**Hri hazard risk index**

TAREG 3.7.1 – Safety of the systemSusustem safety is defined in the glossary and aims to better identify and detect the technical risk inherent in the aviation system, to promote informed decisions on the treatment of risks. System security is best practice and is specifically regulated (or officially designated) by a number of national airworthiness authorities (NAA) and military airworthiness bodies (MAAs), including the FAA, CASA, EASA, US military forces and the UK MoD. Figure 17–1 - Achieving a safe aircraft design shows the contribution to the safety of the system and the basis for aircraft certification to the safe design of the aircraft. Figure 17–1 Achieving a safe design for aircraft use More recently, safety risk management processes have increased in their sophistication and efficiency, as public expectations for preventing accidents, injuries and damage have also increased. The types of ADF aircraft are increasingly complex, with many potential aircraft system hazards requiring proper steering to prevent aircraft from operating in a precarious state. TAREG 3.7.1 requires AEOs to manage aircraft safety risk using the system approach to ensure that hazards are adequately identified and adequately managed. Compliance requirements When verifying compliance with TAREG 3.7.1, compliance assurance staff should seek the following evidence:System Security Programme Plan (SSPP) issued by the relevant Senior Design Engineer (SDE) with the correct level of approval for the organisation involved. The system security programme plan shall be approved, issued, reviewed and amended as necessary. The System Security Groups (SSGs) are chaired by a Design Acceptance Representative (DAR) or an authorised delegate and shall be carried out at the required frequency. System security products, e.g. Explanation and reinforcement of TAREG 3.7.1 clause a.1. — System Safety Program Plan A System Safety Program (SSP) is a combined set of people and tasks (System Safety Management and System Safety Engineering) that implement and execute the system security process on a development project or within a phase in the service of the system lifecycle. The main objectives of the System Security Programme are to ensure that: security objectives in line with world best practice are established and documented;a safety management framework is established that clearly articulates the level of risk to the relevant managing authorities, implemented and maintained;security, in accordance with mission requirements, is designed into a system in a timely, cost-effective manner;hazards are identified, analysed, assessed and eliminated or the associated risk is reduced to an acceptable level throughout the lifecycle of the system;the hazards identified in the service are assessed against the safety objectives identified;the elimination/reduction of hazards is documented;pragmatic risk treatments are properly considered;historical safety data, including lessons learned, are continuously assessed, considered and used; isafety is not ensured by relying solely on design standards (as shown in Figure 17-1). System security is carried out through the System Security Program, as documented in the system security program plan. The objectives of system security will decide on the scope of the SSP and the necessary documentation. For example, during procurement and modification projects, the main objective of system security is to procure aircraft with an acceptable level of safety, as defined in the System Safety Guidance Handout under Key Documents on the DGTA – ADF or System Safety Guidelines website on the DGTA – ADF System Security Tools website. Once in service, the main objective of the security of the system is to ensure that the inherent level of aircraft safety is at least maintained (preferably improved). The SAA focuses on identifying and mitigating the hazards of aircraft systems (including consideration of the hazards targeted – see paragraph 15) affecting airworthiness. This includes hazards directly and indirectly related to aircraft systems and their reliability, degraded condition, fault modes and complex interactions. All hazards of aircraft systems consist of combinations of hardware, software and/or human factors; omitment of any of these aspects will lead to an SSP that considers only a fraction of the overall hazard picture and can therefore provide a false sense of security. The SSP should therefore include activities and analyses to anticipate and assess the inherent safety of each of these three elements in the integrated product. Hardware, software, and human causal factors are further tested as follows:Hardware causal factors. In general, the concept of hardware causal factors is well understood by aerospace engineers. System security provides a suite of processes and tools for analyzing and evaluating hardware causal factors. These processes and tools are equally applicable to aircraft acquisitions and in-service support, and are covered by different system safety standards, e.g. aircraft acquisitions and support. Historically, analysis of software causal factors has either been ignored or considered too late in