Vetronics Standards & Guidelines

R M Connor
QINETIQ/EMEA/TS/CR0702540 Issue 3
June 2009

Administration page

Customer Information	
Customer reference number	03F-04-06-02
Project title	Platform Systems Integration
Customer Organisation	Research Acquisition Organisation
Customer contact	Peter King
Contract number	GM/N04058
Milestone number	N/A
Date due	September 2007

Principal author	
R M Connor	+44 (0)1252 397011
Room G072, Building A5, Cody Technology Park, Farnborough, Hants, GU14 0LX	rmconnor@QinetiQ.com

Release Authority	
Name	M Haines
Post	Project Manager
Date of issue	31/10/2008

Record of changes		
Issue	Date	Detail of Changes
Issue 1	30th September 2007	Initial Issue
Issue 2	31st October 2008	Corrections to Initial Issue
Issue 3	July 2009	Removal of Section 10 to separate document

List of contents

List of Tables

List of Figures

1 Introduction

1.1 Aim

This document seeks to present standards and guidelines for Vetronic infrastuctures that can be applied to both legacy and future land platforms.

The standards specified in this document are based on existing, industry wide, open standards and are organised within a nominal partition of Command & Control, Video Distribution & Processing, Software & Power Distribution and Management.

The guidelines are presented as examples of how the various standards may be employed and are not intended to be prescriptive.

The standards & the guidelines presented in this document are the result of ongoing Applied Research conducted by QinetiQ and procured by the Research Acquisition Organisation on behalf DEC (GM).

1.2 Scope

The document is organised in a number of sections organised as a logical flow from requirements through to implementation guidelines.

Section 2 introduces the reader to the Use of the Document.

Section 3 describes the reasons behind and the expected benefits of the Vehicle System Integration programme.

Section 4 introduces the requirements that drive the need for vetronics infrastructures based on open standards, including both User and Systems requirements.

Section 5 discusses the various architecture options, their advantages and disadvantages with respect to factors such as cost, flexibility, scalability etc.

Section 6 tabulates recommended standards against area of applicability and gives a short description for each standard or technology.

Section 7 contains guidelines for the use of the recommended standards & technologies.

Section 8 contains a summary of the current legislation pertaining to Safety Critical systems.

Section 9 discusses the use of the Safety Management Lifecycle of IEC61508 to fulfil the needs of Def Stan 00-56.

Section **Error! Reference source not found.** has been introduced into this version of the document to provide a method of assessing compliance with VSI principles.

1.3 Endorsement

Industrial participation in the VSI programme, in the form of the UK main vehicle system integrators and prime contractors, has been essential and central to its success. To facilitate

this, a joint MoD/QinetiQ/Industry Steering Group meets biannually to review the status and outputs from the VSI ARP. Wherever possible, active participation in the programme by VSI Industry members is encouraged.

This document has been prepared by QinetiQ on behalf of the collaboration. The standards and guidelines contained within this document have been reviewed by and are endorsed, at this time, by members of the VSI collaboration.

2 Use of this Document

2.1 Introduction

The primary intent of this document is to assist users in the specification, procurement, design and integration of vetronics systems for both legacy and future land platforms. This document is specifically intended to assist those responsible for:

- specifying requirements for platforms/platform subsystems;
- procurement of platforms/platform subsystems;
- platform integration/manufacture;
- subsystem/component manufacturers.

2.2 Configuration Control

This document has been produced as an output of VSI ARP Contract GM/N04508. A downloadable copy of this document can be found at http://www.vsi.org.uk/.

This document supersedes all previous versions of the Standards & Guidelines namely:

- Vetronics Standards & Guidelines – DERA/LSAB/CR000156/1.0 - Issued June 2000
- Vetronics Standards & Guidelines - QINETIQ/D&TS/LAND/PUB0703046 – Issued February 2007.

2.3 Document Structure

This document is organised as a number of primary areas, namely:

- Requirements - a discussion of the user and system requirements that impact vetronics. This section is intended to aid those tasked with specifying vetronics architectures, systems and subsystems.
- Architecture - a discussion of the merits of a various acrhitectures and a recommendation for Platform Command And Control (C2), Video and Power architectures. The recommended vetronics architecture has been defined as a number of related architectures, namely:
  - the platform C2 architecture;
  - the video architecture;
  - the power distribution architecture.
- Recommended Standards - a listing of the preferred vetronics standards applicable to all future platforms and to upgrades/technology insertions for existing in-service platforms. The standards are presented in a number of subsections each of which considers a different aspect of vetronics on land platforms. The standards are grouped within tables, each table containing standards applicable to a particular aspect of land platform vetronics. An indication is given within each table as to the suitability of each standard for legacy and future platforms. A reference, in the form of a hyperlink, is provided to a paragraph or paragraphs containing either additional information or placing the use of a particular standard in context.

- Guidelines - a series of guidelines for the application of the preferred vetronics standards. The application of the standards will depend on the architecture area of interest, the cost and sophistication of the platform, whether a legacy or new platform is being considered, the technologies being contemplated and the extent of the change being made. The guidelines for each area are presented in a separate section with subsections containing details for a particular level of change and platform complexity. Identification of the appropriate subsection is determined by consulting a decision matrix contained within each section.

3 Vehicle Systems Integration

3.1 What is VSI

The VSI Applied Research Programme is an ongoing UK Ministry of Defence sponsored programme that sets out to assess standards & technologies that have originated in the commercial domain and report on how they may be adapted for the Military domain. In addition, the VSI programme looks at open architectures in which these technologies and standards may be applied and their suitability for application to Land Platforms.

VSI aims to recommend architectures that accommodate the desire for longer in-service lifetimes, minimal cost upgrades, flexibility, rapid modification and operational benefits. Failure to take account of the guidelines recommended by the VSI programme will permit the current ad hoc integration to continue, resulting in platforms that will fail to meet their potential operational effectiveness.

The current VSI programme has been successful in identifying open standards that are applicable to both legacy and future platforms with perhaps the best example of this being MilCAN.

3.2 The benefits of VSI

As military vehicles become increasingly complex and expensive, the drive for cost effectiveness requires that these vehicles should have longer in-service lifetimes than current vehicles.

Changing operational commitments and scenarios coupled with new and varied threats suggest that platform reconfiguration and /or Technology Insertions will be required to meet the changing demands. These changes must be achieved at minimal cost and in short timescales, resulting in the need for platforms equipped with an infrastructure based on open architectures.

Current fielded platforms have generally been designed with little thought to changes during the lifetime of the platform. Providing an infrastructure to accommodate upgrade capability has generally been deleted from the production build standard to save on initial procurement cost, with the result that retrospective integration on current vehicles is very expensive and time consuming.

3.3 Benefits of Open architectures

Open architectures, based on VSI standards & technologies, will promote cross-fleet commonality which in turn will lead to savings generated by an anticipated reduction of costs in the following areas:

- initial development, production and upgrade due to the use of common subsystems;
- reduced spares holdings due to common subsystems and resultant reductions in necessary battlefield logistics;
- common training for both vehicle crews and maintainers;
- reduced routine maintenance through the use of Health and Usage Monitoring Systems (HUMS) (vetronics architectures providing the infrastructure to collect & collate this data);

- will facilitate lower cost upgrades since expansion capability will have been specified at the outset;
- will allow capability enhancement programmes to be conducted on a subsystem by subsystem basis, rather than having to undertake complete vehicle upgrades;
- will allow equipment previously designed & developed for other platforms to be applied to a range of other platforms;

Open architectures, based on VSI standards & technologies, will enable prime contractors to meet cross-fleet and upgrade requirements more easily. In addition, they should be able to draw upon a larger competitive supplier base with resultant cost savings.

4 Requirements

4.1 Introduction

Requirements can be expressed in terms of User Requirements (URs) and System Requirements (SRs). An overview of the differences and similarities between URs and SRs follows; URs fall into two categories:

- capabilities needed by users to solve a problem or achieve an objective;
- constraints on how problems are solved or objectives achieved.

Capability requirements describe functions and operations that the system, in this case a vehicle, will provide to the users.

Constraint requirements place restrictions on how the system can be built and operated, yet do nothing to improve capability and often add considerably to the cost of the solution. Examples of constraints requirements are the platform operational environment and non-functional user requirements such as availability, security, usability, etc.

SRs are an intermediate step between user requirements and system design. SRs define what the system must do to meet the URs, however, they should be expressed in an implementation-independent manner unless as a design constraint dictates that implementation details or terminology are included.

Having established the URs for a system, these must be transformed into SRs and the traceability of the SRs to one or more URs recorded. This process is best carried out with the aid of a requirements engineering tool such as DOORS.

The SRs of a system should be defined in terms of:

- functionality;
- behaviour;
- internal relationships;
- stored information;
- data interfaces;
- performance and relationship with external systems expressed in technical terms.

4.2 User Requirements

Stakeholder requirements which be influenced by vetronics, generally fall into one of these common issues:

- a desire to reduce Life Cycle Costs (LCC);
- an improvement in Improved platform availability;
- support for platform reconfiguration and rapid modification;
- support for crew task sharing & automation;
- support for NEC;
- a desire for enhanced operational effectiveness.

A discussion of these issues is contained in subsections that follow.

4.2.1 Life Cycle Costs

There is clear requirement for a reduction in the LCC associated with all land platforms and this is particularly true of the more complex platforms. This requirement can be achieved by ensuring that:

- integration costs at initial platform development & production are contained;
- platform maintenance & logistic support costs are reduced;
- technology insertions throughout the life of a platform can be accommodated;
- open standards/interfaces are employed thereby opening up the subsystem supplier market to wider competition.

The inclusion of advanced subsystems incorporating the latest technologies, will allow platforms to take advantage of the benefits provided by these improvements. However, this will inevitably lead to an increase in the time required for platform vetronics system development and the cost of development unless it is based on an infrastructure that will allow these variables to be contained or even reduced. The containment of integration costs during platform development & production demands that the integration process, particularly for complex platforms, must be simplified. The provision of a standard, subsystem to subsystem, data communication infrastructure, implemented using standard network technologies and protocols, is essential in achieving this simplification.

A reduction in platform maintenance & logistic support costs can be gained by providing a data communications infrastructure that facilitates intelligent Built in Test (BIT) and Health & Usage Monitoring Systems (HUMS). Such systems will simplify fault diagnosis and aid preventative maintenance. In addition, the use of common subsystems and subsystem interfaces will lead to reduced spares holdings, modular repair/replacement and result in reductions in battlefield logistics.

Through Life Improvement (TLI) is the incremental acquisition of small capability upgrades (via technology insertion), throughout the in-service phase, to continuously maintain the platform capability above the minimum acceptable level. The achievement of TLI requires that a platform is fitted with, at the outset, a data communications infrastructure that has sufficient expansion capability, is extensible and scalable. Without these attributes, retrospective integration of new technologies will be both expensive and time consuming.

Refer to [71] for a discussion of the VSI Metrics. Life Cycle Costs are particularly influenced by an architecture that has the attributes of ‘Reconfigurability’, ‘Enhanceability’ & ‘Logistic Support’.

4.2.2 Improved Platform Availability

In providing a vetronics infrastructure, the platform availability should not be degraded; in fact it is desirable that it should be improved. Greater interaction between subsystems will make it possible to impact the maintainability of the platform and will allow for fault tolerant features to be introduced. Maximisation of platform operational availability is dependent on a number of factors but can be improved by consideration of the following:

- platform reliability;
- provision of support for preservation of function;
- provision of support for graceful degradation.

A high degree of reliability must be achieved by the vetronics infrastructure of the platform. Data communications networks can achieve very low failure rates by employing built in

redundancy e.g by adding dual or triple redundant networks as required to attain the desired reliability.

Preservation of function can be embodied as part of the data communications architecture by ensuring that critical functions within a platform are either duplicated or can operate in an active/standby mode. In the latter mode, the function operating in standby automatically takes over in the event of the failure of the primary active function. This form of preservation of function would not be feasible without a data communications infrastructure.

Although not strictly impacting platform availability, if the accepted definition of this term is used, graceful degradation (the need to retain some level of functionality in the event of subsystem failure or battle damage) can be made possible by virtue of an installed data communications network.

Refer to [71] for a discussion of the VSI Metrics. Improved Platform Availability is particularly influenced by an architecture that has the attributes of 'Reconfigurability', 'Usability' & 'Logistic Support'.

4.2.3 Support for Rapid Modification

The ability to accommodate changes to the platform vetronics systems in order to meet short or long term operational needs will become more prevalent. Platform reconfiguration to meet a specific role, Through Life Improvement or Urgent Operational Requirement (UOR) should be regarded as a fundamental user requirement that mandates the provision of a flexible vetronics architecture. Flexibility can be embodied in an architecture by ensuring that it has the following attributes:

- It is scalable in function, performance and cost;
- It is extensible i.e. further instances of similar modules may be added;
- It is enhanceable i.e. new functions and/or modules implementing new functions may be added to the existing architecture;
- It is upgradeable i.e. modules may be replaced with higher performance versions;
- It is adaptable i.e. changes to the architecture may be achieved without the need to modify hardware or software;
- It should support portability i.e. the interchangeability of similar modules between disparate platforms;
- It should support backward compatibility i.e. no changes to existing hardware and software will be required as a result of architecture enhancements.

Refer to [71] for a discussion of the VSI Metrics. Support for Rapid Modification is particularly influenced by an architecture that has the attributes of 'Reconfigurability' & 'Enhanceability'.

4.2.4 Support for Crew Task Sharing & Automation

The control of platform resources and subsystems and the accessibility of platform information at one or more locations will become more important as the complexity of platforms increases. The inevitable growth in the amount of information provided to the users will need to be countered by an optimisation of the tasks performed. Task automation will therefore become an important factor. Control of resources, provision of information at

a particular location within the vehicle and the ability to allow for task automation necessitate that:

- subsystem data is readily accessible;
- the ability to control subsystems is easily achieved.

Both of these requirements can be facilitated via well defined interfaces to a common standard.

Refer to [71] for a discussion of the VSI Metrics. Support for Crew Task Sharing & Automation is particularly influenced by an architecture that has the attributes of 'Reconfigurability', 'Enhanceability' & 'Usability'.

4.2.5 Support for NEC

The integration of platforms as part of the Network Enabled Capability (NEC) must be supported by the vetronics architecture if maximum benefit is to be gained by the increased flow of information. This must be achieved for both legacy and new platforms. A key element in the integration of platforms as part of the NEC is the ability to extract platform information that can be used throughout the command chain. A flexible architecture will provide the ability to extract this information in addition to the distribution and utilisation of incoming information.

Refer to [71] for a discussion of the VSI Metrics. Support for NEC is primarily influenced by an architecture that has good 'External Integration'.

4.2.6 Enhanced Operational Effectiveness

The desire for enhanced operational effectiveness can be achieved by greater interaction between subsystems. A flexible architecture will facilitate this interaction and allow maximum use to be made of all installed and dismounted platform resources and information.

Refer to [71] for a discussion of the VSI Metrics. Life Cycle Costs are particularly influenced by an architecture that has the attributes of 'Scalability' & 'Usability'.

4.3 System Requirements

The areas in which systems requirements for vetronics are likely to have the largest impact are :

- Common, Layered Network Interface;
- Modularity;
- Scaled Performance;
- Distributed Processing;
- Real-Time Processing;
- Minimal Network Protocol Overheads;
- Diagnostics;
- Fault Tolerance;

- Architecture Partitioning;
- Power.

The following sections contain a discussion of these areas.

4.3.1 Common, Layered Network Interface

The layered approach, as demonstrated by the OSI 7 layer model, should be applied to maintain flexibility, i.e. the specific implementation of each layer of the interface is not defined, only the services that each layer provides to those layers above. This approach allows changes to be made to one layer (e.g the type of databus technology) without adversely affecting the other layers.

4.3.2 Modularity

It is desirable that an architecture should exhibit both functional modularity and equipment modularity. Equipment modularity allows equipment to be combined to form system implementations that meet specific platform requirements or instances. Functional modularity allows functions to be combined within specific modules to meet specific platform requirements. An architecture that exhibits modularity will assist in meeting requirements for adaptability, upgradeability, extensibility, scalability and portability.

4.3.3 Scaled Performance

It is desirable that an architecture allows vetronic functions to be implemented in physical modules that offer differing performance/cost trade-offs, as necessary to meet the requirements of specific platforms. This feature will assist in meeting requirements for scalability and upgradeability.

4.3.4 Distributed Processing

An architecture that supports distributed processing is highly desirable. Such architecture will assist in meeting the requirements for:

- Fault tolerance;
  - by avoiding single points of failure;
  - by promoting standalone operation of individual devices and whole system segments in reversionary modes;
  - by supporting graceful degradation;
  - Facilitating the reassignment of essential processing to surviving processors in the event of device failure.
- Network efficiency – by avoiding communication bottlenecks into central system processors;
- Data and resource sharing;
  - by facilitating peer to peer interactions;
  - by promoting the use of a standard message set between distributed devices.
- Flexibility – interactions between system devices are independent of any central controller, so modifications can also be made independently of any central controller.

Distributed processing promotes modular system composition, and is a pre-requisite for system flexibility.

4.3.5 Real-Time Processing

It is essential that the architecture is capable of utilising network protocols that support both hard and soft real time data transfers. It is desirable that network modules utilise a real-time kernel for vetronic network interactions and, where appropriate, local application processing. In providing an architecture that meets the needs of real-time operation, efficient communication between platform equipments can be achieved.

4.3.6 Network Protocol Overheads

Where possible, the use of network protocols that minimise communication overhead should be considered in order to support efficient transfer of messages between platform equipments.

To support rapid system start-up and fault recovery, on-line automated network management activities should be minimised. Off-line manual network mangement activities should also be minimised to support maintainability and adaptability. Protocols that support the minimisation of network management are therefore desirable to this aim and the architecture should therefore support network protocols that:

- are non-connection based, i.e. connectionless.
    - this avoids the need for network communication connections to be established between communicating devices, either at start-up or during operation.
- are based on logical rather than physical addressing.
    - this removes the need for connections because devices do not need to be aware of what devices they are interacting with or where they are.

4.3.7 Diagnostics

It is desirable that the architecture is capable of supporting system wide fault diagnostics, ideally allowing access from any designated system location. Platform equipment should be capable of detecting and reporting network equipment errors, communication errors and local equipment failures to its controlling application software.

The architecture should also support platform HUMS.

4.3.8 Fault Tolerance

In order to facilitate reversionary modes of operation the architecture should support:

- the utilisation of protocols that support the dynamic re-allocation of platform resources to essential functions, based on priority i.e. graceful degradation;
- stand alone function operation i.e. platform functions shall use reversionary parameter values, modes of operation and safe states to continue operation in the event of system equipment failure;
- distributed processing.

Architectures should feature redundant resources where criticality of function demands it. In order to make use of redundant resources the architecture should support:

- the utilisation of network protocols that are based on masterless network operation, particularly for Media Access Control (MAC);
- the utilisation of protocols that support the dynamic redistribution of responsibilities for the processing of vetronic functions in the event of equipment failure;
- n-level network media redundancy where appropriate.

Distributed processing can provide fault tolerance through the reversionary use of processing resources, by reallocating processes to surviving processors according to priority. The processing resources may or may not be redundant facilities during normal system operation.

4.3.9 Architecture Partitioning

It is desirable that the technology employed on a platform be matched in both cost and performance to the function performed by the particular equipment i.e. the imposition of over specified network technology on platform installed equipment in order to satisfy the highest data communication performance requirement should be avoided. In addition to this, the message exchange protocols employed should be independent of, and portable between, specific data bearer technologies.

Since a vetronic system will contain a number of different message types (e.g. automotive, diagnostic etc.), it is essential that any architecture utilises network protocols that support the simultaneous communication of any vetronic message types on the same network segment.

Safety related communications between subsystems should be partitioned in a way that provides isolation between these and non-safety related communications. It is an essential requirement that an architecture is capable of supporting such partitioning.

4.3.10 Power

Given the increasing quantity and complexity of subsystems that will be fitted to current and future land platforms, the installed vetronics architecture must support conservation of platform power. This implies a requirement for intelligent platform power management and the ability to selectively isolate power from low-priority equipment in favour of high priority as required to conserve power. In addition, the utilisation of equipment that implements low-power component technology and low heat dissipation is implicit.

5 Architecture

5.1 Architecture Definition

An architecture is defined in ANSI/IEEE Std 1471-2000 as 'The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.'

5.2 Architecture breakdown

The functions supported by a platform architecture include:

1. Data acquisition from platform sensors and instrumentation;
2. Communication of data/information between internal subsystems and with off-platform assets;
3. Control of platform sensors, functions and subsystems;
4. Management & Control of platform power;
5. Distribution of platform power.

The items 1 to 4 above are effectively covered by a data communication or platform command and control architecture while item 5 is detailed separately.

Consideration of the data types present on platforms is necessary when deciding on an architecture. Data acquisition and communication will include audio data, low bandwidth automotive data and potentially very high bandwidth data as acquired (in digital video format) from visual and thermal band image sensors.

Audio data, in digital form, typically requires 64 kbps per channel while the requirement for automotive data is unlikely to exceed 1 Mbps. Data/information exchange between subsystems is likely to be accommodated within a bandwidth of between 1 and 100 Mbps depending on the type of data being exchanged (e.g control data or information). High bandwidth digital image data may require bandwidths in the order of several Gbps depending on the number of image sources and the location and type of image processing to be performed on the data.

5.3 Platform Architecture Options

There are numerous available options for the platform command and control architecture; three possible options are presented below:

- A single common architecture (Section 5.3.1) employing a single data network capable of accommodating all requirements from low bandwidth audio data through to high bandwidth digital data. In this case all subsystems are either connected via a dedicated node to the network or a number of subsystems are grouped together and connected via shared node.
- An architecture partitioned by data type (Section 5.3.2) can be constructed by using technologies appropriate to bandwidth requirements. In this case high bandwidth subsystem data exchange, low bandwidth subsystem data exchange and high bandwidth digital image data would all be implemented separately using technologies appropriate to their requirements.

- An architecture partitioned by function (Section 5.3.3) can be constructed by allocating technologies according to the function performed rather than classified according to bandwidth required. For example it may desirable to group together the subsystems performing the automotive functions on a single, low bandwidth, network. Similarly, the management and control of power distribution on a platform could be grouped on a single, low bandwidth network. High bandwidth digital image data would be treated separately primarily to ensure integrity of the image data. Highly deterministic data may require segregation particularly where fault tolerance is an issue.

The above options include the acquisition and dissemination of Image data, for further information on this area see Section 5.4.

The Platform Power Architecture requires separate consideration refer to Section 5.5.

5.3.1 Single, common platform architecture

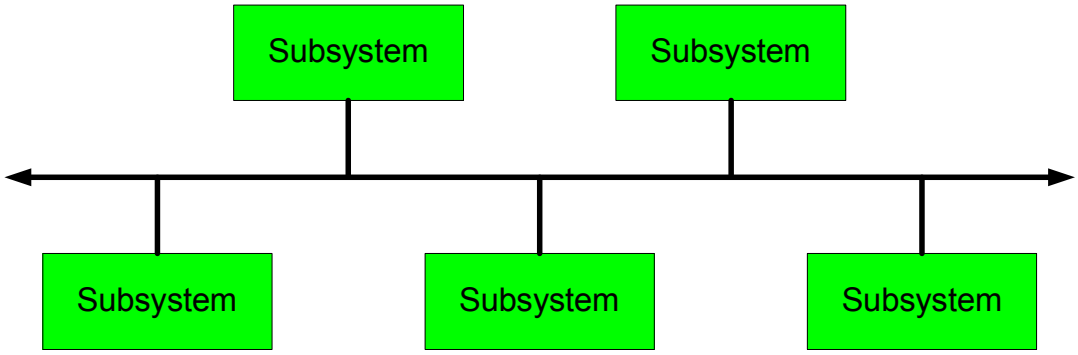

Figure 1 - Logical view of a single common architecture

Figure 1 represents a logical view of a single common architecture, where all nodes communicate through a single network. A physical instantiation of this network would be a switched network such as Gigabit Ethernet.

The main advantages of this architecture are:

- only one type of network interface need be defined for all subsystems;
- Commonality between subsystems and across platforms is easily achieved.

The disadvantages are:

- the network technology must be chosen to meet the both the highest and lowest data rates required and is therefore likely to be a compromise;
- the cost of providing a network interface may be considerably greater than that of the function to be integrated;
- the network technology must be carefully chosen to ensure both Industry support and longevity;
- data transfer via a single network would compromise safety critical functions since changes to the system of a non-safety critical nature may impact those that are safety critical.

5.3.2 Architecture Partitioned by Data Type

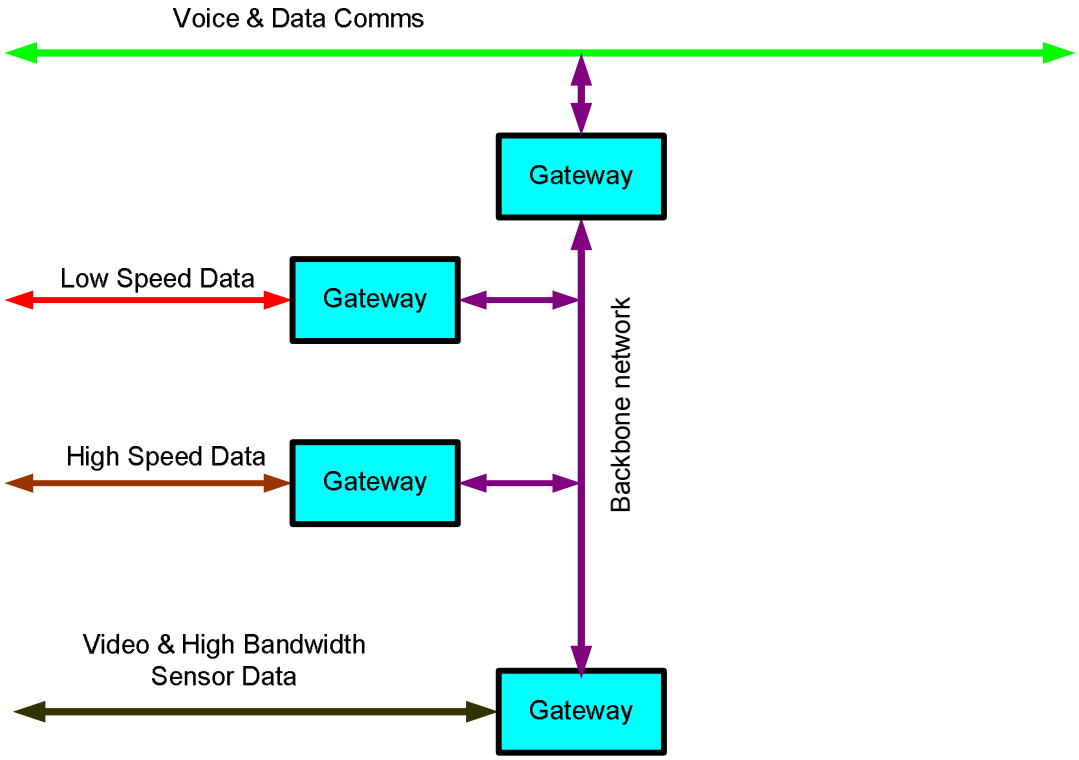

Figure 2 - Architecture partitioned by Data Type

The advantages of this architecture are:

- the network technology can be selected to match data requirements thus avoiding the cost of over specification;
- cross fleet commonality can be achieved by specifying a particular technology for a data type, regardless of platform type or variant.

The disadvantages are:

- the use of multiple network technologies matched to data types will require bridges or gateways wherever there is a need to transfer data between networks;
- safety critical functions would still be compromised since there is no isolation between safety critical and non-safety critical changes elements of the system.

