Radar Warning Receivers (RWR) systems detect the radio emissions of radar systems. Their primary purpose is to issue a warning when a radar signal that might be a threat is detected, like the fire control radar of another aircraft. The warning can then be used, manually or automatically, to evade the detected threat. CVRs (crystal video receiver), IFMs (instantaneous frequency measurement), tuned and digital receivers are usually used in helicopter EWSP applications.

Laser Warning Receiver (LWR) is used as a passive military defence. It can detect, analyse and locate the directions of laser emissions from laser guidance systems and laser rangefinders. Then it can alert the crew and start various countermeasures, such as smoke screen, aerosol screen, laser jammer, etc.

Radio frequency (RF) jammer can radiate interfering signals toward an enemy's radar, blocking the receiver with highly concentrated energy signals. The two main technique styles are noise techniques and repeater techniques. The three types of noise jamming are spot, sweep and barrage. The repeater jamming like digital radio frequency memory (DRFM) jamming can manipulate the received radar energy and retransmits it to change the return the radar sees. This technique can change the range the radar detects by changing the delay in transmission of pulses, the velocity the radar detects by changing the doppler shift of the transmitted signal, or the angle to the aircraft.

The DIRCM allows for a countermeasures laser to be targeted directly at an incoming IR threat. This makes possible a more powerful and effective defence than previous, non-directional infrared countermeasures, as the threat is directly addressed rather than the system essentially painting an area with infrared disruption, which results in a weaker signal in any given direction. As infrared seeking technology has improved and diversified, standard Infrared Counter Measures (IRCM) systems have become less effective at defeating heat-seeking missiles. Measures such as flares have begun to give way to lasers, which, when fitted on a directional pivoting mount, allow for more effective, concentrated and energy-efficient directional targeting of infrared radiation at incoming missile seekers. In addition, the Common Infrared Countermeasures (CIRCM) system, which is initiated by the USA, will provide a directional infrared countermeasure, which employs both threat-tracking capabilities, as well as defensive measures employing modulating laser pulses to confuse the guidance systems of missiles causing them to miss their target [6], [7], [8].

2.3. Opportunities for electronic countermeasures

The performance of electronic systems can be affected by electronic countermeasures (ECM) in four main ways: by reducing the signal-to-noise ratio (SNR) of the sensor, by deceiving the sensor, by disturbing or destroying the sensor and by influencing the feedback loops of the receiver. Table 3 summarises the chances of these countermeasures against each threat technology, and factor discussed above. It should be noted that infrared tracking sensors in particular sensitive to countermeasures in the acquisition phase before a solid track is established thresholds are set.

Table 3
Conceptual solutions for threat technology countermeasures [14]

Technology	ECM – electronic countermeasure type	ECM – electronic countermeasure goal
Infrared (IR) sensors	Noise or SNR (Signal-to-Noise Ratio) reduction	Introduce IR radiating or absorbing medium between target and sensor or introduce noise into the sensor's detector.
	Deception	Introduce decoys in the sensor's FOV (Field-of-View) or introduce deceptive signals into the detector.
	Disrupt/destroy	Induce disruptive or destructive high-power signal to lenses, detector elements or sensor electronics.
IR seekers	Noise or SNR (Signal-to-Noise Ratio) reduction	Introduce IR radiating or absorbing medium in the seeker's FOV, or introduce noise into the seeker's detector.
	Deception	Introduce decoys in the seeker's FOV or introduce deceptive signals into the detector.
	Disrupt/destroy	Induce disruptive or destructive high-power signal into window, detector elements or seeker electronics.
Laser technology	Noise or SNR (Signal-to-Noise Ratio) reduction	Introduce radiating or reflecting medium in the laser path or introduce noise into the laser receiver.
	Deception	Introduce decoys in the laser path or introduce deceptive signals into the detector.
	Disrupt/destroy	Induce disruptive or destructive high-power signal into detector elements of laser receiver or seeker electronics.
Radars	Noise or SNR (Signal-to-Noise Ratio) reduction	Introduce radar reflecting or absorbing medium between target and radar receiver, introduce noise into the receiver.
	Deception	Introduce decoys in the radar's search volume, introduce deceptive signals into the receiver, introduce false targets that overload signal processing capacity.
	Disrupt/destroy	Induce disruptive or destructive high-power signal into the radar receiver's front end or into receiver electronics.
Servos and FCS (Fire Control System)	Noise or SNR (Signal-to-Noise Ratio) reduction	Degrade SNR of sensors that form a part of the servo feedback loop.
	Deception	Introduce beat signals into the servo feedback loop through sensor signals, or signal that offsets the AGC (automatic gain control).
	Disrupt/destroy	Induce disruptive or destructive high-power signal into the sensors or into sensor electronics.
Threat timelines	–	Reaction timelines: Countermeasure directed at sensors as mentioned above, tactical measures to delay detection and identification.

