SAFETY & RELIABILITY SOCIETY SOLENT BRANCH

TESTABILITY: REQUIREMENTS, ASSURANCE, BENEFITS AND CONSIDERATIONS FOR AUTONOMOUS PLATFORMS

BY
ALAN BENNETT, BMT

20TH JANUARY 2021

The Safety & Reliability Society is a Licensed Member of the Engineering Council for CEng and IEng Professional Registration

SaRS SAFETY AND RELIABILITY SOCIETY

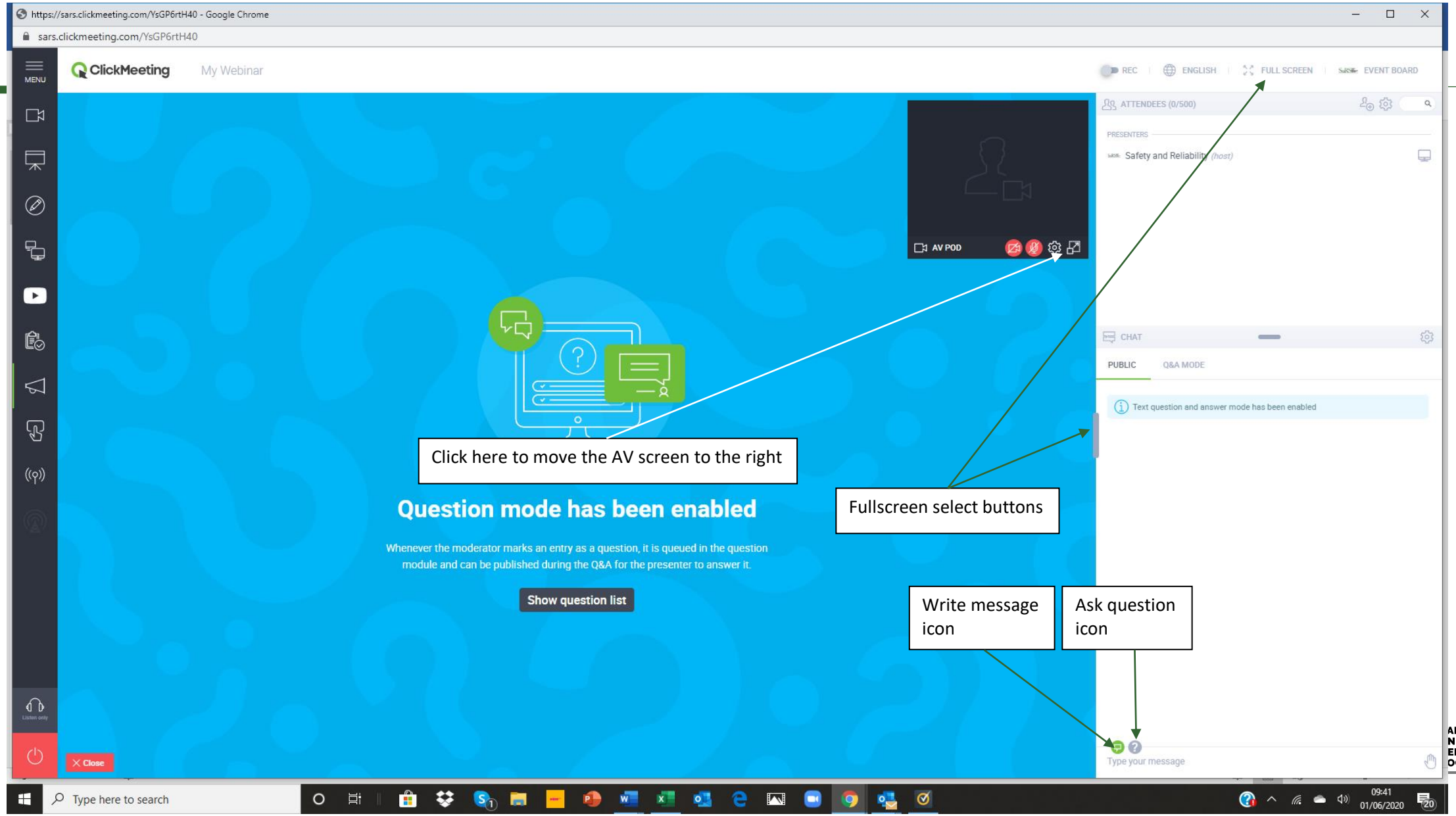
Programme

- Introduction
- Presentation
- Q&A session
- Accessing the webinar and upcoming webinars
- Feedback