the design cycle to have any real positive impact. However, aircraft designers are assigning software to more and more system functions, so this approach is no longer acceptable. The software must be analyzed together with the hardware and human factors that cause a complete analysis of the safety of the aircraft system. eADRM AAP 7001.054 Section 2 Chapter 3 — Aerospace software provides detailed guidance on the analysis and assessment of causal assessment of software Causal factors. Traditionally, human design requirements for aviation systems are considered appropriately using commercial or military guidance documents, supplemented with Commonwealth human design and object experts in the Organization for Defense Science and Technology (DSTO), Aerospace Operational Support Group (AOSG), Aircraft Maintenance and Flight Test Unit (AMAFTU), Aerospace Medicine Institute (AVMED) and Operational Squadrons. However, hazards must be observed and mitigated when analysing and mitigating hazards, especially where the mitigations alone require human input, i.e. air force circumvention, procedures or training. After all, a combination of dangers is likely to be present during the worst-case scenario of danger. The assessment of the workload of human factors on the integrated system should show that the average air force can continue to fly safely and ground the aircraft. Additional information on human factors in the design of the aircraft system and system integration activities is included in eADRM AAP 7001.054 Section 2 Chapter 5 – Human Factors Engineering.Hazard Identification. The Technical Airworthiness Regulator (TAR) does not require specific hazard identification techniques for aircraft SSPs, as each has its own merits for specific applications and therefore depends on the circumstances. However, the use of an appropriate hazard identification checklist should at least be used as a starting point for a broad identification of potential hazards. The generic Hazard Identification Checklist is available in the System Security Guidance Material in the Key Documents box on the DGTA - ADF website. A rigorous approach to hazard identification will inevitably be warranted for aircraft procurement and major modification projects, and relevant guidance is also provided in the Key Documents System Security Guidance Handout on the DGTA -ADF website or the System Security Guidelines on the DGTA – ADF System Security Tools website. Hazard analysis. Tar once again does not require specific hazard analysis techniques for aircraft SSDs, as each has its own merits for specific applications and therefore depends on the circumstances. At the very least, hazard analyses should consider the hazards associated with the aircraft's core system and deviations from that certified baseline. When considering the latter, hazard analyses should address the hazards associated with: legacy aircraft systems;new and modified design, integration, maintenance, operation and disposal of aircraft systems; interface between new and legacy aircraft systems; icomplex system interactions, including common cause (Common Mode, Zonal Safety Analyses and Particular Risk) procurement of aircraft and major modification projects, where more complex systems and interactions are likely to be present, the security of the range of processes and tools for hazard analysis. For relevant guidance, see The System Security Guidelines Handout in key documents on the DGTA - ADF website or system safety guidelines on the DGTA – ADF System Security Tools website. Hazard mitigation and the Order of the System Safety Championship. A fundamental element of the System Security Program is the approved Hazard Risk Index (HRI) matrix, which provides a framework for promoting informed risk treatment decisions. If the danger is deemed unacceptable and mitigation is therefore required, engineers should follow the solutions, bearing in mind the Order of Priority in System Security. This concept recognises that some hazard mitigation methods are often less effective than others and therefore priority should be given to the most effective pragmatic solution. The order of priority is as follows: the risk of design to reduce or eliminate the associated risk, i.e. by re-designing to re-design the hazard scenario irrelevant, to unincorporate the associated risk of danger to an acceptable level, e.g. automatic override in the field after radar, or to detect warning devices to reduce the associated risk of danger to an acceptable level, e.g., ordevelop procedures and training to try to avoid the associated risk of danger , e.g. pilot verification required for the accuracy of automated weight and balance calculations. Hazard mitigation should be documented, including the reasons why the decision on the benefits of the higher order (as noted above) has not been implemented. Often, the inclusion of hazard mitigation will change the likelihood rather than the severity of the accident, that is, the danger will still cause a catastrophic accident, but its likelihood of occurrence may decrease, however there are exceptions. It is important to note that the least preferred four mitigation options, namely