According to this, the central question for the helicopter EWSP system is which radar system to consider. Due to the radars of the given era, EWSP manufacturers have always focused on their emanation. However, this contradicts the general view that modern helicopter EWSP system devices are essentially not related to a particular battlefield circumstance. For example, long-range reconnaissance radars do not normally pose a threat to helicopters [7].

During my research, I have also determined the most important characteristics and aspects of the complex EWSP systems of a military helicopter, considering the expected conditions of use of this helicopter [8].

It can be stated that little information is available due to restricted real observation, military theatre-level experience, and lack of statistical data on the safety and reliability disciplines of EWSP devices, and manufacturers do not always provide such data and information or, if so, it is very incomplete. Obviously, the reliability of these systems is difficult to test even

in a normal environment, not to mention a hostile environment. In addition, the effects of different modes of failure and their hazards can only be described by a few experts [6], [7], [8].

3. Reliability engineering and model based safety assessment

In systems engineering, dependability is a measure of a system's availability, reliability, maintainability, and in some cases, other characteristics such as durability, safety and security [17].

Attributes are qualities of a system. These can be assessed to determine its overall dependability using qualitative or quantitative measures. Dependability attributes are the following:

- availability (readiness for correct service);
- reliability (continuity of correct service);
- safety (absence of catastrophic consequences on the user(s) and the environment)
- integrity (absence of improper system alteration);
- maintainability (ability for easy maintenance [repair]) [1].

Reliability analyses can be performed for different systems and components, such as mechanical, electronic or software. Two different levels at which reliability can be applied are defined: component and system level. These already introduce the bottom-up and top-down approaches, which can be found in some reliability methods, as well.

Systems analysis is a process that allows reliability engineers to understand how systems work and how they can fail by investigating the system behaviour and potential causes of system failure, thereby allowing them to determine necessary actions to prevent system failure. There are generally two forms of analysis. The first is qualitative analysis, which is usually performed by reducing fault trees to minimal cut sets, which are a disjoint sum of products consisting of the smallest combination of basic events that are necessary and sufficient to cause a hazardous situation, e.g. a system failure.

Missing or insufficient data does not allow for quantitative assessment of reliability. Nevertheless, relations within the system, covering hazards, failure causes, events, failure modes, faults, effects and consequences, can be shown and this way an estimate of reliability, failure probability and consequence can still be obtained by using qualitative methods. Before performing any qualitative reliability analyses, first the system structure and functions must be identified and classified. On this basis, a qualitative reliability assessment can be carried out.

The second is quantitative analysis. In this analysis, the probability of the occurrence of a system failure and other quantitative reliability indexes such as importance measures is mathematically calculated, given the failure rate or probability of individual system component. The results of quantitative analysis give analysts an indication about system reliability and help to determine which components or parts of the system are more critical, so analysts can put more emphasis on the critical components or parts by taking the necessary steps, e.g. including redundant components in the system model [19, p. 18–23].