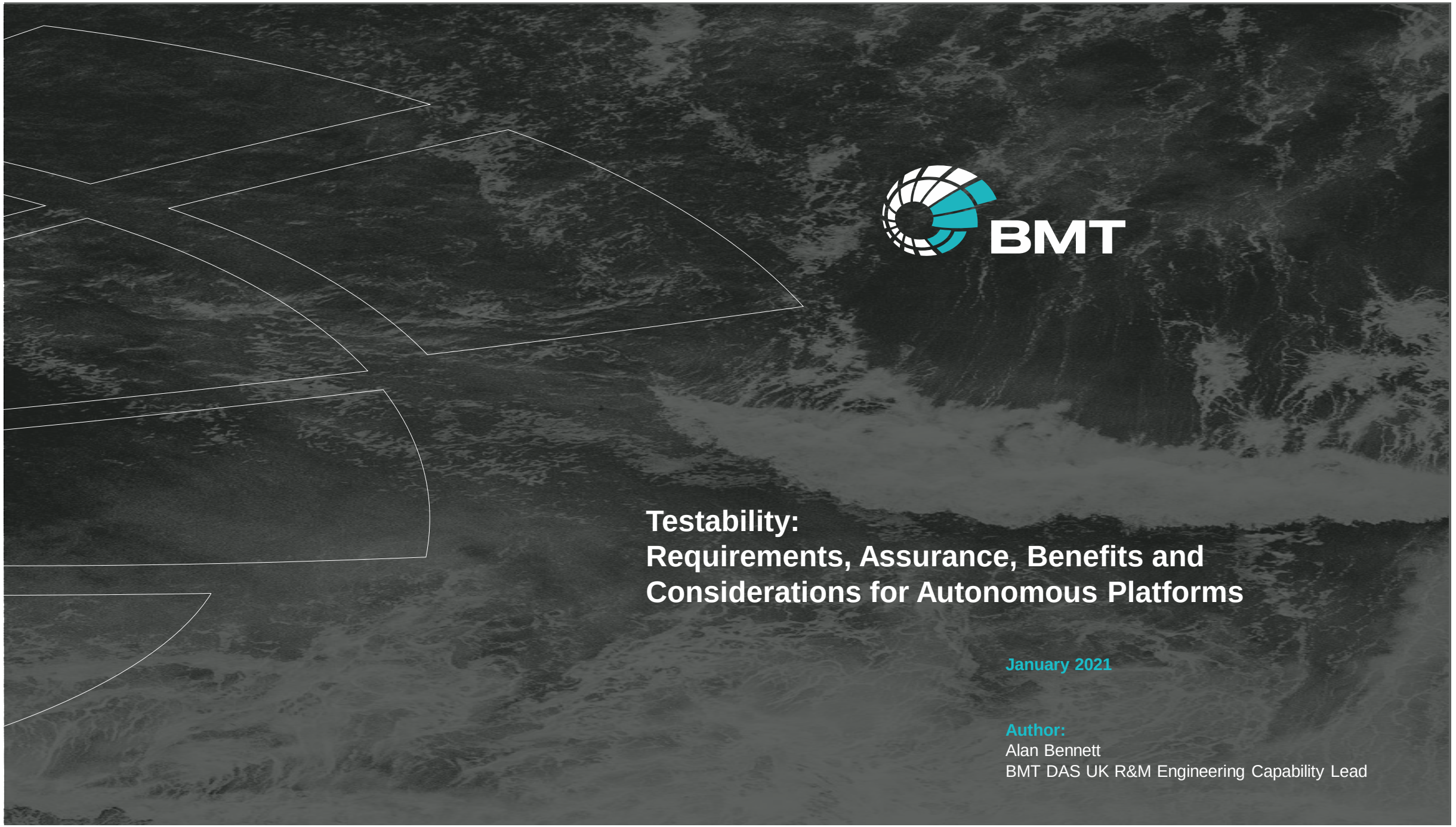
Note: the Webinar is being recorded

SaRS SAFETY AND RELIABILITY SOCIETY

VIEWING IN FULLSCREEN AND Q&A FACILITY



AFETY
ND
ELIABILITY
OCIETY



Testability:
Requirements, Assurance, Benefits and Considerations for Autonomous Platforms

January 2021

Author:
Alan Bennett
BMT DAS UK R&M Engineering Capability Lead

Introduction

For those who don't know me:

- BMT DAS UK R&M Capability Lead
- At BMT since 2017
- ~33 years experience in ARM&T
- ~31 years SaRS membership

  Solent Branch committee member

- This paper has been prepared by the Author, with the support of the Asset Performance Services (APS) business line of BMT DAS UK.
- The kind permission, support and resources granted to the author by BMT are acknowledged with thanks.

- All findings, ideas, opinions, and errors herein are those of the author and are not necessarily those of BMT DAS UK Ltd.

Introduction

- Testability often appears to be the “poor” relation to ARM&T.

BMT

Introduction

- Testability often appears to be the “poor” relation to ARM&T.

- Just the detection part of Maintainability?
- What does the User expect?
- What requirements?
- How to provide assurance

BMT

Introduction

- Testability often appears to be the “poor” relation to ARM&T.