5.3.3 Architecture Partitioned by Function

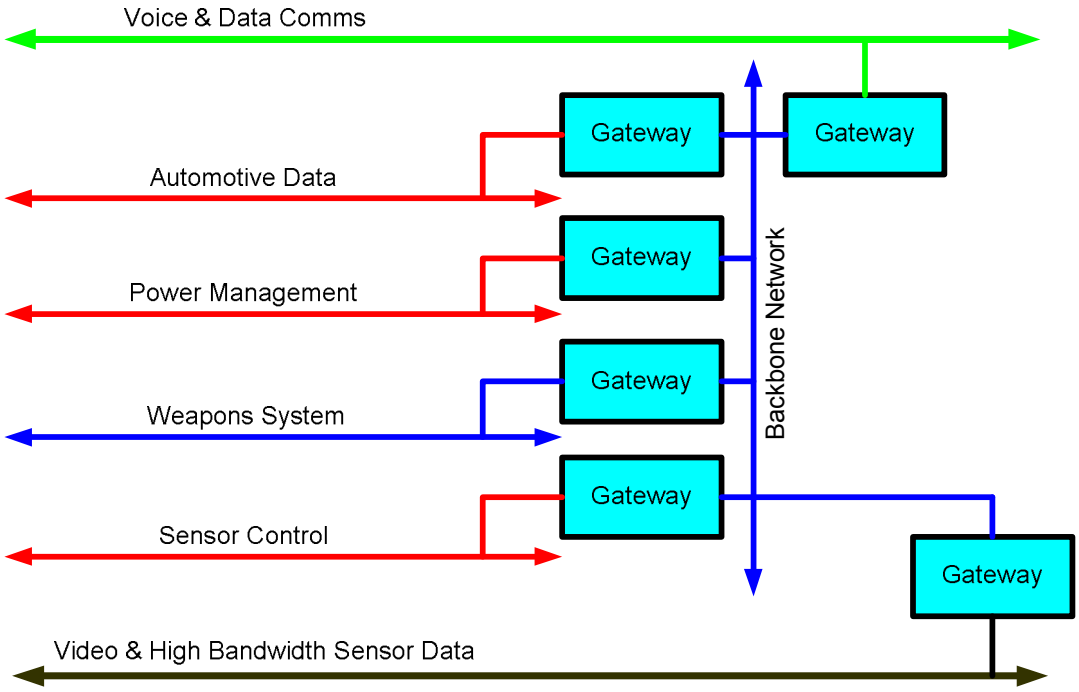

Figure 3 - Architecture partitioned by Function

The advantages of this architecture are:

- the network technology can be selected to match data requirements thus avoiding the cost of over specification;
- cross fleet commonality can be achieved by specifying a particular technology for a data type, regardless of platform type or variant;
- safety critical functions can be isolated from non-safety critical elements of the system thereby allowing changes to be implemented whilst minimising the impact and costs of regression testing.

The disadvantages are:

- where functional partitioning requires isolation of safety critical elements or the use of multiple network technologies and the transfer of data between them, bridges or gateways will be required.

5.4 Platform Video Architecture

The acquisition and dissemination of data from platform image sensors should, in the long term, be implemented using a digital network. Analogue sensor data is likely to become superseded in the not too distant future by digital sensors and should only be considered for short term needs. Having made the decision to employ a digital image distribution network as the basis for the dissemination of image data, the topology of the network is likely to be based on a switched architecture (as opposed to a shared media) in order to comply with the following needs:

- one image source to one display;

- one source to many displays ;
- many sources to one image processor (for image fusion or stitching), this being achieved by combining several one to one connections at the sink (i.e. the image processor).The output of an image processor then becomes a source which can be distributed to one or more displays within the system;
- the distribution system should be scalable & extensible – the addition of more input/output ports is easily accommodated by the introduction of an extra switch or switches to fulfil this requirement.

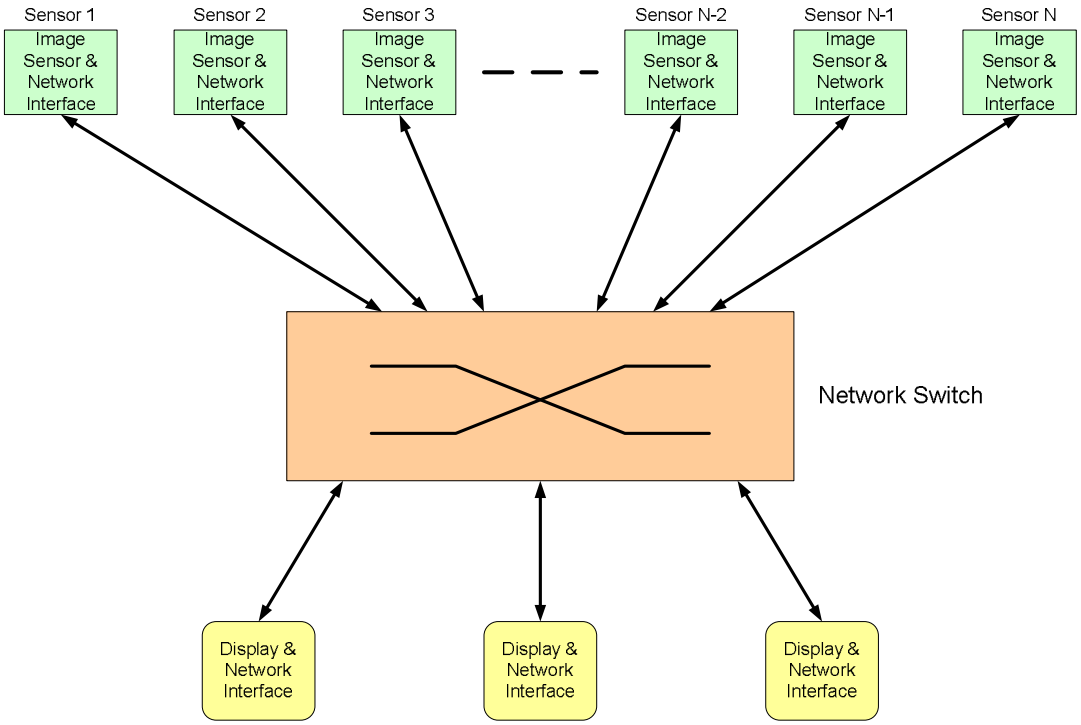

Figure 4 - Video Architecture Topology

A number of technologies are available that could form the basis of a switched topology network but the favoured candidate is Gigabit Ethernet, not least because it has a defined growth path to 10 Gigabit Ethernet. Currently, Gigabit Ethernet is capable of handling uncompressed PAL resolution video encoded as RGB:

768 x 576 x 25 x 24 = 265 Mb/s for RGB encoding

768 x 576 x 25 x 16 = 177 Mb/s for YUV encoding

768 x 576 x 25 x 8 = 89 Mb/s for Monochrome 8 bit encoding

768 x 576 x 25 x 12 = 132 Mb/s for Monochrome 12 bit encoding

However, uncompressed HDTV resolution video encoded as RGB requires a bandwidth of:

1920 x 1080 x 25 x 24 = 1.244 Gb/s for RGB encoding

1920 x 1080 x 25 x 16 = 833 Mb/s for YUV encoding

1920 x 1080 x 25 x 8 = 415 Mb/s for Monochrome 8 bit encoding

1920 x 1080 x 25 x 12 = 622 Mb/s for Monochrome 12 bit encoding

Obviously, uncompressed HDTV resolution video encoded as RGB requires a bandwidth in excess of that provided by Gigabit Ethernet (i.e. 1000 Mb/s) unless some form of processing at the source is carried out to reduce this requirement. This processing could take the form of compression or resolution reduction (either through cropping or decimation).

5.5 Platform Power Architecture

The power distribution system forms the infrastructure from which all electrical systems operate. As such it must be designed for simplicity of operation, maintenance and robustness. As the electrical demands on platforms increase the need to manage the power distribution becomes important. Power management will be designed to ensure a continuation of supply under all operational scenarios. This implies a requirement for intelligent platform power management providing the crew with up to date status of both generated and stored power reserves and the ability to control power to any subsystem from the crew station.

Figure 5 illustrates the recommended power distribution architecture, where the subsystem loads are controlled by networked remote switches. The provision of a power distribution control function is complex and targeted to provide the system with extended operation using existing battery reserves (Silent Watch).

To provide power for high priority systems, a simpler form of this distribution system is required. As these systems tend to be grouped together there is no need for complex power control, however the systems need to be protected at the power distribution unit (PDU) and power to them made available with the minimum of hardware and software support. The power bus bar within the PDU should always default to a condition where power is available to these systems, making them the last ones to be denied power in the event of faults and or damage.

High priority systems are defined as being basic to the functionality of the platform and crew safety, for example:

- Systems associated with mobility - engine, transmission, power generation, brakes, steering (drive by wire).
- What is important here is that the process of powering up these functions should be simplistic, therefore any power management system associated with them should be monitoring, not controlling.

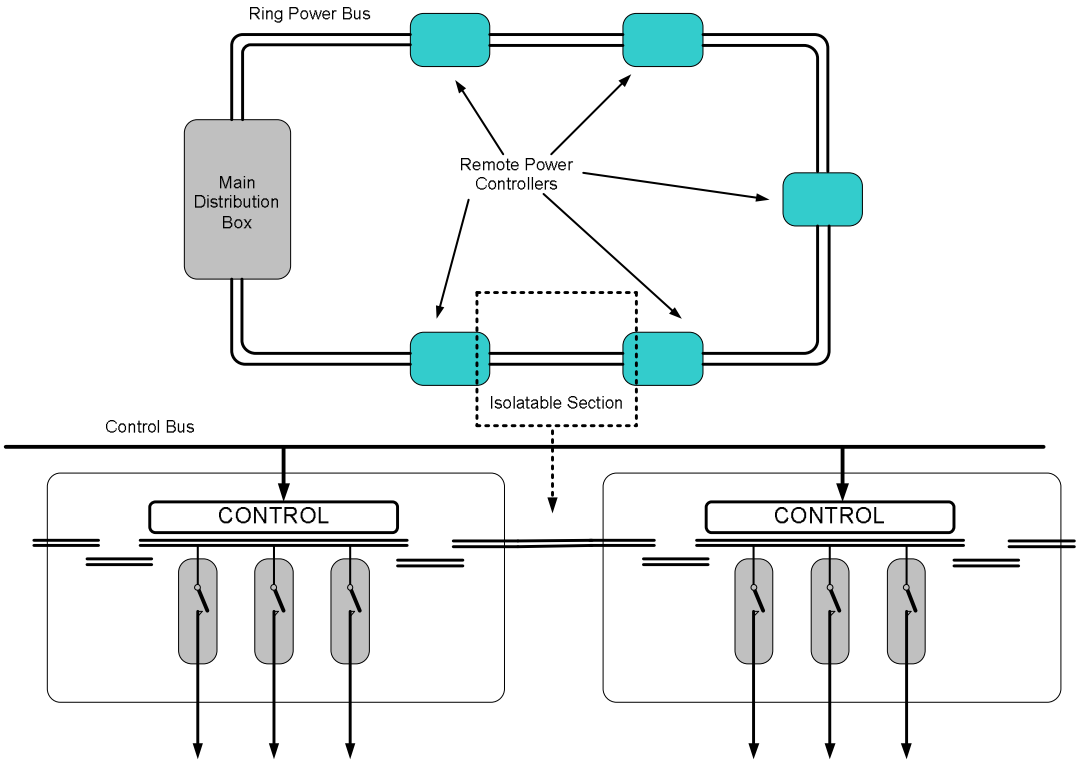

Figure 5 - Recommended Power Architecture

5.5.1 42V and high voltage dc systems

The automotive industry is moving towards designs of a 42V dc power storage distribution and generation system to meet the increasing demand of consumer comfort, safety, and communications and in car entertainment. It is also claimed that a move to a higher power distribution system will result in a number of fundamental component changes, which will result in improved fuel economy. Although these changes are aimed at vehicles with 14V dc systems, eventually trucks will adopt the 42V system.

With the introduction of 42V automotive power distribution all future platform electrical subsystems will be required to operate from that supply either interfacing directly to 42V or via a local converter which could be designed to provide 28V to a number of subsystems. The introduction of 42V will not provide a drastic reduction in cable sizes for high current consumers (50A+) therefore a high voltage distribution system needs to be considered. If the platform has an electrical drive, high voltage will already be present on the platform and this could be extended for subsystem applications. It must be noted that the high voltage system used for electric drive will have a wide operating range therefore any electrical subsystems powered from it must be able to accept this variation in supply. The alternative is to use a converter to 'clean up' the supply reducing the variation. For high currents this will be a large device possibly requiring cooling and it could be electrically noisy. Therefore use of converters should be avoided. If the platform has a conventional mechanical drive the HV distribution system would be introduced solely to support the demands of the high current subsystems. These subsystems would not be used during silent watch therefore battery support would not be necessary and their operation would be restricted to when a generator is on line. The HV could be provided by a dual output or secondary generator. Figure 5 illustrates the architecture

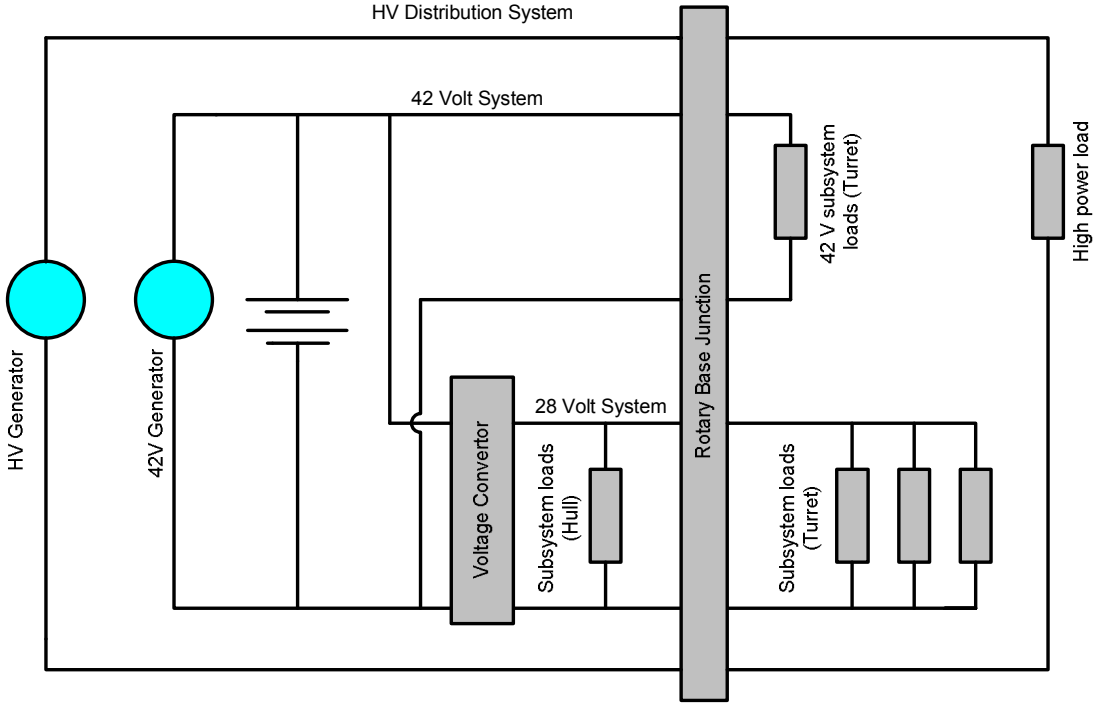

Figure 6 - Example of combined High Voltage and Low Voltage architecture

6 Recommended Standards

Note: Standards and associated technologies that may be applicable to land platforms continue to evolve, hence the need to review this document on a regular basis.

This section is divided into a number of subsections each of which considers a different aspect of vetronics on land platforms.

The tables contained within each subsection identify preferred standards for use in land platforms. Within each subsection, standards have been grouped according to their use and an indication given as to their applicability to legacy and future systems. Similar standards are contained in a single table and a reference is provided to a paragraph or paragraphs containing either additional information or text that places the use of a particular standard in context.

6.1 Standards for Platform Command & Control

The platform command and control (C2) architecture provides the infrastructure by which the control, management and interaction between vehicle subsystems is achieved. This aspect of the C2 architecture may be implemented with the standards contained within the subsections listed below:

- Standards for low speed serial busses;
- Standards for point to point serial interfaces;
- Standards for LAN technologies;
- Standards for peripheral busses;
- Standards for communication and services.

6.1.1 Standards for Low Speed Serial Bus

Standard	Description	Legacy Systems	Future Systems
Def Stan 00-18 (Part 2) [MIL-STD-1553B]	Serial, Time Division, Command/Response Multiplex Data Bus Standard	Y	N
EIA 485	Multi-drop bus	Y	Y
ISO 11898	Controller Area Network (CAN) Bus	Y	Y
MilCAN	A deterministic protocol for CAN which uses ISO 11898	Y	Y
SAE J1939	A high layer CAN protocol for automotive systems	Y	Y
TTP/C	A Fault Tolerant, Time-Triggered technology	Y	Y
FlexRay	A Fault Tolerant, Time-Triggered technology	See below	See below

Table 1 - Standards for Low Speed Serial Bus

Def Stan 00-18 (Part 2)

Serial, time division, command/response multiplex data bus standard is well proven within the military avionics arena and describes a deterministic, central media access control method for subsystem communication. While the available bit rate is 1 Mbit/sec, the method of achieving determinism can be regarded as inefficient in terms of bandwidth. The inability to add subsystems without major changes to the scheduling of messages on the bus severely limits flexibility when implementing a communications infrastructure with this standard. A further disadvantage is the cost of implementing a remote terminal (subsystem node) when considered in the context of land platforms rather than avionic systems.

There are a small number of platforms that currently implement Def Stan 00-18 (Part 2) [MIL-STD-1553B]. It is recommended that the use of this standard be continued in these platforms where no economically viable alternative is available when considering new equipment insertions. When considering new platforms, the requirements for flexibility cost and cross fleet commonality tend to exclude this standard as a candidate.

Electrical Industries Association specification EIA 485

Is the evolution of EIA 422 to include multiple transmitters. In addition, it increases the number of receivers to 32. EIA 485 is a general scheme for signalling along twisted pairs with a multi-point network. The designer must determine length, data rate, cable characteristic, etc. for each particular implementation. All issues of framing, data representation, media access are outside the scope of EIA 485 and must to be provided by some other protocol, the most common being High Level Data Link Control (HDLC).

ISO 11898

Defines requirements for the Data Link layer and the Physical Layer of the ISO Open Systems Interconnect seven layer model only as applied to Controller Area Network bus (CANbus). A higher level protocol is required between the CAN Data Link layer and the Application.

The MilCAN specifications are available at www.MilCAN.org. MilCAN is included in Stanag 4268.

CAN has a maximum bit rate of 1Mbit/s although this is dependent on bus length such that lower bit rates are often used for long bus lengths.

The use of MilCAN has gained widespread support in the defence community and is already well established in both the commercial automotive world and the process industry. MilCAN is recommended for use in applications where a C2 bus does not require a high data rate e.g. less than 1Mbit/s.

SAE J1939

The SAE (Society of Automotive Engineers) Truck and Bus Control and Communications Sub-committee started the development of a CAN-based application profile for in-vehicle communication in trucks during the early 1990s. The J1939 specification, with its engine, transmission, and brake message definitions, is dedicated to diesel engine applications. Other industries have adopted the general J1939 communication functions and ISO have standardized the J1939-based truck and trailer communication (ISO 11992) and the J1939-based communication for agriculture and forestry vehicles (ISO 11783).

TTP/C

TTP is based on more than 20 years of research and development work carried out at the Technical University of Vienna. TTP is based on TDMA (time-division multiple access) and has many fault tolerant features built into the protocol. TTP is a low cost, open data bus standard designed for safety critical and time relevant systems. It is an ideal solution for applications such as Drive by Wire, Fire Control, Defensive
Aid Suites and Combat Identification. TTP has been evaluated against requirements for next generation 'X-by-wire' automobile applications, for example:

- Safety;
- Cost-effectiveness;
- High data rates;
- Composability and ease of system integration;
- Flexibility in terms of vehicle platforms and model variations;
- Extendibility in the field.

TTP is preferred over FlexRay for the following reasons

- TTP has hardware implementation of built in fault tolerant features that are abstracted from the Application programmer.
- TTP is amore mature technology than FlexRay and has been used on a number of Safety Critical systems in the Avionics domain.

Further information is available at www.tttech.com

Ultra Electronics are currently developing a range of TTP products for military vetronics applications
http://www.ultra-electrics.com/LandSpace/Datasheet_LandSpace.asp?ProdID=1209

FlexRay

FlexRay has been developed by the FlexRay Consortium, an alliance of automotive, semiconductor and electronic systems manufacturers working together to develop a deterministic and fault-tolerant bus system with high data rates for advanced automotive control applications.

The FlexRay communications protocol provides flexibility and determinism by combining a scalable static and dynamic message transmission, incorporating the advantages of familiar synchronous and asynchronous protocols. The protocol also supports:

- Fault-tolerant clock synchronization via a global time base;

- Collision-free bus access;
- Guaranteed message latency;
- Message oriented addressing via identifiers;
- Scalable system fault-tolerance via the support of either single or dual channels.

FlexRay has been evaluated by QinetiQ as a competitor to TTP for Safety Critical applications in the Land Domain. However, FlexRay appears less robust than TTP and is therefore not regarded as first choice when selecting a fault tolerant protocol.

Further information is available at www.flexray-group.com

6.1.2 Standards for point to point serial interfaces

Standard	Description	Legacy Systems	Future Systems
RS232	Serial data interface	Y	Y
RS423	Serial data interface - Unbalanced	Y	Y
RS422	Serial data interface - Balanced	Y	Y

Table 2 - Standards for point to point serial interfaces

EIA 232

EIA 232 originated in the telephone industry and was aimed at connecting a telephone circuit modem, known as the Data Communication Equipment, (DCE) to computing equipment, known as the Data Transmission Equipment, (DTE) so that two computers could communicate over the Public Switched Telephone Network (PSTN). In effect EIA 232 is a communication standard for a short distance multi-wire interface but is frequently used to connect together computers (DTEs) which are physically close or for connecting a computer to a slow data rate peripheral. In many cases 'EIA 232 compatible' equipments only implement that part of the standard needed to achieve connection between two DTEs.

EIA 423

EIA 423 defines the electrical characteristics of an unbalanced voltage digital interface circuit for point to point interconnection of serial binary signals. EIA 232 is often quoted as the standard even though the electrical characteristics of EIA 423 are implemented.

Where equipment has an EIA 232/423 interface fitted as standard the use of these standards is accepted. However, the equipment designer should be encouraged to provide equipment conforming to EIA 422.

EIA 422

EIA 422 defines the electrical characteristics of a balanced voltage digital interface circuit for point to point interconnection of serial binary signals. EIA 422 is a differential point to point link that may be used to transmit data at rates of up to 10Mbit/s depending on the cable length between transmitter and receiver. Although EIA 422 is essentially a point to point standard, there is allowance within the standard for up to 10 parallel receivers to be implemented.

6.1.3 Standards for LAN Technologies

Standard	Description	Legacy Systems	Future Systems
IEEE 802.3	CSMA/CD, 10/100/1000BASE-T	Y	Y

Table 3 - Standards for LAN Technologies

IEEE 802.3 (Ethernet) technology should be considered where there is a requirement for high bandwidth, non-deterministic and/or non-real time data transfer within the platform.

Wherever possible, the fibre versions of those listed in the above table should be used where there is a potential Electromagnetic Compatibility (EMC) or TEMPEST threat providing the chosen fibre can operate in the specified military environment.

6.1.4 Standards for Peripheral Busses

Standard	Description	Legacy Systems	Future Systems
USB Specification, Revision 2.0	Universal Serial Bus (USB)	Y	Y

Table 4 - Standards for Peripheral Busses

USB is specified in three defined areas, interconnect, devices and host. The USB interconnect specifies the manner by which USB devices are connected to, and communicate with the host. The specification defines the bus topology, inter-layer relationships, data flow models and schedules. Devices and hubs are physically connected to the host in a tiered star topology. Since USB provides a shared interconnect, access to it must be scheduled, in order to support isochronous data transfers and eliminate arbitration overhead. USB has gained momentum in the commercial world. This standard is suggested for use for the attachment of peripheral devices, e.g. printers.

6.1.5 Standards for Communication and Services

Standard	Description	Legacy Systems	Future Systems
IETF STD 62	Simple Network Management Protocol	Y	Y
RFC 959	File Transfer Protocol (FTP)	Y	Y
RFC 793	Transmission Control Protocol (TCP)	Y	Y
RFC 768	User Datagram Protocol (UDP)	Y	Y
RFC 791	Internet Protocol (IP)	Y	Y
RFC 2616	Hypertext Transfer Protocol (HTTP)/1.1	Y	Y

Table 5 - Standards for Communication and Services

IETF STD 62 describes an architecture for describing Simple Network Management Protocol (SNMP) Management Frameworks. The architecture is designed to be modular to allow the evolution of the SNMP protocol standards over time. The major portions of the

architecture are an SNMP engine containing a Message Processing Subsystem, a Security Subsystem and an Access Control Subsystem, and possibly multiple SNMP applications which provide specific functional processing of management data.

RFC 959 specifies FTP a commonly used protocol for exchanging files over any network that supports the TCP/IP protocol. An FTP transfer usually takes place between a server and a client. The FTP server, running FTP server software, listens on the network for connection requests from clients. The client, running FTP client software, initiates a connection to the server. Once connected, the client can do a number of file manipulation operations such as uploading files to the server, download files from the server, rename or delete files on the server and so on.

RFC 793 specifies Transmission Control Protocol (TCP)**,** a protocol that guarantees reliable and in-order delivery of data from sender to receiver. Applications send streams of octets to TCP for delivery through the network. TCP divides the byte stream into appropriately sized segments. TCP then passes the resulting packets to the Internet Protocol, for delivery through a network to the TCP module of the entity at the other end. TCP checks to make sure that no packets are lost by giving each packet a *sequence number*, which is also used to make sure that the data is delivered to the entity at the other end in the correct order. The receiving TCP module returns *acknowledgement* for packets which have been successfully received; a timer at the sending TCP module will cause a *timeout* if an acknowledgement is not received within a reasonable round-trip time, causing the lost data to be *re-transmitted*. The TCP also employs a checksum; one is computed at the sender for each block of data before it is sent and checked at the receiver.

RFC 768 specifies User Datagram Protocol (UDP)**,** a transport protocol that does not guarantee reliable and in-order delivery of data from sender to receiver in the way that TCP does. Datagrams may arrive out of order, appear duplicated, or go missing without notice. Avoiding the overhead of checking whether every packet actually arrived makes UDP faster and more efficient than TCP, at least for applications that do not need guaranteed delivery. Time-sensitive applications often use UDP because dropped packets are preferable to delayed packets. Unlike TCP, UDP supports packet broadcast (sending to all nodes on local network) and multicasting (sending to multiple nodes).

RFC 791 specifies the Internet Protocol (IP) a data-oriented protocol used for communicating data across a packet-switched network. IP provides an *unreliable* service (i.e., best effort delivery). In terms of reliability the only thing IP does is ensure the IP packet's header is error-free through the use of a checksum.

RFC 2616 specifies a communications protocol used to transfer or convey information on the World Wide Web. HTTP is a request/response protocol between clients and servers. The originating client, such as a web browser, spider, or other end-user tool, is referred to as the user agent. The destination server, which stores or creates resources such as HTML files and images, is called the origin server. HTTP does not need TCP/IP. Since it only presumes a reliable transport; any protocol that provides such guarantees can be used. HTTP is seen as a standard that may be used in platform for provision of a browsing facility, e.g. for the interrogation of electronic manuals.

6.2 Standards for Platform Video

The platform video architecture provides the infrastructure for distribution and display of information of high bandwidth sensors such as Visual band cameras and Thermal Imagers.

The video architecture may be implemented using the standards contained within the subsections listed below:

- Standards for Video Encoding;
- Standards for Video Distribution;
- Standards for Video Compression;
- Standards for Video Display.

