NATO STANDARD

AEP-79

PLATFORM LEVEL EXTENDED VIDEO STANDARD

Edition A Version 1

FEBRUARY 2016

NORTH ATLANTIC TREATY ORGANIZATION
ALLIED ENGINEERING PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

29 February 2016

1. The enclosed Allied Engineering Publication AEP-79, Edition A, Version 1 PLATFORM LEVEL EXTENDED VIDEO STANDARD, has been approved by the nations in the NATO ARMY ARMEMENTS GROUP, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 4697.

2. AEP-79, Edition A, Version 1 is effective upon receipt

3.

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

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
ITA	- ITA ARMY: the technology linked with this STANAG will be adopted only on brand-new nationally manufactured platforms that will be procured in the future. - ITA AIR: the technology linked with this STANAG will be adopted only on brand-new nationally manufactured platforms that will be procured in the future if some physical and technological limitations of national systems will be eliminated (for example: limitation of the geographic network due to band limited signal or crypto IP capability).
NOR	Norway is using different connector (DefStan 23-09 v3) replacing the one described in Annex G of the STANAG
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

CHAPTER 1 PLEVID FRAMEWORK

1.1 PRESENTATION

The PLEVID standard is divided into 4 parts:

- 1: PLEVID framework: presents the uses cases, applicability and compatibility of the different PLEVID documents. It also gives Ethernet switch requirements and flow control recommendations:
  - Annex A contains the Terms and Definitions used in the AEP
  - Annex B contains the presentations and use cases that has lead to this standard
  - Annex C contains the applicability of the standard
  - Annex D contains the compatibility of the different requirements of this standard
  - Annex E contains the specifications of the switch to be used to build the network
  - Annex F contains the recommendations for flow control
  - Annex G contains suggestion for connectors for Gigabit Ethernet
- 2: PLEVID RTP protocol and video protocol (Def Stan 00-82 issue 2): defines an RTP based protocol and the implementation for video for military vehicles. (Def Stan 00-82 is not contained in this AEP)
- 3: PLEVID GigE Vision (Use of the GigE Vision Imagery Transport Standard in AFVs DRDC Suffield TM 2009-290) : defines how GigE Vision should be used in military vehicles:
  - Annex H contains the usage of the GigE Vision Imagery Transport Standard in AFVs
- 4: PLEVID audio protocol: defines the use of PLEVID RTP for audio and data streaming for military vehicles.
  - Annex I contains the Audio Protocol
  - Annex J contains the Audio Coding

It must be understood that, depending on which part of the standard is being considered, the standard either describes precisely how to implement the requirements (currently part 1, the PLEVID framework except flow control chapter and part 2, the PLEVID RTP protocol and video protocol Defence Standard document) or defines the requirements to build a compatible system (part 1 for chapter about flow control recommendations and part 4, the PLEVID audio protocol document). It is anticipated that some requirements in parts 1 and 4 will be expanded to include how they are implemented at a later date as the standard is developed.

1.2. AIM

The aim of this agreement is to promote the interoperability of present and future platform level digital video distribution systems. The video distribution system specified is based on Ethernet (predominately Gigabit Ethernet) as the network technology and allows, as an option, the incorporation of digital audio and data distribution on the same network.
The architecture of the system includes the provision for multiple service providers (individual video, audio and data sources) to access the network infrastructure and for multiple service users (displays, data processors and audio sinks) to receive information from the network infrastructure. The distribution of video, audio or data from one service provider to one service user (unicast) or many service users (multicast) is supported.
The standard describes the mechanisms and protocols that shall be employed to facilitate the distribution of and control of digital video, audio and data. All the protocols and mechanisms selected are open, widely used, Internet standards. This standard does not define any new protocols but provides guidance on how the selected protocols and mechanism are used. For most protocols, the actual Internet standards will need to be consulted to obtain additional detailed information to implement the protocol in an actual system. This document should therefore be used as the starting point when designing and implementing a system.

1.3. AGREEMENT

Participating nations agree to implement the standards presented herein in whole or in part within their platform level video distribution systems to achieve interoperability.

1.4 DEFINITIONS

The terms and definitions used in this document are listed in Annex A.

1.5 DETAILS OF AGREEMENT

The Platform Level Extended Video Distribution AEP defines the architectures, interfaces, communication protocols, data elements, message formats and identifies related STANAGs, which compliance with is required.

1.6 PROTECTION OF PROPRIETARY RIGHTS (SEE ARTICLE 307)

If required.

1.7 IMPLEMENTATION OF THE AGREEMENT

This AEP is implemented by a nation when it has issued instructions that all such equipment procured for its forces will be manufactured in accordance with the characteristics detailed in this agreement.

INTENTIONALLY BLANK

ANNEX A TERMS AND DEFINITIONS

A.1. Acronyms and Abbreviations

The following acronyms are used for the purpose of this agreement. Note: There will only be words associated with this AEP that are not already included in the ISRIWG Dictionary.

A

AIA	Automated Imaging Association
AFV	Armoured Fighting Vehicle
ARP	Address Resolution Protocol

B

C

COTS	Component Off The Shelf

D

DDS	Data Distribution Service
DHCP	Dynamic Host Configuration Protocol

E

EMI	Electromagnetic interference

F

FMEA	Failure Mode and Effects Analysis

G

GEV	GigE Vision
GigE	Gigabit Ethernet
GigE Vision	Video distribution over GigE standard defined by AIA

H

I

IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPD	Inter Packet Delay (time between 2 UDP packets delay)

J

K

L

M

MIB	Management Information Base
MILVA	Military Vetronics Association

N

O

OTS	Off The Shelf

P

PC	Personal Computer
PLEVID	Platform Level Extended VIDeo

Q

QoS	Quality of Service

R

RFC	Request For Comments
RTCP	Real Time Control Protocol
RFI	Radio Frequency Interference
RTP	Real-time Transport Protocol

S

SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol

T

TFTP	Trivial File Transfer Protocol,

U

UDP	User Datagram Protocol
UTC	Universal Time, Coordinated

V

VLAN	Virtual Local Area Network
VoIP	Voice over IP (Internet Protocol)

W

X

Y

Z

A.2. Terms and Definitions

The following terms and definitions are used for the purpose of this agreement.
Stream or flow (of data, audio or video): information made of a succession of packets delivered by a service provider with some periodic aspect between a join and a leave request.
"Join" and "leave" a multicast group in order to receive a flow are requests sent to the network by a service user. They are used in the IGMP context.
There are three device types introduced in PLEVID:

- Service provider: a device that is able to source a stream of information (data, audio or video).
- Service user: a device that is able to sink a stream of information (data, audio or video)
- System supervisor: a device or a set of devices that has a global knowledge of the system (architecture, capacities, flows, failures etc) and performs the relevant actions in case of failure (stop flows, etc).