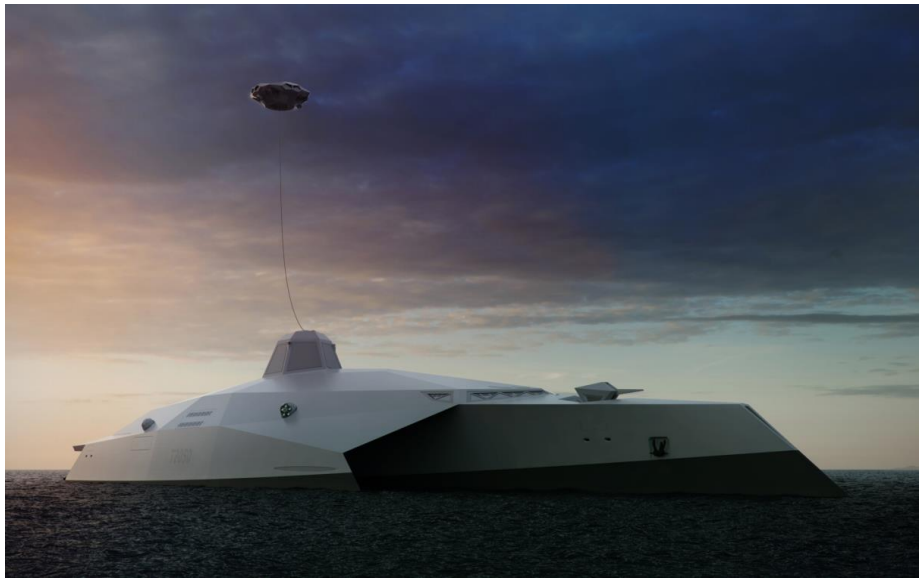
- Just the detection part of Maintainability?
- What does the User expect?
- What requirements?
- How to provide assurance

- Actually, it can be much more than this, but also relatively simple, as I hope to explain

BMT

Testability & Autonomous Platforms

- BMT, amongst other companies, is looking seriously at autonomy
- An achievable step is to reduce manning beyond the ‘Lean Manning’ currently seen
- This requires a higher level of Testability as there will be fewer, if any, operators to identify and mitigate failure.
- To appreciate the benefits of Testability on autonomous platforms, it is necessary to understand what Testability means and how to assure it on any platform.
- To achieve good Testability, it is key to use this knowledge in the early design stages



BMT

Testability Standards & Definitions

- This section includes reference to national and International standards as well as independent publications.
- It includes discussion of how useful, or not some definitions are, and interesting points identified within the documents that are discussed further in the presentation.

BMT

Testability Standards & Definitions

IEV: 192-09-20 (Dependability) (i)

- *testability, <of an item> is defined as: “degree to which an item can be tested.”*

Testability Standards & Definitions

IEV: 192-09-20 (Dependability) (i)

- *testability, <of an item> is defined as: "degree to which an item can be tested."*

Def Stan 00-042, Reliability and Maintainability (R&M) Assurance Activity - Part 4 – Testability (Superseded) (ii)

- "*A characteristic of design that allows the operational status of an entity and the location of faulty replaceable components within that entity, to be confidently determined in a timely and cost-effective manner. Operational status can mean operable, partly operable and inoperable. It should be noted that this definition is applicable to a system that is comprised of one or more of the following elements: electrical, electronic, mechanical, and software*."

Testability Standards & Definitions

IEV: 192-09-20 (Dependability) (i)

- *testability, <of an item> is defined as: "degree to which an item can be tested."*

Def Stan 00-042, Reliability and Maintainability (R&M) Assurance Activity - Part 4 – Testability (Superseded) (ii)

- "*A characteristic of design that allows the operational status of an entity and the location of faulty replaceable components within that entity, to be confidently determined in a timely and cost-effective manner. Operational status can mean operable, partly operable and inoperable. It should be noted that this definition is applicable to a system that is comprised of one or more of the following elements: electrical, electronic, mechanical, and software*."

BS EN 60706-5, Maintainability of Equipment: Testability and diagnostic testing. (iii)

- *"design characteristic which determines the degree to which an item can be functionally tested under stated conditions".*

BMT

Testability Standards & Definitions

Supportability Engineering Handbook: Implementation, Measurement, and Management. (iv)

"Includes sections on Testability Engineering and Testability Engineering Program, which provides the following statement:

- *"An integral part of the overall design effort of electronic systems is testability engineering. The reason for this importance is that testability engineering addresses the requirements for testing that must be considered in the development and design of an electronic system or systems. This includes the extent to which a system or system design supports fault detection and fault isolation in a confident, timely, and cost-effective manner"*

It also identifies 3 goals of a Testability Program:

- Integration with system and design engineering to meet testability requirements
- Support of and integration with maintainability design
- Support of logistic support requirements planning

BMT

Significant points arising from Definitions

- Consideration of these documents, (ii) Def Stan 00-042, (iii) BS EN 60706-5 & (iv) Supportability Engineering Handbook provides the following significant points:
- Testability:
    - Is a Design characteristic, (ii, iii & iv)
    - Is applicable at System / Platform level, (ii & iv)
    - Encompasses electrical, electronic, mechanical, and software elements, (ii)
    - Needs to be timely and cost-effective (ii & iv)
        - Addresses,
            - System Operational Status, (ii)
            - Fault Detection, (ii & iv)
            - Fault Isolation / Localisation, which encompasses Fault Reporting (ii & iv)

BMT

What does the User Expect?

- The ability to know when the system / platform is operating at Full or partial capability, or not-operating,
- the knowledge required to initiate appropriate mitigation in a timely manner to restore operational performance and improve availability of the asset.

What does the User Expect?