development, procedures and training, should not be used as a sole mitigation for risk northerly hazards involving loss of life (usually catastrophic and critical weights under MIL-STD-882) due to over-reliance only on human factors to prevent loss of life. Hazard Risk Index Matrixes. Robust technical risk management is fundamental to achieving system security objectives and greater eTAMM intentions to optimise safety with minimal limitation. HRI matrices are often an important tool in risk assessment and communication, but unfortunately ADF has countless different HRI matrices. While TAR recognises the potential for confusion and difficulty comparing risks across platforms, TAR's desire is to continue using the parent risk matrix that arose during the original aircraft design. This ensures consistent handling of hazards throughout the aircraft's lifecycle, and allows communication with the original equipment manufacturer (OEM) and other aircraft users. Risk communication. In order to promote unambiguous understanding within the SSG, participants should adopt the level of probability and consequences of HRI and the resulting level of risk as a common communication medium. However, this medium may not be suitable for communicating with stakeholders outside SSG. The following approach to external communications is proposed: Communication to the operational fraternity. When communicating risks to an operational fraternity, e.g. However, this translation must always take place as the penultimate step, after the completion of all technical assessments. Note, for example, that some engineering issues are not suitable for AVRM tables, which generally require qualitative (as opposed to quantitative) assessments; Communication with other ADF members or external organisations. Without proper context, HRI matrices can be meaningless (or worse, misleading). Accordingly, a qualitative description should be provided when communicating risks to non-ADF operators or engineers. The depth of the qualitative description will depend on the audience.' Missionized' dangers. With a few exceptions, aircraft systems on ADF aircraft have military-specific roles, including specialized war functions. Under hostile operating conditions, the malfunction of these systems may have a more significant impact on security than similar failures under benign operating conditions. These additional military-unique hazards must also be managed through the System Security Programme. Further information on mission-sanctioned hazards is provided in the System Security Guidance Material in the Framework of Key Documents on the DGTA – ADF website or system safety guidelines on the DGTA – ADF System Security Tools website. Audits of system security programs. SAA audits should be carried out in the context of ongoing audits by the Commonwealth AEO or Approved Maintenance Organisations (AMO) required as part of periodic reviews of engineering management systems (EMS) or quality management systems (QMS). ADF and contractor personnel involved in aircraft procurement or major modifications should refer to the System Safety Guidance Material under Key Documents on the DGTA - ADF or System Safety Guidelines website on the DGTA – ADF System Security Tools website for further detailed guidance. Staff involved in minor changes and support in the service may also find these guidelines useful. Approve a system security program plan. SSPPs in use must be approved before the system can be deployed in SSPs for aircraft procurement and major modification projects should be approved before the start of the project activity. When approving a commercial AEO SSPP, the sponsor of the SDE Authorized Engineering Organization (AEO) should confirm the consistency of safety objectives with its own SSP. Changes to the system security program plan. Amendments subject to tareg 3.7.1 clause a.1.c, would likely include amendments: security bases, i.e. security objectives/HRI matrix, risk retention bodies, acquisition strategies, fundamental nature, structure and role of the System Security Group, Safety Assessment Report and Hazard Log, service support strategies, any element of the SSPP that would invalidate the tar existing understanding of the SSP. TAREG 3.7.1 clause a.2. — The System Security Group meeting with safety systems groups should include representatives for defence and contractors from operations, engineering, maintenance and occupational health and safety (WHS). During the procurement of aircraft, SSG should be established as soon as possible after the signature of the contract and before the start of the project activity. An SSG in service should be established before the award of the Australian Military Type Certificate (AMTC) and the release of the service (SR). SSG's primary objectives in use are: to enable key internal and external experts (technical and operational) to discuss the dangers and their mitigation options;to review the status of the SSP; including the results of technical or operational relevance risk assessments;compressing hazard analyses, including identified problems, resolution status and residual risk;develop and/or confirm system safety requirements and criteria