Note: a switch is not considered as a service provider nor a service user.

INTENTIONALLY BLANK

ANNEX B PRESENTATION AND USE CASES

Presentation

Since the beginning of the 21st century, Military ground vehicles are integrating more and more equipments that generate or need a high volume of streamed information, mainly digital video but also digital audio and data. Those information are more and more mixed and correlated to extract the relevant items. A digital multimedia bus is a key feature to make an upgradeable and expandable architecture while limiting the number of wires and connectors.
Digital multimedia bus with multiple transmitters are in use in civil aircraft since the 1990's (AFDX/ARINC664) but the costs of AFDX switches are incompatible with military ground vehicles.
Military aircraft started to use ARINC 818 since 2007 but this is a point-to-point oriented protocol rather than a multiple transmitters / multiple receivers protocol as required for military ground vehicles.
Civil industry uses many competing standards (Powerlink, Profinet, Ethernet IP, etc) but they are automation oriented rather than video oriented except for GigE Vision, which is recommended in this standard.
It has been therefore decided to gather a relevant set of existing civil standards (rather than inventing a new one) to meet the needs of military ground vehicles from a technical and an economical point of view. Those needs are based on the use cases listed hereafter.

Use Cases

The following reference scenario has been used to guide the PLEVID definition.

B.1. INTRODUCTION

Following the main principles used to define the reference scenario and the associated vignettes:

- Background information and CONOPS have been taken from the NNEC FS (Feasibility Study) and Delphinia scenario;
- The vignettes have been defined, starting from the reference scenario, to stress the need for Local Situational Awareness at platform level. To include meaningful elements to the scenario an attack operation has been considered. Land Forces, at Task Group level, are engaged in an attack operation facing irregular forces to gain control of a small city.
- The scenario and vignettes are detailed enough to include all the relevant elements to define a use case for a PLEVID solution deployed at platform level.

B.2. SCENARIO

Following an UNSC resolution a MultiNational Brigade has been tasked to restore peace and security in the country of Neverland where a situation of failing state and conflicts between irregular militias are leading to a humanitarian crisis.
This operation falls into the CRO Category (Crisis Response Operation) and could be more precisely identified as a Peace Enforcement Operation. From a military point of view this operation is more challenging than traditional Peace Keeping operation due to the fact that military personnel must enforce peace between hostile entities in conflict, without their explicit allowance. In this operation there is also the risk of *"mission creeping"*. As a matter of fact the bordering country Betaland, lead by fundamentalists, does not recognize UNSC authority and resolutions and aims to extend its influence on Neverland.
The MultiNational Brigade Area of Operations is about 150 Km by 80 Km almost made of flat desert stretching to Betaland neighboring country's border. The area of operations includes the province capital of the region – Zetavillage – and other remote villages largely cut off from the rest of society.
The MultiNational Brigade Commander has to restore order and ultimately the rule of law in the AOR improving the genral humanitarian situation in the region. To defeat NLA and control the territory the Commander can rely on three Manoeuvre Task Forces: HOTEL, Bravo and Charlie consisting of combat (almost Mechanized Infantry), combat support and combat service support elements augmented by Tactical and Expeditionary Enablers.
The MultiNational Brigade forward staging base is located close to the small city of Nowhere (60 Kms from Zetavillage) close to the main APOD (Air Point of Disembarkation) of the region.

B.3. SITUATION

Zetavillage, is a small city in the northern region of Neverland in a strategic position close to the border with Betaland. Zetavillage is actually controlled by NLA, the city has about 10 000 inhabitants and a typical small city shape with a city centre of stone or concrete houses with a maximal height of 6-8 floors. The surrounding buildings are 3-4 floors stone or concrete houses. The suburban area is represented by residential districts and industrial estates. The city has a railway station and a small disused military airport.

Figure 1: Zetavillage - Urban environment

Regular troops of Betaland, in any moment, could join the conflict trying to legitimate and empower one of the Betaland warlord whose armed clan calls itself NLA (Neverland Liberation Army) and aims to establish a military government. Intelligence reports the risk that in case of an attack of UNSC Forces to Zetavillage Betaland may offer Fire and Air Combat support to NLA Para-military organization.
The NLA organization in Zetavillage is strong of about 500 regular partisans divided in at least five coordinated units each one with their own leader, armed with RPG, mortars, machine guns, assault rifles and explosives. Each unit is well trained and organized as a Para-military unit with their consolidated tactics, techniques and procedures developed in several years of conflicts in the area. Usually they move in small groups using off-road vehicles and Pick-Up. NLA claims support of another 500 sympathizers that can act on call or independently with little or no method, along terrorist mode of action. Probably strategic buildings and facilities of Zetavillage controlled by NLA are mined with IED (Improvised Explosive Devices).
The MultiNational Brigade Commander decides to take control and secure Zetavillage defeating NLA and discouraging Betaland possible hostile actions.

B.4. TASK FORCE HOTEL DESCRIPTION

The Task Force HOTEL is the key unit utilized for this use case. It is a grouping of manoeuvre units augmented with counter airforce units, combat engineering units (EOD/IEDD), artillery units and other support units. Task Force HOTEL is involved in a MOUT (Military Operation Urban Terrain) where Local Situational Awareness represents a key success factor to improve Force effectiveness and survivability of the units deployed on the ground.

