

Tornado

Safety Case Report

Issue 1 (v1.0)


File Reference: ES(Air)Wyt/595570/3/2/18 Tor IPT

Issue Date: March 04

TORNADO IPT SAFETY CASE REPORT


Prepared

{Original Signed}
2nd Jul 04


C1
Tor ESM 2


Agreed

{Original Signed}
2nd Jul 04


B2
Tor ESM

Approved

{Original Signed}
2nd Jul 04


Air Cdre
IPTL

EXECUTIVE SUMMARY

In accordance with the requirements of JSP 553 and associated departmental guidance, initial safety cases have been established for the overall management of aviation safety of the Tornado weapon system and the Military Aircraft Release (MAR). Together, these two safety cases show the management provisions and controls that are in currently in place to address the totality of risks inherent in the design, support and operational use of Tornado under peacetime conditions.

This document sets out the baseline safety cases. Annex B provides a high level view of the factors, processes and evidence relating to the operation and use of the Tornado Weapon System. Annex C documents the safety case underpinning the MAR and Release to Service (RTS). The annexes also contain references to available evidence and management procedures. Work is ongoing to finalise those remaining areas where management arrangements are still being clarified and documented. These areas are summarised in Annex D.

The safety cases will be progressively updated and maintained to respond to system and management changes. This will assure that there is effective capture and documentation of the basis upon which the Tornado Safety Management Panel (TSMP) ensures that all regulatory requirements are met and that risks are maintained As Low As Reasonably Practicable (ALARP).

The safety cases have been compiled using the Goal Structuring Notation (GSN) technique and the evolving standards are to be maintained using the Adelard Safety Case Editor. Tor ESM 2, the Tornado IPT Safety Manager, will control the authoritative versions of the safety cases.

On the basis of the safety case representations of annexes B and C it is judged that the safety management of Tornado is being undertaken in accordance with UK regulatory and procedural requirements. It is thus considered that there is a valid safety case for the continuing operation of the Tornado Weapon System in accordance with its established and evolving safety management systems.

CONTENTS

EXECUTIVE SUMMARY	3
AMENDMENT RECORD	4
REFERENCES	6
ABBREVIATIONS	7
INTRODUCTION	
Background and Purpose	8
Description and Boundaries	9
Concept and Methodology	9
SAFETY CASE STRATEGY	
Safety Argument and Justification	10
Risk Assessment	11
Mitigation and Safety Management	12
SAFETY CASE MANAGEMENT	
Ownership and Control	13
Baseline Status and Finalisation	13
- Tornado Safety Case	13
- MAR Safety Case	14
SAFETY STATEMENT	14
Annex A - Goal Structured Notation	A -1
Annex B - Tornado Safety Case	B -1
Annex C - Military Aircraft Release Safety Case	C -1
Annex D - Summary of ongoing developmental areas	D -1

REFERENCES

- A ES(Air)Wyt/595570/4/18 Tor IPT - Tornado Equipment Safety Management Plan
- B JSP 553 (previously JSP 318B)
- C Defence Standard 00-56.
- D Business Procedure BP 1201, Equipment Safety Management.
- E Mil Std 882
- F DERA/AT&E/CA/CR0854/1.0 - Safety Case Report Tornado Military Aircraft Release *NOTE: This was subsequently updated to issue 2 (Reference: QinetiQ/AT&E/CR00262/2.0)*
- G DERA/AT&E/CA/CR0853/1.0 - Safety Programme Plan Tornado Military Aircraft Release *NOTE: This was subsequently updated to issue 2 (Reference: QinetiQ/AT&E/CR00263/2.0)*
- H QinetiQ/AT&E/CR01752/1.0 - Goal Structuring Notation (GSN) Representation of the Tornado IPT's Whole Aircraft Safety Argument - Summary Report

ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
AOA	Aircraft Operating Authority
ASCE	Adelard Safety Case Editor
CSA	Customer Supplier Agreement
GSN	Goal Structuring Notation
IBA	Internal Business Agreement
MAR	Military Aircraft Release
NATO	North Atlantic Treaty Organisation
RTS	Release to Service
RTSA	Release to Service Authority
Tor IPT	Tornado Integrated Project Team
TSMP	Tornado Safety Management Panel
US	United States