However, a comparison of different literature shows some discrepancies in the assignment of certain reliability methods and indicates the need for a third intermediate category for such semi-quantitative reliability methods. Some of the qualitative reliability methods

can be extended with some quantitative approximate measures and thus also be used for quantitative reliability assessment.

Furthermore, it must be noted that some of the presented methods are rather risk assessment tools than reliability methods. However, these risk assessment techniques are still included, as the awareness of the existing risks is the decisive basis for reliability analyses. A detailed list of risk assessment methods can be found in ISO/IEC 31010:2019 – Risk management. Risk assessment techniques [18], [25].

The aim of reliability engineering is to improve the reliability of a system to minimise the risk associated with the system failure or to improve efficiency while reducing the cost. Analysts can discover the flaws of a system through analysis, and therefore can take necessary actions to improve the system design by adjusting to reduce those flaws [20].

There are some well-known risk and safety analysis techniques and model-based safety assessment (MBSA) approaches of each category, including the following:

- Qualitative reliability analysis
  - Sheet-based qualitative reliability methods
    - Structured What If Technique (SWIFT), Hazard and Operability Study (HAZOP), Failure Mode and Effects Analysis (FMEA)
  - Diagrammatic qualitative reliability methods
    - Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Bow-Tie Analysis (BTA), Strengths, Weaknesses, Opportunities and Threats (SWOT) Technique
- Semi quantitative reliability analysis
  - Table-based semi-quantitative reliability method
    - Failure Mode, Effects and Criticality Analysis (FMECA)
  - Diagrammatic semi-quantitative reliability methods
    - Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Bow-tie Analysis (BTA), Reliability Block Diagram (RBD), Bayesian Networks (BNs)
- Quantitative reliability analysis
  - Analytical quantitative methods
    - First Order Reliability Method (FORM), Second Order Reliability Method (SORM), Hasofer and Lind (HL) Method, Probability of Failure (PoF) Method, Concept of Limit State Function (LSF)
  - Stochastic quantitative methods
    - Monte Carlo Simulation (MCS), Importance Sampling Reduction Methods (ISRMs), Stochastic Response Surface Methods (SRSMs)
  - Sophisticated quantitative methods
    - Multi-Criteria Decision Making (MCDM) or Multi-Attribute Decision Making (MADM), Markov Analysis (MA), Petri Nets (PNs), Fuzzy Theory-based techniques
  - Data foundations
    - Databases, statistical modelling
- Model-based safety assessment (MBSA)
  - Failure logic synthesis and analysis approaches
    - Failure Propagation and Transformation Notation (FPTN), Failure Propagation and Transformation Calculus (FPTC), Component Fault Trees (CFTs), State-Event Fault Trees (SEFTs), Hierarchically Performed Hazard Origin and Propagation

Studies (HiP-HOPS), Architecture Analysis and Design Language (AADL) Error Model
- Behavioural fault simulation approaches
  - Formal Safety Analysis Platform (FSAP/NuSMV-SA), AltaRica, Deductive Cause Consequence Analysis (DCCA), Safety Analysis Modelling Language (SAML) [19], [25]

4. Application of reliability methods

Safety-critical systems are an integral part of a military helicopter. When they fail, the human, environmental and financial costs are significant. Many approaches such as classical safety analysis technique (e.g. EN 16602-30:2018 and EN 62308:2007) [11], [12] have been widely applied to evaluate system reliability prior to deployment and help increase system defences.

The Hungarian Military Standards (MSZ K 070 and MSZ K 066) issued on reliability in 1981 have not yet included this type of method [15], [16].

Several studies have already been conducted on the reliability of military electronic systems.

In her PhD dissertation, Marianna Lendvay evaluated the reliability analysis methods with respect to application for military electronic systems. She worked out a criterion system to compare these reliability analysis methods for military electronic systems. She established that exacting requirement for military electric systems it can be satisfied above all with FMEA, FTA, RBD [24].