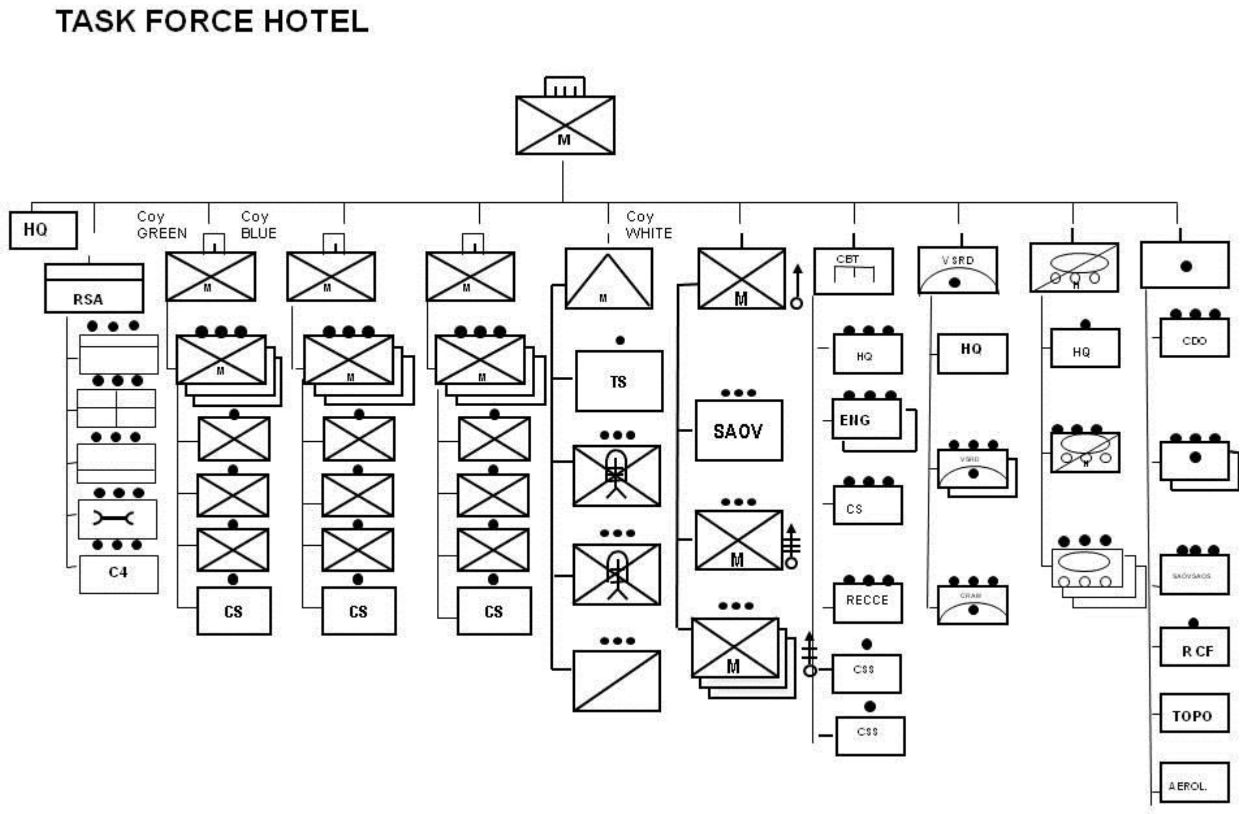

Figure 2: T.F. HOTEL – Task Force Organization

As shown by the previous ORBAT the Task Force HOTEL is made of the following operational nodes:

- Task Force Command Post (Fixed and Tactical);
- Mechanized Infantry Company (3 Companies);
- Mortar Company
- Counter-Tank Company
- Armoured Cavalry Squadron
- Combat Engineering Company
- Artillery Battery
- Air Defence Battery (V-SHORAD)

B.5. TASK FORCE MISSION

Strike and defeat NLA Para-military units in Zetavillage to show the MultiNational Brigade capability to prevail on enemy guerrilla forces thus improving the perception of force effectiveness by the local population.
The Task Force HOTEL Commander has planned to attack decisively the NLA formations in Zetavillage using all the units he can rely on with the exception of the Artillery Battery, the Air Defence Battery (V-SHORAD) and one of the three Mechanized Infantry Companies that will remain in the forward staging base to protect it.
Before mission execution RECCE and patrolling activities will be intensified in different sectors of Task Force HOTEL Area of Responsibility (40 Km by 40 Km) also to "conceal" the incoming attack to Zetavillage.

B.6. TASK FORCE DUTIES

The main duties assigned to the Task Force HOTEL in its Area of responsibility are mainly related to the control of the territory and in particular are:

- standing patrols and checkpoints;
- public order and safety, facing civil disorders and insurgencies;
- border surveillance and control/show the flag activities;
- armed escorts to humanitarian convoys;
- refugee camps protection;
- Intelligence, surveillance and recon activities;
- Combat search and rescue;
- combat (attack/defence) activities even in urban terrain.

In particular for the vignette realized for this use case the attack in the urban area is considered the key part of mission execution. The attack will be executed by the Task Force HOTEL respecting the Rule of Engagement define to safeguard Zetavillage facilities and local population thus reducing as much as possible casualties and fratricide fire. Of course Local Situational Awareness together with Situational Awareness, Combat Identification and effective communications will be a key success factor for the mission.
The attack to Zetavillage will be splitted into several phases:

- attack preparation;
- land tactical RECCE (MILITARY SCOUTING);
- Zetavillage surrounding;
- Control of key waypoints in and out Zetavillage;
- Attack to Zetavillage;
- Securing and clearing Zetavillage from NLA units;
- Humanitarian aid;

- Place some Task Force HOTEL units to guard and protect Zetavillage;
- Return to the forward staging base of Task Force HOTEL exceeding units.

B.7. TASK FORCE HOTEL DEPLOYMENT

To attack Zetavillage the Task Force HOTEL Commander will use the following units:

- An **Armoured Cavalry Squadron** will explore (RECCE by Combat) the area of the land attack and then will move on a rear line ready for intervention.
- A **Mechanized Infantry Company GREEN** during sunrise will start surrounding the north sector of Zetavillage followed by the **Artillery Battery**.
- A **Counter-Tank Company WHITE** during sunrise will start surrounding the south sector of Zetavillage followed by the **Mortar Company**
- A second **Mechanized Infantry Company BLUE** will move after completion of Zetavillage surrounding to execute frontal attack.
- Thr **Combat Engineering Company** will be responsible of mine clearance.
- The **Task Force Command Post** (Tactical Mobile) will follow the deployed forces (midlle of the battle line) behind the **Infantry Company BLUE** and close to the **Armoured Cavalry Squadron** rendezvous point;
- The **Air Defence Battery** (V-SHORAD) and the third Mechanized **Infantry Company RED** will grant the Task Force HOTEL forward staging base (CONDOR) defence.

