NATO STANDARD

ADMP-01

GUIDANCE FOR DEVELOPING DEPENDABILITY REQUIREMENTS

Edition B, Version 1

MAY 2022

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED DEPENDABILITY MANAGEMENT PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)
©NATO/OTAN

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

4 May 2022

1. The enclosed Allied Dependability Management Publication ADMP-01, Edition B, version 1, GUIDANCE FOR DEVELOPING DEPENDABILITY REQUIREMENTS, which has been approved by the nations in the LIFE CYCLE MANAGEMENT GROUP (AC/327 LCMG) is promulgated herewith. The recommendation of nations to use this publication is recorded in STANREC 4174.

2. ADMP-01, Edition B, version 1, is effective upon receipt and supersedes ADMP-01 , Edition A, version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database ((https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60.

Dimitrios SIGOULAKIS
Major General, GRC (A)
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1. GENERAL

1. Dependability is a key characteristic of all items[1], having a direct impact on mission performance and thus mission success. The dependability characteristics of any item are inherent in its design, thus dependability should be considered from the very beginning of the pre-concept stage and be continued, in a disciplined manner, throughout the whole life cycle by the implementation of dependability disciplines as described in the IEC 60300 series standards referenced at Section 1.4 in this document.

2. Dependability is the collective term describing the continued and safe operation of any simple or complex item. The factors that influence the dependability performance of any item are reliability, maintainability, availability, testability, maintenance, and safety. In most items, reliability and maintainability are the key performance characteristics of interest as they have a direct impact on mission success and life cycle cost. The logistic and maintenance strategy of the item are mainly external, but can have significant impact on its availability performance, as it reflects the ability to provide the necessary resources to implement optimised maintenance procedures developed and refined through the life cycle of the item.

3. In the same way as all other performance characteristics defined in procurements, those relating to dependability need to be properly researched and considered in order that they can be specified in a coherent way to deliver the required levels. This is achieved through specifying specific availability, reliability, maintainability or other related requirements and recognising that a change to anyone can have significant knock on effects on any or all of the others and the overall dependability of the item. These requirements need to be realistic for the type of item that is under contract, specific and measurable in a way that can be achieved within the time available and without adversely impacting the overall affordability of the project. It is important to ensure that requirements are flowed down to sub-components of the item in a coherent and balanced way so that a full understanding of the dependability characteristics can be derived. Whilst it is fully recognised that the lives of military personnel may be reliant on the item continuing to work successfully, it is important to ensure that these requirements are not over specified. Setting requirements for 98% reliability or 99% probability of surviving a 48-hour mission is likely to drive up costs significantly and it may be that a lower figure will have little real impact on the operational tempo and could be much more achievable and affordable.

4. It is important to recognise the difference between a requirement and a target or goal, terms which have very different meanings yet are often used in specifications without apparent recognition of the consequences. A requirement is something that is essential to successful operation of the item and should not be traded without full consideration of the consequences and agreement of all stakeholders. The supplier will need to provide evidence to substantiate that the requirement has been met, or where it cannot be met, evidence in support of the request for a relaxation and why it is not now felt that the agreed specification cannot be met. A target or goal is something that is considered nice to have but not essential and often traded

[1] Item includes systems, equipment, be it hardware or software based, and services.

out when costs are rising and attempts are being made to keep the procurement within the original agreed cost profile.

5. The levels of availability, reliability, maintainability and hence dependability that are achieved by an item are very dependent on the conditions under which that item is utilised, often described as its Mission or Usage profile, but referred to in NATO documents as the Life Cycle Environment Profile (LCEP). As an example, item on anti-vibration mounts in an air-conditioned room maintained at 25 Celsius is much more likely to operate without incident than an identical one mounted on a wooden pallet under canvas in a dusty environment where the ambient temperature can fluctuate from -5 to +45 Celsius. For the remainder of this document the NATO term of Life Cycle Environment Profile (LCEP) will be used.

6. Therefore, when specifying requirements for any of the dependability characteristics, it is necessary to define the conditions of storage, transportation, installation and use that will be encountered by that item. It may also be necessary to take account of the anticipated maintenance policy, the area in which that maintenance will be undertaken and the skill levels of the persons undertaking it. A maintenance action that is relatively simple in a purpose-built facility can become extremely difficult under operational conditions.

7. The human impact also needs to be considered and items should be designed to minimise the chances of human errors impacting on dependability performance. Wherever possible tasks that can be automated should be in order to eliminate the risk of human error and where the user is required to provide input care should be taken to ensure that if mistakes do occur, they do not have a significant effect on mission performance. With the increasing complexity of items, action that needs to be taken in the event of a failure to perform the required function should be clearly identified to ensure the user does not exacerbate the problem.

8. All items will exhibit some level of dependability, but it is likely that those produced by organisations that do not actively manage dependability will not achieve the levels that are required by the military. To ensure the dependability of an item, it is essential that reliability and maintainability activities are planned and undertaken such that the item design is positively influenced and that this is verified at every stage of the design and production process. Early attention to dependability plans and allocation of appropriate resources is needed to achieve the desired requirements. An upfront investment in dependability design and construction through a dependability programme as detailed in IEC 60300-1 will always repay itself in terms of operating costs for the item, in the way it is trusted by military personnel who use and depend upon it, its ability to successfully undertake a mission and thus its overall availability to operational command.

1.2. PURPOSE

1. The purpose of this document is to provide guidance on developing dependability requirements. It will explain what needs to be considered for the dependability section of the acquisition specification and why it is important.

2. The functional analysis and the failure classification process are described in a dedicated ADMP (ADMP-03). Indeed, those processes are needed to establish dependability

requirements as well as to assess dependability during in-service life. ADMP-03 supports both ADMP-01 and ADMP-02.

3. It will address the common concepts and factors relating to all dependability requirements and then look at the individual characteristics detailed below in turn considering their applicability at each stage of the item life cycle as defined in the NATO Phased Armament Programming System (PAPS):

a. Availability

b. Reliability

c. Maintainability

d. Testability

e. Maintenance

f. Safety

g. Software

4. It is not intended that this document will provide a template from which all new requirements can simply be selected, nor can it give a step by step guide to cover every eventuality, but it will consider the concepts, issues and factors that influence how a requirement is set, give examples of the differing types of requirement and explain the benefits and pitfalls of each.