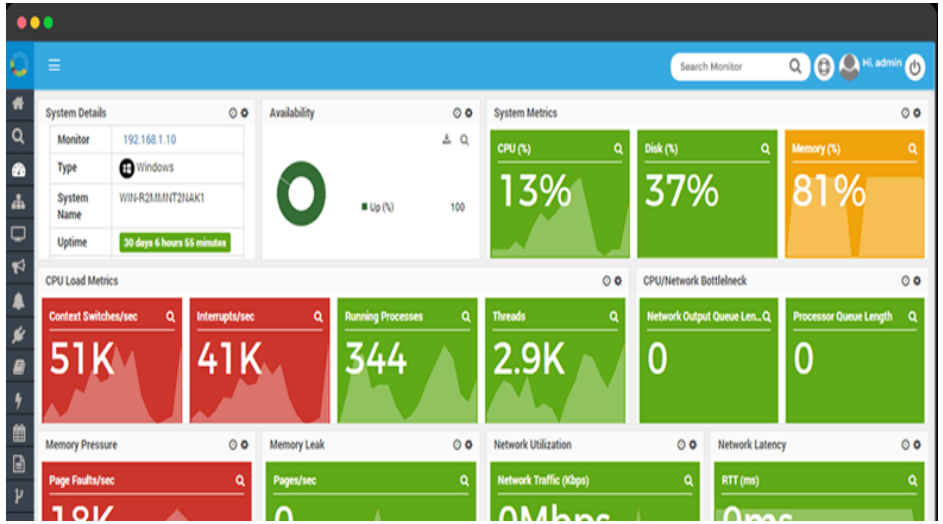
- The ability to know when the system / platform is operating at Full or partial capability, or not-operating,
- the knowledge required to initiate appropriate mitigation in a timely manner to restore operational performance and improve availability of the asset.
- When a failure, or degraded performance indication is provided, confidence that it is actually a true indication, not a False Alarm since False Alarms can result in unnecessary maintenance action and associated loss of system availability and increased cost.

BMT

How can User Expectations be achieved?

To achieve this ability requires:

- Continuous System Status monitoring,
- Reporting to a central location (i.e. Dashboard),
- The ability to know what has degraded, or failed.



Example RAG format Dashboard – Image Reproduced from Motadata (2020)

These, in turn, require:

- Information (at the Dashboard) of critical parameter values .
- Information (at the Dashboard) to identify the most likely Equipment that has failed.
- Access to documentation (ideally electronic) containing fault diagnostic data, to support mitigation action.

Requirements & Assurance

- In order to deliver User Expectations, you need Requirements.
- Requirements may be, Qualitative or Quantitative.
- Requirements should be **SMART**:
  - **S**pecific
  - **M**easurable
  - **A**chievable
  - **R**elevant
  - **T**imely
- We also need to be able to provide assurance that our Platform or System meets the quantitative & qualitative requirements.

BMT

Requirements & Assurance

- The extent to which requirements will be applicable, and the values assigned to them will depend upon the complexity and criticality of the system, the needs of the User and the maintenance strategy.
- The use of COTS products naturally determines the level of BIT inherent in equipment, since there is limited, if any, opportunity to influence their design, however the need to include additional sensors, or monitoring equipment and interfaces to COTS equipment, and provision of central and / or remote reporting, to enhance System level Testability, should be considered from the outset.
- To achieve these requirements, it is crucial that Testability is built into the design.

Requirements & Assurance

In addition to identifying appropriate Testability metrics, we also need to consider how their achievement can be assured. The appropriate means of documenting that assurance, progressively, is the Dependability Case, or specifically for UK Defence programmes, the R&M Case.

- BS EN 62741 - Demonstration of dependability requirements - Dependability Case, 2015
- Def-Stan 00-042, Part 3. Reliability and Maintainability Assurance Guide, Part 3: R & M Case.

Consideration of the significant points, User expectations and benefits has been used to identify potential qualitative and quantitative Testability requirement metrics:

BMT

Qualitative Requirements

- Examples of Qualitative Testability Requirements

a) The system shall have Continuous monitoring of system performance (not intermittent, or interruptive);

b) System status shall be available to User (Dashboard – RAG);

c) The User shall be notified of failure (visual / audible);

d) The User shall be notified of degraded critical parameter performance (visual / audible).

Qualitative Requirements

- Examples of Qualitative Testability Requirements

a) The system shall have Continuous monitoring of system performance (not intermittent, or interruptive);

b) System status shall be available to User (Dashboard – RAG);

c) The User shall be notified of failure (visual / audible);

d) The User shall be notified of degraded critical parameter performance (visual / audible).

Qualitative requirements (a to d), can be assured by inspection and reference to design documentation and / or demonstration. Design documentation may include Platform / System / Product specifications, identifying testability capabilities, but would ideally include testability design documentation'. These should provide descriptions of equipment BIT provision, the use of additional sensors and how data is provided to, and displayed on, a central / remote location and identification of data to be included in incident reports etc.

Demonstration of qualitative requirements, such as reporting to a central / remote location, and generation of incident reports, may be achieved by testing, typically in conjunction with Maintainability / Logistics Demonstration.

BMT

Quantitative Requirements

e) [*TBD*]% of Failures shall be detected (*High % of failures detected, by occurrence*);

f) [*TBD*]% of Failures shall be reported (*High % of detected failures reported, by occurrence*);

g) [*TBD*]% of detected Failures shall be isolated to a single LRU, [*TBD*]% of Failures shall be isolated to no more than [*TBD*] LRUs. (*High % of detected failures isolated to single LRU, higher % to no more than "x" LRUs*).