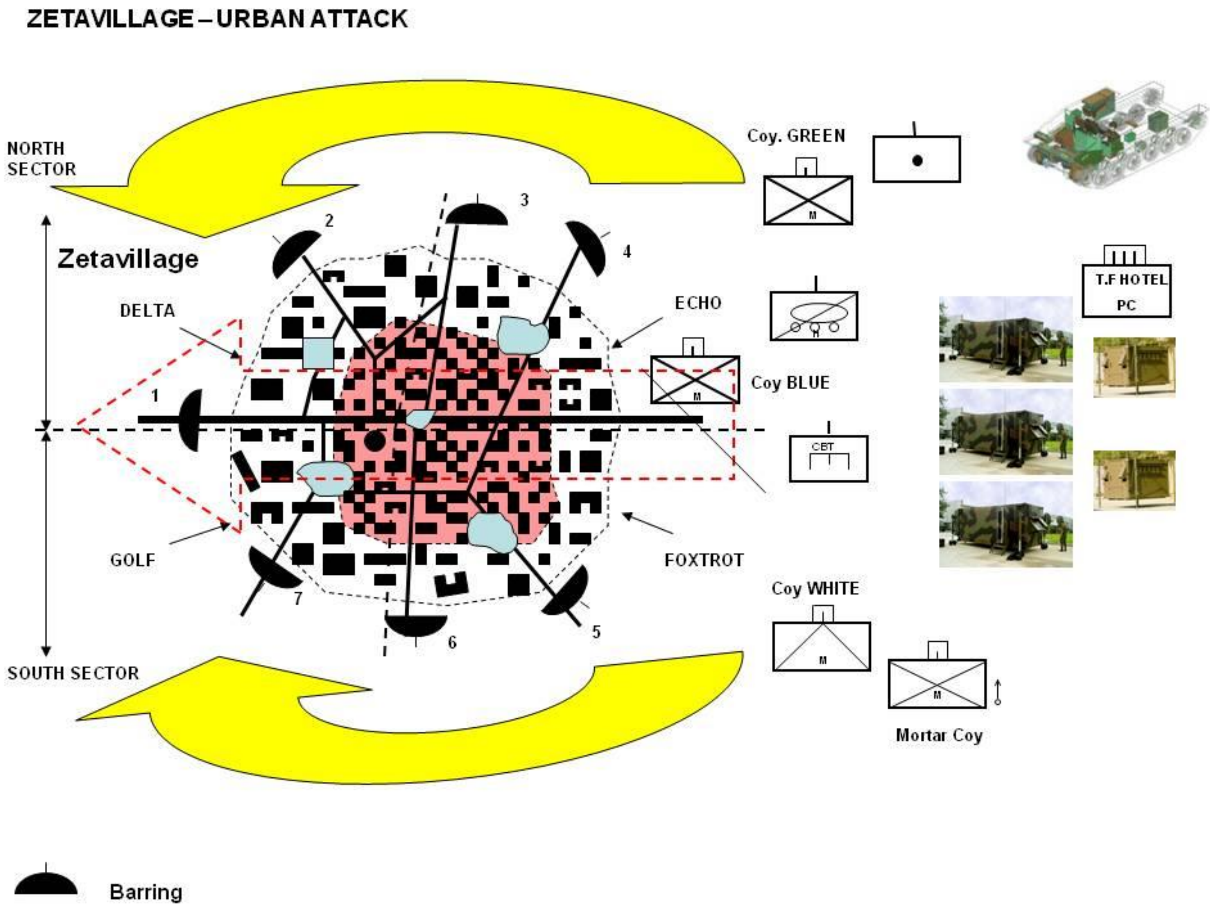

Figure 3: Task Force HOTEL Deployment

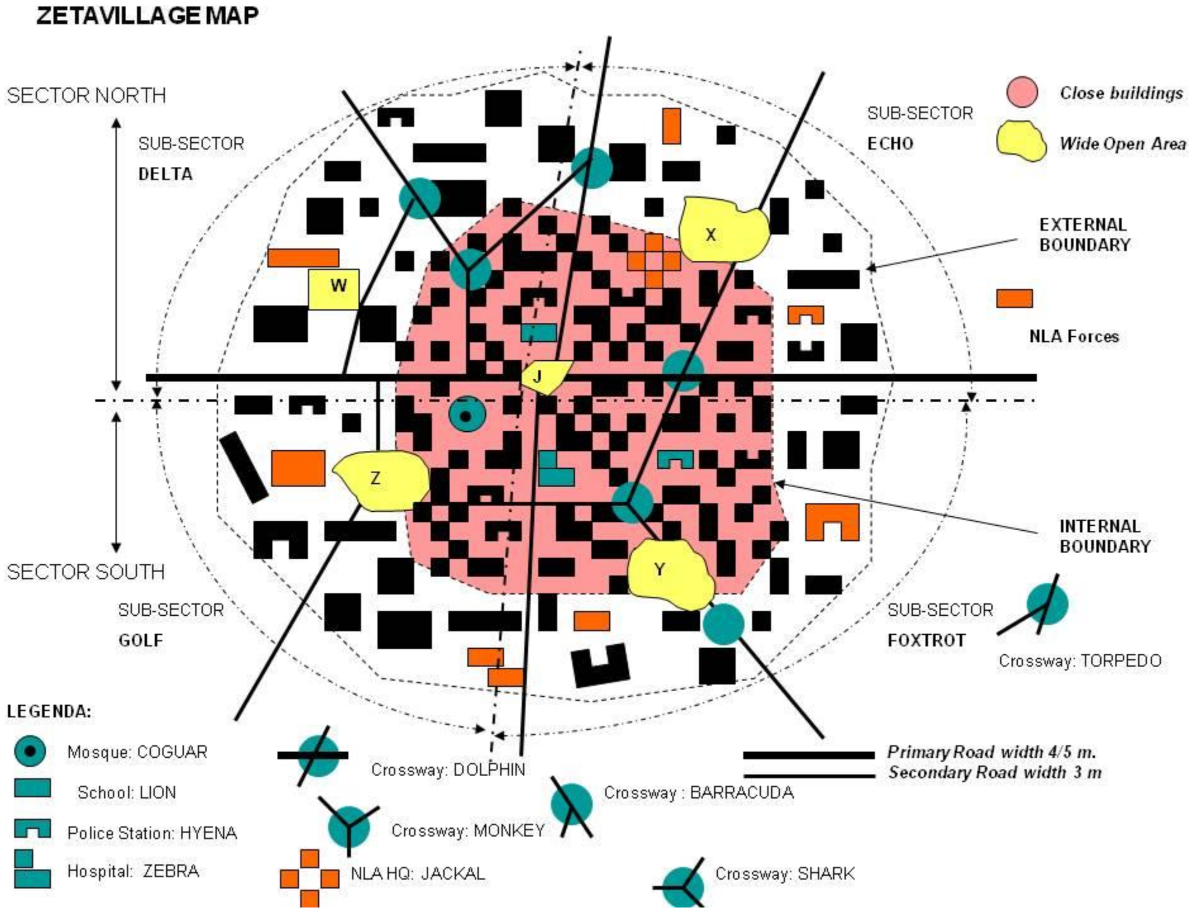

Figure 4: Zetavillage map

B.8. MECHANIZED INFANTRY COMPANY BLUE FRONTAL ATTACK

BLUE Company progresses towards Zetavillage centre. Three Platoons, each made of three Armoured Infantry Fighting Vehicle and a maneuver support squad proceed towards the NLA Facilities traversing parallel ways (some of them are typical “urban canyons”).
BLUE Company Commander inside his Armoured Infantry Fighting Vehicle receives video streaming on multiple displays from Local Situational Awareness Sensors and from a Maneuver Range UAV with an EO/IR Sensor payload.
Each AIFV can rely on LSAS Sensors with panoramic and night vision capability. The real time video from LSAS sensors is available to the AIFV crew members (Gunner and the AIFV Cdr) and can be exploited selectively for generic observation of surroundings, threat assessment, aiming/targeting and any other operational activity that requires the video from the LSAS sensors.

Crew members are well trained to exploit video information and are assisted in real time by image enhancement and analysis to improve their perception of the “outside” while being inside the AIFV.
A large party of NLA forces are located in nearby building supposed to be the NLA HQ. Isolated groups of combatants with RPGs are discovered and engaged as well in close proximity of this building.
The NLA HQ is located into three large buildings, 6-8 floors high, built of bricks, nearly 50m long. The inner walls are made of either plaster or bricks. Outside these buildings is the railway station with two communicating entrances. From the railway station NLA combatants can move, hide, get reinforcements or escape sub-surface (sewage system).
The BLUE Company Commander gives orders to engage enemy forces, secure the building and control the area to make sure to defeat all combatants contained inside and outside the building.
Getting closer to the NLA HQ, going through the main street, one of the three Platoons – NEPTUNE – is engaged simultaneously by snipers located in different surrounding buildings (4-6 floors) and combatants on the ground armed with RPGs. The NLA defensive attack during sunrise (low visibility) requires rapid reaction with the four AIFs of NEPTUNE Platoon to be able to identify and neutralize NLA forces avoiding fratricide fire and casualties among the civilian population.

<u>Top level requirements</u>
The previous use cases are here translated into top-level requirements.

<u>Power-up</u>
System power-up shall be less than 15s.

<u>Video distribution</u>
Any video shall be simultaneously accessible by any member of the crew or any processing device.
Any member of the crew or any processing device shall be able to access simultaneously to any number of videos.

<u>Video performance</u>
The achievable video performance (bandwidth, latency, reliability) shall be compatible of any vehicle usage (processing, observation, driving, aiming).
Note : the standard does not required to have the best video performance for any usage but the standard allows this.

<u>Audio performance</u>
The audio performance (bandwidth, latency, reliability) shall be compatible of any vehicle usage (conferencing, etc).

<u>Multimedia capability</u>