1.3. APPLICABILITY

1. The information in this document applies to all items whenever there is a need to develop and set a requirement at whatever stage it is in its life cycle, be it a brand new requirement, an incremental update, a midlife update, a re-design due to obsolescence or part of a spiral acquisition plan.

2. During any change to the item, be that hardware, software or in the way it is deployed and used, it is imperative to ensure that the dependability attributes are addressed or re-

addressed. It should be used by all members of projects and in service organisations including the various NATO agencies who are responsible for dependability.

1.4. NORMATIVE REFERENCES

A. ADMP-02 (B)(1) Guidance for Dependability In-Service.

B. ADMP-03 (A)(1) Guidance for Classification and Analysis of Dependability Events.

C. IEC 60300-1:2014 Ed. 3 Dependability management - Part 1: Guidance for management and application.

D. IEC 60300-3-10:2001 Ed1 Dependability Management Part 3-10: Application guide – Maintainability.

E. IEC 60300-3-15:2009 Ed. 1 Dependability Management Part 3-15: Application guide – Engineering of System Dependability.

F. IEC 60706-2:2006 Ed. 2 Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase.

G. IEC 60706-5:2007 Ed. 2 Maintainability of equipment – Part 5: Testability and diagnostic testing.

H. IEC 61124:2012 Ed. 3 Reliability Testing – Compliance Tests for constant failure rate and constant failure intensity.

I. IEC 62628:2012 Ed. 1 Guidance on software aspects of dependability.

J. ISO/IEC 25000:2014 Ed. 2 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE.

K. ISO/IEC 25010:2011 Ed. 1 Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models.

L. AAP-20 (C)(1) NATO Programme Management Framework (NATO Life Cycle Model).

M. AAP-48 (B)(1) NATO System Life Cycle Processes.

N. IEC 60050-192:2015 Ed. 1 International Electrotechnical Vocabulary – Part 192:Dependability.

CHAPTER 2 CONCEPTS AND FACTORS

2.1. LIFE CYCLE ENVIRONMENT PROFILE

1. The dependability characteristics that are achieved by any item are very dependent on how it is used. This is defined in a Life Cycle Environment Profile (LCEP) that is either an envisaged scenario based on current or previous experience, or a predicted pattern based on what the future use requirements are expected to be. However the profile is constructed, it is important to consider the following:

a. Period of time required – How long the item is required to be in a fully operational state, how long it is required to be in some sort of low operational or stand by state, how long it is expected to be switched off during the chosen period of interest including any transportation that may be required.

b. Number of repetitions – It may be that the LCEP covers only a single deployment, be that a 2 hour flight in the air environment, a 7 hour journey in the land environment, a 30 day embarkation in the maritime environment or an 8 hour working day in a training / office based environment. Other than for single use devices (missiles, ammunition etc.) it is very rare that an item is only required to achieve a single deployment, thus it is necessary to consider how many times it needs to be repeated over a given duration, what the allowable down time is between deployments and what maintenance and or repair activity is allowable to bring the item back to a ready state, including any extant safety requirements.

c. Loading - Consideration should be given to how heavily the item will be loaded and how often. Whilst the performance part of the specification is usually well covered in terms of maximum loading, what is often overlooked is how often that load will occur and what ‘recovery periods’ there will be between each occurrence.

d. Fall Back Modes – Many items these days have redundancy built in, such that failure of a single path or function does not prevent the item from continuing to provide the capability that is required of it. This must not be confused with fallback modes which are often built in to provide the user with a last resort should a catastrophic failure be encountered. The ability to manually carry out an activity when the automatic system has failed is something that should only be used on rare occasions and whilst there may well be a requirement for the item to have a manual fall-back mode it should not be considered when the LCEP is being generated.

e. Maintenance – All items will inevitably need to be taken down at some point for maintenance activity. This should be considered as early as possible in the specification process to ensure that the item that is being specified can provide the required capability. When considering the maintenance that will be required it is important to take into account where the maintenance is to be performed, the conditions in which maintenance may have to be performed, what information, tools and test equipment will need to be provided, what training will be required and the practicality of undertaking that maintenance particularly if it is required to be performed under operational conditions. Consideration should also be given to the need for maintenance during or after long-term storage or transportation. Section 3.5 of this document gives more details on maintenance specification.

f. Anticipated Fleet Size – When conducting fleet size assessments it is important to consider the reliability and availability of each item. Assuming that any item will be

100% available will lead to wrong assumptions about the total number required to provide the capability and will lead to periods of time when the capability is not available. As discussed in the previous paragraph if a capability is truly required 24 hours a day, 7 days a week, 52 weeks a year the fleet sizing calculations must take account of non-availability of assets.

2.2. BOUNDARY

1. When setting dependability requirements, it is important to remember that it is likely the item being considered will form part of a bigger system or be reliant upon some form of external stimulus in order for it to perform according to its specification. It is likely that the supply of these external stimuli will not form part of the contract for the item and that they will be assumed to be present when required. For this reason, it is important to ensure that the boundaries of the item that is being considered are clearly defined and all external stimuli that are required to be present are identified in the documentation, particularly if the item is part of a payment in respect of performance contract. These external stimuli can take many forms and may include external power, data from other items, the availability of externally managed and provided items or even existing items within the inventory which the item of interest will be required to work with. This can be a complex area to both understand and describe in such a manner that no ambiguity exists.

2. In order to function, most items require some form of external energy, the supply of which is often not included in its specification. In these cases it will be assumed that the required energy, within specified levels, will always be available and for the purposes of all dependability activity they will be excluded. Should any loss of performance occur which it can be shown was directly attributable to the external energy supply, be it over or under specification, then in the simplest situation those events will not be attributed to the item under consideration and any payment associated with its availability would not be withheld. However, it is common for the contract to include the requirement for the item to be protected from damage in the event of over or under specification energy being supplied or even the requirement for the item to have a built in energy source to ensure its continued performance for a period of time or orderly shutdown in the event of loss of the external energy supply. In these cases, the loss of any performance may be attributable to the item and any associated payment may need to be reduced or withheld.