applicable to the SAA;proactively identify safety programmes and platform deficiencies; and make recommendations for preventive action or re-emergence as applicable;allow for agreed mitigation of hazards as soon as possible; iprovid commonwealth governance with consensus recommendations on hazards and security issues. SSG's objectives for aircraft procurement and major modification projects are similar to those outlined above, but have been adapted to focus on early identification and management of new design issues that may affect safety. See System Security Guidelines Material in key documents on the DGTA - ADF website or System Safety Guidelines on the DGTA – ADF System Security Tools website for relevant guidance. SSG is particularly useful for obtaining agreement on specific hazard mitigation strategies where only qualitative data and subjective opinions are available. For example, mitigating some hazards requires either a technological constraint or a compromise on mission effectiveness, so that further mitigation of the risks to achieving the required HRI is not or not militarily desirable. Each of these hazards requires different levels of involvement oversight by the OEM, DAR, TAR and OAAR that depend on potential solutions, their military usefulness and the residual risk in a compromise that any delegate is willing to maintain. The DAR may authorize an appropriately educated system security professional, usually a system security manager, to chair the SSG. The Chair shall assign all action items and confirm the accuracy and completeness of the minutes of the meeting. The DAR must approve the minutes of the SSG, regardless of who chairs the meeting. TAREG 3.7.1 clause a.3. — Safety Assessment Report The Safety Assessment Report (SAR) is a comprehensive evaluation of the security risks assumed before the ADF system is operating, usually through the SFP or AMTC edition. It comforts the design and procedural hazards that may be present in the system and the specific procedural controls and precautions to be observed. TAR cited standard and time. THE SAR should be produced in accordance with the current version of the DI-SAFT-80102 website – Safety Assessment Report, which is available in the System Security Guidance Handout under Key Documents on the DGTA website - ADF or System Security – templates and examples on the DGTA – ADF System Security – Community of Interest website. The Sar template, adapted to the context of the ADF, is also available on these websites. For aircraft procurement and major modification projects, SAR must be produced before applying for a Special Flight Permit (SFP) and/or Australian Military Type/Type Supplements (AMTC/STC) type certificate. During the lifecycle phase of the aircraft in service, the SAR must be updated to remain autan, so that the Commonwealth remains oglynent for retaining significant risks. At the very least, the SAR should be updated and presented as part of a submission to the Annual Airworthiness Board (AwB), in order to facilitate an informed and independent review of any significant risks retained by the Commonwealth.Safety Case Report. The Security Case Report (SCR) can be used instead of sar. The SCR is a well-reasoned summary document detailing what the original objectives of the SAA were in relation to what was actually achieved, namely the assessment of compliance and risk analysis (with recommendations) of differences, namely sar. TARGE 3.7.1 clause a.4. — Hazard Log TAR specified standard. Hazards should be monitored throughout the aircraft's lifecycle, using a closed loop hazard monitoring system or a database of any identified hazards and their associated risks, i.e. hazard logs. Any hazards identified during the SSP analyses, whether during initial design or management in the service, should be added to the Hazards Log, making it a historical document for closed hazards and a status document for workplace hazards. The hazard log may record information on range of topics or topics considered useful for and risk management purposes. The following information should be identifiable in the hazard log:Unique identification reference points. A brief title that captures the nature of danger. Assign responsibility for hazard treatment. Current probability, severity and accompanying HRI. Confirmation that the risk has been maintained at the appropriate level, in accordance with HRI criteria (including correspondence). TAR has set a time. For aircraft procurements, a hazard log should be created before a preliminary design review and updated as soon as possible once any hazard has identified or changed status. For aircraft entering service, any hazards that have residual risk within the record of the dangers of acquisition must be eased to the responsible agency/agencies in service to ensure that the dangers in service are managed. TAREG 3.7.1 clause a.5. — Residual risks The level of the body required to accept the residual risk shall be proportionate to the remaining level of risk. BERs should not accept/retain a significant risk (see Definition Glossary) greater than MEDIUM. Significant risks of SERIOUS and HIGH gifts and usually through TAR should be addressed