Quantitative Requirements

e) [*TBD*]% of Failures shall be detected (*High % of failures detected, by occurrence*);

f) [*TBD*]% of Failures shall be reported (*High % of detected failures reported, by occurrence*);

g) [*TBD*]% of detected Failures shall be isolated to a single LRU, [*TBD*]% of Failures shall be isolated to no more than [*TBD*] LRUs. (*High % of detected failures isolated to single LRU, higher % to no more than "x" LRUs*).

From the Authors experience, it is considered that the primary tool for assurance of quantitative Testability requirements should be by extension of the Design FMECA (Failure Modes Effects and Criticality Analysis).FMECA already identifies all the equipment comprising the system and their failure modes, effects and criticality, with their probability of occurrence, therefore adding additional columns of analysis to a spreadsheet-based FMECA, with calculations to sum detected failure rates, and compare with total failure rate, is, in the Authors consideration, a relatively simple extension.

By identifying whether each failure mode is detected, reported and determining LRU identification ambiguity , the extended FMECA can provide the assurance required to address the quantitative requirements (e to g).

Note that the monitoring function may also fail in such a way that there is a loss of monitoring / detection. This should also be addressed by FMECA, as a Dormant failure, in conjunction with the function being monitored.

It may also be appropriate for there to be a reliability requirement applicable to the monitoring function.

BMT

Quantitative Requirements – Assurance (example)

Ref	Item	Function	Failure Mode	FM F/Rate (fpmh)	Columns hidden for clarity	Detected	Means of Detection	Reported	LRU Identification	LRU Ambiguity	Detection Rate	Reporting Rate	LRU Ambiguity	Identify to No more than "x" LRUs	
														1	2
1	Power Input	To provide service power to LRU	Does not provide service power to LRU	0.01		Y	BIT	Y	N	2. LRU, Service supply	0.01	0.01	2	0	0.01
2	Power regulation	To regulate service power to LRU volatge levels	Does not regulate service power to LRU volatge levels	0.1		Y	BIT	Y	Y	1. LRU	0.1	0.1	1	0.1	0.1
3	5V Supply	To provide 5V to LRU digital circuits	Does not provide 5V to LRU circuits	0.01		Y	BIT	Y	Y	1. LRU	0.01	0.01	1	0.01	0.01
4	`+/- 15V Supply	To provide +/- 15V to LRU analog circuits	Does not provide +/- 15V to LRU analog circuits	0.02		Y	BIT	Y	Y	1. LRU	0.02	0.02	1	0.02	0.02
5	Analog inputs	To provide analog inputs to LRU	Does not provide analog inputs to LRU	0.01		N	N/A	N	N	X. LRU, analog inputs, other LRUs downstream	0	0	X	0	0
			Total Failure Rate	0.15				Sum			0.14	0.14		0.13	0.14
								Percentage of total failure rate.			93.33%	93.33%		86.67%	93.33%
								Percentage of detected failure rate.				100.00%		92.86%	######

BMT

Quantitative Requirements – Assurance (example)

FM F/Rate (fpmh)					Detection Rate	Reporting Rate	LRU Ambiguity	Identify to No more than	
								1	2
0.15					0.14	0.14		0.13	0.14
		Percentage of total failure rate.			93.33%	93.33%		86.67%	93.33%
		Percentage of detected failure rate.				100.00%		92.86%	100.00%

The analysis shows that:

- 93.33% of failures are detected. (0.14 / 0.15 = 93.33%)

Quantitative Requirements – Assurance (example)

FM F/Rate (fpmh)					Detection Rate	Reporting Rate	LRU Ambiguity	Identify to No more than	
								1	2
0.15					0.14	0.14		0.13	0.14
		Percentage of total failure rate.			93.33%	93.33%		86.67%	93.33%
		Percentage of detected failure rate.				100.00%		92.86%	100.00%

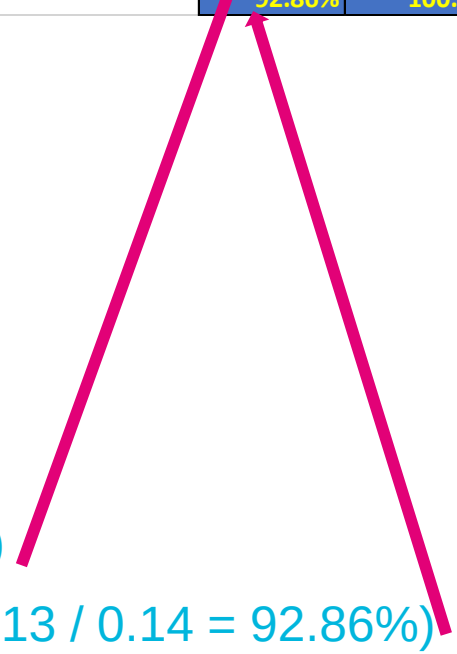
The analysis shows that:

- 93.33% of failures are reported. (0.14 / 0.15 = 93.33%)
- 100% of detected failures are reported. (0.14 / 0.14 = 100%)

BMT

Quantitative Requirements – Assurance (example)