3. As the example above demonstrates, ensuring that the boundaries are clearly identified in terms of sub-components and performance can be become a very complex task but the lack of a clear definition can lead to long and protracted discussions when trying to agree if an event is attributable or not, particularly where a payment is involved.

2.3. ENVIRONMENTAL CONSIDERATIONS

1. The dependability characteristics that are achieved by an item are very dependent on the operational environment in which it is used. Environmental factors are often specified as minimum and maximum values for operation with extended limits for survival. However it is specified, it is important to consider the following:

a. Environment – It is necessary to define the conditions the item is expected to operate in. Temperature is normally specified as a range but often no indication is given on how long the item is expected to operate at each end of that spectrum, or what the normal condition is anticipated to be. Consideration should also be given to specifying the extremes at which an item will be expected to survive in a non-

operational condition. Other factors, e.g. humidity, salinity, and dust contamination can also have significant effect on the dependability characteristics of the item and should be specified if they are to be encountered.

b. Terrain – It is also important to consider the terrain over which the item is likely to operate as this can place significant stress and strain on it. In the land environment this is likely to be an explanation the type of surface that will be encountered, the speed at which it should be accomplished and the amount of time it will spend on any particular surface. In the maritime environment, it is likely that this will be covered by the specification of sea states whilst in the air environment it is likely this will be covered by height above sea level whilst flying.

c. Access For Maintenance – If it is anticipated that any form of maintenance will be required during operation, then it is necessary to include a requirement that clearly articulates what maintenance is envisaged, to ensure the provision of access to allow that maintenance to be carried out and the provision of any necessary tools.

2.4. SUCCESS AND FAILURE

1. When specifying reliability, it is common and good practice to include requirements such as probability of mission success or probability of achieving a given period of time without encountering a mission failure. This pre-supposes that there is an understanding of what constitutes success and thus when failure has occurred i.e. when an item is no longer performing in a manner that is considered acceptable to the user. Whilst most item sponsors who are formulating the requirements will readily be able to define success it is much more difficult to define failure. Setting clear and agreed definitions of failure is an important step that is often overlooked during the specification of dependability requirements.

2. In the early stages, as the final design is unlikely to be known, failure definitions will be defined at a functional level. To enable this, it will be necessary to identify the functions that are essential for the item to perform its required mission, which will normally be recorded in a mission essential function list, typical examples being Move, Fight, Communicate, Protect etc. The next step would be to consider what level of degradation constitutes failure of each of those functions and thus the items ability to successfully complete its mission. Depending on the type and complexity of the item, the number of essential functions can differ, thus it may be necessary to consider which functions failure definitions will be developed for.

3. As the design progresses and the architecture that will provide each function is defined, the failure definitions should evolve such that the cause of each functional failure can be attributed to individual hardware or software components within the architecture. Further information relating to the development of failure definitions, the functional breakdown of an item, and the classification of dependability related events can be found in ADMP-03.

4. Whilst the concept of defining failure is easy to understand the reality of deriving and agreeing them is very different, particularly where failure is not clear-cut. Whatever the definitions are, they have to be agreed by all concerned and adhered to throughout all discussions associated with the item concerned. The following examples will attempt to show this:

a. A vehicle has a requirement to be able to undertake a 200 km journey, without interruption, and be capable of achieving 150Km/hr for the time it is on any major road. If the vehicle becomes immobilised for any reason then it is reasonable to assume that it has failed; but if, due to a malfunction within the vehicle, it is only

capable of achieving 145Km/hr then has the vehicle failed? If not, then at what speed is it considered that the vehicle is not fit for purpose and has failed? Similarly, if the vehicle suffers from a flat tyre which can be repaired within 10 minutes, would this be considered a failure?

b. An Information Technology (IT) system is required to provide office services for 1000 members of staff located across five floors in one building. The system is being provided under an availability contract with monthly payment depending on the number of failures the users experience. If a single user on one floor cannot access the network does this constitute failure of the IT system, or does a group of 10 or more users not having access constitute failure, or is failure not considered to have occurred until a whole floor does not have access? The failure could also be considered in terms of how long it takes users to recover a file from the network, to log on to the system, to launch an application, to access the internet or any combination of these events.

2.5. REQUIREMENTS VERIFICATION AND VALIDATION

1. As stated in the introduction it is important to ensure that all requirements which are set for the item can be shown to have been achieved. In the same way as for other performance requirements, dependability can be proven by test, but unlike many performance requirements a single test is often not enough to show that dependability has been achieved and their statistical nature requires many tests to be carried out to deliver the required level of confidence. This is generated through the provision of objective evidence in support of the claim that specified requirements have been fulfilled (verification)[2] or in support of the claim that a specific intended use has been fulfilled (validation)[3].

2. The number of, or length of tests required will depend on the level of statistical confidence that is considered acceptable, the higher the confidence required the more tests or the longer the test time that will be required, thus a robust test plan must be developed and included within the dependability programme and the main development programme for the item. It should be recognised that the dependability test plan is likely to require a lot of calendar time and can be a major driver in terms of overall development time. Thus, every opportunity to use other development tests to inform the dependability tasks should be taken.

3. Testing to prove that a reliability requirement has been achieved requires the production standard item to be run for a period of time, during which each failure is recorded and assessed for relevance. The achieved level of reliability is a function of the trial time completed combined with the number of relevant failures that occurred. The following examples demonstrate this:

a. An item has been operated for 1000 hours during which time 10 relevant failures have occurred. Statistical analysis based on the chi-squared model shows that this indicates a Mean Time Between Failures (MTBF) of 94 hours has been achieved to a 50% level of confidence, an MTBF of 80 hours has been achieved to a 70% level of confidence and an MTBF of 65 hours to a 90% level of confidence. See IEC 61124 for full details of chi-squared and other statistical models appropriate to reliability testing.

b. A contract has been let for the purchase of 50 single use items with a requirement that each item should achieve a 99% level of reliability to an 80% level of

[2] The definition of verification is taken from IEC 60050-192 derived from ISO 9000
[3] The definition of validation is taken from IEC 60050-192 derived from ISO 9000

confidence. In order to prove this it is necessary to complete 161 tests without a relevant failure occurring. Put another way, in excess of 3 times the number of items that are being purchased would need to be used to prove the reliability. This requirement is unacceptable and it would be necessary to either change the requirement to something that could be considered acceptable, by reducing the level of reliability its associated confidence, or by agreeing other methods of proving that the design is robust and reliable during the development and manufacture of the item.