In his PhD dissertation, Pál Bárkányi collected methods for analysing reliability which are usable for the military reconnaissance systems demonstrating with practical examples and mathematical calculations. He worked out a mathematical model (concept) suitable for examining simple and more sophisticated reconnaissance systems. He created a procedure (Markov modelling for reliability with Graph theory) which makes computerised analysis and calculations of the technical reliability easier. He also presented that the fuzzy method is the most modern technology for analysing the reliability and by now the informatics hardware structures are capable to provide valuable results within a reasonable timeframe [3].

László Domán, László Pokorádi and László Szilvássy in 'Repülőeszközök idegen-barát felismerésének kockázatát befolyásoló tényezők ok-okozati elemzése' [9], identified potential causes of a failure of an identification friend or foe (IFF) system. These causes were grouped into major categories to identify and classify these sources of variation.

László Domán in 'Katonai helikopterek elektronikai hadviselés (önvédelmi rendszerek) értékelési szempontjaival összefüggő súlyszámok meghatározása Fuzzy AHP módszer felhasználásával' [10], presented several aspects of Multi Criteria Decision Making. He highlighted the system of criteria set up for the evaluation of EWSP systems for military helicopters. An application of the classical (Analytical Hierarchy Process – AHP) and Fuzzy Analytical Hierarchy Process (Fuzzy AHP) methods was described to determine the weighting number representing the preference relationships of the comparison of EWSP.

In 'A Review of Reliability-based Methods for Risk Analysis and their Application in the Offshore Wind Industry" by Mareike Leimeister and Athanasios Kolios [25], the authors focused on the review and classification of Risk and methods applied specifically within the offshore

wind and marine renewable energy systems. Finally, they summarised the applicability of the presented methods to the stage, the specific challenges and the set outcomes, and presented their limitations for these systems.

Usually, these types of techniques are manual processes and performed on an informal system model by a single person or a group of persons to fulfil safety requirements of the systems. Although these techniques can produce a great deal of valuable information about the safety and reliability of the system, the overall performance of these techniques largely depend on the skill of the analysts. As these analyses are performed on informal models, it is therefore unlikely that they will be complete, consistent and error free which make it difficult to reuse that information. Furthermore, manual analyses are usually time consuming and expensive; therefore, once performed they are unlikely to be repeated or iterated upon.

Especially in the last two decades, research has concentrated on simplifying the dependability analysis process by automating them, which led to a body of work on model-based safety assessment (MBSA) and prediction of dependability. Several approaches to automated safety analysis have emerged, motivated mainly by the increased complexity of systems and increased time and costs associated with the manual analysis [20].

In model-based safety analysis, system designers and safety analysts both use the same system model or somehow related models. As a result, the models become more formal than a separate model for safety analysis. This can let automating all or some part of the safety analysis process. By automating the safety analysis processes, MBSA can save time and expenses and allow the reusability of the information. Moreover, the MBSA techniques provide a higher degree of reusability by allowing parts of an existing system model, or libraries of previously analysed components, to be reused [20].

MBSA techniques can be classified into two broad categories based on their general underlying formalism and the types of analysis performed. The first paradigm is called Failure Logic Synthesis and Analysis (FLSA) which focuses on the automatic construction of predictive system analyses. The second paradigm is called Behavioural Fault Simulation (BFS) which focuses on behavioural simulation to automatically analyse potential failures in a system [19].

Simon Gradel, Benedikt Aigner and Eike Stumpf in 'Model-based Safety Assessment for Conceptual Aircraft Systems Design' [13], proposed an approach using a Simulink system structure model of MBSA for designing system architectures in conceptual aircraft design. They emphasised that unlike other MBSA approaches (e.g. AltaRica, HiP-HOPS), it is designed such that adding or removing redundant components does typically not require a revision of the component action description. They noted that using qualitative and quantitative results from the trade study, an improved system architecture can be proposed. The authors believed that the ability to alter the system architecture without changing the component performance models makes their proposed approach more suitable for this task then other MBSA approaches.