INTRODUCTION

Background and Purpose

1. The Tor IPT has direct responsibilities for the safety of the design and engineering support for all Tornado variants. Further details on the current standards of aircraft in the active fleet may be found in Reference A. In partnership with the Release to Service Authority (RTSA) and Aircraft Operating Authority (AOA) the IPT exercises a co-ordinating management role for the totality of Tornado Aviation Safety, via the TSMP.
2. In discharging these responsibilities, the Tor IPT is committed to the implementation of a safety management approach consistent with the requirements of References B, C and D. Implicit to these requirements is the need for the generation and maintenance of a safety case to demonstrate that the equipment remains tolerably safe, within the conditions set out in the MAR. Departmental safety requirements also require evidence to show that the broader risks inherent in the operation and control of Tornado aviation are maintained at levels consistent with ALARP criteria.
3. In common with many other legacy platforms, Tornado was developed and cleared for service use via a procedural route to certification. As a NATO programme, many of the procedures were based upon US practice rather than those of UK. Much of the approach to safety management was derived from Reference E. Accordingly, the tri-national contracts for post design support contain no provision for the designers to produce or maintain formal safety cases, even for ongoing design changes. To date, neither the German nor Italian MoD have indicated the intent to adopt UK's safety case approach. Management of qualification, airworthiness, safety and flight certification is co-ordinated by NETMA, the tri-national management agency, on behalf of the design approval and airworthiness authorities of the partner nations.
4. In view of the above, the Tor IPT has derived a safety case approach that can be taken forward as a UK only activity. Thus, in the UK the safety case can be maintained without compromise or conflict with the established tri-national certification and clearance procedures. Where appropriate, supporting evidence is drawn from the NETMA managed baselines, but provision is also made to accommodate clearance activities that have been undertaken on a UK only basis and to incorporate the legacy from earlier DPA clearance standards.
5. The safety case has been established by a detailed and systematic analysis of established project processes and practice to capture the basis on which all clearances are established and maintained. It embraces the entirety of the support and engineering authority roles. The safety case also shows the broader management provisions and controls, external to the IPT, which are in place to address the totality of risks inherent in Tornado aviation and operational use under peacetime conditions.
6. This document provides a view of the baseline safety cases from which all future changes will be captured and documented. Annex C provides a broader view of the factors, processes and evidence relating to the operation and use of the Tornado Weapon System. Annex D provides a breakdown of the safety case underpinning the MAR and RTS. Taken together, these two complementary views of the project safety management arrangements are intended to show the integrity, completeness and consistency of the many inter-related processes and procedures.
7. The safety cases will be progressively updated and maintained such that they can support IPT management decisions. They will thus provide a continuing record of the basis

upon which the TSMP ensures that all regulatory requirements are met and that risks are maintained to an ALARP standard.

Description and Boundaries

8. At this initial issue, the safety case addresses the safety of RAF operations, in peacetime conditions, in accordance with the clearances as set out in the Release to Service. It embraces the F3 and GR4 clearance standards, as set out in the respective Release to Service statements. The safety case encompasses the entirety of the weapon system (aircraft, weapons, ground support infrastructure), together with the operating personnel, base infrastructure and information systems and the broader environmental factors that have an effect on, or may be affected by the weapon system. However, the safety case does not yet embrace:

- The safety of contractor flying under MoD control or regulation,
- Operation outside the RTS (e.g. with SDs approved by Commandant Air Warfare Centre) or operations in conditions, where there are hazards above and beyond those of the peacetime environment.
- The safety of flying under NETMA/Panavia procedures.

9. In encompassing the full spectrum of activities that contribute to the safety of use of Tornado in RAF service, the safety case seeks to capture and represent the contributions of all safety stakeholders. However, primary attention has been given to the Tornado IPT, RTSA and AOA as the major safety management stakeholders. The contributions of other parties are shown via the management inputs or safety products that they provide. For baseline issue, priority is given to the definition and documentation of the IPT safety role, such that some aspects of the RTSA and AOA roles are not yet fully developed. These areas will be addressed further as part of the ongoing maintenance of the safety cases.

Concept and Methodology

10. The need for safety case development was first identified and defined in late 2000, following the Tor IPTs earlier assumption of management responsibility for the GR1/4 and F3 variant MARs in late 1999/early 2000. The initial task involved the evaluation and scoping of the regulatory requirements together with evaluation and preparatory work. This established the optimum project approach and the availability of supporting safety rationales, based upon the established project processes, procedures and evidentiary records.