4. Evidence can take many forms with the test results detailed above forming only one part of the overall evidence required to show that the requirements have been met. It is most likely that the dependability programme will require the evidence to be presented in the form of an assurance case, which builds over the life of the item, progressively delivering assurance that the item will be dependable. It is important to recognise that the case is not only a repository for results but is a vehicle to allow reasoned and auditable claims and arguments to be made about the dependability of the item.

5. The nature of dependability characteristics are such that many of them are often set as quantitative values where the proof of the requirement is provided by values measured during tests such as those outlined above. This type of requirement necessarily brings with it a structured mathematical process by which values are calculated and claims made based on them. Not all requirements have to be quantitative and where they cannot be measured will be set as qualitative. These types of requirements depend much more on the argument made that the evidence provided meets the requirement than the results of the tests themselves and can often be better expressed using formalised methods such as Goal Structuring Notation (GSN).

2.6. PROCUREMENT STRATEGY

1. It is important to ensure that any dependability requirements that are set reflect the procurement strategy.

2. If the item is expected to be supported using organic methods internal to the military, then it will be necessary to consider setting requirements that ensure enough spares are provided to the stores organisation and that maintainer training includes full coverage of failure diagnosis and repairs, including familiarisation with any special to type tools or test equipment.

3. If the item is to be supported by the contractor using a performance-based contract then it will be necessary to ensure that statements / requirements relating to response times, penalty clauses and agreements on what is and is not within the scope of the contract are included. It should be recognised that just having an overarching item availability requirement may not be enough to ensure that the item is available when it is required. If an item is required to achieve 99% availability over a year (8760 hours) then it can be unavailable for 87.6 hours during the year. Whilst it may be acceptable for the item to be non-operational for 1.5 hours a week,

having it non-operational for 48 hours at any one time may not be, even though both examples would exceed the requirement of 99% availability over the year if they were the only downtime.

2.7. TECHNOLOGY CONSTRAINTS

1. It is necessary to ensure that any dependability requirements that are set are consistent with the technology that it is anticipated will be used in the design. Cutting edge technology is often less dependable than technology that has been in use for a period of time.

2. If expectation is that the item will be software intensive, then setting a requirement for a Mean Time To Repair (MTTR) of 120 minutes may not be appropriate when the predominant failure mode is likely to be a software lock up which requires a 5 minute reboot to fix.

3. If an item is anticipated to have a special coating that takes 240 minutes to cure after application and which would need to be re-applied each time a fastening was removed for maintenance, then setting an MTTR of 20 minutes would most likely be inappropriate unless the cure time was specifically excluded from the time measurement.

4. Similarly, if the technology which it is anticipated will be used in the item has a history that shows it only achieves 1000 hours MTBF, then incorporating it into a design where it is vital it achieves 2500 hours MTBF is highly likely to lead to failure. In the military and security fields the performance requirements of the item need to be ahead of others, the technology that is being used is often new and unproven. In these cases it is necessary to review if the technology can achieve the levels of dependability being specified, recognising that a less reliable item may be more beneficial than no item at all.

2.8. EXTERNAL INFLUENCE

1. The dependability characteristics of a defence item can be significantly affected by decisions and changes in other areas, some of which are out with the control of the procurement staff. In the past, advances in technology were often influenced by the needs of defence but recently this has changed and technology advances are now very much driven by the commercial world. Environmental concerns also have an effect on what materials can be used in the construction of defence items and this can have significant effect on the eventual dependability characteristics.

2. Recent changes in environmental policy have required that the use of lead in items is stopped. As lead has been used in the construction of electronic circuit cards for many years, and was introduced into the process to suppress other issues that had been encountered, the latest legislation means other methods are now required to combat these issues and that the properties of electronics that contribute positively to dependability and were well known, now need to be researched and reviewed. In the interim, it is necessary to ensure that methods are in place to control lead free issues.

3. As referenced above, commercial industry is driving the change in electronics at a pace which means that many defence items are suffering from obsolescence issues before they even enter service. This requires considerable planning work to be done up front to ensure that spares issues do not cause unavailability of item. The reverse of this situation is that where defence has issues with technology, it is unlikely that industry will be willing to move things

forward as the total number of items affected is significantly less than that experienced in any commercial run of an electronic item.

4. The issues identified above are particularly relevant when considering Commercial-Off-The-Shelf (COTS) items, which also bring issues such as lack of design influence and a lack of understanding of the dependability characteristics that are likely to be exhibited in a military environment when compared to the commercial environment.

5. In some cases, existing military items will be an integral part of the design or will need to interface with the new design items. In these cases, the dependability characteristics of the final item will be influenced by the characteristics of those existing parts. If an existing item only has 90% reliability then any development that incorporates it can only ever achieve 90% reliability unless some form of redundancy is included in the design.

6. Communication Systems can rely on commercial items to provide ‘routeing’ or other handling, often on a cost by the hour basis. In these circumstances, the military have very little influence over how and when maintenance is conducted or the overall availability of the service. In these cases, the dependability requirements of the military item will need to take account of the parts that are outside of military influence or control.

2.9. COST CONSTRAINTS

1. It is always necessary to consider that any dependability requirements may need to be reviewed against the overall budget for the item. To achieve high levels of dependability can be costly, and it is likely that a balance between cost and dependability will have to be made.

2. An item that achieves higher levels of reliability will intuitively require less maintenance and less spares through its life; thus investing more during the design stage to improve reliability can lead to lower life cycle costs, however this can be very difficult to achieve and prove. It should also be recognised that the cost of achieving reliability often increases in an exponential way thus achieving the last few percentage points of a requirement may not provide good value for money.