FM F/Rate (fpmh)					Detection Rate	Reporting Rate	LRU Ambiguity	Identify to No more than	
								1	2
0.15					0.14	0.14		0.13	0.14
		Percentage of total failure rate.			93.33%	93.33%		86.67%	93.33%
		Percentage of detected failure rate.				100.00%		92.86%	100.00%



The analysis shows that:

- 86.67% of failures identified to a single LRU. (0.13 / 0.15 = 86.67%)
- 92.86% of detected / reported failures identified to a single LRU. (0.13 / 0.14 = 92.86%)

BMT

Quantitative Requirements – Assurance (example)

FM F/Rate (fpmh)					Detection Rate	Reporting Rate	LRU Ambiguity	Identify to No more than	
								1	2
0.15					0.14	0.14		0.13	0.14
		Percentage of total failure rate.			93.33%	93.33%		86.67%	93.33%
		Percentage of detected failure rate.				100.00%		92.86%	100.00%

The analysis shows that:

-
- 93.33% of failures identified to no more than 2 LRUs. (0.14 / 0.15 = 93.33%)
- 100% of detected / reported failures identified to no more than 2 LRUs. (0.14 / 0.14 = 100%)

BMT

Quantitative Requirements - Assurance

- **Assurance through Demonstration**
- The demonstration of Quantitative Testability requirements is particularly difficult, as this may require the insertion of faults, ideally without damaging the equipment, therefore. the costs and effectiveness should be carefully considered.
- A limited selection of faults may be simulated and demonstrated as part of a Maintainability Demonstration.

BMT

Testability & Autonomous Platforms

BMT Pentamaran Concept Autonomous Platform

Introduction to Autonomous Platforms:

With a widespread move to autonomous operation of platforms, additional capabilities, associated with Testability could provide further benefits, including:

- reduced workload (central, comprehensive reporting reduces the need to check equipment for status,
- providing appropriate data to a remote central support location enables Support planning and Digital Twin,
- Supporting Data Reporting and Corrective Action System (DRACAS) and remote “what-if” solution scenarios.
- These capabilities and their benefits are described in more detail below.

Achieving this may involve a more comprehensive testability design bringing additional benefits, however the cost and performance benefits of specifying and implementing these capabilities should be considered.

BMT

Additional Capabilities & Benefits:

- There are additional benefits that could be available when this data is recorded and reported at a central and/or remote location.

  - Central / Remote Status Reporting
  - Central / Remote Data download (Digital Twin)
  - Spares & Support initiation
  - DRACAS / RCA data
  - Reconfiguration

Additional Capabilities & Benefits:

There are additional benefits that could be available when this data is available at a central location.

- **Central / Remote Status Reporting**
- Central / Remote Data download (Digital Twin)
- Spares & Support initiation
- DRACAS / RCA data
- Reconfiguration

- Continuous provision of system status to a central location, to provide awareness to the local User, or the System, to enable immediate operational decisions, without the need to inspect equipment locations.
- Continuous provision of system status to a remote location, to provide awareness to a remote operator / service organisation, to enable immediate or long-term operational decisions.
- Data available to the User / Operator / Customer to provide the ability to undertake analysis of Performance, Utilisation, Availability etc. at Platform, or Fleet level.

BMT

Additional Capabilities & Benefits:

There are additional benefits that could be available when this data is downloaded to a remote location.

- Central / Remote Status Reporting
- **Central / Remote Data download (Digital Twin)**
- Spares & Support initiation
- DRACAS / RCA data
- Reconfiguration

- Ability to provide all data to a remote location, such that when a failure occurs, the remote operator has all the information available to instigate appropriate mitigating action.
- This may not be on a continuous basis, to minimise bandwidth / data storage, but only on occurrence of pre-defined triggers.
- This capability can provide data for a Digital Twin of the platform to be maintained remotely to the platform itself, thereby providing the potential to perform “what-if” scenarios for potential reconfigurations, before applying them to the actual platform

BMT

Additional Capabilities & Benefits:

There are additional benefits that could be available when this data is recorded and reported at a central location.

- Central / Remote Status Reporting
- Central / Remote Data download (Digital Twin)
- **Spares & Support initiation**
- DRACAS / RCA data
- Reconfiguration

- If notification of failure, or onset of failure, is reported centrally, this allows for:
- Automatic generation of repair work orders, so that maintainers are ready at the appropriate time.
- Automatic generation of Spares order (on confirmation of Failed item), so that Spares are available at the appropriate time.
- This allows efficient maintenance planning and improved availability of the asset.

BMT

Additional Capabilities & Benefits:

There are additional benefits that could be available when this data is recorded and reported at a central location.

- Central / Remote Status Reporting
- Central / Remote Data download (Digital Twin)
- Spares & Support initiation
- **DRACAS / RCA data**
- Reconfiguration

- Downloaded data providing automatic generation and distribution of defined Incident Reports, to support DRACAS, RCA and In-service Reliability assessment.
- Reduces reliance on manually entered data.

Additional Capabilities & Benefits:

There are additional benefits that could be available when this data is recorded and reported at a central location.