Data and audio shall be transmittable along with video.

Enhanceability
A system must be enhanced (adding new service providers and users, applications, etc) with a minimal reengineering effort.

Plugability
A device that generates video/audio/data should be easily transferable from a vehicle to another in order to allow quick fixes as close as possible to the battlefield (i.e. without reengineering and reconfiguration).

All those top-level requirements have been translated into requirements that are available in the different PLEVID sections.

ANNEX C APPLICABILITY

This standard defines a network and protocols capable of transporting data, audio and video streams over Ethernet (mainly Gigabit Ethernet) physical media. While this specification allows all three types of data streams, it is not mandatory that all streams are implemented. The applicability of implementing each of the data stream types is dependent on a number of technical and system design choices.

Video

This standard shall be applied when the physical media is digital.
This standard specifies that one or both of the following video protocols shall be used:

- the "RTP based" protocol, which uses RTP, SAP/SDP and SNMP, as defined in part 2 of PLEVID
- the "GigE Vision based" protocol: AIA GigE Vision specification (Camera Interface Standard for Machine Vision) as defined in part 3 of PLEVID

Service providers and service users may implement only one of those two protocols or both.

Data

This standard may be applied when all the following conditions are true:

a. There's a need to transfer data on the same network as video.
b. The data transfer is streamed (as opposed to a one shot file transfer).
c. The transferred data have a level of safety compatible with the level of safety of the implemented PLEVID bus (otherwise other technology choices should be considered).

Audio

This standard shall be applied when all the following conditions are true:

a. The physical media is Ethernet.
b. The audio transfer is streamed (as opposed to a one shot file transfer).
c. There's no existing audio or intercom standard already implemented within the customer vehicle fleet.

ANNEX D COMPATIBILITY OF THE DIFFERENT REQUIREMENTS

Data, audio and "RTP based" video protocols share the same RTP - SAP/SDP - SNMP protocol.
GigE vision uses a different protocol but PLEVID is written so that any combination of data, audio, and video streams - RTP based or GigE Vision based streams - may be implemented on the same PLEVID bus. This chapter explains how this has been made possible in the 3 following points.

Point 1:

Both "GigE Vision based" and "RTP based" protocols:

- are built on top of IPv4 protocol,
- support multicast through IGMPv2,
- don't manage multicast address assignment (but rather leave it system dependent).
- may share the same IP address configuration protocol as follows:

Protocol	RTP based	GigE Vision for PLEVID	Original AIA GigE Vision 2.0 (reminder)
Persistent (static)	Mandatory Modifiable	Mandatory Modifiable	Optional Use ARP / Disableable
ARP	Mandatory	Mandatory	Recommended if persistent IP supported
BOOTP RARP	Unused	Unused	Authorized
DHCP	Forbidden	Forbidden	Mandatory Disableable
LLA	Forbidden	Forbidden	Mandatory Always enabled

Point 2:

The Ethernet switch requirements are compatible with all protocols (see switch specification in this document).