3. One of the acknowledged ways of increasing reliability is to add redundancy by increasing the number of sub-components contained within an item. Although this will reduce the number of mission failures, the number of sub-component failures will increase thus the number of spare parts, the amount of maintenance required and the life cycle costs will also increase.

CHAPTER 3 DEPENDABILITY CHARACTERISTICS

3.1. AVAILABILITY

1. Availability is defined[4] as 'ability to be in a state to perform as required' and is a measure of the time the item is in an operable state when compared to elapsed calendar time so in its simplest form can be represented mathematically by the formula

$$\frac{Uptime}{Totaltime} \text{ or } \frac{Uptime}{Uptime + Downtime}$$

2. As defence contracting moves from the traditional approach using organic support towards performance based contracts, Availability is becoming the most commonly used characteristic when defining dependability requirements. As will be shown later on there are differing types of availability, some of which are easy to define and calculate values for and others which, whilst easy to define, are much harder to calculate or measure values for. There are also many ways to break down and specify availability be it for an individual part within an item, the whole item or a number of items either at the fleet level or at some operational unit level.

3. As described earlier in the document under the procurement strategy heading, care must be taken when specifying availability to ensure that the achieved level of availability actually delivers the capability that the user anticipated. No availability requirement can ever be 100% as failure will always occur at some point in time and whilst the design can be such that most failures can be mitigated through redundancy or alternate methods of service provision, the cost of mitigating against those 1 in 100,000 events soon rises to unacceptable levels, thus it is normal to have to accept some downtime, however small that may be. To ensure that capability is not compromised to an unacceptable level during these outages, the down time should be bounded by specifying the length of time the capability can be unavailable for and how often the capability can be unavailable in a calendar period.

4. Taking the provision of a 'network' as an example, the user has specified that it has to be available for 99.8% of the time. In a calendar year of 365 days, this allows for the network to be unavailable for 17.5 hours but the requirement as it stands puts no constraints around how that down time is accrued. At one extreme, the network could be down for 17.5 hours once during the calendar year, which for a communication network would have serious consequences. At the other extreme, it could be unavailable for close to 3 minutes every day, which could erode user confidence in the network far more than the one off occurrence previously referred to. In either case, the demonstrated level of availability is the same and meets the 99.8% requirement as specified. To get around this it is recommended that the user defines the maximum number of times it is acceptable to have any down time during the year, and when the network is down the maximum time it can take before it is back on line. This

[4] The definition of availability is taken from IEC 60050-192

would typically be done by setting reliability and maintainability requirements that are commensurate with the availability requirement.

5. Having considered the generic concept of availability there are a number of standard definitions that are used depending on what is included within the measured downtime:

a. Inherent availability is a measure of the availability of the item under ideal conditions, i.e. assuming that a trained maintainer, the spare parts, the tools and test equipment required to undertake corrective maintenance action are all to hand immediately. It is the most common metric that is included in a contract as it only includes the down time associated with carrying out corrective maintenance action activity which is within the control of the design authority and it focuses attention on ensuring that down time due to design is optimised. If inherent availability is used within a specification, care must be taken to manage expectations as it is very unlikely that it can be achieved in service because there will always be some logistic delays that will need to be included.

b. Operational availability gives a more realistic view of the levels of availability that can be achieved in service because it includes logistic delays but it is more difficult to measure and thus gain a figure that is agreeable to everyone. What truly constitutes logistic delay is a much-debated topic with no clear answer and no clear rules that can be applied to every corrective maintenance action. If the piece of test equipment or tool that is required has not been returned to its 'correct location' following a previous activity and it takes 30 minutes to locate it, can this be counted as logistic delay against the item? Putting an operational availability requirement into a contract highlights this type of issue and requires many rules to be written to ensure the requirement is clear and unambiguous.

6. Availability requirements for an item can be specified at a number of levels depending on what is required. If the item is part of a fleet, it may be appropriate to set an availability requirement for the whole fleet or for different parts of the fleet, for example vehicles are often split into operational and training fleets with the operational fleet having a higher availability requirement than the training fleet. It may be that the item itself has an availability requirement or it may be beneficial to set an availability requirement for a part of the item, for example, the diesel generators in a ship may have an availability requirement as well as the ship itself. Care needs to be taken to ensure that the requirements are commensurate with each other such that the level of availability requested for the higher assembly is not in excess of that which is possible given the lower level availabilities.

7. Contracting methods have for some years been moving away from the traditional organic support solutions towards performance-based contracts where specified levels of availability or capability are included. In such situations, it is necessary to ensure that the data needed to measure the success, or otherwise, of the metrics is specified and a method of collecting it is included. It may be necessary, or preferable, for the collected data to be fed into an agreed model for the assessment against the requirements particularly if provision is wide spread or against a large number of assets.

8. Whatever the requirement, it is imperative to ensure that what is offered / contracted for is fully understood and commensurate with what is required. It is not uncommon in a performance-based contract for there to be a number / range of exclusions, which, if not fully understood, can have significant impact on what the user is expecting. As an example, when contracting for an air vehicle, the engines are often part of a separate contract as can be such things as wheels and tyres, certain electronic items and even spare parts which have not been

demanded in the preceding few years. Similarly, failure modes and mechanisms that have not, or cannot be, predicted such as corrosion or tyre puncture are often outside of the contractual terms and will require to be costed and contracted for separately.

9. Availability can be a good parameter to define at any stage of procurement from early pre-concept up to and including utilisation and support. As has been shown in the preceding paragraphs, care should be taken to ensure that the characteristics which have the greatest impact on availability are also more closely defined as the item matures. In pre-concept and concept stages it may be reasonable to only specify a top level availability requirement to ensure that operational needs can be met, but as the design matures, and the use requirements become clearer, it becomes more and more important to ensure that downtime is bounded so that it does not have a significant impact on operational requirements.

3.2. RELIABILITY

1. Reliability can either be defined[5] as a characteristic for an item or as a performance measure. As a definition of a characteristic for an item it is the ability to perform under given conditions for a given time interval whilst as a performance measure it is the probability of being able to perform as required under given conditions for the time interval.