- Central / Remote Status Reporting
- Central / Remote Data download (Digital Twin)
- Spares & Support initiation
- DRACAS / RCA data
- **Reconfiguration**

- If combined with appropriate algorithms, LFE, machine learning etc, central reporting could also aid in providing manual, or automated system reconfiguration following degradation, or failure.
- Limiting operation to safe-operating limits, or provision of advice to the User of safe-operating limits, if limiting is not viable.
- If reported remotely, ability to maintain a Digital Twin and undertake “what-if? Scenarios, relating to potential system reconfiguration, before applying to Platform.

BMT

Other Considerations:

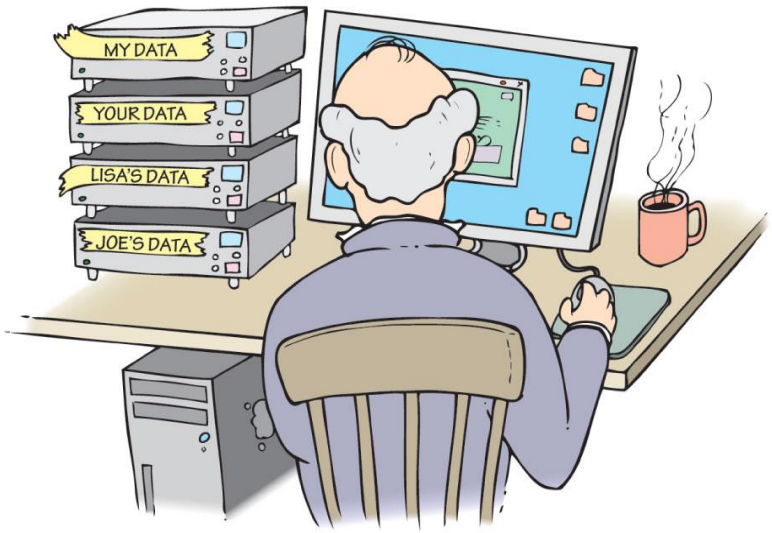
Whilst improved Testability design aids in enabling autonomous operation, there are other considerations which need to be taken into account.

- Data Ownership
- False Alarms
- Cost

BMT

Other Considerations – Data Ownership

- Some of these additional capabilities may necessitate the sharing of Configuration, Status and Testability data between the system OEMs, Design Authority, User, Support Contractor and Customer.
- The system status data being routed around the platform and potentially transmitted remotely may contain information that is sensitive with regards to the platforms capability
- Consideration should be given to the security of the data to ensure its integrity to intended users and its restricted availability to unintended recipients.
- It is therefore crucial that the ownership, sharing and security of data is addressed in any commercial agreement if this data is to be of benefit during operation.



Other Considerations - False Alarms

.

- It is difficult to discuss Testability without consideration of False Alarms.
- It is particularly critical for autonomous systems that the rate of False Alarms is low, since the ability to manually check the status is reduced and any intervention costly and time consuming.
- False Alarms cause unnecessary effort and cost to be incurred, whilst negatively impacting on system / platform availability.
- A reliability requirement relating to Monitoring systems and specifically False Alarms should be considered.

BMT

Other Considerations - False Alarms

- Causes of False Alarms.
  - False Alarms may be caused by intermittent failures, which cannot be predicted and are difficult to replicate, or which disappear upon re-instalment of the suspect item.
  - False Alarms may be caused by monitoring being too sensitive, which it may be possible to assure, or at least reduce, by testing.
  - False Alarms may also be caused by failure of the BIT / monitoring function, such that it provides a false indication of failure of the function or equipment that it is monitoring.
    - This can be considered as a functional failure of the BIT / monitoring function and addressed by inclusion of this as a function in the FMECA.

BMT

Other Considerations – Cost

Financial Cost

- There are costs associated with improved Testability, which should be considered:
- Additional Equipment (Sensors, Cabling, Dashboard etc) have an impact on:
  - Financial,
  - Weight,
  - Space
- Remote monitoring has an impact on:
  - Facility,
  - Data Bandwidth

Space

Weight

BMT

Conclusions & Recommendations

- Testability has been shown to be a design characteristic, which provides the User (local, or remote) with knowledge of the platform, or system, with operational status and allows the User (Or the System itself) to instigate mitigation, in a timely manner.

- User expectations, with regards to Testability have been discussed and Testability metrics, which are appropriate to be placed on a Platform, or System (rather than individual equipment) have been identified. In an ideal world, these requirements would be flowed down by the customer, however, it is recommended that where this is not the case, they are applied to the system by the contractor, to ensure that Testability is considered at the design stage.

- The means of assurance have also been explored, with a view presented that quantitative testability requirements can mostly be assured by extension of the design FMECA activity and qualitative requirements can be assured through design documentation and demonstration.

- False Alarms are a complex issue, which, whilst identified as being important, cannot be resolved entirely by good testability in design, or assured by analysis, or documentation. The inclusion of Reliability requirements for the status monitoring system may be of benefit. Further, in-depth consideration of False Alarms is outside of the scope of this presentation.

- Testability has been shown to be a key enabler of Autonomy enabling local Users, or the System itself, to make critical operational decisions, including safe system re-configuration.