Note: GigE Vision mandates only IGMP: jumbo frames is left as a quality of implementation. However, high performance devices typically support it. A GEV device can reports its capabilities via bootstrap registers.

Point 3:

Each of the 3 features of flow control may be implemented for both video protocols:

- Bandwidth control: this feature may be implemented - regardless of the service provider - on the switch and service user side *.

- Traffic shaping:
  - GigE Vision requires that this feature shall be implemented on service providers (service users may use this feature or not).
  - The RTP based protocol recommends that this feature should be implemented on service providers (service users may use this feature or not).

- Prioritization: this feature shall be implemented in the switch (service providers and users may use this feature or not).

* Note: RTP based protocol devices may implement bandwidth control on the service provider side as opposed to GigE Vision providers.

ANNEX E SWITCH SPECIFICATIONS

E.1. General

The following requirements shall apply to all switches or routers employed within the system.

Note: some of this requirements are necessary only if some optional part of PLEVID are implemented (for example flow control); nevertheless, a network shall use only use switches that implement all of the following requirements in order to guarantee a reduced cost when upgrading the system.

E.2. Port Requirements

A switch shall implement 10/100/1000 Mbps auto sensing on all ports.

A switch shall implement MDI/MDI-X crossover detection on all ports.

A switch shall implement the Virtual Local Area Network (VLAN) schemes specified in IEEE 802.1Q.

E.3. Packet size

A switch shall be able to support Jumbo frames.

E.4. Latency

A switch shall forward packets with a maximum latency of 10 microseconds measured from the end of the reception of the incoming packet to the beginning of retransmission assuming there is no queue in the output buffers.

A switch shall not limit or slow the traffic due to their switching capacity.

E.5. Bandwidth Control

A switch shall be able to open and close any switch port in response to an SNMP request.

A switch shall be able to measure the traffic received on a particular port and compare it to a maximum bandwidth value received from the network.

A switch shall be able to issue an SNMP "trap" message when the traffic on a particular port exceeds a given maximum bandwidth value as set by an SNMP message.

A switch shall be able to limit ingoing and/or outgoing traffic when the traffic on a particular port exceeds a given maximum bandwidth value as set by an SNMP message.

Note: RMON is currently under investigation as a candidate for bandwidth control protocol

E. 6. Priority

A switch shall implement the three-bit user priority scheme specified in IEEE 802.1Q or the IP layer DiffServ priority scheme

A switch shall be able to manage the priority of packets using the 3 bit priority field included in the Tag Control Information defined by the VLAN IEEE standard.

A switch shall be able to configure packet priorities on a port-by-port basis.

A switch shall be capable of managing at least 3 outbound priority queues per port.

Note : Although the VLAN standard (IEEE 802.1Q) allows 8 priority levels, most switches usually map packets to only 5 or even 3 queues, which is likely to be enough for Vetronics application.

E.7. Multicast

A switch shall implement IP multicasting as defined in the Internet Group Management Protocol (IGMP) standard, RFC 2236.

A switch shall be capable of acting as an IGMP V2 querier on winning the querier election.

A switch should provide a mechanism to accomplish IGMP V2 election within 5 seconds after the end of power up sequence[1].

---

[1] systems that requires faster power-up might imply to leave switches always powered

A switch shall stop sending multicast traffic to a multicast group immediately after the final member of that multicast group leaves.

A switch shall implement "fast leave" also called "immediate leave".

E.8. Power up time

All switches should be operational within 10 seconds after power up[2].

E.9 Time synchronisation

Note : GigE Vision 2.0 mandates IEEE 1588 for fine time synchronisation. However, this document does not put neither IEEE 1588 nor any other time synchronisation requirements on switch for the following reasons:

- with IEEE 1588, a system using non IEEE 1588 switches can all the same achieved a fairly good time synchronisation, sufficient for most applications
- some Ethernet systems prefer SAE AS6802 standard for time synchronisation
- care must be taken while using some TDMA switches as they may degrade IEEE 1588 precision

[2] systems that requires faster power-up might imply to leave switches always powered

ANNEX F RECOMMANDATIONS FOR FLOW CONTROL

F.1. General

This document defines how flow control should be performed if required on the video, data or audio flows specified by PLEVID.

Flow control is divided into 3 distinct features:

- bandwidth control
- traffic shaping
- prioritization

Bandwidth control is necessary to ensure that no data delayed or lost because of the over usage of any link in the network due to a incorrect configuration or failure (babbling idiot). Typically sending two streams of 0.8Gbit/s on a 1Gbit/s link will result in a few ms in extra delay and - within a few 1/10th of seconds - in packets being dropped by switches. Bandwidth control is a coarse control: the typical time scale is 1 second.

Traffic shaping may be necessary for 2 reasons:

- a service user cannot process a stream at the service provider full speed
- a very precise timing is required at the service user side and several flows are competing (ie sharing the same bandwidth) on part of the network and as consequence one flow may periodically delay another for several ms.

Traffic shaping is a fine control: the typical time scale is 1ms.

Prioritization serves 2 purposes

- send messages quickly to equipments even when the network is congested due to a babbling idiot;
- achieve latency of less than 1 ms for urgent messages even if the network is heavily loaded with jumbo frames e.g. to ensure control messages have low latency even when the link is being used for streaming data.

F.2. CAVEAT

Flow control for PLEVID IS NOT a way to cope with undersized network. This means that the bandwidth on any link must be sufficiently large so that whatever the flows in a nominal case (ie no faulty behaviour), all the bits of a given flows sent in a given relevant period (ie any video frame period for a video flow) should reach all the destinations within this period.

F.3. Objective

The objective is to define a scheme that is:

- based on open standards;
- simple to implement;
- divided in items (requirements and recommendations) that are individually implementable;
- compatible with the service providers, service users and switches specified by PLEVID in the other PLEVID documents

F.4. Background

The background is defined by the PLEVID Framework document.

F.5. Applicability

Almost all items are optional (ie recommendations hence the usage of "SHOULD" or "MAY") except for a few one (ie requirements hence the usage of "SHALL").

F.6. FMEA

[PLEVID_FMEA]
An FMEA SHALL be performed on a system using PLEVID to define what are the recommendations stated hereafter that SHALL be implemented.

The choice of the recommendation can be specific for each stream and for each usage of each stream.

F.7. Bandwidth Control

F.7.1. General Requirements

[BW-BROADCAST]
Service user and service providers SHOULD not use broadcast.