6.2.1 Standards for Platform Video Encoding

Standard	Description	Legacy systems	Future systems
ITU-R BT.601	ITU-R BT.601 Encoding Parameters of Digital Television for Studios	Y	Y
ITU-R BT.656	ITU-R BT.656 Interfaces for Digital Component Video Signals in 525-line and 625-line Television Systems operating at the 4:2:2 level of Recommendation ITU-R BT.601 (Part A)	Y	Y
SMPTE 274M	1920 x 1080 Image sample Structure, Digital Representation and Digital Timing Sequences for Multiple Picture Rates	Y	Y
SMPTE 296M	1280 x 720 Progressive Image Sample Structure - Analog and Digital Representation and Analog Interface	Y	Y
NATO MAS STANAG 3350 AVS	Guide to the Analogue video standard for aircraft system applications	Y	N
ITU-R BT 472	Video Frequency characteristics for 625-line colour or monochrome television systems	Y	N

Table 6 - Standards for Platform Video Encoding

ITU-R BT.601 specifies the sampling scheme to be used for digital representation of 625/525 line video for broadcast quality.

ITU-R BT.656 describes a simple digital video protocol for streaming uncompressed PAL or NTSC Standard Definition TV (525 or 625 lines) signals. The protocol builds upon the 4:2:2 digital video encoding parameters defined in ITU-R BT.601, which provides interlaced video data, streaming each field separately, and uses the YCbCr color space and a 13.5 MHz sampling frequency for pixels.

SMPTE 274M specifies the sampling scheme to be used for digital representation of 1920 x 1080 video.

SMPTE 296M specifies the sampling scheme to be used for digital representation of 1280 x 720 video.

NATO MAS STANAG 3350 AVS specifies parameters for 875, 625 and 525-line analogue video systems.

To provide systems designers utilising legacy analogue video systems with details regarding line and frame timing, Table 4-6 makes reference to **ITU-R BT.472**. However, where analogue video techniques must be used for distribution of colour images, component signal formats, such as YUV or S (Y/C), will provide clearer images than will the use of the composite format.

6.2.2 Standards for Platform Video Distribution

Protocols that are used to distribute digital video over Gigabit Ethernet according to the Standard for Video Distribution in Vetronic Systems using Gigabit Ethernet [70].

Standard	Description	Legacy systems	Future systems
IEEE 802.3ab	Gigabit Ethernet over copper wiring	Y	Y
RFC 791	Internet Protocol	Y	Y
RFC 768	User Datagram Protocol	Y	Y
RFC 2365	Administratively Scoped IP Multicast	Y	Y
RFC2236	Internet Group Management Protocol, Version 2	Y	Y
RFC 3550	RTP - Transport Protocol for Real-Time Applications	Y	Y
RFC 4175	RTP Payload Format for Uncompressed Video	Y	Y
draft-ietf-avt-rtp-jpeg2000-15	RTP Payload Format for JPEG 2000 Video Streams	Y	Y
RFC 2974	Session Announcement Protocol	Y	Y
RFC 4566	Session Description Protocol	Y	Y
RFC 3171	IANA Guidelines for IPv4 Multicast Address Assignments	Y	Y
SMPTE 259	SDI- Serial Digital Interface	Y	Y
SMPTE 292	HD-SDI Serial Digital Interface	Y	Y

Table 7 - Standards for Platform Video Distribution

RFC 791 specifies the Internet Protocol (IP) a data-oriented protocol used for communicating data across a packet-switched network. IP provides an *unreliable* service (i.e. best effort delivery). In terms of reliability the only thing IP does is ensure the IP packet's header is error-free through the use of a checksum.

RFC 768 specifies User Datagram Protocol (UDP), a transport protocol that does not guarantee reliable and in-order delivery of data from sender to receiver in the way that TCP does. Datagram's may arrive out of order, appear duplicated, or go missing without notice. Avoiding the overhead of checking whether every packet actually arrived makes UDP faster and more efficient than TCP, at least for applications that do not need guaranteed delivery. Time-sensitive applications often use UDP because dropped packets are preferable to delayed packets. Unlike TCP, UDP supports packet broadcast (sending to all nodes on local network) and multicasting (sending to multiple nodes).

RFC 2365 defines the "administratively scoped IPv4 multicast space" to be the range of IP address from 239.0.0.0 to 239.255.255.255. The Organization Local Scope range also defined, and is the multicast space from which an organization should allocate sub-ranges when defining scopes for private use. In addition, it describes a simple set of semantics for the implementation of Administratively Scoped IP Multicast.

RFC 2236 defines The Internet Group Management Protocol (IGMP) as used by IP hosts to report their multicast group memberships to any immediately-neighbouring multicast routers. This RFC describes only the use of IGMP between hosts and routers to determine group membership.

RFC 3550 specifies the Real-time Transport Protocol (RTP), which provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. Those services include payload type identification, sequence numbering, timestamping and delivery monitoring. Applications typically run RTP on top of UDP to make use of its multiplexing and checksum services; both protocols contribute parts of the transport protocol functionality. RTP supports data transfer to multiple destinations using multicast distribution if provided by the underlying network.

RFC 4175 specifies a packetisation scheme for encapsulating uncompressed video into a payload format for the Real-time Transport Protocol, RTP. It supports a range of standard- and high-definition video formats, including common television formats such as ITU-R BT.601, and standards from the Society of Motion Picture and Television Engineers (SMPTE), such as SMPTE 274M and SMPTE 296M. The format is designed to be applicable and extensible to new video formats as they are developed.

draft-ietf-avt-rtp-jpeg2000-15 describes an RTP payload format for the ISO/IEC International Standard 15444-1 | ITU-T Rec. T.800, otherwise better known as JPEG 2000. JPEG 2000 features are considered in the design of this payload format. JPEG 2000 is a truly scalable compression technology allowing applications to encode once and decode many different ways. A JPEG 2000 video stream is formed by extending from a single image to a series of JPEG 2000 images.

RFC 2974 describes version 2 of the multicast session directory announcement protocol, Session Announcement Protocol (SAP) and the related issues affecting security and scalability that should be taken into account by implementers.

RFC 4566 defines the Session Description Protocol (SDP). SDP is intended for describing multimedia sessions for the purposes of session announcement, session invitation and other forms of multimedia session initiation.

RFC 3171 provides guidance for the Internet Assigned Numbers Authority (IANA) in assigning IPv4 multicast addresses.

SMPTE 259 Serial Digital Interface (SDI) is a serial implementation of ITU-R BT.601 and is used internationally for video distribution within broadcast studios.

SMPTE 292 1.5 Gb/s Serial Digital Interface.

6.2.3 Standards for video compression

Standard	Description	Legacy systems	Future systems
ISO/IEC15444-1	JPEG 2000 Image Coding System	Y	Y
ISO/IEC 13818 (MPEG2)	Information technology - Generic coding of moving pictures and associated audio information	Y	Y
ISO/IEC 14496 (MPEG4)	Coding of moving pictures & audio	N	Y

Table 8 - Standards for video compression

ISO/IEC15444-1, JPEG 2000 image coding system. Defines a set of lossless (bit-preserving) and lossy compression methods for coding bi-level, continuous-tone grey-scale, palletized colour, or continuous-tone colour digital still images; specifies decoding processes for converting compressed image data to reconstructed image data; specifies a code stream syntax containing information for interpreting the compressed image data; specifies a file format; provides guidance on encoding processes for converting source image data to compressed image data; provides guidance on how to implement these processes in practice. JPEP 2000 is a wavelet-based image compression that does not generate the characteristic 'blocky and blurry' artefacts of JPEG and MPEG-2. When used for video, each frame is processed individually, with no intra (reference) and predicted frames as in various MPEG schemes resulting in errors confined to the frame they occur in.

ISO/IEC 13818, commonly termed MPEG2, specifies techniques for compression of moving images, and is typically used for compression of video and audio down to data rates ranging from 6 to 50 Mb s-1. At the higher end of this scale, it is considered to be visually lossless. It has been extremely successful on an international scale and is now widely used for terrestrial and satellite video. This standard is in widespread civilian use and may be suitable for limited Platform applications. However, it is unlikely to be suitable for applications associated with real-time or automated target detection, due the introduction of image latency or false picture elements caused by the lossy nature of the algorithm.

ISO/IEC 14496, commonly termed MPEG4, specifies techniques suitable for heavy compression of moving images and is typically used for compression of video and audio down to data rates ranging from 150 to 400 Kb s-1. It is now being widely adopted for video conferencing and internet streaming applications. Disadvantages of the standard from the Platform viewpoint are that the encoding process discards video data, incurs signal latency, and produces images of low quality. This standard is preferred because it is international,

open, will be in widespread use in the commercial arena and is suitable for a limited range of Platform applications.

6.2.4 Standards for video display

Display formats appearing in the standards list are those suitable for display of computer generated images. It is anticipated that displays compliant with these standards will certainly be used on complex platforms, and may be used on simple platforms.

Standard	Description	Legacy systems	Future systems
DDWG DVI	Digital Visual Interface (DVI)	Y	Y
VESA PnD	Display monitor plug & display	Y	Y
VESA XVGA	Extended VGA display monitor timing	Y	Y
VESA SVGA	Super VGA display monitor timing	Y	Y

Table 9 - Standards for video display & recording

The Digital Display Working Group (DDWG) **Digital Visual Interface (DVI**), specifies a digital interconnect between processing unit and flat panel display, which utilises Transmission Minimised Differential Signalling (TDMS) signals. It has been more recently developed than the Video Electronics Standards Association (VESA) Plug and Display standard, and appears to be having more commercial success. Use of digital signals in this last link in the distribution chain will enhance the quality of displayed images.

The **VESA Plug and Display** standard specifies a digital interconnect between processing unit and flat panel display. Use of digital signals in this last link in the distribution chain will enhance the quality of displayed images.

The **VESA Extended Video Graphics Adapter** (XVGA) specification gives details of display timings for resolution of 1024 x 768 display pixels. It is anticipated that many platforms will be fitted with flat panel displays operating at this resolution.

The VESA **Super Video Graphics Adapter** (SVGA) specification gives details of display timings for resolution of 800 x 600 display pixels. It is anticipated that many platforms will be fitted with flat panel displays operating at this resolution.

6.3 Standards for Platform Software

In order to realise the benefits of software architecture, especially with regard to development, maintenance and consistency, a common approach to software projects through best practice and supported by standards is preferable. Within the software industry, standards are evolving. As a result, projects may start by applying a standard which is later modified or withdrawn during the project lifetime. However, continued use of the initially applied standards is essential for the well-being of a project, if cost and time estimates are to be met. With this in mind, some of the standards identified may be suitable for continued use in current projects, though not applicable to new projects. Relevant standards for the different software areas are identified below:

- Standards for programming languages;
- Standards for safety;

- Standards for software architecture;
- Standards for information transfer coding.

6.3.1 Standards for Programming Languages

Standard	Description	Legacy systems	Future systems
ISO/IEC 8652:1995(E)	Programming Language Ada	Y	Y
ISO/IEC 9899:1999	Programming Language C	Y	Y
MISRA-C : 2004	Guidelines for the use of the C language in Critical Systems	Y	Y
ISO/IEC 14882:2003	Programming Language C++	Y	Y

Table 10 - Standards for Programming Languages

Ada is no longer mandated by the UK Ministry of Defence (MOD), but is suited to military applications.

C is provided for completeness, however, C++ is expected to replace C for most, if not all, new applications.

MISRA-C: 2004 specifies a subset of the C programming Language that is intended to be suitable for embedded systems. It contains a list of rules concerning the use of the C programming language together with justifications and examples. The guidance has been used in rail, military, aerospace, medical and general embedded systems products as well as the originally intended automotive market.

C++ is becoming the preferred programming language for military applications.

6.3.2 Standards for Safety

Standard	Description	Legacy systems	Future systems
Def Stan 00-56 Part 1	Safety Management Requirements for Defence Systems - Part 1 Requirements	Y	Y
Def Stan 00-56 Part 2	Safety Management Requirements for Defence Systems - Part 2 Guidance	Y	Y
ISO61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems	Y	Y

Table 11 - Standards for Safety

Def Stan 00-56 is concerned with the safety management requirements for defence systems. The standard specifies safety management procedures, analysis techniques and the safety verification techniques that are applicable during the project lifecycle. Its purpose is to minimise the possibility of equipment entering service with unacceptable safety characteristics.

IEC 61508 Is a standard that covers the functional safety of systems. Functional safety is an element of the overall system safety and is concerned with the correct operation of the system in response to inputs and stimuli. The standard defines the requirements to ensure that systems are designed correctly and the required safety integrity levels are achieved.

6.3.3 Standards For Software Architecture

Standard	Description	Legacy systems	Future systems
STANAG 4250	OSI Reference Model	Y	Y
ISO/IEC 7498-1	Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model	Y	Y
ISO/IEC 8822	Information Technology - Open Systems Interconnection - Presentation Service Definition	Y	Y
ISO/IEC10746	Information Technology - Basic Reference Model of Open Distributed Systems	Y	Y
SAE AS 4893	Generic Open Architecture (GOA) Framework	x	Y

Table 12 - Standards for software architecture

ISO/IEC 7498-1 Information Technology - Open Systems Interconnection - Basic Reference Model: This standard is part of the Open systems interconnection suite, and is concerned with the definition of the OSI reference model. The reference model is international in scope, and provides a framework within which system designers and planners can describe and plan networking systems. It comprises seven layers - physical, data link, network, transport, session, presentation and application, to which the complementary OSI protocol suite can be applied.

ISO/IEC 8822 Information Technology - Open Systems Interconnection - Presentation Service Definition. This standard is part of the Open systems interconnection suite, and is concerned with the definition of the OSI presentation service definition. The presentation-layer implementation of the OSI protocol suite consists of a presentation protocol and a presentation service. The presentation protocol allows presentation-service users (PS-users) to communicate with the presentation service.

ISO/IEC10746 (various parts) Information Technology - Basic Reference Model of Open Distributed Processing. These suites of specifications are concerned with the provision of a framework to support the distribution, internetworking, interoperability and portability of open distributed processing systems. They provide a reference model for open distributed processing systems (RM-ODP), and explanatory material for interpretation and applications.

AS 4893 Generic Open Architecture (GOA) Framework. These suites of standards, some of which are under development under the auspices of the SAE, cover the four layers that are specified as a Generic Open Architecture. These are application software, system services, resource access services, and physical resources layers.

6.3.4 Standards For Middleware

Standard	Description	Legacy systems	Future systems
OMG Specification formal/03-11-01	Real Time - CORBA Specification	Y	Y
OMG Specification formal/02-08-01	Minimum CORBA	Y	Y
OMG Specification formal/07-01-01	Data Distribution Service for Real-time Systems, v1.2	Y	Y

Table 13 - Standards for Middleware

The use of Middleware is seen as a method of mitigating problems due to integration of new systems or upgrades into current and future platforms. Middleware consists of software components that provide a set of services within a system that allow multiple processes instantiated on one or more systems to operate across a network. Middleware is often likened to glue that binds applications and the platform processing, i.e. it abstracts one from the other enabling development of one independently of the other. The purpose of the introduction of middleware into the architecture is to allow a high degree of data availability and to mitigate the effects of platform upgrade and improvements.

Real Time CORBA (RT CORBA) is an extension to the CORBA specification, developed by the OMG, which enables the Object Request Broker (ORB) based architecture to operate in real time. Real Time CORBA is an open, vendor-independent architecture and infrastructure that applications use to work together over networks. Real-Time CORBA adds a number of extensions to the CORBA specification but sacrifices some of the general purpose nature of CORBA in order to support the development of Real-Time systems. The use of RT CORBA would be associated with architectures that conform to a Client/Server model

Minimum CORBA is a specialised subset of the CORBA specification designed for systems with limited resources. The use of minimum CORBA would be associated with architectures that conform to a Client/Server model

Data Distribution Service (DDS) is a standard developed by the OMG. This specification standardises the APIs required by an application to use a Publish and Subscribe model. In a Publish and Subscribe model the Publisher pushes or broadcasts data onto the network. Any system that wants the data subscribes to the broadcast, neither the Publisher nor the Subscriber requires any knowledge of one another. This is a highly flexible model that lends itself well to distributed architectures. The main advantage from the military User's perspective is that this model is designed for loosely distributed applications which have beneficial implications upon development, maintenance & obsolescence.

6.3.5 Standards for Information Transfer Coding

Standard	Description	Legacy systems	Future systems
ISO/IEC 8824-2	Information Technology - Abstract Syntax Notation One (ASN.1): Information Object Specification	Y	Y
ISO/IEC 8825-2	Information Technology - ASN.1 Encoding Rules: Specification of Packet Encoding Rules (PER)	Y	Y

Table 14 - Standards for information transfer coding

ISO/IEC 8824-2 this standard concerns the specification of an ASN.1 notation, which allows information object classes, as well as individual information objects and sets thereof, to be defined and given reference names. An information object class is a template for the collection of information that makes up the attributes of any members of that class.

ISO/IEC 8825-2 this standard concerns the specification of a set of basic encoding rules that may be applied to values of types that are defined in the ASN.1 convention. Application of the encoding rules produces transfer syntax for such values. It is implicit in the specification that these encoding rules are also used for decoding.

6.4 Standards for Platform Power

Standards which have relevance to the specification and implementation of platform power generation management and distribution systems are identified:

6.4.1 Standards for Power

The Table 15 identifies standards which have relevance to the specification and implementation of platform power generation management and distribution systems. Due to the specific requirements of land platforms, the majority of standards were previously controlled by government standardisation organisations. The current list has been updated with commercial standards of relevance, particularly with those from the automotive industry, which have similar requirements to military. The exception to this is EMC, where military equipment is required to operate within high EMC fields and at higher frequencies than their commercial equivalent.

Standard	Description	Legacy systems	Future systems
Def Stan 59-411	Electromagnetic Compatibility (EMC)	Y	Y
Def Stan 61-05 Part 6	Electrical Power Supply Systems below 650 volts28 volt dc Electrical Systems in Military Vehicles Status obsolescent (no longer supported)	Y	N
MIL-STD-1275	Characteristics of 28 volt dc Electrical Systems in Military Vehicles	Y	Y
MIL-STD-704 part 4/7	Guidance for test procedures for demonstration of utilization equipment compliance to aircraft electrical power characteristics 270V dc	Y	Y
ISO 16750-Part 3:2003	Road vehicles – Environmental conditions and testing for electrical and electronic equipment -- Part 3: Mechanical loads	N	Y
ISO 16750-Part 4:2003	Road vehicles – Environmental conditions and testing for electrical and electronic Road vehicles – part 4 climatic loads	N	Y

ISO 16750 Part 5:2003	Road vehicles – Environmental conditions and testing for electrical and electronic Road vehicles – part 5 chemical loads	N	Y
ISO 16750 Part 2:2003	Road vehicles – Environmental conditions and testing for electrical and electronic Road vehicles – part 2 electrical loads	N	Y
ISO 21848	Road vehicles - Electrical and electronic equipment for a supply voltage of 42 V - Electrical loads	N	Y
ISO 7637-2,	Road vehicles - Electrical disturbance by conduction and coupling - Part 2: Commercial vehicles with nominal 24 V supply voltage - Electrical transient conduction along supply lines only	N	Y
SAEJ2622	Battery Connections for 42V Electrical Systems – Tests and General Performance Requirements	N	Y
STANAG 2601	Standardisation of Electrical Systems in Tactical Land Vehicles	Y	Y
STANAG 4133	Methods of Specifying Electrical Power Supplies – Standards Types of Electrical Power	Y	Y
STANAG 4334	Electrical Power Conditioners Solid State General Purpose for Interoperability	Y	Y

Table 15 - Standards for Power

Def Stan 59-411 is identified as it provides guidance and information on EMC testing for platform equipment. The frequency spectrum of interest is based on the operational scenario of the platform and its equipment fit. However there may be a need to address the European Community directive on EMC which covers a wider spectrum and thus will be an addition to the military requirement.

28 volt vehicle power supplies are defined in both the **Def Stan 61-05 Part 6** and **MIL-STD-1275**. Both standards, which are very similar, are identified in order to address international programmes. Def Stan 61-5 part 6 is now obsolete, (Obsolescent Standards are no longer required for the procurement of new equipment but retained for maintenance purposes in support of existing in–service equipment).

Due to the increase in demand for electrical power, it is recommended that higher voltages be considered in support of high current consuming functions. 270 volt systems are considered internationally and components are available for use. **MIL-STD-704** includes 270v dc system requirements.

There is limited component support for 600 volt systems but to date no standards have been identified.

ISO16750-11993 Road vehicles - Environmental conditions and testing for electrical and electronic equipment.
This gives definitions and general specifications for the potential environmental stresses, and corresponding tests and requirements, for the mounting of electric and electronic systems and components on road vehicles. It is applicable to environmental conditions and tests affecting electrical and electronic equipment mounted directly on or in the vehicle. It does not cover electromagnetic compatibility (EMC).

ISO16750-2 1993 Road vehicles– Environmental conditions and testing for electrical and electronic equipment.

This specifies electrical loads and corresponding tests and requirements for the mounting of electric and electronic systems and components on road vehicles. It is applicable to environmental conditions and tests affecting electrical and electronic equipment mounted directly on or in the vehicle. It does not cover electromagnetic compatibility (EMC).

In parallel SAE, (Society of Automotive Engineers) are researching future 42V internal and external vehicle lighting systems. The concern here is that incandescent light filaments for a 42V system will be thin and liable to break under shock and vibration. The research is looking at using existing filaments and using pulse width modulation to control the current, hence maintain the rated output power.

Massachusetts Institute of technology (MIT), Advanced Automotive Electrical/Electronic Components and Systems operates a multi-national WG to develop a standard design and specification for a 42V battery connector for PowerNet (the 42V) power architecture.

The SAE is in the process of publishing specification **J2622** Battery Connections for 42V Electrical Systems – Tests and General Performance Requirements.

Meanwhile in 2003 ISO published the following road vehicle standards to specify the environmental requirements of road vehicles electronic equipments.

ISO 16750-3:2003 Road vehicles - Environmental conditions and testing for electrical and electronic equipment - Part 3: Mechanical loads.
ISO 16750 Part 3 describes the mechanical loads that can affect electric and electronic systems and components in respect of their mounting directly on or in road vehicles, and specifies the corresponding tests and requirements.

ISO 16750-4:2003 Road vehicles - Environmental conditions and testing for electrical and electronic equipment - Part 4: Climatic loads.
ISO 16750 Part 4 specifies climatic loads and corresponding tests and requirements for the mounting of electric and electronic systems and components on road vehicles. It is applicable to environmental conditions and tests affecting electrical and electronic equipment mounted directly on or in the vehicle.

ISO 16750-5:2003 Road vehicles - Environmental conditions and testing for electrical and electronic equipment - Part 5: Chemical loads.
ISO 16750 Part 5 specifies chemical loads and corresponding tests and requirements for the mounting of electric and electronic systems and components on road vehicles. It is applicable to environmental conditions and tests affecting electrical and electronic equipment mounted directly on or in the vehicle.

ISO 21848 This International Standard describes the electrical loads that can affect electric and electronic systems and components of road vehicles for a supply voltage of 42 V, which may be used in a single or a multiple voltage electrical system. In addition, it specifies the tests and resulting requirements, test equipment accuracy being agreed upon between the vehicle manufacturer and the supplier. It does not cover electromagnetic compatibility (EMC). This International Standard also provides design guidance for the interaction of 42 V with other system voltages.

ISO 7637-2 Road vehicles - Electrical disturbance by conduction and coupling - Part 2: Commercial vehicles with nominal 24 V supply voltage - Electrical transient conduction along supply lines only.

SAE J2622 Battery Connections for 42V Electrical Systems – Tests and General Performance Requirements.

A number of **NATO Standardisation Agreements** (STANAGs) have been produced and ratified and are included for information. Detailed information such as voltage levels ripple etc are not usually found in STANAGS. For these details the original standard SAE, ISO etc should be consulted.

7 Guidelines

7.1 Platform Command and Control

Land Platform Command and Control is normally taken to involve the flow of information, both in terms of voice, data and image formats, around the battlefield, the primary communication medium being the Combat Net Radio (CNR). The definition needs to be extended to include the C2 aspects relating to subsystems and how they interact within land platforms.

The table below provides a method that indicates the choices to be made when undertaking an integration exercise.

	Extent of Change		
Complexity	Minor Change	Major Change	New Vehicle
Low	CAN RS422	CAN RS422	CAN
Medium	CAN RS422	CAN RS422	CAN
High	CAN RS422	CAN RS422 IEEE 802.3 TTP/C	CAN RS422 IEEE 802.3 TTP/C

Table 16- Platform Command and Control Changes

The above table allows for three types of platform form of fit:

- Minor change - where modifications are being made to a subsystem (e.g. the attachment of a low-level entity). This scenario is expected to be primarily applicable to many B vehicles.
- Major change – this applies when a new subsystem is being fitted, a system is being modified or existing platform subsystems are required to interact thereby providing enhanced functionality and/or a means of interaction with the Digitized Battlespace.
- New vehicle – this is self-explanatory.

The table above also allows for three levels of platform complexity, these can be defined as:

- High complexity – e.g. a level of complexity similar to Challenger 2 (CR2) or FRES Scout .

- Medium complexity - e.g. a level of complexity similar to Warrior Observation Post Vehicle (OPV).
- Low complexity – this category will largely cover the B fleet of vehicles where there is little in the way of included subsystems.

There will be instances when the identification of the vehicle complexity appears unclear. Guidance should therefore be sought from the customer with regard to the function that the platform is intended to provide, both for the immediate modification and in the long term. With this information a more informed assessment of the modification path may be taken.

Assistance may also be sought from the author of this document.

7.1.1 Minor change, low complexity

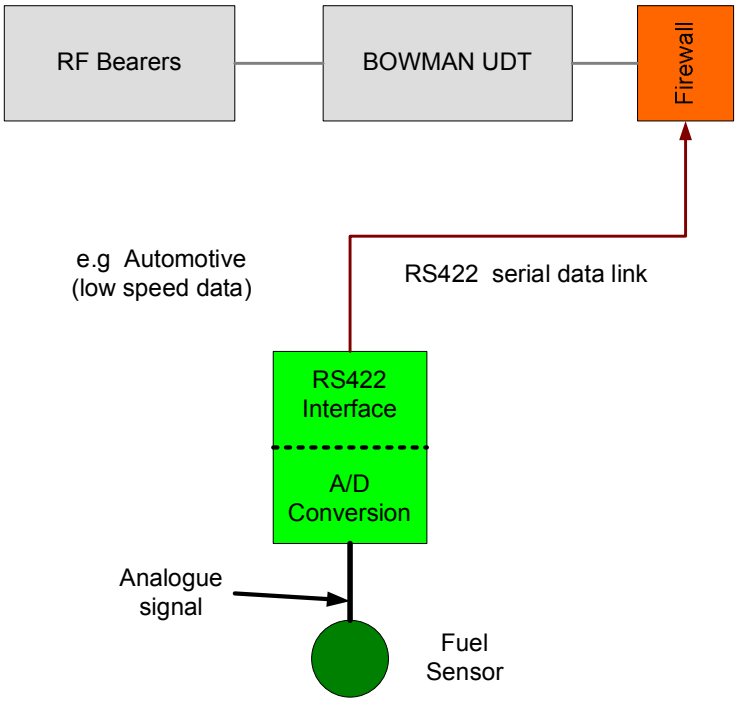

Figure 7 - Example of Low Complexity, Minor Change

The application of the appropriate technology is dependent on the perceived future of the vehicle and possible subsequent modifications to it. In this category the vehicles lack sophistication in terms of equipment fit, and as such the chosen technology must be cost effective. The primary reason for the change is likely to be to provide a mechanism to enable information extraction via the BOWMAN User Data Terminal (UDT). This implementation is intended where minor sensors may be required to be accessed. Figure 7 shows the integration of a fuel sensor as an example; the analogue output from this sensor is digitised prior to being converted into RS 422 format. This information can then be exported via the BOWMAN UDT.