11. Working in concert with the then Defence Evaluation and Research Agency, a MAR safety case concept was developed and documented (Reference F). A parallel programme of work was also defined to address a number of potential deficiencies in the management arrangements (Reference G). Following a review and endorsement of the safety case concept and programme plan, a joint programme of work commenced to address the outstanding issues and uncertainties. A series of tasks were placed on QinetiQ to provide support and advice on the development, documentation and maintenance of the safety case. This enabled the safety case to be produced in parallel with the IPT documentation and implementation of changes to project safety and MAR management processes.

12. At an early stage, it became apparent that documentation and maintenance of the safety case in basic Word format would be cumbersome and inefficient. It was thus decided that a more appropriate approach would be to use goal-structuring techniques for the ongoing evaluation, capture and maintenance of the underpinning safety arguments and evidence. At the same time it was recognised that the MAR Safety Case did not embrace all aspects of the Tor IPT contribution to aviation safety. It was also recognised that the full

spectrum of responsibility of the TSMP could best be captured and documented by use of a conceptual Whole Aircraft Safety Case. This needed to define the respective roles, responsibilities and management contributions of the IPT, RTSA and AOA. Examples of these two complementary goal structured safety cases were subsequently considered and endorsed by the TSMP. These were subsequently refined and documented in GSN representations of the safety arguments (Reference H).

13. A final phase of work has developed these two safety argument representations into GSN representations of the actual safety cases. These have been compiled using the Adelard Safety Case Editor (ASCE) and contain references to available evidence and management procedures. Work continues to finalise the project safety management arrangements and to document management systems for the airworthiness audit trail,

14. The GSN safety cases, are summarised in annexes B and C and constitute the substantive baseline from which the IPT will assess and control ongoing changes to design and management arrangements. For readers new to the GSN methodology, a simple introduction to GSN is provided at Annex A. However, it is important to note that whilst Annexes B and C provide a view of all the information contained within the GSN safety cases, the annexes are produced by exporting from ASCE. They thus exhibit some limitations of capture and representation of complex safety argument in document format. The annexes provide a comprehensive record of the baseline, for reference purpose, but should not be read as text documents. Detailed review and analysis of the safety case should always be based upon the source ASCE GSN files.

SAFETY CASE STRATEGY

Safety Argument and Justification

15. For the overall Tornado safety case (documented at Annex B), the argument is structured such that satisfaction of the top-level claim that "MoD operations of the Tornado operational weapon system are acceptably safe" can be demonstrated providing that:

- All components of the weapon system and its project specific support infrastructure are controlled such that they can be used with appropriate safety
- Safety management arrangements are such that the weapon system is only used with appropriate safety
- Safety management arrangements ensure that the interfaces between the operational weapon system and the broader environment are acceptably safe and that the effects of the operating regime are controlled
- Tri-national support arrangements for safety and airworthiness are consistent with UK needs and appropriately supported
- There are comprehensive and co-ordinated Project Safety Management Systems to ensure that all risks remain ALARP

The overall argument is underpinned by a further claim that in-Service experience confirms acceptable system safety which draws upon the extensive flight experience of Tornado in UK, German and Italian service use and the sound safety record.

16. The overall safety case is also supported by a complementary MAR safety case (documented at Annex C). This safety case seeks to capture and document the legacy and predominately implicit safety case that underpins the safety of the Tornado MARs. Hence the top-level claim has been chosen to be that the "Tornado MAR supports safety and airworthiness of the defined weapon system during RAF service use" can be demonstrated providing that:

- Weapon system design standards are appropriately safe
- Appropriately safe weapon system clearances are recommended for inclusion in the Release to Service
- Comprehensive instructions and advice to users and support staff is maintained and promulgated
- Management systems ensure the integrity of the MAR and its supporting safety case
- In-Service safety performance is monitored, failures investigated and MAR improvements identified and actioned.

The MAR safety case also provides a high level representation of how the MAR supports the RTS and contributes to the RTSA safety case for that document.

17. Much of the safety argument is based upon legacy evidence, process and practice, as derived and employed in the course of the development and production phases of the project. However, the continuing integrity of the safety cases now hinges on the effectiveness of factors such as risk assessment, mitigation and management. These provide the focus of the ongoing project safety activity.