By allowing imprecision and approximate analysis, fuzzy logic enables incorporating uncertainty in the analysis. Many classical risk assessment approaches such as FTA and FMEA rely on precise failure data. However, such data are often unavailable or scarce, introducing uncertainty in the process. Both aleatory and epistemic uncertainties have been addressed by combining fuzzy set theory with risk assessment approaches. The *theory* of *fuzzy logic* was firstly used in FTA for system reliability analysis in the early 1980s. Since then, several researchers have developed different fuzzy set theory-based methodologies for system safety

and reliability analysis, and many researchers have used these methodologies in a variety of application areas.

Sinan Koçak in 'Fuzzy Logic and its Mechatronics Engineering Applications' [21], presented a comprehensive literature review on the fuzzy set theory. This literature reviewed also explains the concept of operation fuzzy sets. He emphasised some researcher works with his interpretations of fuzzy sets.

Fuzzy set theory has also been applied in conjunction with dynamic extensions of the fault trees. The application of fuzzy set theory in safety and reliability engineering has been extended to FMEA, ETA, Bayesian networks, Markov chains and Petri nets. These approaches enable us to draw helpful conclusions even in the absence of concrete failure data.

5. Discussion

Analysing methods listed earlier considering their advantages and disadvantages, I summarise and present the main challenges, as well as the individual solutions:

- The EWSP are very complex systems and usually have several different, interconnected and dynamic failure modes and not all such data is known due to limited observation and scarcity of statistical data.
- Missing, insufficient and vague data, especially in the EWSP, is a major problem in a detailed and meaningful assessment of the reliability of such devices. The failure probability of a relatively new component with insufficient historical failure data could, in theory, be estimated based on expert judgement or experience from similar components [20].
- The classification and ranking of failure modes is often quite subjective, and risk priority numbers (RPN) do not always provide meaningful information, especially when different technologies and EWSP systems need to be compared.

Considering the advantages provided by the MBSA approaches over manual approaches, the main disadvantage of these methods is that it cannot handle either aleatoric or epistemic uncertainties. The aleatoric uncertainty is due to randomness of a physical system or natural variation, whereas the epistemic uncertainty is because of ambiguity, incompleteness and lack of knowledge [20]. Although the issue of uncertainty in the failure data has been addressed in classical risk assessment approaches (Qualitative and Quantitative) by incorporating fuzzy set theory, no effort has been made to address the same issue in the context of MBSA.

For this reason, in this article, I have considered only the traditional risk assessment methods when analysing EWSP systems. A summary of the usable approaches, their applicability with respect to stage, specific challenges and aimed outcomes, as well as their limitations, is presented in Table 4. The considered stages are divided into design (D), construction (C), operation (O), maintenance (M) and life cycle planning (LC) [25].

Table 4
Applicability of presented reliability methods [25]