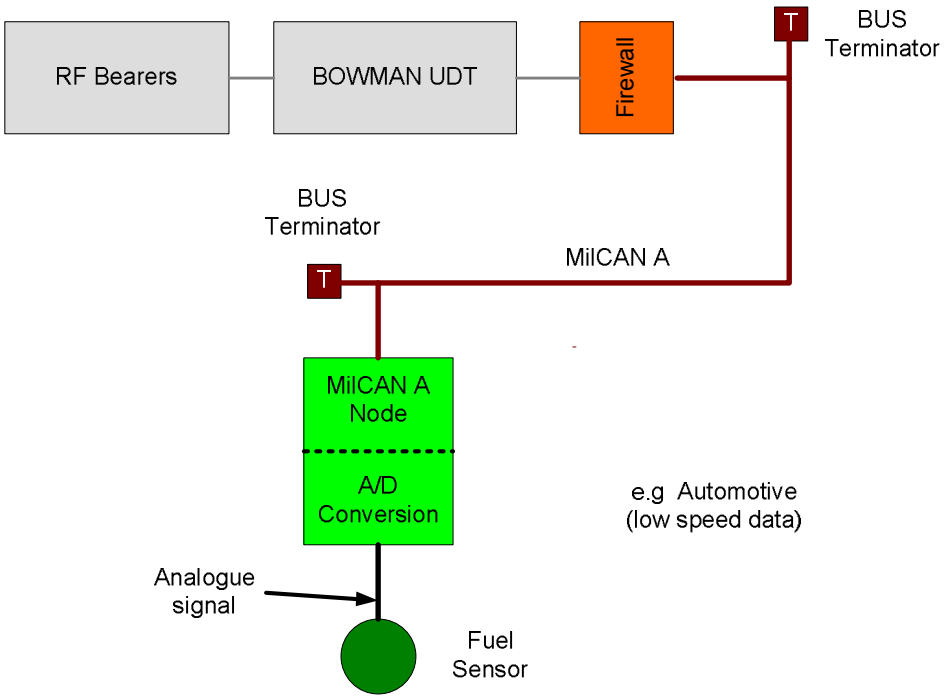

Figure 8 - Example of Low Complexity, Minor Change using MilCAN A

However, if a long term view is adopted and it is envisioned that subsequent changes may be made, then the use of MilCAN A technology is proposed, as shown in Figure 8. In this example, a MilCAN node is used to interface the output of the Analog to Digital (A-D) function to the CANbus. Adopting this approach enables the system to be extended in the future by adding further sensors, interfaced to the CAN bus by additional MilCAN nodes.

7.1.2 Minor change, medium complexity

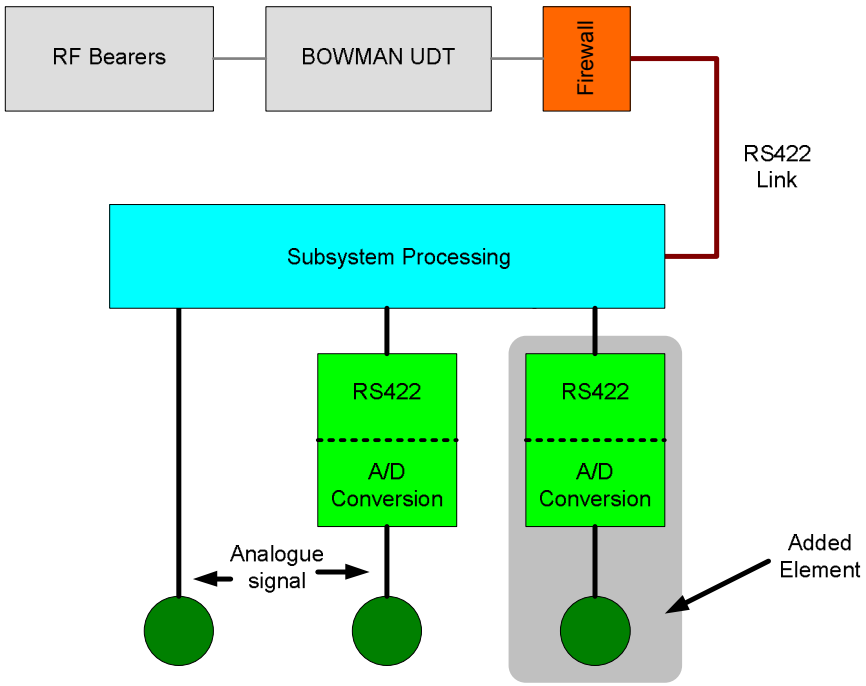

Figure 9 - Example of Medium Complexity, Minor Change

For medium complexity vehicles the technology used will depend on the extent and nature of the change. If a single element is to be added that is stand alone, then reference to the details in 7.1.1 should provide the necessary guidance. However, it is likely in platforms of this complexity, that the sensors and actuators are connected to a subsystem. This is illustrated in the Figure 9 above which shows a generic subsystem that contains a number of subsystem elements, sensors and actuators, and some form of associated processing.

The attached elements may be connected to the subsystems using a variety of formats, analogue, RS 232, RS 422 etc. In the figure the shaded area indicates where a change is to be made. This change, for example, may be the addition of the subsystem element or a requirement to acquire information from an existing element. A range of approaches can be used to acquire this information. At the simplest the information can be acquired in the manner shown. This approach is restrictive in that it is inflexible and answers only the immediate requirement.

Where there is the possibility of future expansion, the use of CANbus as shown in Figure 10 below is preferred. The shaded area highlights the area of modification. Using this option allows the possibility of incremental development. The figure illustrates some salient features. The MilCAN node has intelligence and is capable of handling various forms of input/output (I/O). The MilCAN node can be used to attach a sensor or actuator as shown. The subsystem itself can also be attached to the node thereby accessing the attached element. The MilCAN node may be used to access the element directly for use by the BOWMAN UDT or indirectly via the subsystem. This arrangement can be expanded to augment the subsystem by addition of further elements indicated by the dashed connection. Moreover, the possibility exists that the subsystem itself may supply information from the pre-existing elements via the MilCAN node to the UDT.

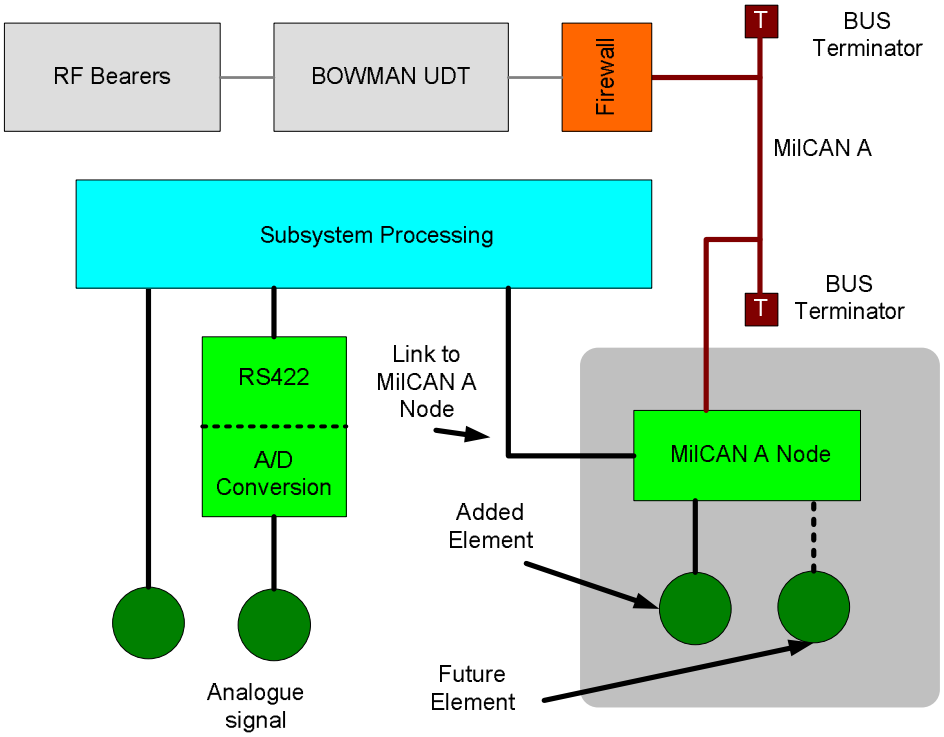

Figure 10 - Example of Medium Complexity, Minor Change

This approach eases long-term development and allows successive modifications be to be made to the subsystem, Figure 11 illustrates the goal of such a progression. The shaded areas show incremental changes to the system. MilCAN nodes are added as required either to enhance the system or to enable access to information for transmission via the UDT.

In Figure 11, the MilCAN node performs the format adaptation from the subsystem elements. However, MilCAN nodes may also be used to integrate pre-adapted systems as indicated by the block containing the A-D Conversions.

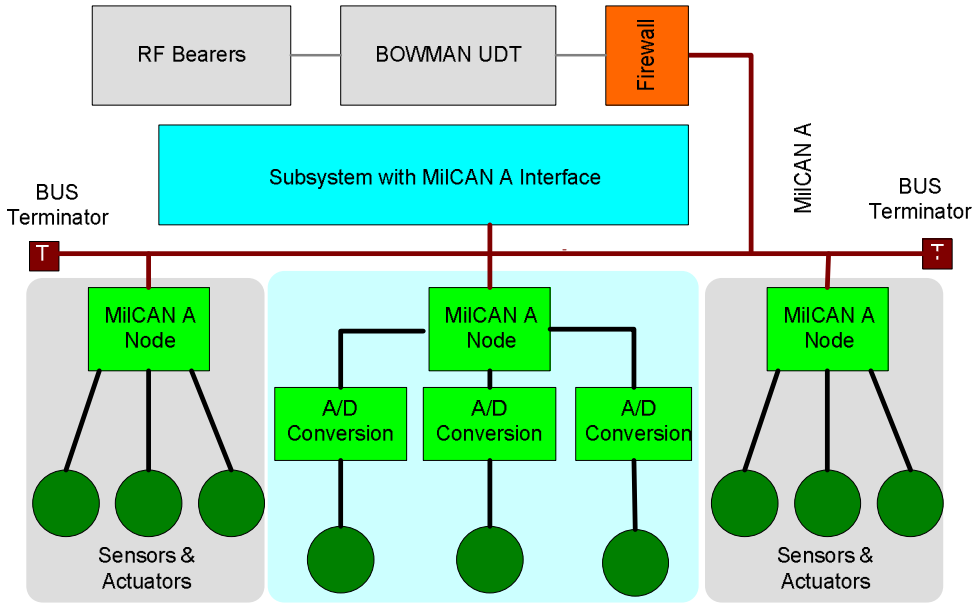

Figure 11 - Example of Medium Complexity, Minor Change using MilCAN A

7.1.3 Minor change, high complexity

For complex platforms there may be many subsystems and it is these platforms that are most likely to experience successive modification in either the area of subsystem to subsystem interaction (i.e. where the modification is made to allow the sharing of data between subsystems) or where an element is added to a subsystem. It may also be the case that some form of data bus architecture is already present on the platform and will dictate that consideration is given to its development.

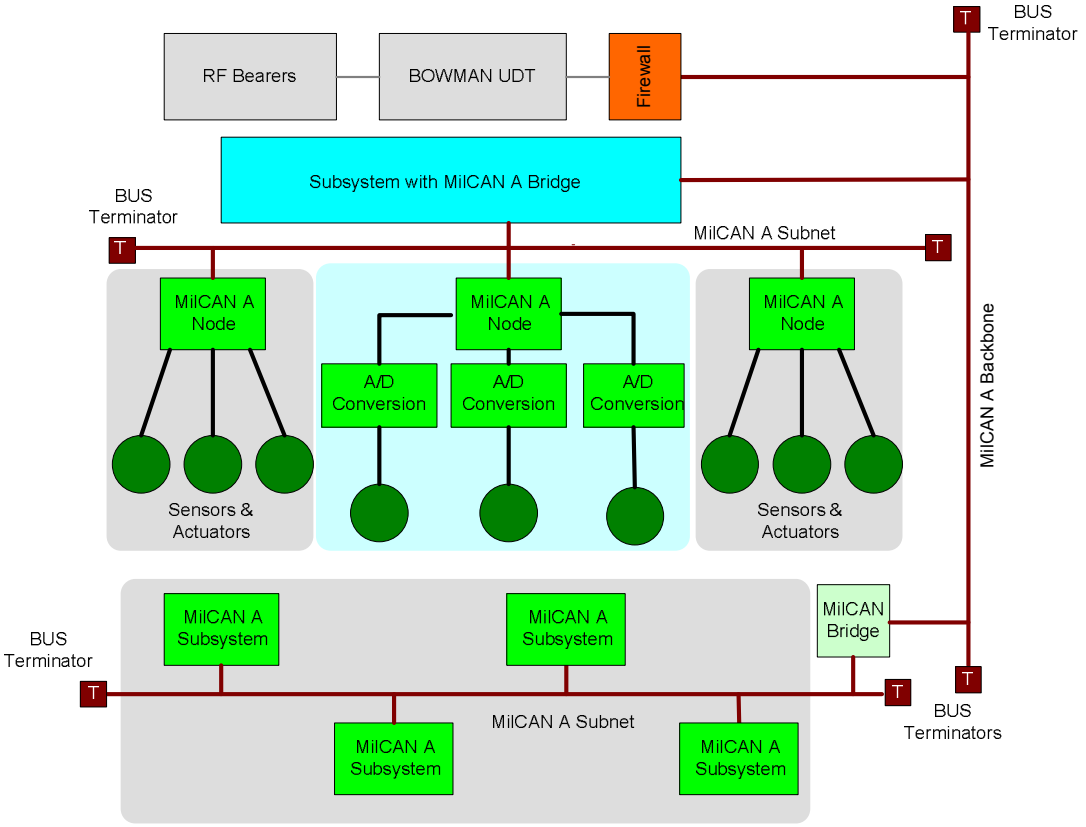

Figure 12 - Example of High Complexity, Minor Change using MilCAN A subnet

In Figure 12 the MilCAN node is capable of handling various forms of I/O. The node can therefore be used to attach sensors or actuators as shown. The subsystem may itself contain a MilCAN node thereby accessing any data available on the MilCAN subnet. Data can be passed to the MilCAN backbone for use by the BOWMAN UDT via the bridge embedded within this subsystem. This arrangement can be expanded as required by adding further MilCAN nodes to the subnet.

In complex platforms there is a high probability that they will receive successive modification over time, Figure 12 shows how a system can evolve over time.

CAN technology allows partitioning of the vehicle architecture on a functional basis. Bridges are used to limit the traffic passed from a subnet to the MilCAN backbone and vice versa. Bridges are essentially message filters that connect two networks, and are added to prevent data overloading as the architecture is enhanced. The backbone only carries the message traffic that is either essential for subsystem to subsystem interaction, import or export via BOWMAN, or to carry data for use at the BOWMAN UDT.

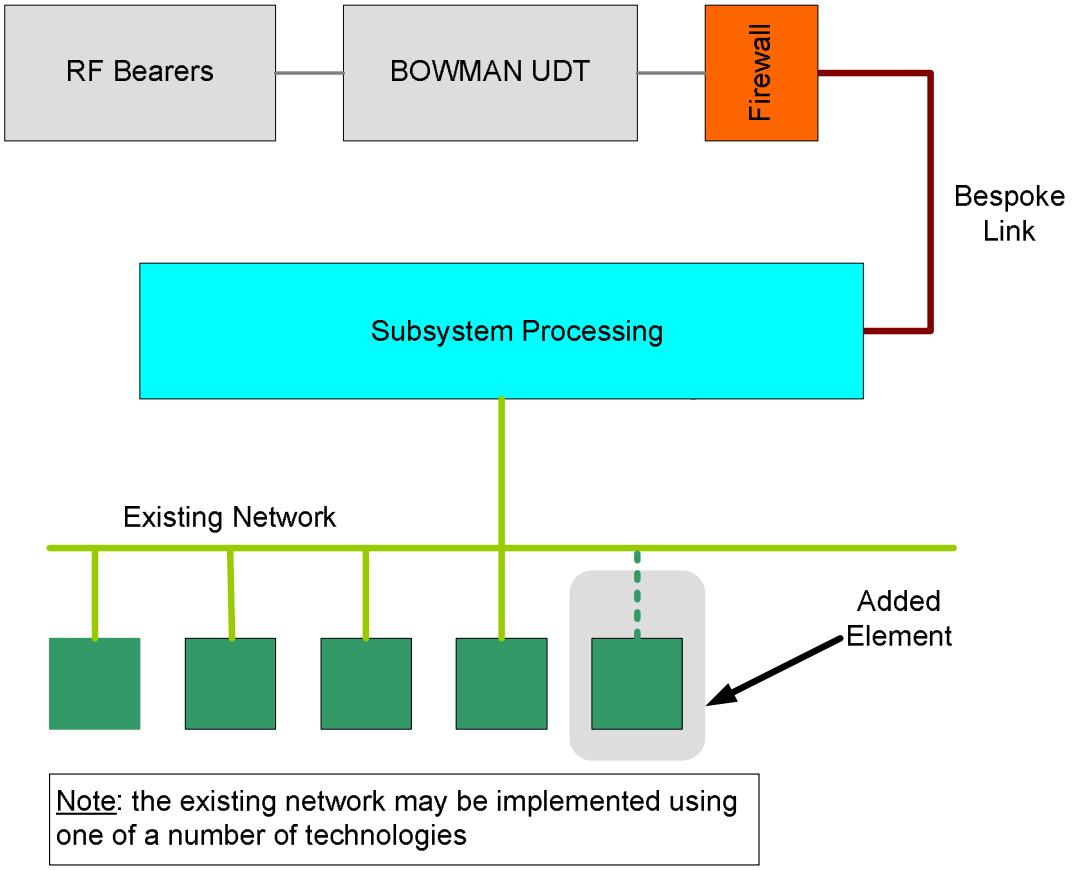

Figure 13 - High Complexity, Minor Change using an existing network

Some high complexity platforms may already have a data network implemented within the platform. The nature of the change and the long term requirement will dictate how the modification is approached. In the case where the additional element is added to enhance an existing system then first consideration should be given to an interfacing regime that is consistent with the existing network, Figure 13 illustrates this.

In an additional element is attached to the existing network, and the subsystem processing uses the data from this. When a new element is added (shaded portion) then this should be done in a fashion that is consistent with the network and pre-existing elements. There is a caveat to this however. The subsystem processing may have to supply a connection to the BOWMAN UDT if information is required for import or export and this could be achieved by a bespoke link. Moreover, the subsystem may also prove difficult, in the long term, to accommodate further modification and difficult to integrate with other subsystems.

A possible alternative approach is shown in Figure 14.

Here there is the possibility of a series of future planned modifications and these may well be seen as a stand-alone subsystem element. In this case the use of CAN technology may be justified if seen in the context of long term platform integration.

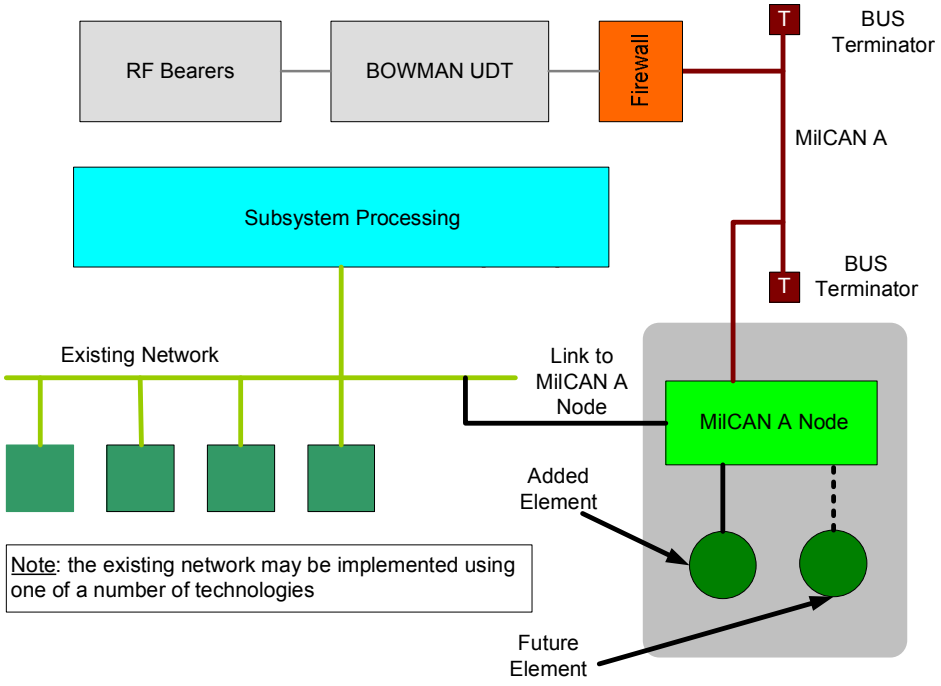

Figure 14 - High Complexity, Minor Change adding a MilCAN A node

7.1.4 Major change, low complexity

For vehicles of low complexity the course of action when a major change is required is dependent on the type of alteration required, the likely gain in functional benefit and the number of subsystems fitted. Considering the case of a re-engineered subsystem, the example show in below, in Figure 15 the subsystem has been adapted to communicate over MilCAN. MilCAN nodes also provide the interface between the low level elements such as sensors and actuators. The central group of elements illustrates an existing grouping of sensors and actuators that have previously been converted to digital information and can be interfaced to MilCAN by the addition of a further node.

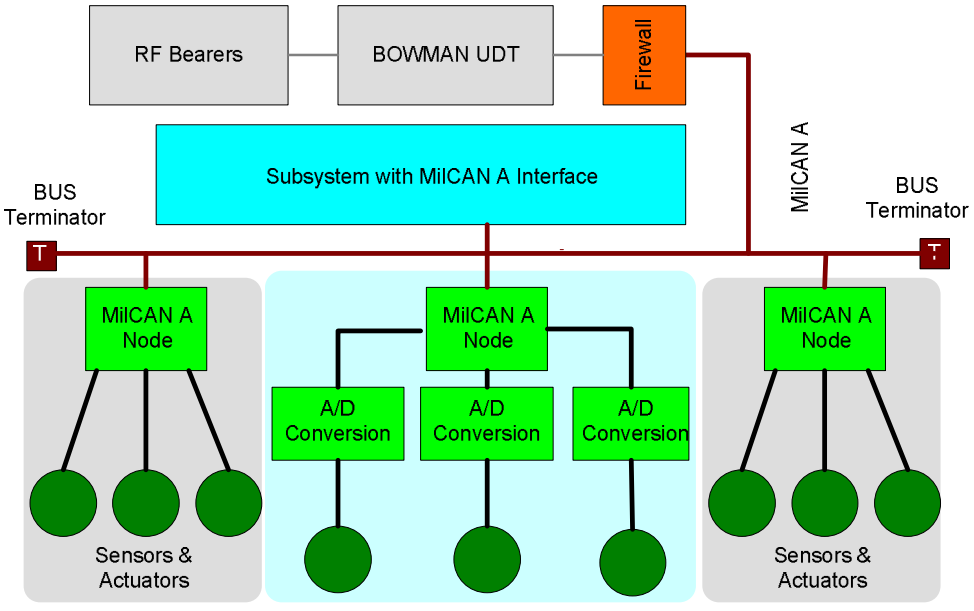

Figure 15 - Example of Low Complexity, Major Change adding a MilCAN A node

This general model does however enable progressive alteration allowing the system to evolve over time and Figure 16 below illustrates this concept. In the example in Figure 16, an entire subnet has been added, effectively providing a functional partition of the vehicle architecture. The MilCAN backbone provides the means by which the subnets intercommunicate and also allows the BOWMAN UDT access to information available on all subnets. Figure 16 also illustrates the use of bridges between the subnets and the backbone bus. Bridges are used to limit the traffic passed from a subnet to the MilCAN backbone and vice versa. Bridges are essentially message filters that connect two networks, and are added to prevent data overloading as the architecture is enhanced. The backbone only carries the message traffic that is either essential for subsystem to subsystem interaction, import or export via BOWMAN, or to carry data for use at the BOWMAN UDT. The function of the bridge could be embedded in the subsystem processing if required.

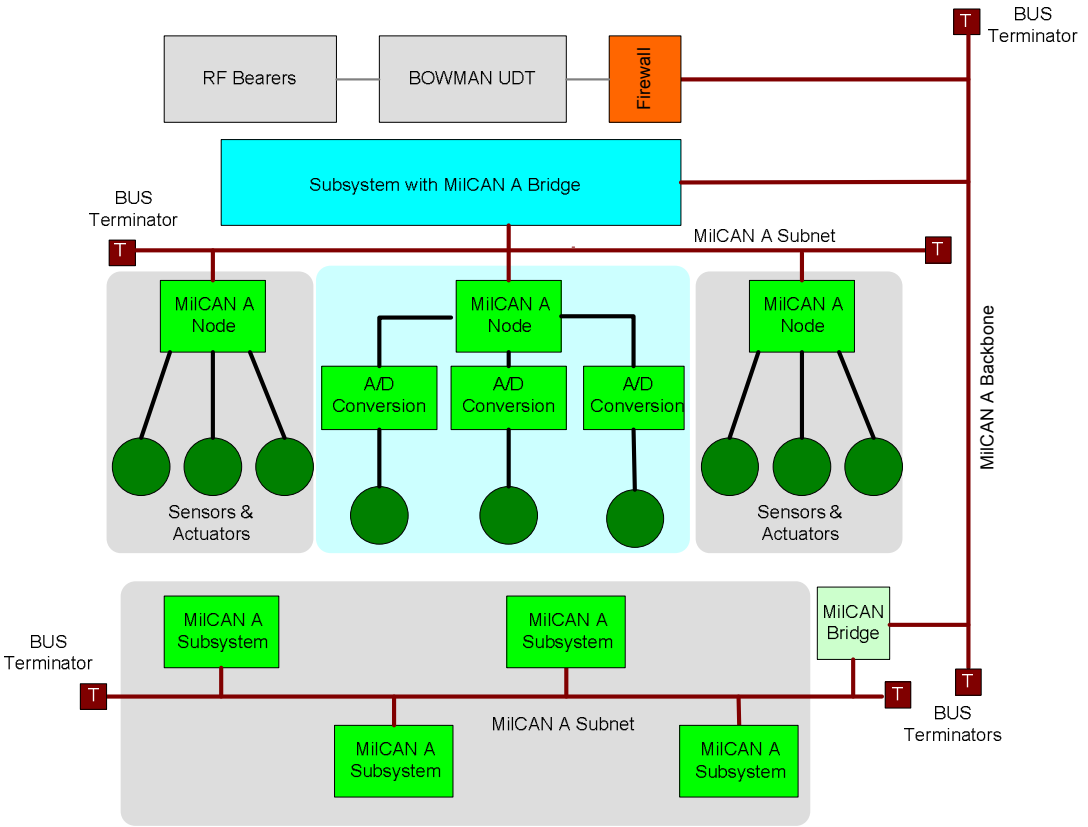

Figure 16 - Low Complexity, Major Change adding a MilCAN A Subnet

7.1.5 Major change, medium complexity

For vehicles of medium complexity the course of action when a major change is required is dependent on the likely gain in functional benefit and the number of subsystems fitted. Subsystems in this type of platform will benefit from the use of an interconnecting data network. The use of MilCAN should be assumed from the outset. If this cannot be justified in terms of cost, then elements of CAN technology should be used if possible in specific locations, with a view to extending the architecture when it is merited. Figure 17 illustrates

the vehicle modification. It is however, appreciated that some subsystems or elements of subsystems may be difficult or uneconomical to modify, hence a hybrid model is acceptable.