NB. Broadcast may be limited to a very small percentage of the bandwidth based on a system analysis

[BW-UNREQ]
Service providers SHALL not send unrequested broadcasts or unicast messages above the following limits:

- 0.1% of the bandwidth
- 1 message every second

[BW-JL]
If [BW-NW-AVAIL], [BW-SW-TRAP] or [BW-SW-LIMIT] is implemented then a service user SHOULD inform the system supervisor before joining and after leaving stream.

[BW-COMPUTE]
Service providers and users SHOULD compute the maximum bandwidth of a stream by using one of the following method:

- system pre-shared information,
- computation based on the parameters of the flow (simple example for a video : resolution x bytes per pixel x frame rate x compression ratio).

N.B.: parameters of a flow can be taken from the provider SAP/SDP messages, from the provider MIB or from the GigE Vision protocol according to the provider capacities.

F.7.2. Bandwidth availability check

[BW-NW-AVAIL]
A service user SHOULD check the bandwidth availability over the network before requesting a stream.

N.B.: this requires information provided by [BW-JL].

N.B.: check if [BW-TERM-AVAIL] may be used instead of this requirement since [BW-NW-AVAIL] implementation may be difficult.

[BW-TERM-AVAIL]
A service user SHOULD check the bandwidth availability on its terminal link before questing a stream.

N.B.: this solution could be acceptable alone without [BW-NW-AVAIL] whenever the network includes only one switch or the links between the switches cannot be overloaded (even in case of babbling idiot) except on the terminal link

N.B.: [BW-TERM-AVAIL] is included in [BW-NW-AVAIL].

F.7.3. Switch configuration

[BW-SW-TRAP]
The system supervisor SHOULD configure the switches to send a message whenever a switch input or output exceeds the maximum expected traffic.

N.B.: this requires [BW-JL]

[BW-SW-LIMIT]
The system supervisor MAY configure the switches to limit the traffic whenever a switch input or output exceeds its maximum expected bandwidth.

N.B.: this requires implementation of [BW-JL]

N.B.: to be used with caution since this limitation can cause dropping of packets from a non-faulty device

[BW-SW-CFG-RELAXED]
The system supervisor SHOULD configure the switches at system start-up.

[BW-SW-CFG-STRICT]
The system supervisor MAY configure the switches before each join request and after each leave request.

N.B.: since this requirement may be difficult to implement, check if [BW-SW-CFG-RELAXED] is sufficient to satisfy [PLEVID_FMEA].

F.7.4. Bandwidth usage check

F.7.4.1 Provider check

Note: since the following provider check requirements are usually not implemented in GigE Vision devices, it may be better to implement only "user check" recommendations to satisfy the results of [PLEVID_FMEA].

[BW-PROV-CHK]

All service providers SHOULD implement mechanisms to ensure that they do not exceed their maximum bandwidth by checking their current bandwidth.
N.B.: check period is defined on a system-defined basis (typically around 1s)
N.B.: this requirement is implemented in a different way in GigE Vision V1.0 devices
N.B.: useful only if [BW-PROV-ALERT] or [BW-PROV-CLOSE] is implemented

[BW-PROV-ALERT]
When a service provider detects that he has exceeded its maximum bandwidth for one of its services it SHOULD inform the system supervisor.
N.B.: this requirement is usually not implemented in GigE Vision V1.0 devices
N.B.: requires [BW-PROV-CHK]

[BW-PROV-CLOSE]
When a service provider detects that he has exceeded its maximum bandwidth for one of its services, it SHOULD take the appropriate action(s) among the following ones:

- stop / restart the service
- reset the service provider and restart the relevant services

N.B.: this requirement is not implemented in GigE Vision V1.0 devices
N.B.: requires [BW-PROV-CHK]
N.B.: this recommendation may be redundant with [BW-SUP-CLOSE]

F.7.4.2 User check

[BW-USER-CHK]
Any service user receiving a stream SHOULD check that this flow does not exceed its maximum allocated bandwidth.
N.B.: check period is defined on a system-defined basis (typically around 1s)

[BW-USER-ALERT]
A service user that detects that a stream has exceeded a maximum bandwidth SHOULD inform the system supervisor.

F.7.4.3 System supervisor action

[BW-SUP-CLOSE]
When the system supervisor receives the information that a stream delivered by a service provider has exceeded its maximum, it SHOULD take the appropriate action(s) among the following ones:

- stop / restart the service
- reset the service provider and restart the relevant services
- configure the switch to prevent the service user to access the network

N.B.: maximum time to perform the appropriate action is system dependent and is typically 1s.

N.B.: this recommendation may be redundant with [BW-PROV-CLOSE].

F.7.5. MIB

[BW-MIB-REC]
Any service user or provider that sends a bandwidth related information should record it in its MIB.

N.B.: MIB objects TBD

[BW-MIB-START-STOP]
Any service provider SHOULD provide in its MIB for each of its service an object whose value can be changed with an SNMP SET command to start or stop the relevant service.

N.B.: MIB objects TBD

F.8. Traffic shaping

A simple but effective method to overcome potential problems with non-uniformly distributed or bursty network traffic is to have a programmable Inter Packet Delay (IPD) for each streamed packet.

A service user may request a service provider to use a specified IPD. Multiple service users using the same service provider may exchange information to determine an optimum IPD, although the mechanism to do this is outside the scope of this standard.

[TF-IPD]
Each video service provider SHOULD implement a programmable IPD for each of its services.

The IPD SHALL be measured from the end of a packet to the beginning of the next packet of the same stream.

Note:

- for RTP like service providers, this requirement is included in the PLEVID document 2
- for GigE Vision service providers, this requirement is included in the PLEVID document 3

Note: IPD is irrelevant for audio since IPD is implicitly defined by codec at a higher level.
Note: IPD is irrelevant for data since IPD is implicitly defined by service provider capability at a higher level.

F.9. Priorization

[PR-SYS-SET]
Messages related to:

- system supervision and system configuration,
- service provider configuration (start/stop/reset, etc),
- join and leave requests,

SHOULD be given a higher priority respect to streams.

N.B.: the methods used to prioritize the messages are system dependent (see PLEVID Framework)

F.10. Protocols

[BW-PROT]
SNMP SHALL be exclusively used for all messages related to bandwidth control:

- Configurations and settings: SNMP SET messages
- Information messages: SNMP TRAP messages.