Risk Assessment

18. The assessment of risk is derived from many sources and must be constantly reviewed and updated to ensure that it remains consistent with the current designs, operating practices and environmental/operating conditions.

19. Knowledge of Tornado risks is founded upon the initial designer safety and reliability assessments that have been progressively amended and developed in the light of service arisings and the introduction of designer and service configuration changes. Comparable safety assessments have been undertaken in respect of all government furnished equipment (stores and weapons) and infrastructure, such that there is a comprehensive understanding of the risks associated with current in-Service weapon system configurations. Where appropriate the risks and safety assessments of non-aircraft equipment is documented and promulgated via complementary safety cases, such that they underpin those of Tornado.

20. Whilst there has been a progressive development of the risk assessment, the more recent need to extend the life of Tornado beyond its original 4000 flying hour design requirement, has necessitated a rigorous re-appraisal and in-depth analysis by the Panavia partner designers to establish the potential for life extension. This, in turn, has revised and revalidated the initial design assessments. In a parallel activity, BAES has undertaken to develop an updated loss model that can inform company and IPT evaluation of risks for the remaining life of the aircraft.

21. At the platform level, the cumulative risk of Tornado operations is judged against the original design safety objectives and current UK airworthiness criteria by monitoring the RAF and other operator loss rates due to technical and all causes. As an interim measure, the TSMP has directed that the airworthiness standard (technical causes loss rate) must be managed such that the loss rate does not exceed 2×10^{-5} per flying hour. This reflects a need to maintain the high safety standards that have been achieved in the past 20 years of RAF Tornado operations (over one million flying hours). A comparable aviation safety target (all causes loss rate) is planned when further direction is available from the Defence Aviation Safety Board or the Defence Aviation Safety Centre.

Mitigation and Safety Management

22. Effective risk mitigation comprises a major element of the safety case and requires a broad spectrum of activities to be undertaken by all safety stakeholders. The legacy project arrangements included robust practices that embraced:

- Control of Clearances and Limitations via the MAR and RTS
- Maintenance of comprehensive user instructions and guides via Aircrew and Engineering Publications
- Assessment and management of Human Factors Integration by Designer, QinetiQ and Operational Evaluation Units
- Monitoring, investigation and rectification of in-Service events and arisings via answering, defect, incident and accident procedures
- Ageing Aircraft and Fleet Management via IPT (Structural Integrity Working Group), and IPT/AOA fleet management plans
- Monitoring and control of operating conditions via the Tornado User Working Group and Statement of Operating Intent and Usage
- Control of design, certifications and flight clearances via NETMA/Panavia/Turbo Union procedures
- The control of GFE by other IPTs
- Compliance with RAF Safety Management Systems

23. In the course of the initial safety case analysis, it was recognised that in spite of these sound procedures and practices the activities of each stakeholder were largely undertaken on a standalone basis. Co-ordination of activities was rather limited, often related to ad-hoc reviews, necessitated by the issue of MAR or RTS updates, or the response to significant in-Service arisings. It was recognised that significant improvements could be achieved by introducing a greater degree of structure and co-ordination to the management of the safety activities. This would require the interchange of safety information between the stakeholders and provide for improvements in the analysis, interpretation and potentially the mitigation of overall risk. Accordingly, in parallel with the development and documentation of the safety case, activities were put in hand to:

- Establish a Tornado Safety Management Panel to provide a forum for all safety stakeholders
- Document and promulgate Safety Management Plans for the IPT and RTSA
- Formalise working relationships between the safety stakeholders via IBAs and CSAs
- Establish a formal hazard management system for the project and develop a Tornado Hazard Log, under IPT co-ordination and control, for access by all stakeholders. Once completed, this system will include objective project safety targets, Hazard Risk Indices and ALARP criteria tailored to the specific requirements of the Tornado platform and through life plan
- Develop Software Safety Management Plans

Significant progress has been made in each of these areas, but work will be ongoing for some time to fully complete and document the arrangements. The ongoing work is defined and managed via the IPT's Safety Programme Plan, which is maintained and controlled by Tor ESM2. Activities relating to the plan are recorded in file reference ES(Air) WYT 595570/3/2/19.