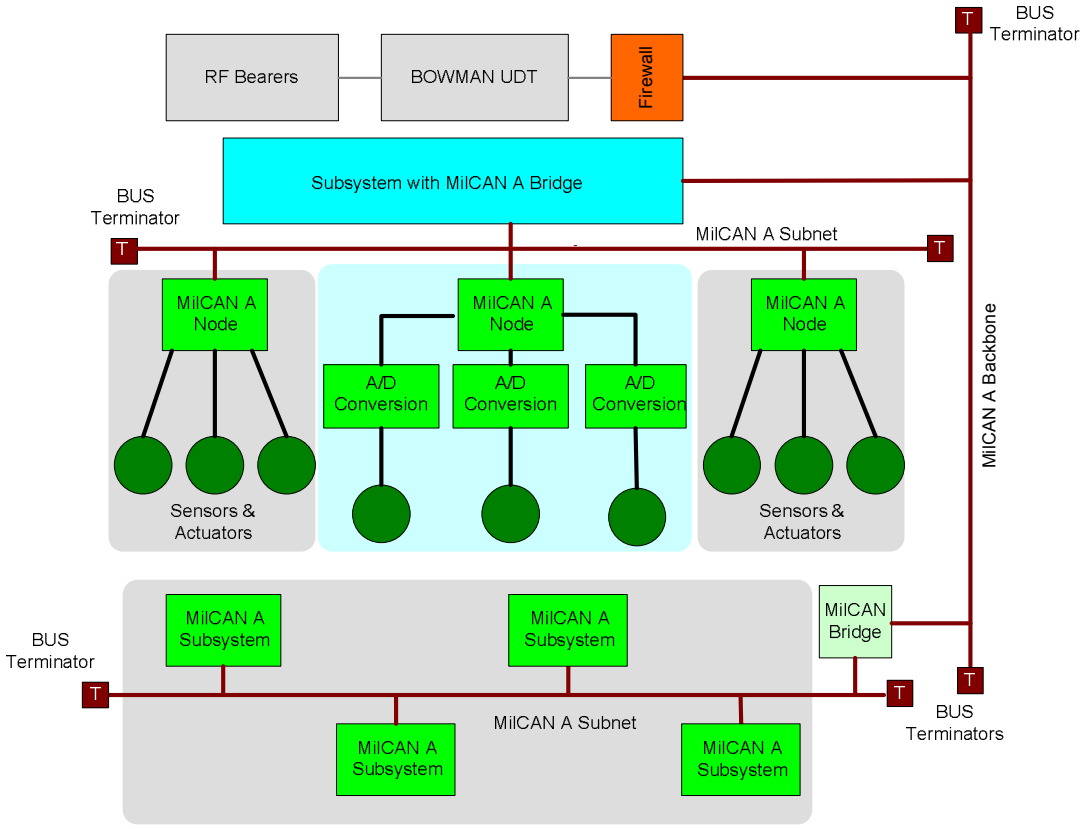

Figure 17 - Medium Complexity, Major Change

The MilCAN backbone provides the means by which the subnets intercommunicate and also allows the BOWMAN UDT access to information available on all subnets. The figure also illustrates the use of bridges between the subnets and the backbone bus. Bridges are used to limit the traffic passed from a subnet to the MilCAN backbone and vice versa. Bridges are essentially message filters that connect two networks, and are added to prevent data overloading as the architecture is enhanced. The backbone only carries the message traffic that is either essential for subsystem to subsystem interaction, import or export via BOWMAN, or to carry data for use at the BOWMAN UDT.

For the majority of platforms, the use of MilCAN for the backbone may well be the extent of any modifications required on the vehicle. However, in some circumstances a platform may well evolve markedly over time, with the additions of new subsystems. This may result in the MilCAN backbone being unable to meet the data flow required. In this instance removal of the MilCAN backbone and replacement with one of a higher capacity is required. Figure 18 illustrates this. Essentially, the infrastructure contained in the functional blocks remains constant; the only change is the addition of the high speed data bus. The choice of high speed data bus will depend on the specific requirements for that platform. If the interconnecting backbone has no safety related subsystems attached to it then the use of Ethernet would be a good choice. Bridges/Gateways are required between the MilCAN subnets and the Ethernet backbone.

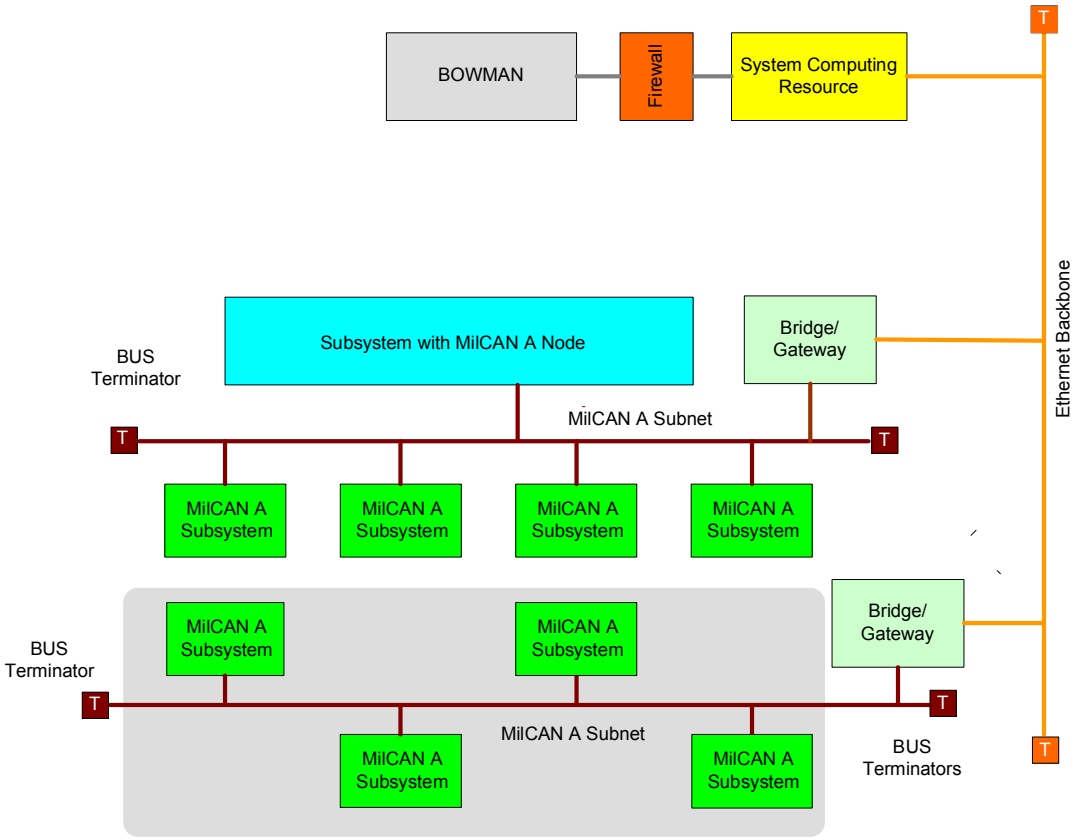

Figure 18 - Medium Complexity, Major Change using Ethernet Backbone

If, however, the interconnecting backbone has safety related subsystems attached to it then the use of a fault tolerant network technology is required. Figure 19 shows an example of such a backbone implemented using TTP/C. Bridges/Gateways are required between the MilCAN subnets and the TTP/C backbone.

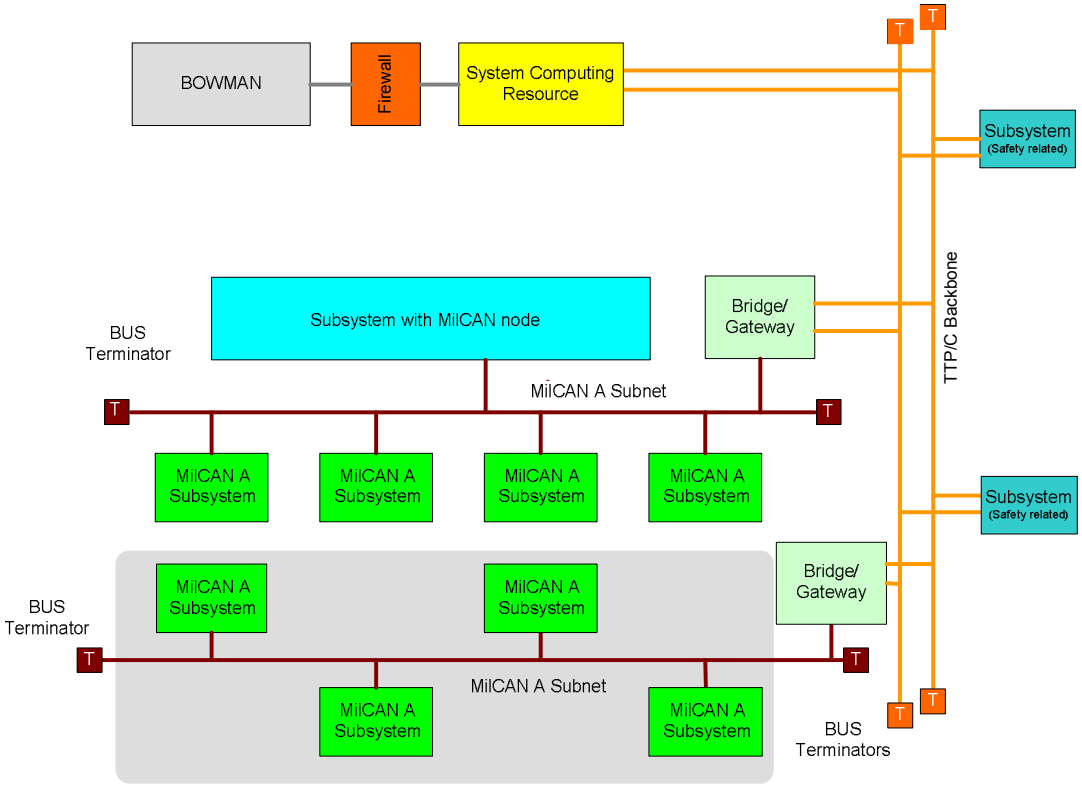

Figure 19 - Medium Complexity, Major Change using TTP/C backbone

7.1.6 Major change, high complexity

For high complexity vehicles scheduled for a major change, the starting point will be to assume that the subsystems will be interconnected via MilCAN subnets as shown in Figure 20. The MilCAN subnets may be interconnected via Bridge/Gateways using some form of backbone. In Figure 20 the backbone technology shown is ethernet. The selection of the backbone technology is dependent on a number of factors:

- the data throughput required of the backbone;
- the data latency requirements for messages passed between subnets;
- the anticipated growth potential requirements for the backbone.

Where the data throughput requirement is low and is not expected to grow, the backbone technology could be MilCAN. This would have the added advantage that the connection between the backbone and the subnets would be simple MilCAN bridges. However, if the data traffic on the backbone is greater than the capacity of MilCAN then an alternative technology such as Ethernet, either 100 Mbps or 1Gbps is suggested.

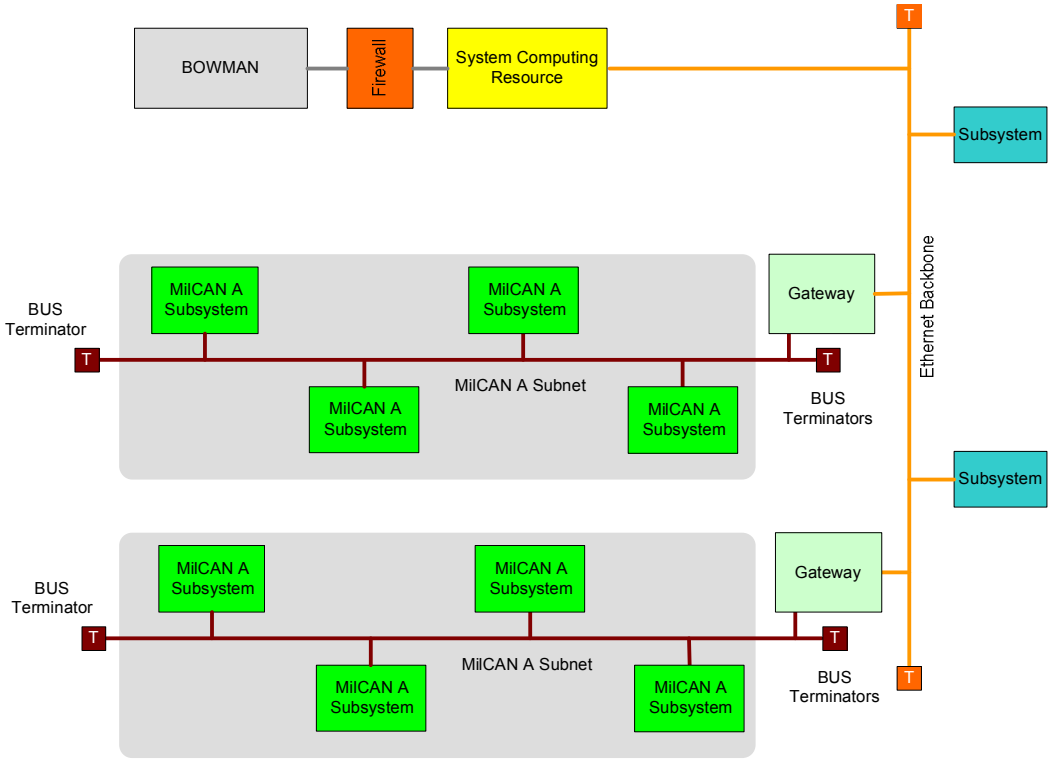

Figure 20 - High Complexity, Major Change using Ethernet Backbone

It is acknowledged that subsystems may already employ a network technology within a specific subsystem. Alteration to this may take place if the benefit in functionality can be balanced against the LCC of the platform. If this is not feasible then the existing subsystem should provide an interface to the MilCAN or high-speed backbone as required.

Where a safety related system such as Defensive Aids System (DAS) is to be added to a vehicle, this may consist of a TTP/C subnet connected to the selected backbone technology via a Gateway. In Figure 21 a safety related subnet is shown linked to an ethernet backbone via gateway. The safety related aspects are hosted on the TTP/C bus and are entirely contained within this subnet.

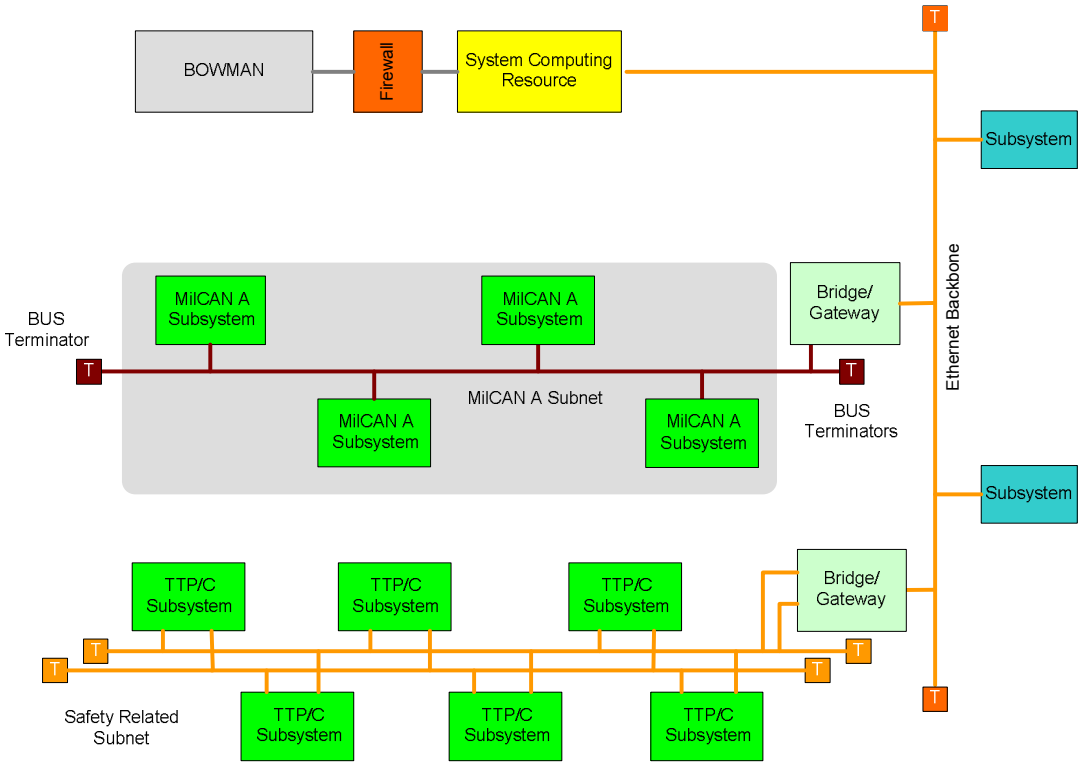

Figure 21 - High Complexity, Major Change featuring TTP/C

7.1.7 New vehicle, low complexity

For new vehicles, MilCAN should be considered as the primary technology for interconnecting vehicle subsystems unless there are safety related considerations to be taken into account or the data throughput is likely to exceed MilCAN capability. Where subsystems to be utilised contain an interface other than MilCAN there are effectively two choices:

- employ an 'add on' protocol converter module between the subsystem and the MilCAN bus;
- redesign the subsystem to include a MilCAN interface.

Figure 22, a MilCAN subnet is shown connected to a MilCAN backbone via a Bridge. Since the vehicle is of low complexity it is unlikely that further subnets will be required but the architecture is sufficiently scalable to accept these if required e.g. A TTP/C safety related subnet could be added. As subnets are added the technology used for the backbone may need to be reviewed.

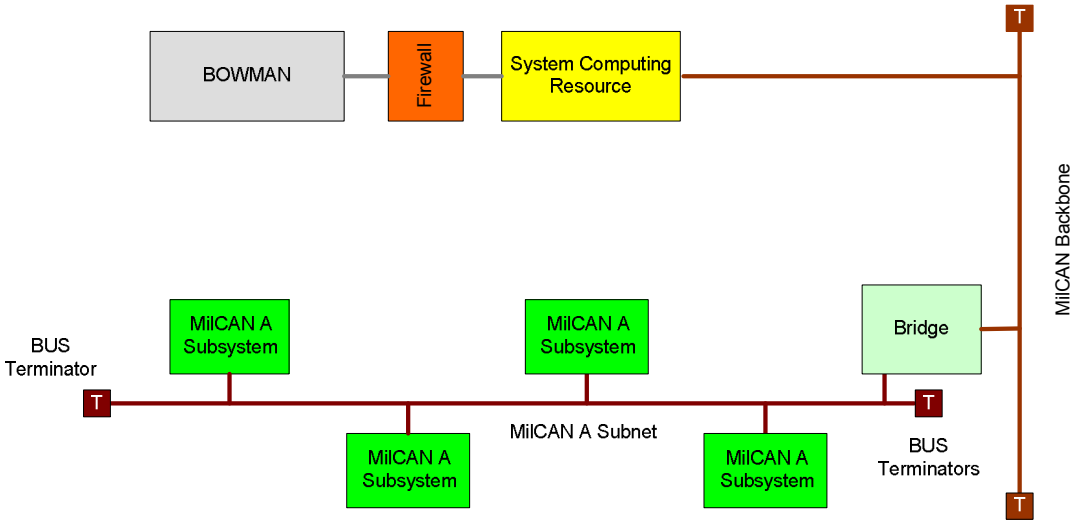

Figure 22 - Low Complexity, New Vehicle

7.1.8 New vehicle, medium complexity

For new vehicles of medium complexity extensive use of MilCAN for interconnection of subsystems is merited. In Figure 23, two MilCAN subnets are shown interconnected via bridges to a MilCAN backbone. The use of MilCAN in this way allows the architecture to be partitioned on a functional basis since each subnet can perform a different function e.g. automotive, power distribution control etc. Bridges are used to limit the traffic onto the MilCAN backbone and effectively limit data throughput on the backbone as the architecture is enhanced. The backbone only carries the traffic that is either essential for subnet to subnet interaction, import or export via BOWMAN, or to carry data for use at the BOWMAN UDT.

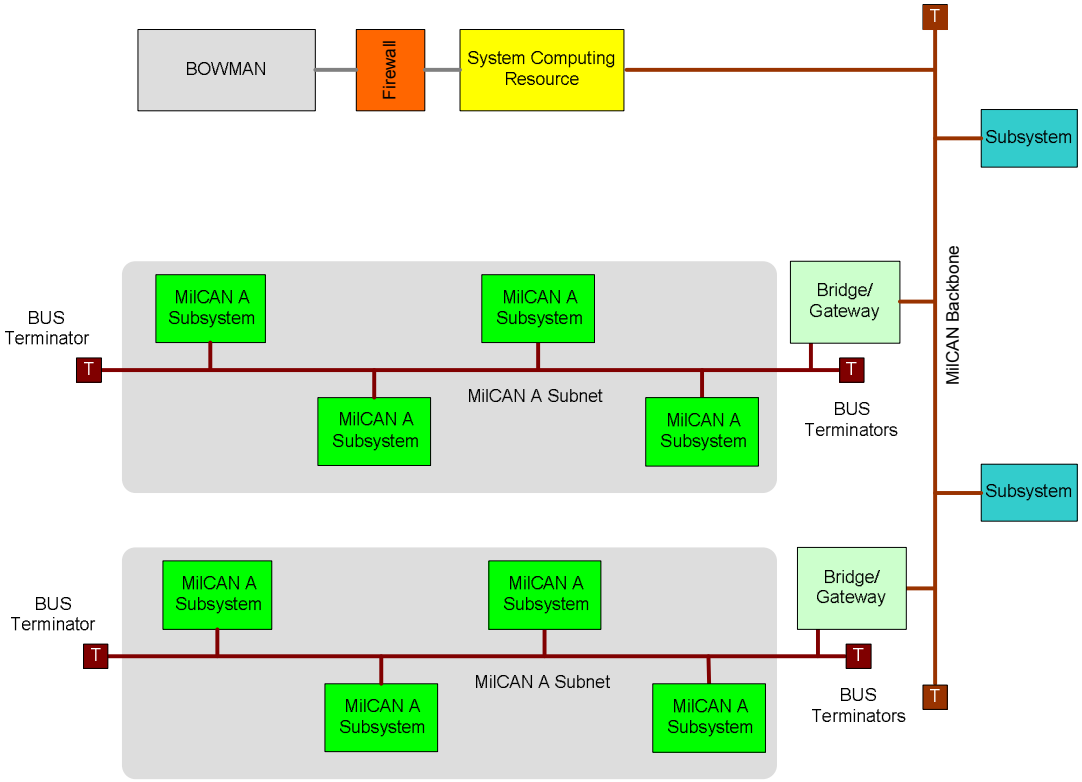

Figure 23 - Medium Complexity, New Vehicle

Where the subnet to subnet data carrying capacity is likely to exceed that of MilCAN technology or where subsystems connected directly to the backbone require higher data throughput than MilCAN can provide, then consideration should be given to use of a high bandwidth technology such as Ethernet, see Figure 24.

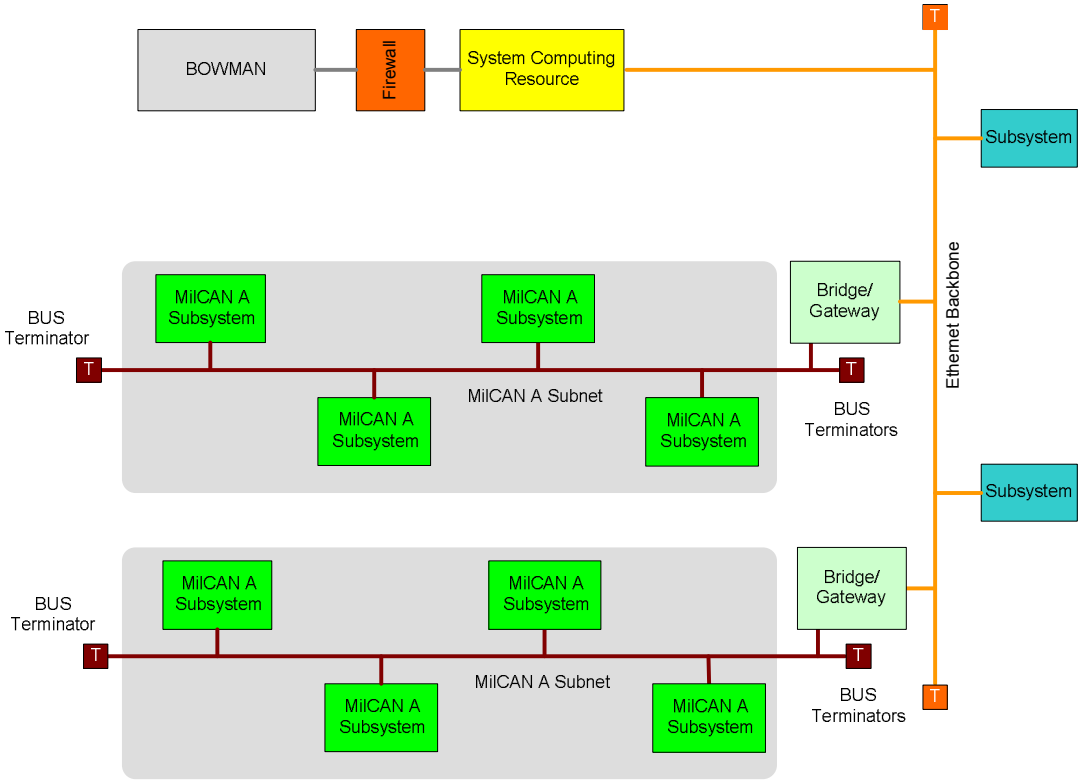

Figure 24 - Medium Complexity, New Vehicle with Ethernet Backbone

7.1.9 New vehicle, high complexity

For new high complexity vehicles the starting point will be to assume that the architecture will be comprised of a number of functionally partitioned subnets. The subnets should be interconnected by a backbone constructed from a suitable high data rate technology such as ethernet. The technology selected for the subnets will depend on a number of factors:

- the safety related and fault tolerance requirements for the subnet;
- the data latency requirements for messages passed within the subnet;
- the anticipated growth potential requirements for the subnet.

Where MilCAN can meet the requirements for a particular subnet it should be selected. If there are particular safety related requirements or if fault tolerance is a particular concern then TTP/C is the best choice for that subnet.

It is particularly important that the architecture is scalable and that technology insertion is taken into account. This can be achieved by adding further subnets, either MilCAN or TTP/C based, as required. Figure 25 illustrates this.

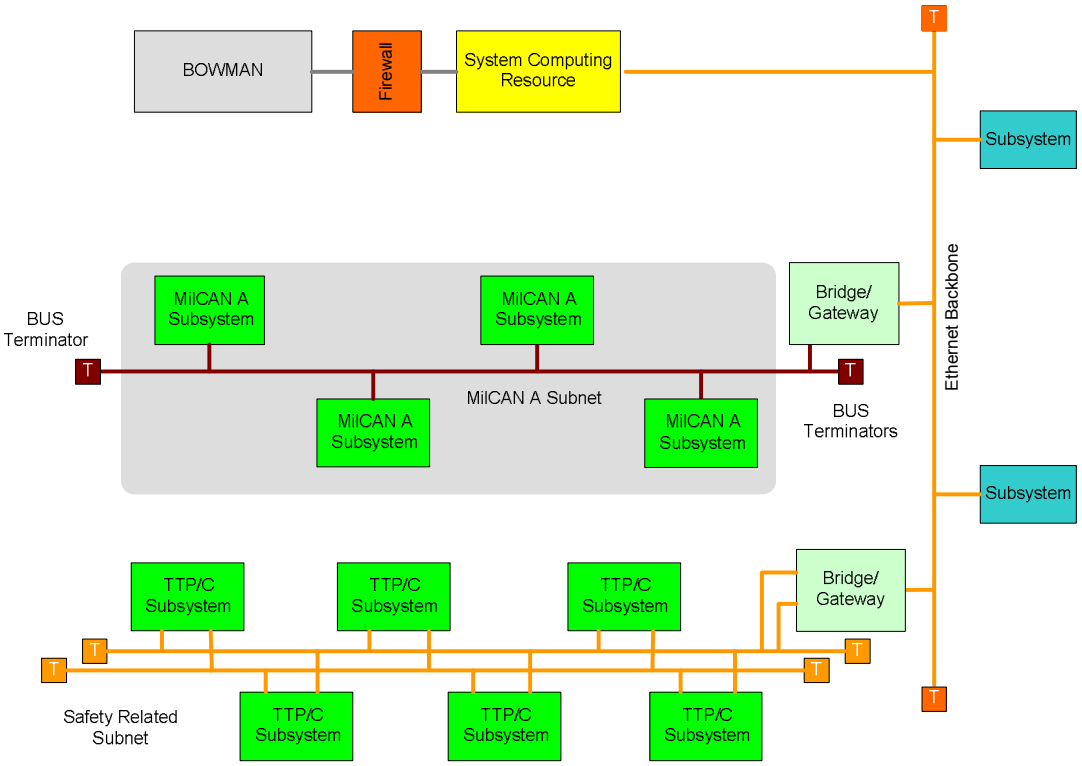

Figure 25 - High Complexity, New Vehicle with Ethernet Backbone

7.2 Video Guidelines

The key parameters to be considered when video system implementation/changes are contemplated may be summarised as a trade-off between:

- Performance required;
- Cost of implementation;
- Provision for future systems enhancement.