2. Various levels of reliability can be defined for an item to cover differing levels of degradation in performance, the most common being Mission Failure and basic failure as shown below:

a. Mission Reliability – A measure of item reliability including only those failures, which render the item inoperable or non-mission worthy.

b. Basic Reliability – A measure of item reliability reflecting the overall failure rate of the item.

3. To put this into context, the failure of an interior light on a family motor car may be considered a minor nuisance by the user, particularly when getting in and out of the car in the dark but would not render the car inoperable and would most likely be considered a basic failure. However, failure of the fuel or water pump would render the car inoperable and would thus most likely be considered as a mission failure.

4. It should be noted that Basic reliability includes all levels of failure, including mission failures, to properly reflect the total failure frequency of the item.

5. Mission and Basic are two of the descriptors that can be applied to reliability, but many others exist too, including, but not limited to Storage, Dormant, Major, and Critical. Whatever descriptors are chosen to be applied for the item that is under consideration it is imperative that the level of degradation or definition(s) of those failure descriptors are included within the

[5] The definitions of reliability are taken from IEC 60050-192

specification to ensure everyone associated with that item has a clear and unambiguous understanding of the term.

6. Reliability can be specified in a number of different ways and whilst no one way can be considered as best to cover any circumstance, some methods can be less appropriate than others under certain conditions.

7. The most common, and probably most recognised, method of specifying reliability is to quote it as a mean value using a term such as Mean Time Between Failure (MTBF) for a repairable item or Mean Time To Failure (MTTF) for a non-repairable item. The values specified should be those that achieve the users' minimum operating requirement and should be commensurate with any availability requirement that has been defined. It is important to recognise that any requirement specified in this way is only a mean value and it should be expected that significant numbers of the population will fail before the mean time is reached, thus specifying a 200-hour MTBF to support an operating requirement of 200 hours will result in failure. It should also be noted that specifying a mean value without any supporting information is of no benefit to the items being purchased. Consideration must be given to whether the 'time' is based on hours of operation, calendar time or some transformation based on known factors such as take offs and landings for an aircraft, distance for a vehicle or number of firings for a gun. It is also necessary to ensure that any mean value is clearly supported by an LCEP.

8. Reliability can also be specified as a probability of success, with or without an associated specified operating time. The requirement for a one shot device, typically a missile, would be specified as a probability of success without a time qualification as the user wants assurance that when that item is used it will operate successfully against its predefined LCEP. An item that would be expected to repeat similar or differing LCEP many times, a vehicle for example would be specified with a time qualification where the time qualification is equal to the length of the mission.

9. All of the example requirements above are of a quantitative nature, i.e. can be specified and measured in a numerical way, but it is also possible to specify requirements in a qualitative way, i.e. relating to the quality of the item. For reliability, this type of requirement often relates to the design of the item, examples of which are below:

a. Single Point of Failure - The item shall be designed such that no single fault can cause a mission or safety critical failure within it.

b. Path Separation – The item shall be designed such that redundant parts within the item are kept independent by ensuring that cables, power supplies and signal routes have well defined separate paths.

10. However reliability is specified, it is imperative that failure definitions relevant to each level of reliability are included as defined in section 2.4 of this document.

11. As described in the section on availability above, it is important to remember that a separate reliability requirement may be required when contracting for availability or capability.

12. Reliability as a parameter can be specified at any stage of procurement but can be more difficult to define in the pre-concept and concept stages particularly where the technology and design solution of the final item are not known. In these instances, care must be taken to ensure that if a reliability requirement is set it does not dictate the design solution

or constrain the design such that innovation or taking advantage of emerging but unproven technology is not considered.

3.3. MAINTAINABILITY

1. Maintainability can either be defined[6] as a characteristic for an item or as a performance measure. As a definition of a characteristic for an item it is the ability to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance whilst as a performance measure it is the probability that a given maintenance action, performed under stated conditions and using specified procedures and resources, can be completed within the time interval ($t1$, $t2$) given that the action started at $t = 0$. For the purposes of setting meaningful requirements, maintainability is taken to be a performance measure.

2. The user is interested in understanding how long it will take to bring an item back to a fully operational condition following any incident. The time will be dependent on two factors: the physical time it takes to diagnose and undertake the repair and the time to obtain the required spares, tools and a maintainer capable of undertaking the work, this later time being referred to as logistic delay and which is mostly outside of the influence or control of the item designer. In order to differentiate between these two differing times it is normal for the diagnose and repair time to be referred to as Active Repair Time (ART) and the time including logistic delay to be referred to as Time To Repair (TTR).

3. If every recovery task applicable to the item was timed and plotted then a unique distribution would be generated which could then be defined by a fixed number of points. When setting maintainability requirements it is points on this distribution that the user is required to define, either based on historical knowledge of similar items, expectation of current technology or on the perceived time the user can accept the item not being available. It is usual to specify more than one point on the distribution in order to bound its shape, typical measures being the Mean, Median or percentage points.

4. The most common, and probably most readily recognised, method of specifying maintainability is through the use of a mean time, either as a Mean Active Repair Time (MART) or as a Mean Time To Repair (MTTR). As stated above, simply specifying a mean on its own has very little influence on the design of the item thus it is considered best practice to include at least one percentage point in addition to the mean.

5. Specifying two or more percentage point times for maintainability requirements requires the item designers to consider such things as access to cabinets, ease of removal of parts and ability to diagnose a malfunctioning item in a reasonable time. It is normal to specify a percentage point towards the top end of the distribution such that either 90% or 95% of all repairs shall be completed by the specified time. In conjunction with either a Mean time, or possibly a time for 50% of all repairs to be complete this defines the approximate shape of the repair time distribution. If the item is heavily dependent on software then it may be applicable to set a lower percentage point time within which all software restarts shall be accomplished.

6. There are occasions, particularly in a performance-based contract, where it may be applicable to set a maximum time by which all actions or activities shall be completed. Contractual penalties may then be applied to any activity that is not completed by the required time. Care needs to be taken in setting such limits to ensure that it is not so wide that it has an

[6] Maintainability is defined in IEC 60050-192

adverse effect on operation of the item and that is not so narrow that the supplier has very little chance of meeting the time.