SAFETY CASE MANAGEMENT

Ownership and Control

24. The safety cases are owned, controlled and maintained in accordance with the arrangements as set out in Annex G to the Tornado Equipment Safety Management Plan (Reference A). This will be a continuing activity for the remaining service life of the platform.

Baseline Status and Finalisation

25. Whilst work on the safety management arrangements and safety case will continue for the remaining life of the Tornado project, progress has now reached a stage where it is possible to establish and document a meaningful safety case baseline. This will inform and underpin all future safety activities and decision making.

26. For the reasons explained above, it should be recognised that in documenting these baseline views of the Tornado and MAR safety cases certain aspects of the supporting argument and evidence are yet to be fully developed and finalised. The current status of each safety case can be summarised as follows:

Tornado Safety Case (See Annex B)

27. For the purposes of the baseline exercise, priority has been given to documenting the spectrum of Tor IPT safety activities within the broader framework of RTSA and AOA safety responsibilities. Together, these constitute the totality of departmental safety responsibilities relating to the aviation safety of Tornado. The baseline has been developed primarily using IPT and QinetiQ inputs and resources and, as yet, may not fully reflect the totality of the RTSA and AOA roles. Further development and population of these areas of the safety case will be undertaken as the stakeholder management arrangements and systems are implemented. The safety case may also need to be reviewed and refined as the Defence Aviation Safety Management System is progressed by the Defence Aviation Safety Centre, under the direction of the Defence Aviation Safety Board.

28. Development of the safety case is ongoing in a number of areas that include:

- a. Extension of the safety case to include the operation of development aircraft under MOD regulation and control, export and lease arrangements and flying on operations.
- b. Definition of objective safety targets
- c. Completion and documentation of supporting management system references and working arrangements
- d. Definition of ancilliary equipment standards such as rigs, AGE, GFE and training aids
- e. Personnel management arrangements
- f. AOA management practices and systems
- g. Obsolescence and life extension
- h. Environmental safety and management of hazardous materials
- i. Safety and Hazard analysis

Further details on this ongoing work can be found at Annex D.

MAR Safety Case (Annex C)

29. The MAR Safety Case has been documented within the context of a higher-level safety argument that seeks to demonstrate the safety of the RTS. For the purposes of this baseline exercise, the argument and evidence of the broader RTS safety challenge are developed only to a conceptual level. They need to be further developed, verified and validated by the RTSA, as the responsible owner of the RTS Safety Case. Whilst much of the safety case is now in place some further work remains to be completed in a number of areas. This includes:

- a. Identification of the IPT/RTSA CSA and RTSA safety targets
- b. Identification of outstanding management process and document references
- c. Development and documentation of inter IPT management arrangement via the TESMP
- d. Justification that test facilities, planning aids, ground test software, miscellaneous ground support items and technical publications are appropriately safe
- e. Arrangements for Independent Safety Audit and safety reviews
- f. Data management and back-up systems

Further details on this ongoing work can be found at Annex D.

30. The above areas of development of the baseline safety cases form part of the safety programme plan for Tornado, under the control of Tor ESM 2 as Tornado Safety Manager.

SAFETY STATEMENT

31. Although the above paras show that there are many areas where work is ongoing and that some further clarification or documentation of the safety case is required, a substantial part of both the overall Tornado safety case and its supporting MAR safety case has now been carefully evaluated and captured. The work to date has shown that whilst the legacy project has pursued largely a process and procedural route to airworthiness and safety, the approach at aircraft platform level was sound and comprehensive. Where weaknesses have been exposed these have been primarily concerned with the management of interfaces e.g. with Government Furnished items and activities and the failure to document some process and practice. Many of these shortcomings have already been addressed and there is an ongoing programme of work to correct the remaining weaknesses.

32. No evidence has been uncovered of fundamental weakness or failures in the overall management approach and the project has established a demonstrably safe record in service, spanning over 20 years. This encompasses more than 1.2 million flying hours of RAF operations and more than 1.1 million flying hours with other partner nations.

33. The safety case representations of annexes B and C provide an explicit representation of the projects legacy and implicit safety case. In concert with the in-Service safety record they are judged to provide a satisfactory demonstration that the safety management of Tornado is being undertaken in accordance with UK regulatory and procedural requirements. It is thus considered and that there is a valid safety case for the continuing operation of the

Tornado Weapon System in accordance with its established and evolving safety management systems.