System performance requirements govern the relative importance of technical performance, cost and upgradeability, and the trade-offs, which need to be made between them.

The degree of provision to be made for future systems enhancement will normally depend upon the complexity of the vehicle, the number of vehicles and its expected remaining in-service life.

7.2.1 Principles for video technology selection

The three important principles for video technology selection are summarised here:

- there is a preference for digital video technology over analogue, since it facilitates the processing of video in remote locations if required and is an inherently more robust signal;
- there is a preference for component video formats over composite since component formats are capable of producing clearer colour images than composite formats;
- there is a consensus that a design process should be utilised to select which video technology is appropriate to a platform application since this will encourage system designers to consider the implications of utilising digital video techniques rather than traditional analogue techniques.

7.2.2 Suggested Video Network Requirements and rationale

In this section a set of requirements for a video network is tabled along with the rationale for each requirement.

a. The network shall be based on open standards and protocols.

In keeping with the overall philosophy of VSI, there is a desire to avoid proprietary standards and protocols thereby avoiding vendor lock-in.

b. Image data shall be transmitted in digital form.

It is preferable that all future video systems installed on military land platforms transmit video in digital format.

c. The network shall be scalable over the range of platforms to which it may be applied.

It is desirable that the same technologies used to construct the video network for platforms of low complexity (e.g. Utility vehicle) can be applied to platforms of high complexity (e.g. Reconnaissance vehicle).

d. The network shall be extensible to allow for future addition of sensors, displays & processing resources, without changes to the protocols or standards employed.

It is desirable that a particular instantiation of the network in a platform can accept new sensors, displays and image processing resources without the need to add or change hardware, software or protocols other than the additional sensors, displays or image processing resources being added. There will of course be a need for additional cabling.

e. The video network shall be capable of transporting a range of video formats & resolutions suitable for military platforms e.g. visible band colour & IR monotone video, PAL & HDTV resolutions.

It is desirable that the video transport network is capable of carrying a range of uncompressed video formats & resolutions without impact to the underlying transport protocols.

f. The network shall be capable of transporting a range of compressed video formats (e.g. MPEG 4 & JPEG 2000).

It is desirable that the video transport network is capable of carrying a range of compressed video formats & resolutions without impact to the underlying transport protocols

g. Video transmissions from each source shall be announced in terms of their format and resolution such that receivers (i.e. displays or image processing) are able to use this announcement to correctly process the image data.

h. The network shall be capable of unicast video transmission i.e. single video source to single display.

i. The network shall be capable of multicast video transmission i.e. single video source to two or more displays.

j. The network shall be capable of transmission of metadata associated to the source of the image data.

Metadata transmitted should be transmitted as part of the video transmission in order to convey data pertinent to the sensor from which the video is derived.

k. The network shall embody a control mechanism to select image sources for display and for routing these images to the correct displays.

The control mechanism is required to start & stop image grabbing and for displays to join and leave multicast groups. Additionally, control will be required for image processing and selection of sensor functionality.

l. The network shall be capable of accepting and exploiting the full functionality of upgraded sensors and displays, without changes to the protocols or standards employed.

The desire is for 'plug & play' capability whereby sensors and displays can be added & removed from of the network and the functionality added or removed can be discovered automatically.

7.2.3 Architecture Overview

An architecture that fulfils the requirements stated in 7.2.2 is shown in Figure 26 .The architecture interconnects multiple video sources (typically cameras) and sinks (typically displays) via a switched network. The network may use one or more network switches each of which is multicast enabled. Control is provided in order to select image sources , image routing and display(s) on which the image is provided to the crew.

A typical network architecture is shown in Figure 26.

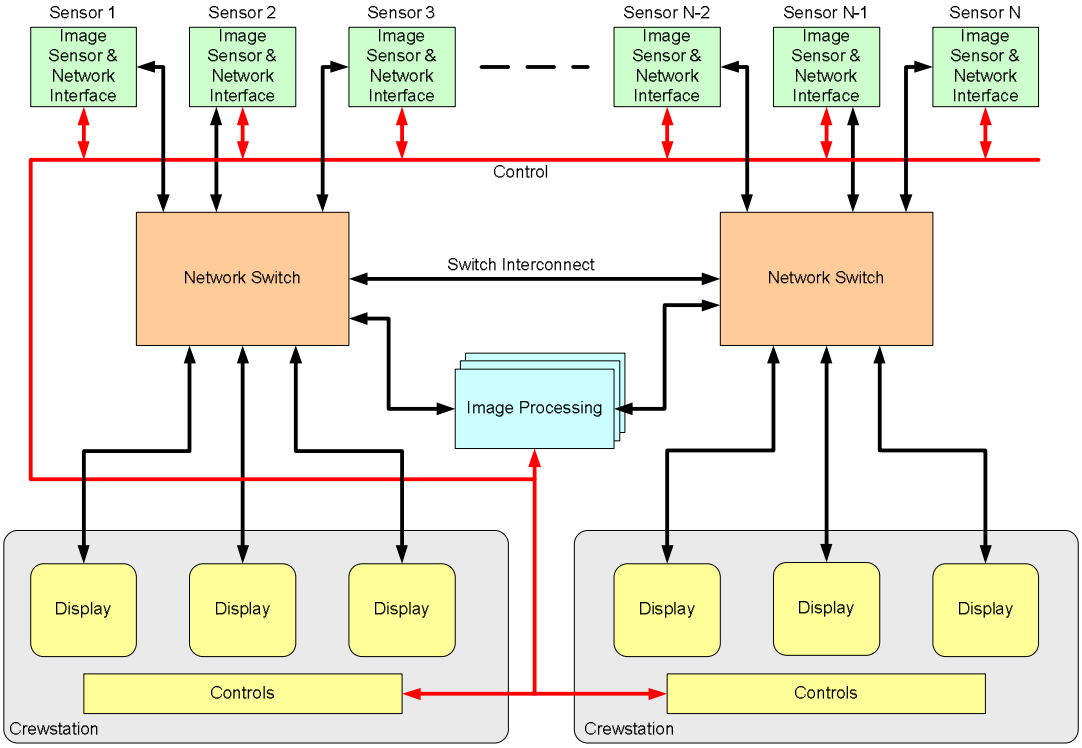

Figure 26 - Candidate video network architecture

7.2.4 Candidate Video Architecture

The following section gives a brief overview of the mechanisms and protocols specified in the Standard for Video Distribution in Vetronic Systems using Gigabit Ethernet [70] and currently employed in the VIVA2 system. VIVA2 is a collaboration between QinetiQ and Diehl BGT Defence on behalf of the UK MOD & German BWBand as such is work in progress and will be an input to the joint standardisation initiative founded as a Working group of the Military Vehicle Association (MilVA).

The candidate architecture is based on a Gigabit Ethernet Physical layer and uses the IEEE 802.3 Data Link Layer.

The Network layer employs Internet Protocol (IP), Internet Group Management protocol (IGMP) to meet the Multicast requirement, Internet Control Message Protocol (ICMP) to provide error messages, and Address Resolution Protocol (ARP) to map IP addresses to Ethernet MAC addresses.

The Transport Layer employs User Datagram Protocol (UDP) rather than Transport Control Protocol (TCP) since this application does not require guaranteed delivery. In this application, UDP will be faster and more efficient than TCP, as it avoids the overheads of checking whether every packet actually arrived.

The Application Layer employs Real-time Transport Protocol (RTP) provides end-to-end delivery services that support real-time transmission of voice and video. These services include payload and source identification, sequence numbering for receiver reassembly,

timestamping, timing recovery, media synchronisation and delivery monitoring. The Application Layer also employs Session Announcement Protocol (SAP) and Session Description Protocol (SDP). SAP is a simple protocol that describes how multimedia sessions can be periodically announced or advertised on a range of well-known multicast addresses. SDP is intended for describing multimedia sessions. A future enhancement at the Application Layer is the use of Simple Network Management Protocol (SNMP). Although SNMP is predominately used to monitor and configure routers and switches in a network, it is increasing being used to control edge devices, including IP enabled cameras.

Application layer	Real-time Transport Protocol (RTP)	Session Announcement Protocol (SAP)	Session Description Protocol (SAP)	Simple Network Management Protocol (SNMP)
Transport layer	User Datagram Protocol (UDP)			
Network layer	Internet Protocol (IP)	Internet Group Management Protocol (IGMP)	Internet Control Message Protocol (ICMP)	Address Resolution Protocol (ARP)
Data Link layer	IEEE 802.3			
Physical layer	Ethernet physical layers (1000BASE-T, 1000BASE-SX etc.)			

Figure 27 - Specified protocols mapped to the TCP/IP model

7.2.5 Decision matrix

The decision matrix presents three states in the extent of the change to be made – minor change, major change and new vehicle. These can be defined as follows:

- Minor changes are those involving the addition of limited video capability, for example the addition of a low-light camera and display, with a simple point-to-point link.
- Major changes are those which may involve the addition of a multi-sensor, multi-display capability, requiring complex video routing arrangements.
- New vehicle is a self-explanatory term; the systems designer will have limited constraints regarding legacy equipment which has to be fitted.

The decision matrix presents three levels of systems complexity – low, medium and high. These can be defined as follows:

- Low complexity systems are those with limited or no legacy video fit. Examples of systems at this complexity level are ‘B’ vehicles, such as logistics support vehicles and Land Rovers.
- Medium complexity systems are those with limited fit of legacy video, but where future mission requirements may dictate more use of video imaging. Examples of systems at this complexity level are ‘A’ vehicles such as Warrior.

- High complexity systems are those with limited fit of legacy video, but where future mission requirements will dictate more use of video imaging, involving the use of both multiple and high-bandwidth sensors. Examples of systems at this complexity level are 'A' vehicles such as CR2.

	Extent of Change		
Complexity	Minor Change	Major Change	New Vehicle
Low	Analogue point-to-point link ITU-R BT 472	Digital Video Network	Digital Video Network
Medium	Digital Video Network	Digital Video Network	Digital Video Network
High	Digital Video Network	Digital Video Network	Digital Video Network

Table 17 – Video Decision Matrix

7.3 Power distribution & Management

In providing guidance for the implementation of power distribution systems a number of general aspects should be considered:

- system performance of current UK Land Platforms is specified in Def Stan 61-5 Part 6;
- electromagnetic compatibility of UK Land Platforms is specified in Defence Stan 59-411;
- 42V automotive power systems performance is defined in ISO 21848;
- new platforms, which are the subject of an international collaboration will have to comply with the requirements of all participants;
- There are no standards defining the performance of high voltage (>270V) power distribution systems for platforms.

More specific requirements to be considered are:

- Expansion capability – based on historic information future platforms will have a long lifetime in service and the variation in roles they undertake will require them to be fitted with numerous additional equipments needing electrical power. This will be done by expanding or connecting to the existing system. Future power distribution systems must be designed with the provision of expansion capability. This will involve additional connectivity and in some cases power distribution boxes. It is also possible that upgrades could involve generators that provide more electrical power which needs to be distributed within the platform. This will require upgrading existing cables and connectors or adding additional high current cabling networks all of which need physical

space. Although it is impossible to be more specific power distribution system design should consider and include these provisions.

- Batteries are one of the vulnerable parts of the system. To enable the crew to manage their power resources a battery state of charge / battery monitoring system with crew information shall also be provided. Distribution system voltage monitoring as an individual function or as part of health and usage monitoring (HUMS), would also assist in providing crew information which could be used for power management and to gain an understanding of how to fight the platform effectively.

7.3.1 Design guidance for the provision of a robust supply

One method to increase the robustness of signal paths is to use multiple cable paths, routing them with as much physical separation as possible. This will afford some protection against battle damage. Each cable will be screened and filtered to protect against EME and RFW. In a similar fashion power cabling is also protected in order to maintain sub system support and therefore maximum functionality of the platform.

All platforms have at least two sources of electrical power the generator and batteries Power from these is input to the Power Distribution Unit (PDU) which then distributes it to the various subsystems. The PDU connects power sources to subsystems as well as controlling and protecting the power distribution circuits. It will provide controlled switching to ensure that the various power distribution systems can be isolated from each other to minimise the effect of a fault (short circuit) on one circuit promulgating through the system. It can also be used to ensure that under fault conditions any available energy is allocated to subsystems based on priority.

The internal PDU switching systems and subsystem remote power controllers are networked and software controlled to facilitate power management. This puts a delay into platform systems becoming fully operational from switch on as well as increasing the risks of failure. High priority platform systems (namely automotives) should be available without delay and with minimal possibility of failure. Therefore the need to operate this system using networked control electronics should be questioned.

The power distribution system, connecting the loads to the PDU has specific requirements to ensure that any form of damage can be minimised and that the power supply is maintained to as many loads (subsystems) as possible. Figure 28, Figure 29 and Figure 30 describe candidate power distribution architectures. In Figure 28 each electrical subsystem receives its power from two separate sources which can be used to isolate it from either power feed. The power management system is required to check the integrity of the subsystem load and if a fault condition is detected, isolate the load maintaining the integrity of the power distribution system. The PDU will likewise check the integrity of the power feeds to identify a fault condition and isolate the faulty feed.

In Figure 29 the power is distributed is via a ring. For each subsystem there is a power distribution isolator which maintains the power distribution ring and a subsystem isolator which can isolate the subsystem. The power management system will be able to detect faults in, and be able to isolate the subsystem feed. Each distribution isolator will also be able to detect faults and by means of sector isolator cut out any faulty section of the ring. Reducing the ring to two separate feeds maintaining power to as much as the system as possible.

A third architecture, Figure 30, is based around a PDU which provides separate power lines for each subsystem. Each power line is controlled at the PDU. This configuration can occur in a platform as a main PDU and as a local PDU as illustrated.

Undertaking the switching activities to support, these requirements must be possible with minimal interruption of the supply. The switching systems must therefore be able to operate quickly, therefore fast automatic detection and switching is required.

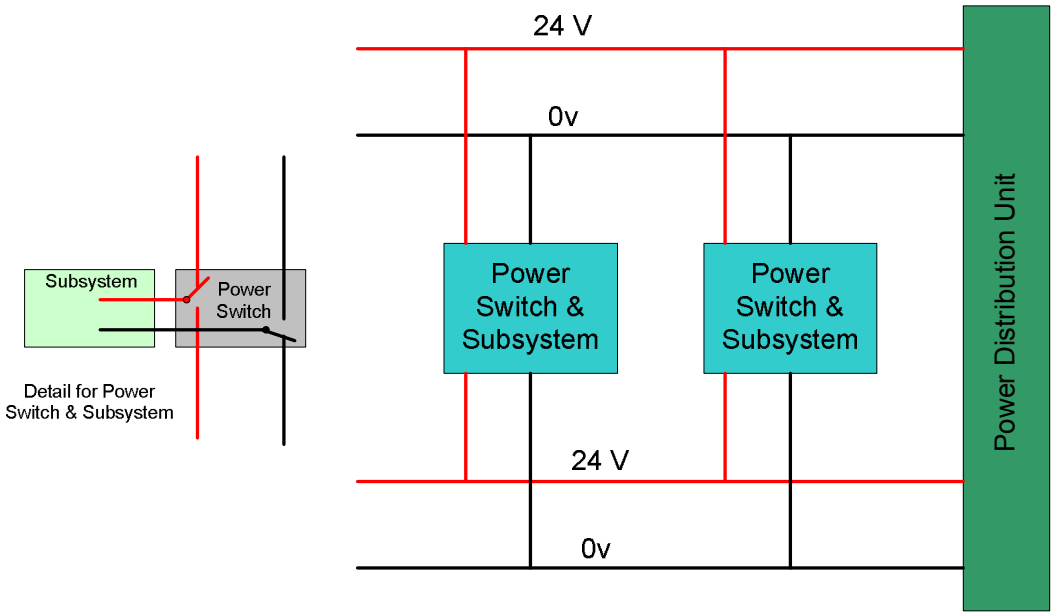

Figure 28- Dual source power feed

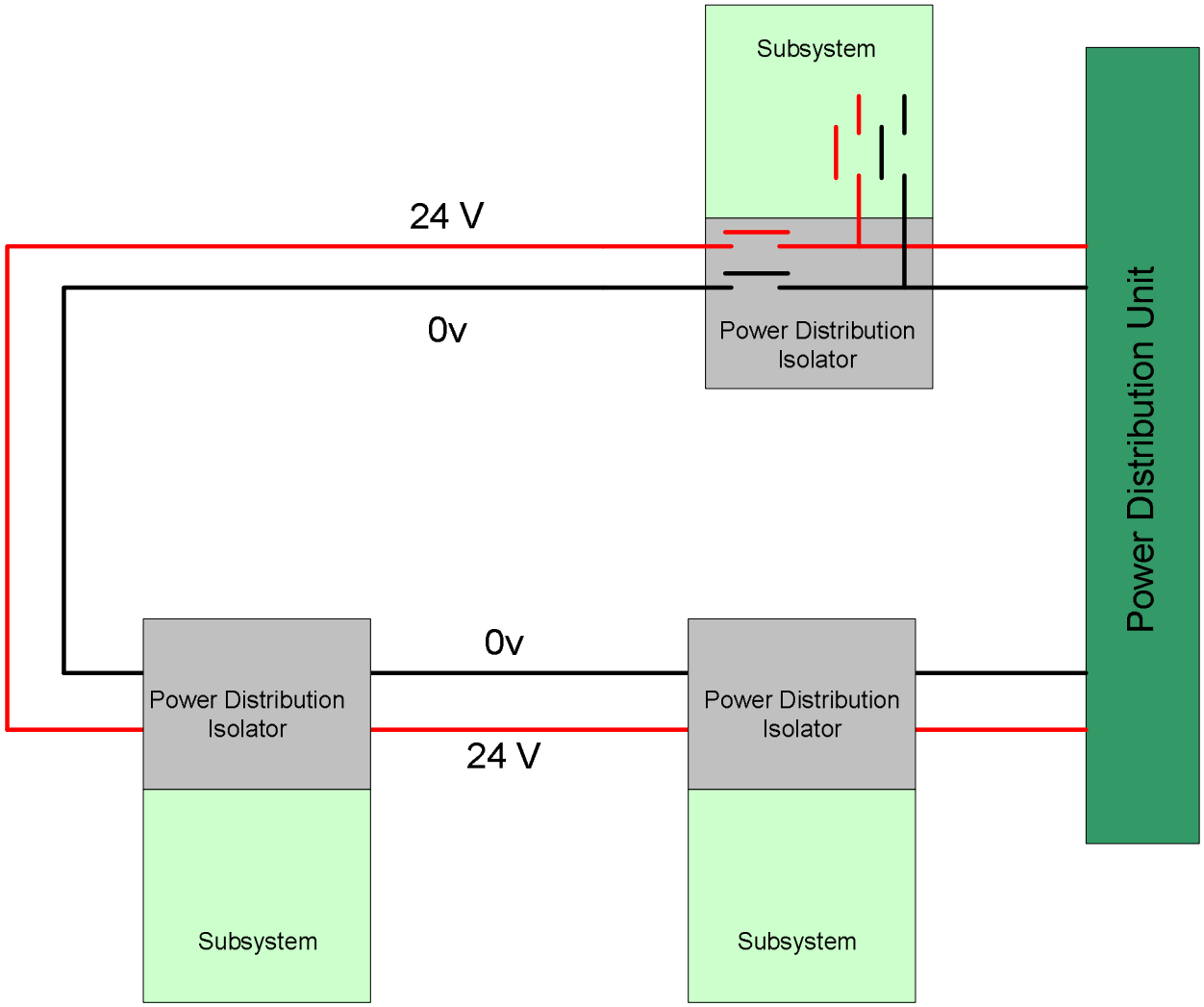

Figure 29 - Ring power feed

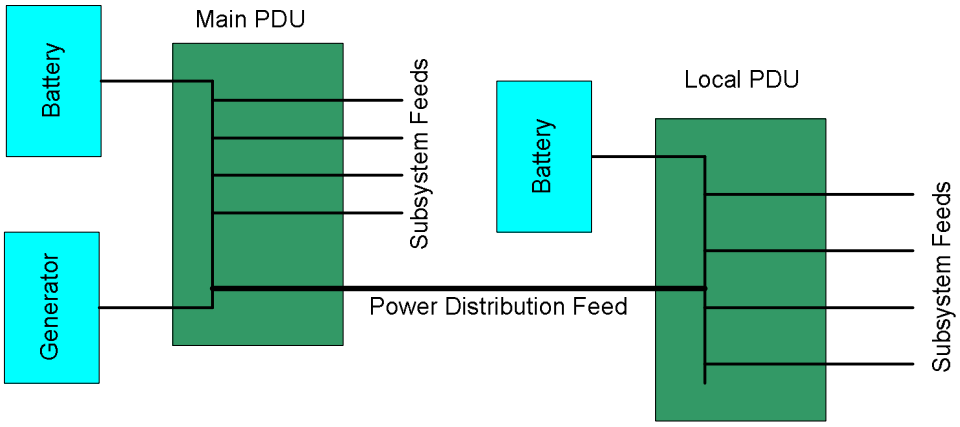

Figure 30 - Main PDU with local PDU

7.4 Introduction of middleware

Generally, the data and information within the platform's systems remains within the system itself. To meet the aspirations of programmes such as NEC and to make the platform more effective, platform information should be readily accessible. The data within any sub-system, firstly, needs to be made available within the platform to other sub-systems, and secondly, all platform data should be accessible at the internal system boundary, linking with broader C4I environment. What is desired is access to the data within the subsystems, and to make the data available throughout the platform. The following table provides guidance with respect to the introduction of middleware into military platforms. The areas where the greatest benefit is perceived are the instances where there is major modification to a platform either to extend its useful life and or capability.

	Extent of Change		
Complexity	Minor Change	Major Change	New Vehicle
Low	No middleware	No middleware	No middleware
Medium	No middleware	Middleware	Middleware
High	No middleware	Middleware	Middleware

Table 18 - Middleware selection matrix

8 Safety Legislation

8.1 Introduction

A major feature in the design of a safety critical system is the satisfaction of the legal requirements for the domain of operation. These legal requirements will vary form domain to domain, for example, the requirements for use of a drive by wire vehicle will be different from that in firing a weapon. However, the purpose of the underlying legislation is to make the system as safe as feasibly possible by presenting a framework of regulations within which the system will exist. This section covers a summary of the current legislative frame work, and distils the elements that are applicable to the design.

8.2 Caveat

As stated in clause 3.3 of Defence Standard 00-56 [3], it is accepted that related documents, standards and legislation may have changed since their creation. The documents referred to in this section are intended as a starting point and should not be viewed as a definitive list of legislation. It is still the responsibility of the users of Defence Standard 00-56 to ensure that they have a complete and up-to-date list of legislation relevant to the system they are developing.

8.3 UK Defence Requirements

In the most recent Issue of Def Stan 00-56 [3] [4], the requirements placed upon a contractor for developing safety critical/related systems have changed focus. The previous issue focussed on the theory of Safety Integrity Levels (SILs), which were widely accepted as problematic [5]. Not only were the SILs difficult to allocate but, once allocated, a SIL mandated certain techniques that had to be used to generate the evidence required to demonstrate that the system was safe. This generic 'once size must fit all' approach proved difficult and costly to achieve, especially for those programmes working to achieve SIL 3 – 4 certification.

To remedy this issue the focus of Def Stan 00-56 Issue 3 has now changed to identifying the goals that are required (Goal Based) rather than trying to impose the use of a set of tools/methods to achieve compliance.

Froome [6] describes the top level goals of Def Stan 00-56 Issue 3 as follows:

1. Identify the *Safety Requirements*.
2. Show that the requirements are *met.*

Although the standard is now more flexible allowing the contractor to decide how they will comply, this has given rise to uncertainty as to what tasks must be undertaken to achieve compliance [7].

The current Issue of Def Stan 00-56 consists of 2 parts. Part 1 of the standard clearly specifies a clause by clause description of the requirements placed upon the contractor i.e. what they have to achieve, not how they have to achieve it.

Part 2 of the standard is clearly identified as non-mandatory on its cover page. Its use is to provide a *possible* approach that the contractor could take to comply with the requirements set out in Part 1. Section 1 of Part 2 provides a clause by clause amplification of the

requirements in Part 1. Section 2 of Part 2 focuses on providing guidance for the development of Complex Electronic Elements (i.e. Software and Electronic Hardware).

8.3.1 HSE Documents

MOD procurements are no longer protected by Crown immunity, therefore the MOD, like its Contractors must adhere to Health and Safety Law. Defence Standard 00-56 makes this clear to the reader in Clause 2 as follows:

> 2 WARNING
>
> The Ministry of Defence (MOD), like its contractors, is subject to both United Kingdom and European laws regarding Health and Safety at Work, without exemption. All Defence Standards either directly or indirectly invoke the use of processes and procedures that could be injurious to health if adequate precautions are not taken. Defence Standards or their use in no way absolves users from complying with statutory and legal requirements relating to Health and Safety at Work.

The sections 8.3.2 through to 8.3.5 expand on this statement by identifying the related health and safety documents referenced within 00-56 Part 2.

8.3.2 Reducing Risks Protecting People (R2P2)

The R2P2 document was published by the HSE aiming to explain to the general public the HSE decision making process and is not intended as a document for providing guidance to individual duty holders on what they need to do.

The document provides a useful source of information and guidance on how the HSE carries out its Risk-Management processes and how they apply the ALARP (As Low As Reasonably Practicable) principle on which Risk measurements in Def Stan 00-56 are judged. The following is taken from Def Stan 00-56 Part 1:

> 0.1 Under UK law, all employers have a duty of care to their employees, the general public and the wider environment. For the MOD, this includes an obligation to manage the safety risks associated with military systems and their operation. In addition safety is a vital characteristic of defence systems as it often has a significant impact upon operational effectiveness. In accordance with general guidance provided by the Health and Safety Executive, MOD will discharge this duty by ensuring that, in so far as risks are not judged to be unacceptable, they are reduced to a level which is As Low As Reasonably Practicable (ALARP).

Further guidance on the ALARP principle is provided in Annex B of Def Stan 00-56 part 2. Section B.2.2 of Part 2 discusses how the hypothetical figures of risk that a hypothetical person is exposed to with 1 year can be used during the Risk assessment process to aid in defining Tolerability Criteria. The definition of Tolerability Criteria for ALARP decisions is a requirement placed upon the Contractor, but, as clause 10.7.1 states this is an activity that the Contractor should undertake with the Duty Holder to obtain their agreement.

> 10.7.1 Unless otherwise specified, the Contractor shall establish Tolerability Criteria based on relevant legislation, standards and MOD policy, in agreement with the Duty Holder. These shall form the basis for making an assessment as to whether a risk is broadly acceptable or tolerable and ALARP.

Amplification of clause 10.7.1 in 00-56 Part 2 also provides further guidance on how to achieve this.

8.3.3 Health and Safety at Work Act 1974

The Health and Safety at work Act provides "*legislative protection for health and safety to everyone who is employed, whether paid or not (except domestic servants) and imposes more general but wider duties on both employer and employee. The Act makes provision for protecting others against risks to health and safety from the way in which work activities are carried out. It also seeks to control certain emissions into the atmosphere and to control the storage and use of dangerous substances*" [8].