Type	Category	Method	Stage	Results	Capabilities	Limitation
Qualitative	Failure mode analyses	FMEA and FMECA	D	Failure modes	Easy implementation, employable from the beginning of the project	Competent facilitator for reaching consensus in scoring is required
		Quantitative FMEA	D, C	Prioritisation of failure modes	Straightforward application due to well-defined bands of scores	Appropriate scoring for different classes of application
		Correlation FMEA	D, LC	Weak points	Coping with mutual correlated failure mode	No incorporation of detectability factor in 2D representation
	Tree and graphical	FTA, ETA and BN	D, C	Decision making	Visual representation of interdependencies of events	Cumbersomeness in case of highly granulated system analysis
	Analyses	Dynamic FTA	D, C, O, M	Maintenance references	Coping with sequentially dependent and redundancy failures	Effect of inappropriate sequencing of events on analysis results
		BTA	O, M	Real time risk monitoring	Efficient link of ETA and FTA; visualisation of dependencies	Common cause and dependency failures
	Hazard analyses	HAZID or HAZOP	D, O, M	Monitor integrity; operational risk factors	Structured description of hazards and system effects of deviations from design intent	Extensive documentation; only to be applied to well-defined system
Quantitative	Analytical methods	LSF, HL, PoF	D, O, LC	Design optimisation and novel designs	Systematically considered uncertainties; no global safety factors	Combined failure modes their individual contributions
		Analytical probabilistic analyses (FORM and SORM)	D, C, O, LC	Reliability sensitivity	Robust consideration of input uncertainties	Complex derivation of joint probability distribution functions
	Stochastic methods	MCS	O, M	Decision making	Easy to implement due to direct simulations	Large computational effort
		SRSM	C	Computational efficiency	Time-varying and dependent variables	Sensitive to initial assumption of Response Surface shape
		ISRM	C	Computational efficiency	Overcome limitations of direct MCS	Performance in multiple variables; modelling requirements
	Multivariate analyses	MCDM or MADM	D, O, M, LC	Decision making; prioritisation of interventions	Easy implementation due to intuition-based input data	Skewness of results due to extreme values

Type	Category	Method	Stage	Results	Capabilities	Limitation
	Data foundations	Databases	D, O, M	Data collection; optimised operation and maintenance	Availability of generic occurrence frequencies	Processed data; different sources and reporting protocol forms
		Statistical modelling	O	Optimisation (design, operation, and control strategies)	Failure prediction in complex and repairable systems	Sufficiently accurate system modelling required
		Markov Chain Approach for Data Modelling	O, M	Sensibility to parameter variations	Coping with dynamic reliability problems, degradation and maintenance processes	Non-explicit expression of dependencies between hidden states; computational effort
	Fuzzy theory-based	F-MCDM	D, O, M, LC	Decision making; prioritisation of interventions	Easy implementation due to intuition-based input data, broad range of values where precise data is not available	Skewness of results due to extreme values
		F-FMEA	D, LC	Failure modes	Easy implementation, employable from the beginning of the project, broad range of values where precise data is not available	Competent facilitator for reaching consensus in scoring is required
		F-FTA, F-ETA, F-BN	D, C	Decision making	Visual representation of interdependencies of events, broad range of values where precise data is not available	Cumbersomeness in case of highly granulated system analysis
		F-MA, F-PN	O, M	Sensibility to parameter variations	Coping with dynamic reliability problems, degradation and maintenance processes, broad range of values where precise data is not available	Non-explicit expression of dependencies between hidden states; computational effort

6. Conclusion and future research

In these approach forms, failure rates, failure probabilities or other numerical data related to the failure behaviour of system components are usually considered known. This situation is especially relevant in the early design stages, when the requirements and specifications of system components are incomplete, and in the case of new and complex software components.

System safety and reliability could be evaluated based on generic statistical data, which may be taken from existing reliability databases. However, the use of generic data will add further uncertainty and imprecision to the results of the analysis.

Consequently, system safety and reliability such as EWPS could be evaluated based on generic statistical data, which may be taken from existing reliability databases. However, the use of generic data will add further uncertainty and imprecision to the results of the analysis.

In their normal forms, the reliability analysis methods rely on precise failure data. However, such data are often unavailable or scarce, introducing uncertainty in the process as I pointed out in the introduction for EWSP systems. The author has found that both aleatory and epistemic uncertainties should be addressed through a combination of fuzzy set theory and risk assessment approaches.

For these reasons, it is advisable to use fuzzy theory-based approaches including Fuzzy FTA, Fuzzy FMEA, Fuzzy ETA, Fuzzy Markov methods, Fuzzy Petri nets, or Fuzzy Bayesian networks to analyse such systems like EWSP.