7. Maintainability requirements if set during the early stages of the life cycle can be used to influence the design in terms of its maintainability before design decisions have been made. This would be done to ensure that the distribution relating to any of the mean values outlined above are not adversely skewed by a single, or group of repair activities. This would typically be done by setting a maximum time (M_{Max}) which no repair should be expected to exceed under normal circumstances taking account only of those factors, which are under the control of the designer.

8. As an example consider an item, housed in a container and mounted on a large structure, access to which is gained by removing one of the covers of that container. How the covers are attached can have a significant influence on the time it takes to carry out any repair activity that is required by the item. If it is held on by 25 non captive bolts that have to be removed and replaced using only a spanner, the time taken to gain access to the container will be significantly longer than if it is held on by a similar number of captive bolts or quick release fastenings.

9. In this instance, an M_{Max} requirement could influence the choice of fittings that are used, although the time requirement may have to considered and possibly traded off against the cost of the fastening devices and the requirement for any special tools to operate them.

10. The requirements defined above are all of a quantitative nature, but maintainability can also be defined in a qualitative way. Some examples of qualitative requirements are given below:

a. The item shall not contain any fixing device that cannot be removed using a number 2 cross head screwdriver available from any commercial tool stockist.

b. The item shall be designed such that any operator can conduct the regular checks required without specialist knowledge or training.

c. The item shall be such that all items the user is required to inspect or top up on a regular basis shall be immediately obvious.

11. Maintainability as a parameter can be specified at any stage of procurement but can be more difficult to define in the pre-concept and concept stages particularly where the technology and design solution of the final item are not known. In these instances, care must be taken to ensure that if a maintainability requirement is set it does not dictate the design such that innovation or taking advantage of emerging but unproven technology is not considered.

3.4. TESTABILITY

1. Testability is defined[7] as the degree to which an item can be tested and is key to ensuring that when an item is no longer functioning as expected the cause of the problem can be identified. Testability is a characteristic that must be designed into the item and cannot simply be added at some later stage.

2. A full understanding of how the item functions, and thus how it can cease to function as expected, is required by the development team in order to determine the best place to monitor

[7] The definition of testability is taken from IEC60050-192

data signals so that the functionality can be proven and erroneous or missing data can be detected and reported to the operator as appropriate.

3. Fault detection can be achieved using different types of 'Built-In-Test' (BIT) routines, some of which run continuously in the background, others that are instigated by the operator. The test routines which run continuously in the background would normally be used to detect the loss of a function. When the loss of function is identified, the operator / maintainer would run the instigated BIT routines to further identify the cause of the failure.

4. When the item is a complex system that incorporates many parts, often designed by other organisations, it is important to understand the data signals that are monitored within those parts to ensure those of significance can be accessed by the operator. Many computer-based items incorporate a 'keep alive' battery that maintains basic date and time information that are critical to its ability to function correctly. Almost all of these items have a 'warning signal' to say that battery needs changing and it is vital that this signal is brought to the attention of the operator so that replacement action can be taken at a convenient time rather than letting it fail and maybe rendering the complex system unserviceable.

5. Similarly many vehicle engines have complex management systems these days, thus when taking a commercial engine and integrating it into a military environment it is vital to understand all of the functions of that management system. A 'get you home' mode that limits engine revolutions to protect it in the event of potential failure may be perfectly acceptable in a training role but when under fire in a hostile environment may not be something the operator is happy to accept.

6. Setting requirements that drive the design and are measurable is not easy since providing evidence of compliance can require expensive and lengthy testing or has to be done 'on paper' using such tools as the Failure Modes Effect and Criticality Analysis (FMECA) or Fault Tree Analysis (FTA) to show which failure modes have been addressed. Typical requirements could be:

a. Test Coverage[8] – The ratio of the number of faulty functions actually capable of diagnosis by the given test instruction to the total number of functions. Test Coverage can also be considered on the base of failure rates instead of failure numbers. The test coverage rate (τ) is weighted by the failure rate (λ):

$$\tau = (\Sigma\lambda_{\text{failures detected by the test}} / \Sigma\lambda_{\text{All failures of the item}})$$

This second definition is more appropriate for mission reliability assessments. Indeed, failures during mission may result from failures occurring after the test or from failures occurring before the test but undetected. The mission reliability can then be assessed directly from failure rates and test coverage. It may be required to specify the coverage required against specific function i.e. safety or mission critical failures. A typical requirement may be that "92% of all possible fault conditions shall be identified by the built in test routines. Additionally 100% of the fault conditions that could cause safety and mission critical failures shall be identified."

b. Fault detection rate – The number of fault conditions that can be identified and reported to the operator by the item either through the generation of a visual display on the operating console or through the illumination of a detection lamp. It may be required to specify detection rates against specific functions i.e. fault conditions that

[8] The definition of Test Coverage is taken from IEC 60706-5:2007

could cause safety or mission critical failures. A typical requirement may be that 90% of all possible faults, and 100% of faults that could cause safety or mission critical failures shall be detected and reported to the operator.

c. Fault isolation rate – The number of fault conditions that, once detected, can be isolated to a single unit that can then be changed by the operator. A typical requirement may be that 87% of all possible faults can be isolated to a single replaceable unit and 95% of all possible faults to no more than 2 replaceable units.

d. False Alarm Rate – The number of alert messages provided to the operator, which on subsequent investigation result in no problem being found (also referred to as being unable to replicate) is limited normally in percentage terms. A typical requirement may be that 'No more than 4% of the failure messages displayed to the operator shall subsequently result in no fault being found.'

7. The requirements defined above are all of a quantitative nature, but testability can also be defined in a qualitative way. Some examples of qualitative requirements are given below:

a. The item shall have a go no/go capability that can be run by the operator at any time to give confidence that it is fully operable and committable.

b. The item shall contain a continuously running built in test routine that identifies and reports the loss of major functions to the operator.