In addition to the Act of Parliament other regulations, made under or within the context of the Act, also apply. A more defined list is provided in paragraph 2.1.1.2 of Defence Standard 00-25 Part 21/Issue 1 [8]. A shortened list of the Regulations that may apply is as follows:

- Management of Health and Safety at Work Regulations 1999;
- Control of Substances Hazardous to Health (COSHH) Regulations 2002;
- Workplace (Health, Safety and Welfare) Regulations 1992;
- Manual Handling Operations Regulations 1992;
- The Electricity at Work Regulations 1989;
- The Noise at Work Regulations 1989;
- The Reporting of Injuries Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR);
- The Confined Spaces Regulations 1997.

As stated in the WARNING provided in Clause 2 of 00-56, the Health and Safety at Work Act and its derived Regulations are of paramount importance to any project now undertaken by a Contractor for the MOD.

8.3.4 Management of Health and Safety at work Regulations 1999. Approved Code of Practice and Guidance.

The management of health and safety at work regulations are again an extension of the Health and Safety at Work Act. Def Stan 00-25 part 21 states that the extensions to the Act, among other things, require employers to:

- Carry out Risk Assessments;
- Have arrangements for the planning and control of protective and preventative measures;
- Appoint competent persons to give health and safety assistance;
- Have procedures to cope with serious and imminent danger;
- Give Information to employees;
- Take into account the employee's training and capabilities when entrusting tasks.

For further details the guidance itself should be consulted. The guidance book is available from the HSE Books web site [9].

8.3.5 Safety, Competency and Commitment. Guidelines for Safety Related System Practitioners

The safety, competency and commitment guidelines were initially produced as a consequence to the lack of detail provided in IEC 61508 [10] for the requirement to ensure that competent employees are tasked for safety critical/related projects [11]. Issue 2 of 00-56 did not address this whereas Issue 3 has picked up on the importance of mandating that contractors use demonstrably competent staff thus the inclusion of clause 7.1 of 00-56 Part 1 that states:

> 7.1 The Contractor shall provide evidence that tasks within their control that influence safety are carried out by individuals and organisations that are demonstrably competent to perform those tasks.

Part 2 of 00-56 in the amplification of Clause 7.1 then explains that a method of achieving compliance with this requirement would be to use the Safety, Competency and Commitment Guidelines [12] developed by the Institute of Electronic Engineers, the British Computer Society and the Health and Safety Executive.

8.3.6 Defence Standard 05-57 (Configuration Management of Defence Material)

In Issue 2 of Defence Standard 00-56 [3] it was required that the contractor "*shall meet the requirements of Def Stan 05-57, or an alternative equivalent standard is agreed in writing prior to any work commencing*". Whereas part 1 of Issue 3 only states that:

> 6.7.4 The Contractor shall implement a suitable configuration management process for all safety work.

The mandated requirement probably does not specify a suitable configuration process so as not to place constraint on a project and allow for the most suitable option for the project to be selected. This would be particularly useful for a Contractor who has no experience of UK Defence projects yet has a suitable configuration management system in place that is comparable to 05-57. The amplification of this Clause in 00-56 Part 2 states:

> 6.7.4 Def Stan 05-57, Configuration Management of Defence Material, will probably be called upon in the contract to ensure that configuration control is applied to all documentation, including safety documentation. Should Def Stan 00-57 not be called up under contract, the Contractor should seek agreement with the Duty holder that configuration control procedures for safety related documentation are appropriate before they are implemented

8.3.7 ISO 14001: Environmental Management Systems

Clause 0.4 of Defence Standard 00-56 Part 1, Issue 3 states:

> This Standard does not specifically address the environmental damage element of safety or the management of environmental issues. MOD policy and guidance on this topic can be found in JSP418 and ISO 14001

ISO 14001 is the international standard on Environmental Management Systems (EMS). As described in a Ministry of Defence guidance booklet available on the Acquisition Management System web site [13], "*An EMS provides a mechanism for ensuring that an*

organisation's key environmental issues are managed appropriately. The EMS is a "living" system which provides continual improvement in environmental performance".

ISO 14001 focuses on what an EMS is required to achieve rather than a methodology. The MOD corporate EMS is based on the ISO 14001 standard and can be found in more detail within JSP418: Environment Manual.

8.3.8 JSP 418: Environment Manual

JSP418, as aforementioned, is based upon the contents of the Environmental Management System described in ISO 14001, and provides information on MOD policy for Environmental Management. JSP418 [14] states that it is designed to provide "*a framework for managing environmental agendas and for tracking, evaluating and communicating performance*".

Paragraph 3002 of JSP 418 states that "*MOD Environment policy is to comply with international conventions to which the UK is a signatory*". In addition to Chapter 3 of JSP 418, which provides an overview of Environmental Law, Paragraphs 4019 through to 4026 of JSP 418 list the relevant International conventions, EC Legislation and UK Legislation as:

International:

- The Convention on International Trade in Endangered Species (CITES);
- The Montreal Protocol 1987;
- Rio Summit Agreement on Climate Change 1992;
- The Kyoto Protocol 1997.

European Commission:

- The EC Ecolabeling Scheme 1992;
- The EC Regulation 3093/94/EEC implementing the Montreal protocol.

UK:

- The Environmental Protection Act 1990;
- The Environmental Protection (Controls on Injurious Substances) Regulations 1992 (SI 1992/1583) amended by the Environmental Protection (Controls on Injurious substances) (No 2) Regulations 1993 (SI 1992/1643);
- The Environmental Protection (Non-Refillable Refrigerant Containers) Regulations 1994 (SI 1994/199);
- Environmental Information Regulations 1992 (SI 1992/3240) amended by the Environmental Information (Amendment) Regulations 1998 (SI 1998/1447).

As a good starting point to the subject of Environmental management in the Acquisition in the management process the Project Oriented Environment Management System (POEMS) website on the MOD AMS contains an introductory booklet [13] that introduces what is a vast subject.

8.3.9 Defence Standard 00-25: Human Factors for Designers of Systems

Human factors are widely accepted within the System Safety domain as being an important tool in the design of Safety Critical/Related Systems [15]. Defence Standard 00-25 currently appears in 9 parts from parts 14 – 21 and 25, which provide guidance on Human Factors across each of the forces.

Although Def Stan 00-56 Part 1 does not explicitly specify a requirement to address Human Factors, the amplification of Clause 1.2 of Def Stan 00-56 part 2 considers the definition of a system provided by Part 1. In its consideration Part 2 suggests that Human Factors 'should' be considered where the system includes a people element:

> 1.2 Systems will include a combination of elements. The two main elements will usually be equipment and people. Human Factors should receive appropriate consideration including where they relate to the use of tools and techniques; ref Def Stan 00-25, Human Factors for Designers of Systems.

Although there is no specific requirement in part 1 for the Contractor to take Human Factors into account it is believed that its inclusion is implicit in the requirement to construct a demonstrably safe system. This is because developers of modern safety critical systems have realised that considering Human Factors in the early stages of Safety Critical System design plays a vital role in its success.

The only point where 00-56 part 1 specifically mentions Human Factors is in clause 10.8.1, where risk mitigation strategies are discussed. Def Stan 00-56 Part 1 ranks the use of Human Factors to mitigate risk as a third line of defence after firstly eliminating a risk completely or secondly by including an engineered mitigation strategy to reduce the risk. This could be why the inclusion of Human Factors in the amplification (1.2) states that the contractor should (not shall) take into account the requirements of Def-Stan 00-25 in its aim to impose requirements that are 'goal setting' and do not constrain the development process.

8.3.10 Defence Standard 00-40: Reliability and Maintainability

Def Stan 00-40 is referenced in Def Stan 00-56 part 2 in the amplification of clause 13.6 in part 1 that requires the Contractor to operate a process for recording in service use of the system, in order to strengthen the argument and evidence in the safety case.

Def Stan 00-56 Part 2 references Def Stan 00-40 as it mandates the use of a Data Reporting, Analysis and Corrective Action System (DRACAS) that could meet the requirement of clause 13.6 of 00-56 Part 1.

8.3.11 Related Safety Standards

Part 2 of Def Stan 00-56 makes reference to other available safety standards such as the three listed below.

- RTCA DO178B: Software Considerations in Airborne Systems and Equipment
- IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems
- Def (Aust) 5679: The Procurement of Computer Based Safety Critical Systems

In making this reference, 00-56 states that other appropriate international standards could be used to define safety integrity requirements, to achieve compliance with the requirements in Part 1. Although this gives the Contractor greater flexibility, it may prove to be useful only where the related standard is domain specific (e.g. DO178B) and thus takes into account the issues involved with certifying systems from a specific domain (e.g. aircraft). To the authors knowledge, domain-specific certification standards, suitable to Land Systems, currently do not exist. As stated in 00-56 part 2, for further guidance on this subject the contractor should consult the Duty Holder:

> C.2.3 The Duty Holder and Contractor may agree to adopt a safety integrity level scheme

in order to define safety integrity requirements, if there is a suitable scheme, preferably defined in an international standard appropriate to the domain and application of the system.

8.3.12 MOD Acquisition Management System (AMS)

The MOD Acquisition Management System is a tool maintained by the MOD for the provision of guidance. The areas of possible interest to a reader of this document are the safety pages [16] and the Project Oriented Environment Management System (POEMS) [17] and Project Oriented Safety Management System (POSMS) sites.

The safety page provides links to the relevant Safety Groups within MOD and also provides a centralised list of reference documents that may provide the reader with useful guidance.

The POSMS and POEMS sites provide guidance on safety management and environmental management respectively. As guidance tools these are both especially useful. Process maps for both the Environmental and Safety Management System exist that provide guidance throughout the CADMID (Concept, Assessment, Demonstration, Manufacture, In-Service, Disposal) lifecycle and refer off to procedural documents that provide guidance for each step of the lifecycle for both management systems.

8.4 Legislation Pertaining to Ordnance

Military vehicles frequently employ remote controlled operation of weapon systems (guns and missiles) by electronic means. The link between the initiator (usually a human being) of the firing command and the launching or firing of the weapon is the Firing Circuit. Such circuits must incorporate sufficient elements to prevent inadvertent firing events.

In the UK, DOSG (the Defence Ordnance Safety Group; formerly the Ordnance Board) is responsible for approving such circuits before they can be accepted into any trials or service involving HM forces. To assist in this, DOSG publishes a range of documents – the Pillar Proceedings – containing rules and good practice guides for designers of firing circuits and other ordnance related systems.

Pillar Proceeding P101 is the key document relating to the safety of firing circuits for electro-explosive devices. It advises the use of hardware logic between the weapon operator's Fire button, other safety devices (on-target indicators, blind-arc detectors etc.) and the weapon's electrical initiator. If any or all of these elements are remotely located, a dedicated hardwire link has been traditionally used, to prevent interference from other functions.

A distinction between remote weapon actuation and remote mobility functions (drive-by-wire) is that in the former case, a simple "do nothing" failure mode is generally acceptable, whereas in the latter case, such a simple implementation is unlikely to be satisfactory – continuing to drive at the same speed and in the same direction would not be safe for very long.

The fail-safe mode argument was used in a recent MOD demonstration programme, in which an Ethernet data bus (part-fibre-optic, part-wireless) was used to interconnect the remotely located elements of a firing circuit. Hardware circuits at either end of the data bus link generated and validated key codes in a challenge-response sequence, gave sufficient confidence in the reception of a valid fire command for DOSG to permit its use on controlled firing trials. This is illustrated simply in Figure 31.

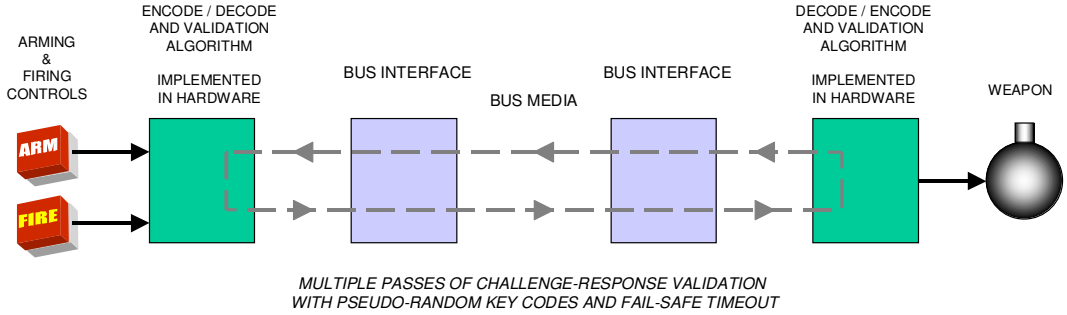

Figure 31 - Remote Weapon Firing Link

The above example uses hardware validation circuits to implement a safety critical function over a non safety critical specific bus (Ethernet).

The Defensive Aid Suite (DAS) situation is slightly different in that the consequence of doing nothing is likely to be more hazardous. A weapon system can "fail safe", in that it is generally preferable that it does not fire than that it fires inadvertently. But if a DAS system fails to respond to a threat, it becomes useless and puts the Users in danger, since they are likely to be under attack. The mitigation may be a manual override, but the whole point of employing a DAS is to be able to respond in a timely manner. A late response can be worse than useless, because it confirms details about own-platform to the enemy, without being able to defeat the threat. Other safety implications for friendly forces or civilians in the vicinity of a DAS equipped vehicle. If the system triggers accidentally the crew of the vehicle will be OK but those around the vehicle may be at risk.

The timely response requirement has implications on data bus architecture. The bus must be deterministic and able to guarantee that the threat detection is countered by an appropriate response in an appropriate timescale. Technologies such as TTP/C, FlexRay and 1553B meet this requirement and also include a hardware validation element. Combined with a multiple redundant architecture and formal verification methods a sufficiently robust system could be realised.

No acceptance criteria exist at the moment for a system of this kind. It will probably be incumbent on the first company to propose such a system to develop suitable acceptance and validation procedures in conjunction with DOSG. As the development tools would be the same as those used for drive by wire, a starting point would be to base weapon system / DAS procedures on those being developed for the automotive industry.

8.5 UK Specific Automotive Legislation

In this section automotive legislation for the UK is introduced. Initially UK-specific legislation is introduced followed by EU legislation, which itself is becoming incorporated into UK legislation.

The primary piece of legislation regarding vehicle construction and use can be found in The Road Traffic Act 1988 [18] and 1991 [19] amendments. This Act consists primarily of:

- Driver Standards;
- Vehicle Standards;
- Licensing Standards;
- Operator Standards.

The Road Vehicles (Authorisation of Special Types) (General) Order 2003 is the only piece of legislation found that specifically provides guidance for "*Operational Military Vehicles*". The Order recognises that military vehicles are a "*Category of Special Vehicles in any case where compliance made under section 41 of the Road Traffic Act 1988 by any such vehicle would directly compromise the vehicles operational capability*". As such any operational vehicle must be certified by the Secretary of State as being a vehicle, or type of vehicle, which for operational reasons cannot comply in all respects with the requirements of the Road Traffic Act.

The 2003 Order states the regulations applicable to military vehicles as being:

- Road Traffic – The Road Vehicle (Construction and use) Regulations 1986 Statutory Instrument Number 1078 as amended last amendment by 2004 No 2102;
- Road Traffic – The Road Vehicle Lighting Regulations 1989 Statutory Instrument Number 1796 as amended last amendment by 2001 No 560;
- Road Traffic – Road Vehicles (Authorised Weight) Regulations 1998 Statutory Instrument Number 3111 as amended last amendment by 2001 No 1125.

Additional UK legislation governing vehicles that are mass produced for sale within the UK and Europe are known as the Type Approval regulations that also reference the relevant EC Type Approval Directives.

- The Motor Vehicles (Approval) Regulations 2001 Statutory Instrument Number 25 as amended last amendment 2004 No 623.

In section 4.3 European legislation (EC Directives and Regulations) required by current UK legislation are described in more detail although the specific amendments required and the specific details of the incorporation of European law into UK Law has not been investigated and would require further investigation by the reader.

8.6 European Community Automotive Legislation

European legislation is now introduced because of a statement made by the Secretary of State for Defence in July 2002, "*Overseas, the Ministry will apply UK standards where reasonable practicable and in addition comply with relevant host nations standards*" [20].

JSP 418 provides a good introduction to the structure of the European regulatory framework (Although from an environmental perspective).

According to JSP 418 European Law is divided up into 4 different categories of Legislation:

- **Regulations**, which are directly applicable (i.e. they do not require national legislation to give them effect) and binding on all member States.
- **Directives**, again binding on Member States, but which lay down the results to be achieved, leaving it to Member States to transpose them into national legislation.
- **Decisions**, which are binding on the Member States, companies or individuals to whom they are addressed.
- **Recommendations**, **Opinions**, **Resolutions** and **Declarations**, which are not binding but serve as policy reviews or declarations of intent.

8.6.1 ECE Regulations

The ECE Regulations for Motor Vehicles can be found on the European Union Website [22]. The website provides a list of all regulations that would be directly applicable to all

vehicles produced for sale and use in Europe. In addition, the regulations are referenced within UK Construction and Use (C&U) Regulations. The specific ECE Regulations that can be found in UK C&U regulations have not been investigated and would require the reader to investigate further.

To date the inclusion of regulations for the development of complex electronic elements for motor vehicles is still sparse, but are being actively developed. As of 2004 the only ECE regulation to make any mention of software and electronics based Systems is Regulation 13 Annex 18 "*Complex Electronic Systems*" [23]. Regulation 13 is the braking regulation and the inclusion of complex electronics in the regulation is born of recent advances in braking technology e.g. ABS, Traction Control, Stability Control, Adaptive Cruise Control etc. All of which can override control of the primary braking system, which makes them safety critical/related.

Regulation 13 also introduces the requirement for the manufacturer to demonstrate the safety of the complex electronic system. To achieve this, it is expected that the manufacturer would need to develop a safety argument for the system, to show, for example, that the system can fail-safe or is fault tolerant.

According to Ward [23], at the time of writing (2004) there existed a proposal to extend this regulation to include all Complex Electronics within a vehicle as in their current state the regulations did not appropriately address the issues concerning the inclusion of Complex Electronics within vehicles.

More recently, (21st April 2005) the UN Economic Commission for Europe published an amendment to Transport Regulation 79 – "*UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REGARD TO STEERING EQUIPMENT*" [24]. Like Regulation 13, Regulation 79 provides instruction on what is required for Steering systems for wheeled vehicles that are controlled by Complex Electronics. According to the TTA-Group [25] they expect that further legislation will soon become available to set out the steering requirements of off highway vehicles, which includes Track Steered vehicles.

8.6.2 EC Directives

All mass produced motor vehicles for sale within Europe must follow a Type Approval Process as defined by EC Directive 70/156/EC amended at last amendment by 2004/104/EC.

Each of the directives for motor vehicles, motor bikes and tractors that will be operated within the European Union can be found on the EUROPA web site [26]. For each class of vehicle the relevant directives are either listed or associated with a graphical representation of that class of vehicle.

The following base directives for motor vehicles [26] (not including amendments) includes the directives that currently cover the steering and braking control requirements for vehicle developed in accordance with EU Type Approval legislation.

- 70/156/EC Type-approval of motor vehicles and their trailers;
- 70/311/EC Steering equipment for motor vehicles and their trailers;
- 71/320/EC Braking Devices of certain categories of motor vehicles and their trailers;
- 72/245/EC Radio Interference (Electromagnetic Compatibility) of vehicles.

Even though the ECE Regulations have very recently provided coverage for future vehicles which implement drive by wire systems the EU directives currently do not. It is believed

that the directives will be amended to include such provisions and that they should be ratified by the year 2010 [27].

In addition to these the legislation pertaining to off highway vehicles (e.g. tractors, construction vehicles etc) could also be relevant to certain military vehicles. For example, a new amendment to off highway steering legislation, to include fully electronically controlled steering systems in off highway vehicles. This Directive is known as 75/321/EEC "*Steering Equipment*", draft for amendment 2003.

8.7 Routes to Certification

With regards to safety case development for any vehicle that shall be used on public roads there is currently no independent regulatory body to which such a safety case could be submitted [28].

The provision for mass produced vehicles is the type approval process as aforementioned which prescribes the legislative requirements by which vehicle manufacturer shall construct and produce their vehicles. The type approval process in the UK is initiated in conjunction with the UK Vehicle Certification Agency, which is an executive Agency of the Department for Transport.

With regards to the Approval of Military Vehicles for public road use the Land Systems Safety Office (LSSO), Defence Logistics Organisation (DLO) ES(Land) Tech, Department for Transport (DfT) and the Vehicle Certification Agency (VCA) have each been approached to provide an indication of the process that would have to be followed to obtain certification of a Military Vehicle.

The results of conversations with DLO ES(Land) Tech, DfT and LSSO indicated that there is no specific answer and that each vehicle would have to be assessed depending upon its intended role and operational requirements. Conversation with these organisations did refer to the Construction and Use regulations as required by The Road Vehicles (Authorisation of Special Types) (General) Order 2003 as a good place to start.

A more beneficial conversation was held with a representative of the VCA who again mirrored the answers as previously given but gave more detail. The VCA again recommended at the beginning of the project that the User Requirements of the vehicle be provided to the VCA such that the relevant legislative requirements could be identified. For example the VCA would require knowledge of where the vehicle is intended to be operated so that national specific legislation could be investigated in addition the general EC and UNECE legislation. It was also indicated that the involvement of the VCA from the offset would be beneficial as there involvement would help ensure that the correct legislative requirements were identified from the beginning. The primary reason is that before the vehicle can be certified for use on public roads it is still required that the VCA issue the certificate of Approval for the vehicle.

It was also indicated that full vehicle type approval for most military vehicles is likely to be impossible to obtain due to reasons of operational effectiveness. So for example most military vehicles operate with the requirement to have kill switches on the vehicles lights (including brake lights) such that they can be fully disabled to reduce the probability of detection. In accordance with vehicle lighting regulations such a function on the vehicles lighting system would result in the vehicle not being able to obtain approval. As such the Duty Holder/Contractor is required to provide the relevant authority to make the vehicle exempt from any requirements that may reduce its operational effectiveness. Yet on the other hand the Duty Holder/Contractor is also obliged by the requirements of Defence Standard 00-56 [4] to make the safety of the vehicle "*as civil as possible*".

Figure 32 shows a potential structure to how the relationship between the four stakeholders may work. Ultimately the MOD will appoint a prime contractor to complete the work required. In addition to this, if during the Concept phase of the CADMID lifecycle the MOD Duty holder identifies unacceptable potential hazardous events, resulting from the system, then an Independent Safety Auditor will be appointed to monitor the outputs of the Contractor. The required independence between the ISA and the Contractor will be governed by the assessed integrity requirement of the system to be constructed. Therefore, as the integrity required of the system increases the more independent the ISA will have to be. The requirement for the ISA is mainly driven by a requirement in Defence Standard 00-56. In addition to this, the VCAs independence in terms of the system being constructed could become open to question if they are to provide guidance on legislation to the Contractor. In this instance the VCA would act more as an assessor of the System being constructed than an auditor.

The Independence of the ISA would then allow the work of the VCA and contractor to be audited in the same way a regulatory body would wish to act to ensure good practice from the Contractor and to verify the decisions made by the VCA.

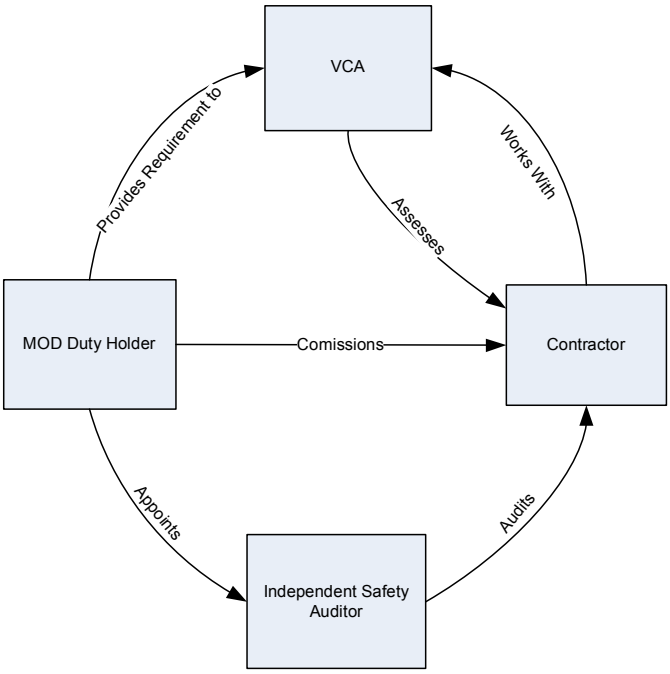

Figure 32 - Relationship between MOD, VCA, ISA and the Contractor

Currently, the only project that could be identified that had achieved certification (within some constraints) of a drive by wire military vehicle is the Wiesel 2 vehicle commissioned by the German BWB. In this instance the German BWB informed us that they commissioned a contractor to modify a Wiesel Armoured Fighting Vehicle with drive by wire. The system is believed to have been implemented using a constrained CANbus interconnect with triple redundancy in the physical layer. It is understood that a body in the German government that is responsible for the certification of military vehicles known as the ZMK performed the vehicle certification. The German TUV acted as the Independent auditor for the project to ensure compliance with Functional Safety standards.

9 Safety Management Lifecycle

QinetiQ recently conducted a research package, in conjunction with BAE Systems and Ultra Electronics, to look at the process required to qualify an X-by-Wire vehicle. Although the research stopped short of actually qualifying the vehicle, the aim of the research was to look at the process & to highlight any problems in using IEC61508 [10] safety management lifecycle to meet the requirements specified by the Interim Defence Safety Standard 00-56[4].

9.1 The rationale for choosing IEC61508

The flow diagram shown in Figure 33 shows the interrelationship of the risk management activities (on the right) and the three most basic systems engineering activities (on the left) that are required to develop a safety related/critical system.

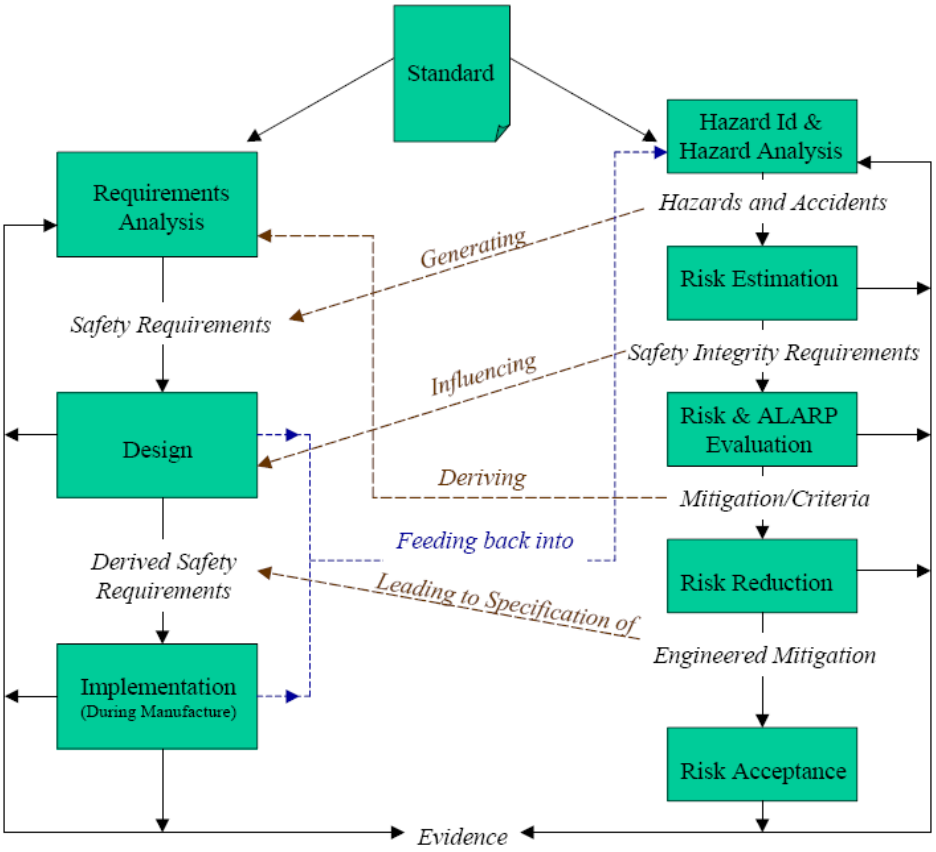

Figure 33 - Interrelationship of risk management processes from Def-Stan 00-56.