In this paper, I have reviewed a basic description of the military helicopter EWSP system and up-to-date safety analysis techniques including fuzzy theory based and MBSA approaches. In the future, the author will focus on performing the following research tasks:

- investigation of fuzzy rule-based PRA approaches in the reliability analysis of EWSP systems for military helicopters;
- development of a methodology for comparing risk assessment methods based on fuzzy theory for the analysis of military helicopter EWSP;
- to work a fuzzy theory-based risk assessment analysis for EWSP.

References

[1] A. Avizienis, J.-C. Laprie, B. Randell and C. Landwehr, 'Basic Concepts and Taxonomy of Dependable and Secure Computing'. *IEEE Transactions on Dependable and Secure Computing,* Vol. 1, no. 1. pp. 11–33. 2004. Online: https://doi.org/10.1109/TDSC.2004.2

[2] R. E. Ball, *The Fundamentals of Aircraft Combat Survivability Analysis and Design.* AIAA, 2003. Online: https://doi.org/10.2514/4.862519

[3] P. Bárkányi, *Katonai elektronikai felderítő rendszerek műszaki megbízhatósága.* PhD thesis, NKE KMDI, 2012. Online: https://doi.org/10.17625/NKE.2013.001

[4] Department of Defense, *Guide for Achieving Reliability, Availability, and Maintainability.* 03 August 2005. Online: www.acqnotes.com/Attachments/DoD%20Reliability%20Availability%20and%20Maintainability%20(RAM)%20Guide.pdf

[5] L. Domán, 'Helikopterek túlélőképességét befolyásoló tényezők elemzése'. *Katonai Logisztika,* Vol. 28, no. 1–2. pp. 131–150. 2020. Online: https://doi.org/10.30583/2020/1-2/131

[6] L. Domán, 'Az Airbus H145M helikopter és a túlélőképesség'. *Repüléstudományi Közlemények,* Vol. 31, no. 1. pp. 85–102. 2019. Online: https://doi.org/10.32560/rk.2019.1.8

[7] L. Domán, 'Katonai helikopterek komplex elektronikai hadviselés önvédelmi rendszereinek értékelése'. *Repüléstudományi Közlemények,* Vol. 33, no. 2. pp. 1–19. 2021. Online: https://doi.org/10.32560/rk.2021.2.4

[8] L. Domán, 'A Mi–24 elektronikai hadviselési képességei és fejlesztési lehetőségei', in *Szemelvények a katonai műszaki tudományok eredményeiből II,* ed. G. Hausner. Budapest, Ludovika Egyetemi Kiadó, 2021. pp. 99–115. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/16208/905_KDMI_II_hallgatoi_tanulmanykotet.pdf