8. Testability as a parameter can be specified at any stage of procurement but can be more difficult to define in the pre-concept and concept stages particularly where the technology and design solution of the final item are not known. In these stages, qualitative requirements are likely to be more appropriate than quantitative ones which should be developed for inclusion in the later stages of the procurement.

3.5. MAINTENANCE

1. Maintenance is defined[9] as combination of all technical and management actions intended to retain an item in, or restore it to, a state in which it can perform as required. The way in which the maintenance will be undertaken on the item needs to be considered very early in the design process to ensure that any required actions can be performed without the need for lengthy delays whilst suitable access is gained to the item and without putting the maintainer at risk of harm.

2. Maintenance normally falls into one of two categories, preventive or corrective where preventive is defined[10] as maintenance carried out to mitigate degradation and reduce the probability of failure and corrective is defined[11] as maintenance carried out after fault detection to effect restoration.

3. Corrective Maintenance needs to be carried out at a convenient point soon after the fault has been detected and there is little that can be done in a specification to control it. However, the timing and frequency of Preventive Maintenance activity is much more flexible and can be

[9] The definition of Maintenance is taken from IEC60050-192
[10] The definition of Preventive Maintenance is taken from IEC60050-192
[11] The definition of Corrective Maintenance is taken from IEC60050-192

influenced by requirements. These requirements can be of a quantitative or qualitative nature as shown below:

a. Preventive maintenance shall not exceed 2 hours per week.

b. When the item is deployed for a 30-day mission, down time due to Preventive Maintenance shall not exceed 20 hours, with no single activity taking more than 90 minutes.

c. No preventive maintenance shall need to be undertaken during the required hours of operation, these being 09:00 to 17:00, Monday to Friday.

d. Preventive Maintenance shall be capable of being undertaken by one person using only the minimum tool set described elsewhere in the specification.

e. All daily user checks shall be capable of being undertaken by unskilled users.

3.6. SAFETY

1. This section is not intended to describe general safety criteria, but to discuss the issues surrounding the interrelationship between dependability and safety requirements and how at times dependability may need to be traded for safety. Just because an item has good dependability characteristics does not mean it will be safe, and equally an item that is safe may not be as dependable as required.

2. In order to ensure that an item is safe it may be necessary to add additional items to enable constant monitoring of particular attributes and some form of recording device where the data can be stored. Whatever the dependability characteristics of this item are, it will have an overall negative effect on how reliable, maintainable and thus available the overall item is.

3. Similarly, the requirement for an item to be safe, thus demonstrating a very low probability of catastrophic failure may drive the levels of redundancy that are built into an item. This can drive up the level of reliability in an item to a much higher level than may normally be considered cost effective to include.

4. The requirement to provide an operational environment that protects the users of the item from some external influence may also have an impact on the dependability characteristics of an item. Recent military requirements have meant that vehicles have necessarily been up-armoured in order to protect the users from the blast effects of explosive devices. The addition of this armour has taken the all up mass of the vehicles over the original design intent which has had adverse effects on reliability of the under carriage, suspension, braking systems and power output. Additionally, in many instances it is necessary to remove the armour to undertake maintenance or repair; thus attributes such as Mean Time To Repair and the 95-percentile repair times have been extended beyond the original design requirement.

5. Reliability requirements often define the probability of mission success whilst safety requirements often define the probability of non-occurrence of a hazardous event. Therefore, when setting reliability requirements, the safety requirements should be taken into account. Indeed, safety requirements may determine the minimum acceptable level of reliability. For example, an armament safety switch may have an allowable hazard rate of one per 10^6 flying

hours. The design and reliability analysis of the switch should, therefore, take this hazard rate into account.

6. Dependability requirements often have qualitative requirements relating to safety included within them with statements such as “Generation of hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive sub-components from damage or adverse effects is unacceptable” and “Packaging or handling procedures and characteristics that could cause a mishap is unacceptable.”

7. A number of the techniques used to assess the dependability of an item are common to those used when assessing the safety aspects of an item, FMECA being a common example. Although the process employed in conducting the FMECA for safety and dependability will be the same, the final analysis of the criticality is likely to be different and care should be taken to ensure that the results from a safety assessment are not read across directly into a dependability assessment.

3.7. SOFTWARE

1. Software has become an increasing large proportion of many items during the recent past and continues to provide an ever-increasing proportion of their functionality, being a wholly integral part of the item vital for its continued day-to-day operation.

2. Unlike hardware, which suffers from wear out properties that often give advance warning of failure and when it fails needs to be removed and physically repaired, software does not wear out, often fails without advance warning providing little or no indication that failure has occurred. Software can however be rebooted or re-initialised in a relatively short space of time returning it to full functionality. Physical changes to software can be more flexible, less time consuming and less costly to instigate than for hardware, but on large safety critical systems the cost of testing to prove successful operation can be high.

3. The reuse of software is becoming more commonplace but as with any integration care must be taken to ensure that all of the inputs, outputs and interdependencies are fully understood. Just because a software module was dependable in a previous application does not automatically mean it will be in any new one.

4. From the point of view of dependability specification, all of the individual characteristics that are used for hardware can equally be used for software. Availability requirements can be set to cover readiness of software operation; Reliability requirements can be set to cover the continuity of software service; Maintainability requirements can be set to cover the ease of software modification, upgrade and enhancement; In addition recoverability requirements can be set to cover software restoration following a failure, with or without external actions.

5. It is currently considered best practice to set the requirements at the item level including hardware and software, not breaking out the requirement in terms of hardware and software as the operator is not particularly interested in what has caused the item not to function properly, merely that the situation has occurred. When adopting this approach it is critical to ensure that the failure definitions robustly account for software-induced failure modes so that they are accounted for during any statistical analysis. The ability to recover quickly from a software-induced failure should not be reason to just accept it and take no action to correct it.

6. If software is to be specified independently, an initial risk analysis can be undertaken to assesses the contribution of the software to system-level events/hazards in order to determine

software integrity levels, and thus to specify design requirements. Software design requirements focus on the software quality assurance process and on software specific methods.

INTENTIONALLY BLANK

ADMP-01(B)(1)