In comparison Figure 34 shows the safety management lifecycle taken from IEC61508 part 1. The flow of activities from both lifecycles do bear resemblance as they both consider the core set of activities required to developed safety critical systems. The most obvious differences, comparing the two flow chart representations, are that IEC 61508 appears to give little, if any, consideration to how the traditional engineering activities fit into the process. In addition, the IEC61508 process is modelled as a linear set of activities from which there no recourse to revisit any of the previously completed phases, (unless the user is

in the maintenance phase). A more detailed comparison of where the IEC61508 standard currently does not fit into the model presented in Figure 33 is described in section 9.1.2.

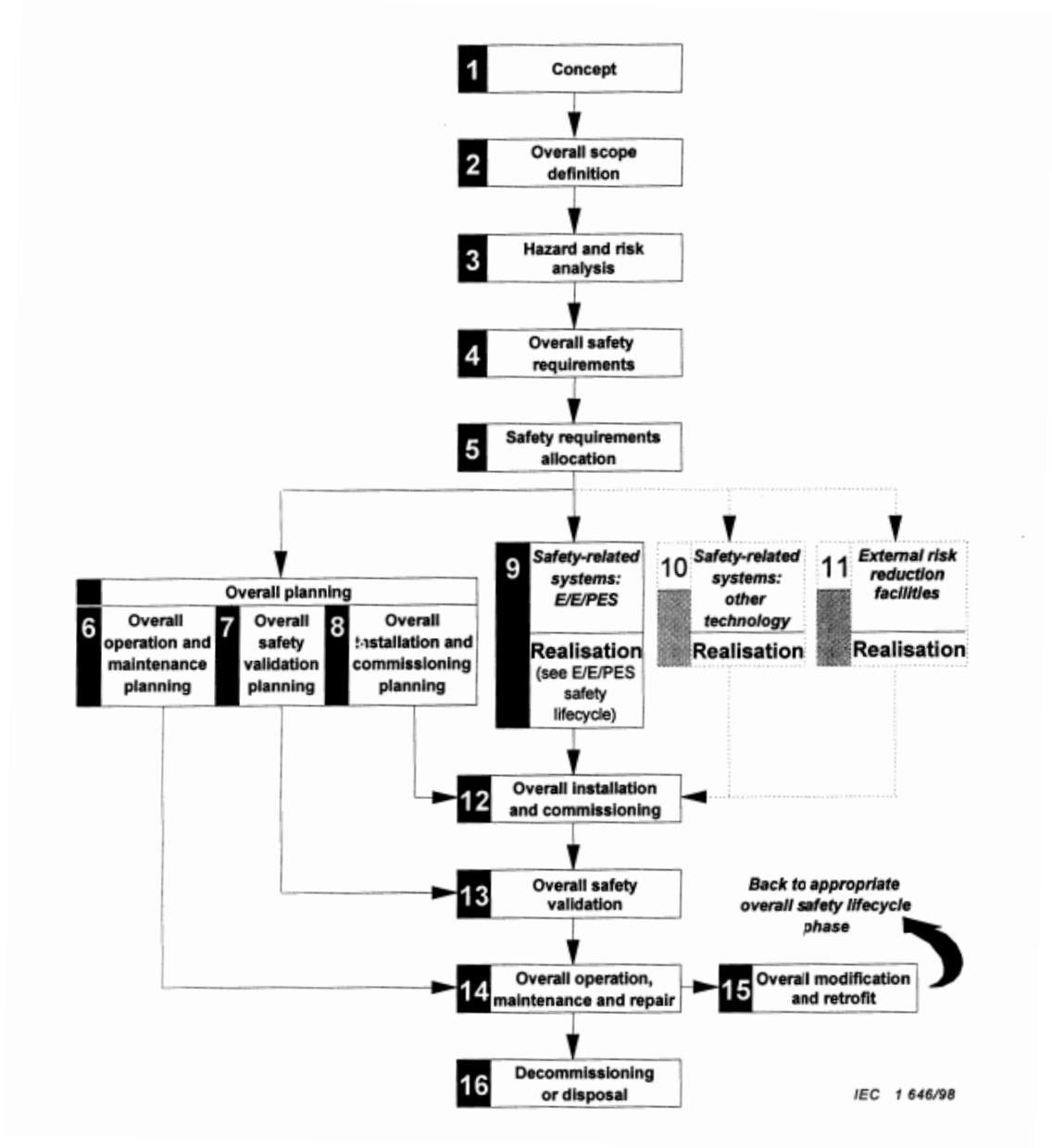

Figure 34 - The IEC61508 Safety management Lifecycle

Both Defence Standard 00-56 and IEC61508 subscribe to the following basic concepts of Hazard and Risk Management:

- Demonstrate what can go wrong.
- Firstly attempt to show that it cannot go wrong.
- Secondly demonstrate how protection has been engineered into the system if it was to go wrong.

To this extent it is therefore reasonable to suggest that the IEC61508 standard could be used to meet both the requirements of the Defence Safety Standards and whilst also taking into consideration what the civil automotive industry believe to be a ‘state of the art’ safety

management process (the use of 'state of the art' is a requirement of civil legislation [24]). The rationale for this method of thinking being to develop a military system that is as civil as possible.

9.1.1 Fallacies of SILs

The IEC61508 standard offers various examples for translating the risk to a safety integrity level. These are based on identifying the required amount of reduction of the likelihood of a hazardous event, which can be calculated by using the process adapted from Redmill [41], as follows:

- Derive the tolerable risk for the hazardous event by using the systems Hazard Risk Index (HRI)
- Read the tolerable frequency and the Equipment Under Control risk frequency
- Subtract the tolerable and Equipment Under Control risk frequencies to obtain the target frequency of the safety function;
- Read the SIL of the safety function from by correlating it with the appropriate (High or Low demand) target frequency as defined in IEC61508 Part 1 (See Figure 35 and Figure 36)

Safety integrity level	Low demand mode of operation (Average probability of failure to perform its design function on demand)
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	

Figure 35 - Relation of SILs and Target Failure Probabilities for Low Demand Safety Functions in IEC61508

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$
NOTE – See notes 3 to 9 below for details on interpreting this table.	

Figure 36 - Relation of SILs and Target Failure Probabilities for High Demand Safety Functions in IEC61508

Following the derivation of the SIL for a safety function it is then assumed that the correct application of the associated SIL process should provide the user with the required level of risk reduction for the associated safety function. Unfortunately there is no empirical evidence to argue that this is the case. Redmill [43] argues that the assumed relationship between product quality and development processes has no proven foundation. He argues that there is possibly a correlation between bad processes and poor products but the evidence to prove that good processes result in good products does not exist.

The rationale for using IEC 61508 safety management lifecycle as a template to meet the requirements of Defence Standard 00-56 is viable as long as the user does not base their argument of acceptable risk on the application of SIL's by claiming an achieved level of risk reduction (via a reduction in the probability of failure) as is currently specified by the standard. Further rationale to support this claim is that it is widely agreed that software cannot fail randomly and therefore the association of probabilities of failure to a function that can only fail systematically becomes increasingly dubious when used to support a safety argument.

Unless an argument of achieved acceptable risk can be supported by a set of robust and diverse evidence within a well formed and structured argument that can show that each failure mode of the software has been identified and for each failure mode the design has either eliminated it, or can tolerate its occurrence via some form of mitigation (E.g. Fault Tolerance through Redundancy) then any argument of acceptable safety can be brought into question and as such it could make it difficult to defend.

9.1.2 Where IEC 61508 does not address the requirements of DS 00-56

From the literature and from experience gained whilst implementing the safety management lifecycle as described in IEC61508 part 1 the following lists areas where IEC61508 does not make provision for the requirements of Defence Standard 00-56. It is not suggested that this list is in anyway comprehensive.

1. IEC61508 does not require a safety case to be developed, which presents an argument as to why the system constructed is acceptably safe. Instead IEC61508 part1 provides guidance on the types of documentation that the user would be expected to generate (e.g. Concept Document, Scope Document etc).
2. As can be seen by comparing both Figure 33 and Figure 34, the IEC61508 process does not model iteration between the hazard analysis stages and the resulting design changes. Whereas the Defence Standard requires that any changes to the design result in an impact analysis on the new design to assess the risk it poses. IEC61508 appears to suggest that any design to mitigate a certain hazard will not result in any other hazards or result in any changes to existing hazards.
3. Point 2 is backed up by Fan Ye [44] who suggests that the guidelines for SILS in IEC61508 are defined in terms of the amount of risk reduction achieved by adding protection mechanisms and that they fail to take into account the possibility that such addition may result in new failure modes and new risks.
4. Currently 61508 does not provide guidance for the engineering of a COTS based safety system whereas Defence Standard 00-56, having the advantage of being issued more recently recognises the importance of providing a method for certifying COTS and as such provides the user with guidance on what would be expected of them if they wished to use COTS.

9.2 Generating Evidence for COTS Based Systems

Utilising COTS components in safety critical systems can potentially cause difficulties if the components have not been developed with this intention in mind. Examples of potential difficulties could be quality issues (to what standard has the product been developed) and licensing issues (e.g. certain COTS suppliers forbid their products from being used in safety critical systems).

As a result of both of these issues the utilisation of fit for purpose (i.e. 'safety critical') off the shelf components should always be a prime consideration. The rationale for this being

that it is much more likely that the standard to which these components have been developed are much more robust and that evidence of how these products have been developed and the integrity of their functions can also be obtained (even if out of context). This is mentioned further in Defence Standard 00-56 part 2 as follows.

> **17.3.1.2** Where COTS or other existing complex electronic elements are used, the Safety Case should detail the processes used for evaluation, validation and implementation of the complex electronic element, processes used for any bespoke software or hardware (such as software wrappers or hardware interlocks) and any information from the complex electronic element supplier about the development process (where available). In general, the more onerous the safety integrity requirements, the more rigorous and compelling the process evidence that should be provided. For a COTS or pre-existing element, the rigour may have to be provided at the evaluation stage

The following subsections present a brief summary of the evidence that the respective suppliers, as used in the research, claim to be available for their products.

9.2.1 Evidence Generated for TTP Technology

The following provides a list of components supplied by TTTech that have been use on the research programme and the associated evidence that has been generated as a result of any work carried out to verify its correctness.

- TTP/C Protocol – Various aspects of the Time Triggered Architecture have been formally verified by authors such as John Rushby [49] at SRI international and Dr Holger Pfeifer [50] at the University of Ulm amongst some others [51]. Aspects of the protocol specification that have been verified include:
  - Partitioning in the Time Triggered Architecture;
  - Transmission Window Timing Mechanism;
  - Central Bus Guardian;
  - TTP Group Membership Algorithm;
  - Time Triggered Clock Synchronisation Algorithm.
- TTC200 and Associated Software Libraries – Seethaler [40] claims that the TTC200 and associated software libraries have each been developed in accordance with the IEC61508 functional safety management lifecycle. In addition to the TTC200 ECU has also been developed to the requirements of a large list of standards as defined [52].
- TTP Tools – The TTP Tools (Plan, Build, View, Load etc) have each been developed in accordance with TTTech's quality processes and nothing more. In order to verify that the output of the TTP Plan tool is correct (i.e. the Message Descriptor List) TTTech has developed a tool called TTPVerify [53] According to TTTech, TTP Verify has been developed in compliance with RTCA DO178B [54] requirements. To verify the outputs of the TTP Build tool (FT-COM layer) TTTech has previously provided a script based testing service in cooperation with an aerospace customer to verify the correctness of the FT-COM layer. Alternatively for another aerospace customer TTTech have generated what they call a Table Driven –COMmunications (TD-COM) layer, which has been developed in accordance with the requirements of RTCA DO178B DAL A. In order to verify the TD-COM layer TTTech are also planning to produce a TD-COM Verify tool, which would operate in a similar way to the TTP Verify tool.

- TTP/C C2NF Controller – Has been developed with automotive requirements in mind and as such TTTech claim that it is Automotive Certified. It is not entirely clear what that means from TTTech's website [55]. For its use in the Airbus A380 aircraft it is understood that the requirements of D0254 [56] were reverse engineered to demonstrate the correctness of the Controller and its implementation of the protocol [57]. It is also understood that the C2NF controller has been used in the
  - RTCA DO-160D Environmental Conditions and Test Procedures for Airborne Equipment
  - ISO7637 - Road vehicles -- Electrical disturbances from conduction and coupling
- TTP Operating System – The TTP Operating System and Fault Tolerant Communications Layer are generated by the TTP Build Tool. TTTech claim that their Operating System has been 'Reverse Engineered' to comply with the DO178B safety management standard.
- TTP SCADElink – Currently no evidence has been generated as to the correctness of this tool. The main reason for this being that the tool is only available as a prototype.

9.2.2 Evidence Generated for SCADE Technology

The SCADE suite of tools has been developed in accordance with both RTCA DO178B and IEC 61508 safety requirements. As a result of this Esterel Technologies have compiled a manual that explains how the SCADE tool can be used to meet the requirements of IEC61508 and that also details the requirements of IEC61508 that the SCADE tool satisfies [58]. Similar evidence showing how SCADE satisfies D0178B should be sought from Esterel Technologies.

9.2.3 Counter Evidence

As recommended by section 17.4 of Defence Standard 00-56 part 2 all counter evidence to a product must be collected and presented as well as the evidence that promotes its use. The following provides a summary of evidence that suggests that the TTP/C Bus architecture (RS485 Physical Layer) suffers from what are known as Slightly off Specification Faults.

Slightly Off Specification Faults

Ademaj [59] presents the work done on the problem of Slightly off Specification (SOS) faults in the TTP Bus architecture. An SOS fault is one where an analogue signal (converted from digital) is received in slightly different ways between different receivers because of differences in hardware tolerances. For example if a bit value is transmitted as a 1 and the signal strength is weaker than the specified level. The weak signal (½) could be received differently by different nodes that have different hardware tolerances (i.e. some could read this as a 1 and some could read this as a 0). To solve this problem Ademaj stated that in addition to protecting from babbling idiot faults the TTP Bus Guardian shall also perform active signal reshaping to "*prevent the occurrence of SOS failures in order to be considered as a fault containment unit*". In to modifying its function the Bus Guardian (BG) was also centralised into a TTP/C star coupler and resulted in the formulation of the TTP Star architecture (see Figure 37)

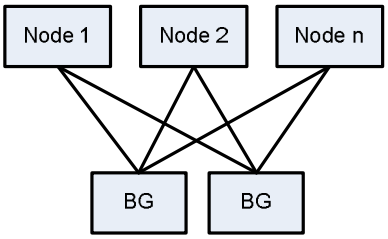

Figure 37 - An example Star Architecture showing the BG as the TTP Star Coupler

Further work by Ademaj et al [60] shows the fault injection tests that were performed on the TTP Bus architecture causing it to fail, were also performed on the TTP Star architecture and resulted in no faults detected. Work by Morris et al [61] questions Ademaj's work by stating that the fault injection experiments performed by Ademaj et al did not "*analyse the behaviour of the system in the presence of faults in the star couplers (BGs) themselves*". A fault in the BG could now possibly result in the loss or the corruption of the messages on an entire channel. Morris et al also explores the additional issues that could be created by allowing the BG in a Star Architecture the ability to actively reshape and change signals.

10 Metrics

The metrics have been removed from this document and are now contained in [71]

References / Bibliography

[1] Crolla. A, Meadwell. R, Green. M, Searle. A, "*Databus Standards for Military Vetronics – Initial Assessment*", QINETIQ/D&TS/LAND/WP050648, May 2005.

[2] Crolla. A, Meadwell. R, Green. M, "*Databus Standards for Military Vetronics – Detailed Assessment*", QINETIQ/D&TS/LAND/WP052423, May 2006.

[3] UK MOD, "*Interim Defence Standard 00-56 Issue 3 – Safety Management Requirements for Defence Systems – Part 1*", UK MOD, December 2004. (Now at Issue 4 as of 1st June 2007)

[4] UK MOD, "*Interim Defence Standard 00-56 Issue 3 – Safety Management Requirements for Defence Systems – Part 2*", UK MOD, December 2004.

[5] Redmill. F, "*Safety Integrity Levels – Theory and Problems*", Safety Critical Systems Symposium, 2000.

[6] Froome P, "*Planning and managing the safety lifecycle for Defence Standard 00-56 Issue 3*", Adelard, 2005.

[7] McDermid J, "*Safety Critical Projects Management – Lecture 19*", University of York, 2005.

[8] UK MOD, "*Defence Standard 00-25 Issue 1 – Human Factors for Designers of Systems – Part 21*", UK MOD, July 2004.

[9] HSE, "*Management of Health and Safety at Work Regulations 1999. Approved Code of Practice and Guidance*", ISBN 0717624889, HSE Books

[10] IEC 61508, "*Functional Safety of electrical/electronic/programmable electronic safety related systems*", CENELEC, 2001.

[11] May. R, "*Personal Competencies and the Requirements of IEC 61508*", The Institute of Electrical Engineers, 2001.

[12] IEE, "*Safety, Competency and Commitment: Competency Guidelines for Safety-Related System Practitioners*", IEE, 1999.

[13] UK MOD, "*An Introduction to the Environment and Environmental Management in the Acquisition Process - Issue 1*", UK MOD AMS, May 2004.

[14] DESB, "*JSP 418 – MOD Environment Manual*", Defence Environment Safety Board, July 1996.

[15] Flight Safety Foundation, URL: http://www.flightsafety.org/news/nr97-26.pdf, Accessed on 22/03/2005.

[16] UK MOD AMS, "*Topics – Safety*", URL: http://www.ams.mod.uk/ams/content/topics/2610.htm, Accessed on 07/04/2005.

[17] UK MOD AMS, "*Acquisition Safety and Environmental Management System (ASEMS) Homepage*", URL: http://www.ams.mod.uk/ams/content/docs/asems/index.htm, Accessed on 07/04/2005.

[18] HMSO, "*Road Traffic Act 1988*", Her Majesty's Stationary Office, 1988

[19] HMSO, "*Road Traffic Act 1991*", Her Majesty's Stationary Office, 1991

[20] UK MOD, "*An Introduction to the Environment and Environmental Management in the Acquisition Process - Issue 1*", UK MOD AMS, May 2004.

[21] DESB, "*JSP 418 – MOD Environment Manual*", Defence Environment Safety Board, July 1996

[22] UNECE, "*Vehicle Regulations - Agreement Concerning the Adoption of Uniform Technical Prescriptions (Rev2)*", URL: http://www.unece.org/trans/main/wp29/wp29regs1-20.html, Accessed on 08/04/05

[23] Ward. D, Woodgate. R, "*Meeting the challenge of drive-by-wire electronics"*, URL: http://mira.atalink.co.uk/articles/104, Accessed on 03/08/2005

[24] UNECE, "*UNIFORM PROVISIONS CONCERNING THE APPROVAL OF VEHICLES WITH REGARD TO STEERING EQUIPMENT*", 21/04/2005, URL: http://www.unece.org/trans/main/wp29/wp29regs/79r2e.pdf, Accessed on 11/07/2005

[25] TTA-Group, "*TTA-Group Steer-by-Wire Working Group*", SAE International, 2005

[26] EUROPA, "*EC Directives for Motor Vehicles, Motorbikes and Tractors*", URL: http://europa.eu.int/comm/enterprise/automotive/directives/index.htm, Accessed on 30/03/2005
[27] Rest. G, "*Steer-by-Wire Study*", University of Vienna, October 2005.
[28] Barker. S, Kendal. I, Darlison. A, "Safety Cases for Software-Intensive Systems: An Industrial Report", In Proceedings of 16th International Conference on Computer Safety , Reliability and Security (SAFECOMP'97), pages 332-342, York, 1997.
[29] Press. SJ, "*Design and Initial trials of a remote Control Tracked Vehicle based upon Hagglunds BV206 Running Gear (SHAP)*", DRA, FV&S5
[30] Kopetz. H, "*The Fault Hypothesis for the Time Triggerred Architecture*", Technical University of Vienna, August 2004.
[31] Pease. M, Shostak. R, Lamport. L, "*Reaching Agreement in the Presence of Faults*", SRI International, 1980.
[32] Kopetz. H, "*Real-Time Systems, Design Principles for Distributed Embedded Applications*", Kluwer Academic Publishers, 1997.
[33] Rushby. J, "*A Comparison of Bus Architectures for Safety-Critical Embedded Systems*", NASA report NASA/CR-2003-212161, March 2003.
[34] Seethaler. C, "*Architecture for Steer-by-Wire*", TTControl, 2005
[35] Email from Andreas Hainzl to Andrew Crolla, "*Teleconference Summary*", Received on 12/01/2006
[36] Navet. N, Ye Qiong Song, Simonot-Lion. F, "*Design of Automotive X-by-Wire systems*", PSA, LORIA UMR 7503, 2004.
[37] Heitzer. D, Seewald. A, "*Development of a Fault Tolerant Steer by Wire System*", TRW Automotive, 2004.
[38] Tudor. N, Adams. M, Clayton. P, O'Halloran. C, "*Auto-Coding/Auto Proving Flight Control Software*", QinetiQ/KI/TIM/TR041838
[39] Adams. M, Clayton PB, "*CLawZ: Cost Effective Formal Verification for Control Systems*", Systems Assurance Group, QinetiQ.
[40] Seethaler. C, "*The TTC-200 ECU, An Overview*", TTControl, 2006
[41] Redmill. F, "An Introduction to the Safety Standard IEC61508", Redmill Consultancy 1999.
[42] Still. R, "*SHAP SCDB Hazard Log Probability and Accident Severity Criteria (Version 2.1)*", QinetiQ/D&TS/Land/ RA0607424, 2006
[43] Redmill. F, "*The COTS Debate in Perspective*", in Proceedings of the 20th International Conference on Computer Safety, Reliability and Security, Springer Verlag, 2001.
[44] Fan Ye, "*Justifying the Use of COTS Components within Safety Critical Applications*", University of York, September 2005
[45] TTControl, "TTC200", URL:http://www.ttcontrol.com/products/hardware/safety-critical/ttc_200/index.htm Accessed on 29/09/2006.
[46] TUWIEN, "*X-by-Wire – Safety Related Fault Tolerant Systems in Vehicles*", URL: http://www.vmars.tuwien.ac.at/projects/xbywire/index.html, Accessed on 29/09/2006.
[47] Pimentel J.R, "*An Architecture for a Safety-Critical Steer-by-Wire System*", SAE 2004-01-0714, Kettering University USA, 2004.
[48] TTControl, "*TTC-200 V2, User Manual*", Manual Edition 1.1, 26/08/2004, D-TTC200-M-HW-001.
[49] Rushby. J, "Recent Papers by John Rushby", URL: http://www.csl.sri.com/users/rushby/biblio.html.
[50] Pfeifer. H, "Homepage", URL: http://www.informatik.uni-ulm.de/ki/pfeifer.html.
[51] TTA Group, "*TTA Group FAQ*", http://www.ttagroup.org/technology/faq.htm.
[52] TTTech, "*TTC200 EMC and Environmental Standards*", TTTech Computertechnik, November 2005.
[53] TTTech, "*TTP Verify – The TTP Design Verification Tool*", URL: http://www.tttech.com/products/software/ttpverify/overview.htm, Accessed on 29/09/2006.

[54] RTCA, "*DO-178B, Software Considerations in Airborne Systems and Equipment Certification*", Errata Issued 26/03/1999.
[55] TTTech, "*Products*", URL: http://www.tttech.com/products/index.htm, Accessed on 29/09/2006.
[56] RTCA, "*DO-254, Design Assurance Guidance for Airborne Electronic Hardware*", Issued 19/04/2000.
[57] Rajkovic. I, Gagea. L, "*Reverse Engineering Experience According to DO-254*", TTTech Computertechnik AG, 2006.
[58] Esterel, "*Efficient Development of Safe Automotive Software with IEC 61508 Objectives using SCADE Drive*", Esterel Technologies, 2005.
[59] Ademaj. A, "*Slightly-Off-Specification Failures in the Time-Triggered Architecture*", Vienna University of Technology, IEEE, 2002.
[60] Ademaj. A, Sivencrona. H, Bauer. G, Torin. J, "*Evaulation of Fault Handling of the Time Triggered Architecture with Bus and Star Topology*", IEEE International Conference on Dependable Systems and Networks, 2003.
[61] Morris. J, Kroening. D, Koopman. P, "*Fault Tolerance Tradeoffs in Moving from Decentralised to Centralised Embedded Systems*", Proceedings of the IEEE International Conference on Dependable Systems and Networks, 2004.
[62] TTChip, "*AS8202NF TTP-C2NF Communication Controller Data Sheet*", Rev.1.6, July 2006
[63] SAE, "*ARP-4761: Aerospace Recommended Practice: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*", 12 th edition, 1996.
[64] Still. R, Crolla. A, "*SHAP Fault Tree Review*", QINETIQ/D&TS/LAND/RA0610916, 2006.
[65] Ward. D, "*MISRA Standards for Automotive Software*", URL: http://www.iee.org/oncomms/pn/auto/Auto%20S&S%202%20-%20David%20Ward.pdf#search=%22ISO%2026262%22
[66] Ward. D, "*MISRA Software Engineering Activities*", URL: http://www.jasa.or.jp/et/ET2005/conference/05PDF/search=%22ISO%2026262%22, Accessed on 29/09/2006.
[67] Kahn .P, "*Normalisation et sûreté de fonctionnement : Panorama, tendances et diversité*", URL: http://www.inrets.fr/services/manif/ForumNTIC/forum18-05-06/pdf/KAHN_Patrice.pdf#search=%22ISO%2026262%22, Accessed on 29/09/2006.
[68] UK MOD, "*HAZOP Studies on Systems Containing Programmable Electronics - Part 2*", UK Ministry of Defence, May 2000.
[69] Crolla. A, "Hazard and Risk Analysis - HAZOP on TTP/C Protocol", QINETIQ/D&TS/LAND/RA0607429, 2005.
[70] Searle A, "VIVA – A Standard for Vetronic Video Distribution using Gigabit Ethernet" , QINETIQ/EMEA/TS/SPEC0702833/1.0 , July 2007.
[71] Press S J, "Annex to Vetronics Standards & Guidelines: VSI Metrics for Electronic Architecture Assessment", QINETIQ/TS/FPPS/TR0900176.

Initial distribution list

External	
Peter King	RD(GM)
Nicky Stevens	SIT-RAO MNV SUP2
Colin Newell	DEC GM
DSTL Programme Coordination Office	
DSTL Knowledge Services	
QinetiQ	
Information Resources	
Michael Haines	
Project File	

Report documentation page

Originator's Report Number	QINETIQ/EMEA/TS/CR0702540 Issue 2		
Originator's Name and Location	R M Connor, QinetiQ, Farnborough		
Customer Contract Number and Period Covered	GM/N04058		
Customer Sponsor's Post/Name and Location	Peter King, RAO, Shrivenham		
Report Protective Marking and any other markings UNMARKED Enter protective markings in use	Date of issue October 2008	Pagination Cover + 100	No. of references Enter references
Report Title Vetronics Standards & Guidelines			
Translation / Conference details (if translation give foreign title / if part of conference then give conference particulars) Not Applicable			
Title Protective Marking	UNMARKED		
Authors	R M Connor		
Downgrading Statement	Not Applicable		
Secondary Release Limitations	None		
Announcement Limitations	Not Applicable		
Keywords / Descriptors	Enter keywords and descriptors		
Abstract Enter abstract			
Abstract Protective Marking:			

This form meets DRIC-SPEC 1000 issue 7

Blank page