[9] L. Domán, L. Pokorádi and L. Szilvássy, 'Repülőeszközök idegen-barát felismerésének kockázatát befolyásoló tényezők ok-okozati elemzése'. *Repüléstudományi Közlemények,* Vol. 31, no. 3. pp. 15–30. 2019. Online: https://doi.org/10.32560/rk.2019.3.650
[10] L. Domán, 'Katonai helikopterek elektronikai hadviselés (önvédelmi rendszerek) értékelési szempontjaival összefüggő súlyszámok meghatározása Fuzzy AHP módszer felhasználásával', in *Szemelvények a katonai műszaki tudományok eredményeiből III,* ed. L. Földi. Budapest, Ludovika Egyetemi Kiadó, 2022. pp. 1–20.
[11] EN 16602-30:2018 ICS: 49.140 Space System and Operations Space Products Assurance – Dependability Standard.
[12] EN 62308:2007 Equipment Reliability. Reliability Assessment Methods.
[13] S. Gradel, B. Aigner and E. Stumpf, 'Model-based Safety Assessment for Conceptual Aircraft Systems Design'. *CEAS Aeronautical Journal,* Vol. 13, no. 1. pp. 281–294. 2021. Online: https://doi.org/10.1007/s13272-021-00562-2
[14] J. Heikell, *Electronic Warfare Self-protection of Battlefield Helicopters: A Holistic View.* PhD dissertation, Espoo, Helsinki University of Technology, 2005. Online: https://indianstrategicknowledgeonline.com/web/isbn9512275465.pdf
[15] Hungarian Military Standards MSZ K 070 Military Purpose Appliance, Instruments, Kits and Equipment. General Technological Requirements, Checking and Examination Methods.
[16] Hungarian Military Standards MSZ K 066 Military Purpose Appliance, Instruments, Kits and Equipment. General Technological Requirements, Checking and Examination Methods. Reliability Demands.
[17] International Electrotechnical Commission, *Electropedia,* 192-01-22. Online: www.electropedia.org/iev/iev.nsf/display?openform&ievref=192-01-22
[18] ISO/IEC 31010:2019 – Risk Management. Risk Assessment Techniques.
[19] S. Kabir, *Compositional Dependability Analysis of Dynamic Systems with Uncertainty.* PhD thesis, University of Hull, 2016.
[20] S. Kabir and Y. Papadopoulos, 'A Review of Applications of Fuzzy Sets to Safety and Reliability Engineering'. *International Journal of Approximate Reasoning,* Vol. 100. pp. 29–55. 2018. Online: https://doi.org/10.1016/j.ijar.2018.05.005
[21] S. Koçak, 'Fuzzy Logic and its Mechatronics Engineering Applications'. *Repüléstudományi Közlemények,* Vol. 29, no. 2. pp. 41–48. 2017. Online: https://folyoirat.ludovika.hu/index.php/reptudkoz/article/view/4315
[22] Gy. Keszthelyi, 'A Mi-24 típusú harcihelikopter hatékonysága korunk fegyveres konfliktusaiban III. rész. A helikopter önvédelmi rendszerei és alkalmazási hatékonyságuk'. *Katonai Logisztika,* Vol. 28, no. 4. pp. 5–57. 2020. Online: https://doi.org/10.30583/2020.4.005
[23] N. G. Law, *Integrated Helicopter Survivability.* PhD thesis, U.K., Cranfield University, 2011. Online: https://core.ac.uk/download/pdf/140841.pdf
[24] M. Lendvay, *Katonai elektronikai rendszerek megbízhatóságelemzése.* PhD thesis, ZMNE KMDI, 2006.
[25] M. Leimeister and A. Kolios, 'A Review of Reliability-based Methods for Risk Analysis and their Application in the Offshore Wind Industry'. *Renewable and Sustainable Energy Reviews,* Vol. 91. pp. 1065–1076. 2018. Online: https://doi.org/10.1016/j.rser.2018.04.004
[26] MIL-STD-882E, Department of Defense, *Standard Practice: System Safety.*

A megbízhatóságon alapuló kockázatértékelési módszerek áttekintése és lehetséges alkalmazásuk a katonai helikopterek önvédelmi elektronikai hadviselési rendszereinél

A katonai helikopterek önvédelmi elektronikai hadviselési rendszereit a tervezési folyamattól az eszközök operatív kezeléséig számos bizonytalanság veszi körül. A hagyományos kvalitatív elemzések mellett előtérbe kerülnek a kifinomultabb és újszerűbb technikák, például a fuzzy elméleten alapuló módszer. Ennek a cikknek a célja, hogy bemutasson néhány lehetséges módszert a katonai helikopterek önvédelmi elektronikai hadviselési rendszereinek kockázatértékelésére.

Kulcsszavak: *katonai helikopter, elektronikai hadviselés, fuzzy logika, kockázatelemzés, megbízhatóság*

Domán László őrnagy
főtechnológus (osztályvezető helyettes)
Magyar Honvédség Légijármű Javítóüzem
Műszaki Fejlesztési és Technológiai Osztály
doman.laszlo79@gmail.com
orcid.org/0000-0002-4472-2609

Major László Domán
Chief Technologist (Deputy Head of Department)
Hungarian Defence Forces Aircraft Repair Plant
Technical Development and Technological Department
doman.laszlo79@gmail.com
orcid.org/0000-0002-4472-2609