BMT

Conclusions & Recommendations

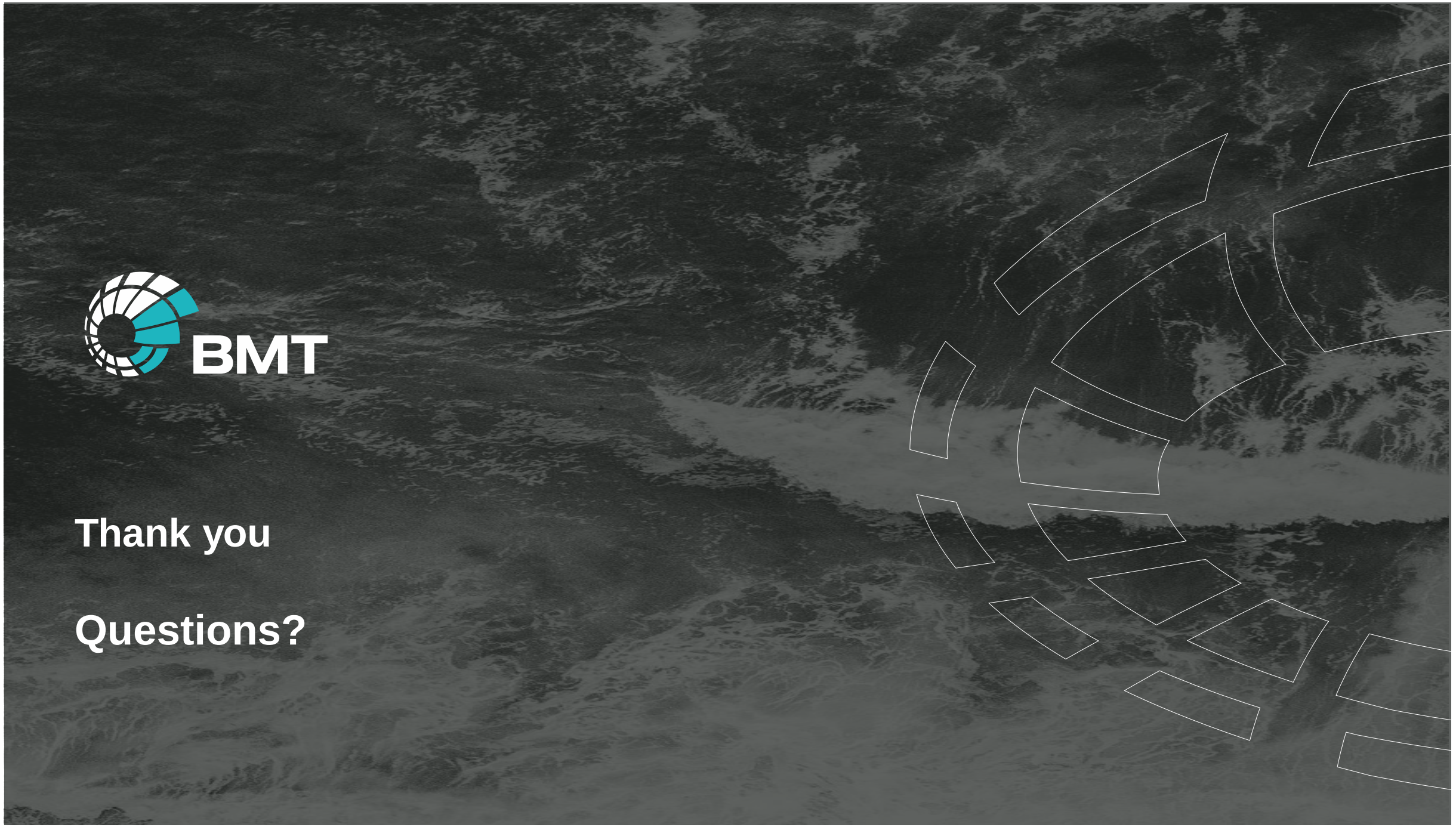
- The provision of this system status data remotely, either continuously, or “as required” enables the maintenance of a Digital Twin, such that “what-if” scenarios can be trialled remotely from the operational platform.
- Provision of System status data remotely also enables Spares and Support to be arranged at a convenient time and location to maximise asset availability and DRACAS data to be provide without manual data input, enabling more accurate data and timely investigation and Corrective Action.
- The provision of a comprehensive system of monitoring system status continuously has implications to cost, space and weight, which should be considered when designing for Testability.
- The paper has identified the issue of data ownership, security and sharing, particularly for remote reporting. Whilst this is a commercial issue, it must be addressed in any contract to ensure the benefits of good testability in design are experienced during operation.

BMT

References

- IEC (International Electrotechnical Commission) Vocabulary, IEC 60050, available as www.elecropedia.org
- Def Stan 00-42, Reliability and Maintainability (R&M) Assurance Activity Part 4 Testability, Issue 2, 2008 (Superseded)
- BS EN 60706, Maintainability of Equipment, Part 5 Testability and diagnostic testing, 2007
- Supportability Engineering Handbook: Implementation, Measurement, and Management, James V Jones. (McGraw-Hill)
- BS EN 62741 - Demonstration of dependability requirements - Dependability Case, 2015
- Def-Stan 00-042, Part 3. Reliability and Maintainability Assurance Guide, Part 3: R & M Case

BMT


BMT
Thank you
Questions?