to the relevant Operational Authority, i.e. OAAR/OAA, in accordance with the SSPP approved by TAR, for treatment. The use of the release document is an appropriate mechanism for capturing and communicating risk treatment if tar and OAAR/OAA decisions are required. TAREG 3.7.1 clause b. — Residual risk detection The residual risk is described as a residual permitted or system risk after taking appropriate engineering or management measures to eliminate or reduce risk. Keep on having at all the note that the decision not to serve risk results in the residual risk being the same as the initial risk. The residual risk may be maintained if operational priorities so lay down. If the approved designs contain residual risk (technical and WHS), this must be disclosed to sponsor AEO DAR in order to allow accurate and timely communication with operators and potential further risk treatments. The level of residual risk to be maintained at all times is the decision of the risk retention authority and should not be assumed. This requirement applies to all AEOs that carry out design approval. Examples of eligible compliance means Senior design engineers and design acceptance representatives may use the following list to determine the degree of compliance and maturity of their SSP: Any hazard identification, analysis and/or management activity carried out by commercial or contractor AEO on behalf of an organization not sponsored by TAR is approved by the sponsor of the AEO's SDE. Processes have been defined to identify changes in system security procedures that require tar re-approval. These processes should provide authorisation for identified requested before the new procedure is used. A procedure is defined to ensure that system safety procedures are reviewed at least every two years. The degree of rigour associated with identification activities should be proportionate to the potential impact of the design change on technical airworthiness. All identified hazards shall be analysed by a method approved by tar and the justification for the likelihood and allocation of consequences has been documented. The System Security Group (SSG) or its equivalent meeting may identify the shortcomings of the platform for further analysis. SSG, or its equivalent meeting, reviewed the results of technical or operational risk assessments of relevance or importance. The AEO conducted a meeting or group of meetings to allow key internal and external topic (SME) (technical and operational) experts to discuss the dangers and their mitigation options. The SSG or its equivalent meeting should include the following permanent members: a representative for the acceptance of the design; System Security Manager (or equivalent);d uch U.S. intermediate health weapons system AEO (where appropriate for the construction of AEO and including contractors); Maintenance representative; iOperation Representative. SSG, or equivalent meeting(s), reviewed and identified shortcomings related to system security processes that can be used within the AEO. An SSG or equivalent meeting develops and confirms changes in system security processes. An SSG or equivalent meeting is chaired by a DAR or an authorized delegate. SSG summed up and reviewed significant hazard analyses, including identified problems, hazard resolution status and residual risk. Processes are defined to ensure that the

Annual Airworthiness Board is provided with a Safety Assessment Report (SAR). Sar provides a comprehensive assessment of the security risks assumed during the operation of the system. Sar is comforted by the new project and/or procedural hazards present in the system and the specific procedural controls and precautions to be followed. The SAR includes a concise, easy-to-read list of significant risks taken during the operation of the system. Sar provides all precautions or procedural controls necessary to treat significant risks during the operation of the system. A hazard monitoring system is implemented that records the following for each hazard identified with a valuable level of risk and/or extraordinary mitigation:Unique Hazard Identification Reference Number,Short title recording nature of the hazard,Allocation of responsibility for hazard treatment if there are extraordinary mitigations,Current probability, severity and accompanying hazard risk index (HRI) or level of risk, and The need to maintain the risk in accordance with the approved risk criteria (must include correspondence and the date of risk HRI and risk retention matrices used to classify the likelihood, weight and hazard risk retention authorities are proportionate to the configuration, role and operational environment (CRE) of the aircraft under consideration. Significant risks are defined. Processes are defined to ensure that any significant risks are readily accepted each year by the appropriate authority in accordance with the approved risk retention matrix. A risk retention body has been defined for all combinations of severity and likelihood of danger. The level of risk associated with each hazard is initially accepted by the appropriate risk retention authority in accordance with the approved risk retention matrix. Matrix.