Note: RTCP does not provide any convenient protocol since it can only reply to sender
N.B.: SNMP characteristics are given by the PLEVID part 2.
N.B.: SNMP message for switch are not standardized and adding requirements to attempt to standardize the switches for PLEVID would prevent the usage of COTS

Note: RMON is currently under investigation as a candidate for bandwidth control protocol

[TS-PROT]
The protocol that SHALL be used to configure IPD are:

- for GigE Vision devices : GigE Vision protocol,
- for RTP/MIB devices : MIB settings with SNMP,

ANNEX G SUGGESTED CONNECTORS FOR GIGABIT ETHERNET

This list suggested connectors for Gigabit Ethernet is not part of the standard but only a short list of commonly used connectors by some MILVA members.

Copper connectors

Prototyping

RJ Field type:
Pro:

- compatible with RJ45,
- cheap

Con:

- big footprint,
- no housing compatibility between vendors yet

Mass production

High speed Quadrax :

- quadrax = 4 inner contacts (grounded), 100 Ohms, gauge 8
- 2 quadrax required for one Gigabit Ethernet link
- MIL-DTL 38999 series III housing can contain from 1 to 8 quadrax

Pro :

- used for ARINC 404 and 600,
- small footprint,
- available from more than 6 vendors

Con :

- expensive,
- requires some manufacturing skills,
- no housing compatibility between vendors yet

Optic connectors

MIL-PRF-29504/5D specifies termini but may be not suitable for embedded use (vibration problems).
In field easily cleanable termini may be suitable for embedded use.

ANNEX H Use of the GigE Vision Imagery Transport Standard in AFVs

H.1 Background

H.1.1 Digital Video Standardization

Modern Armoured Fighting Vehicles (AFVs) are increasingly reliant on electronic imagers for observation, targeting and situational awareness. Modern electronic imagers exceed the capability of legacy analogue video transport mechanisms both in spatial resolution (the number of picture elements – pixels – in an image frame) and in dynamic range (the number of brightness or colour values associated with a pixel). Further, both modern imagers and modern multi-function displays are inherently digital devices and maintaining a digital signal path between them preserves image fidelity. While the use of any digital video transport mechanism can preserve image quality, there are additional requirements that motivate the selection of particular transport mechanisms and that further motivate the selection of a common video transport mechanism for all AFV applications. These requirements flow from operational requirements within the vehicles and from the goal of maximizing operational capability while minimizing acquisition and life cycle costs.

Increased operational capability requires that all image sources within the vehicle can be viewed from any crew position within the vehicle so that information can be shared. This provides greater flexibility in managing workload and supports redundant modes of operation. The ability to insert additional sensors over a vehicle lifetime, either through pre-planned upgrades or to exploit new sensor capabilities is also a requirement. Growth potential within the video installation to incorporate image processing for image enhancement or for automation of target detection and recognition is highly desirable. Avoiding excessive weight in cabling is also very desirable for AFV installations, as is tolerance for high levels of radio frequency interference (RFI).

Reducing acquisition and support costs motivates the use of a commercial video transport standard that will allow the exploitation of commercial-off-the-shelf (COTS) technology, design expertise and support tools. The standard should also minimize the software development effort to integrate new sensors or to upgrade existing sensors or display stations. Plug and play capabilities, where the sensor embeds sufficient information to allow the video network and the display to self-configure after installation of a new, or upgraded, sensor is highly desirable.

Adoption of a common video transport standard allows ready use of common imaging systems on a fleet-wide basis, reducing inventory and sparing costs. Common imaging systems, coupled with plug and play capabilities would allow a broader range of field repair options to maintain essential imaging systems or to improve vehicle availability through cannibalization.

After a review of alternative video transport mechanisms it is recommended that Gigabit Ethernet (IEEE standard – 802.3) be used as a transport medium. This is a broadly available commercial standard that has already seen limited use in military applications. It has growth potential to higher speeds (10 gigabit at a minimum) and both copper and fibre implementations are readily available. Ethernet switches are available that allow mixing both fibre and copper segments, allowing selective use of fibre connections to imagers where either electro-magnetic interference (EMI) or radio frequency interference (RFI) is an especial issue. Other transport options such as FireWire® (IEEE 1394, various versions), Universal Serial Bus (USB V2.0 or V3.0), or Camera Link can support digital video transport, but none of these have the flexibility and intensive commercial support that Gigabit Ethernet provides.

Standardization of both the medium and the protocol is required to allow any level of interoperability. It is further recommended that the GigE Vision® (GEV version 1.1[3] or later) protocol be used. While other video transport protocols are available for Ethernet, the GigE Vision® standard was developed by the Automated Imaging Association (AIA) for industrial machine vision applications. This industry has experience with supporting industrial automation systems, which have important similarities to military applications, including: designs with uncompromising performance standards, small installation volumes and long support cycles. As a result it is expected that military vendors will be able to better leverage industrial expertise in respect to this standard.

H.1.2 GigE Vision® Protocol

The GigE Vision® protocol was defined by a committee within the Automated Imaging Association to provide a standard supporting the use of low cost Gigabit Ethernet links between machine vision cameras and applications. It has seen broad use in this context, where a single, or small number of cameras, are connected to a machine vision processing applications by what are essentially, point to point links. Less commonly, a number of cameras are installed in a switched network where data is routed to a number of data users (displays or image processing applications). This is less common, as the bandwidth requirement for a single camera can readily approach the one gigabit per second limit of a single link within such a network. However, the latter configuration is much more likely to occur in a combat vehicle, where data is routed from imagers to the displays based upon the demands of the crew.

The capability to support a switched network is included in the GEV protocol, however, the specification requires limitation or clarification in a few critical instances to safely select components and implement a system that meets typical military requirements.

[3] GigE Vision® is a registered trademark of the Automated Imaging Association

This document details the limitations and extensions of the GEV protocol definition that a designer should adopt in designing a system for military vehicle applications. The GigE Vision® standard is expected to evolve over time and the reader should ensure that they understand how evolution of the standard will affect the potential to add sub-systems that are compliant with later versions of the standard.

H.2 GigE Vision® Guidance

As noted above, this document is intended to further define how to use the GigE Vision® standard in the context of a multi-source[4] (imager), multi-sink (typically a display), switched network employed in a mobile platform. Much of the guidance is straightforward and would be obvious to any reader of the standard, however, this document attempts to illuminate all areas of the standard which define behaviour (either by default, or as an option) that could compromise performance in and AFV.
Where the word *must* appears this implies that the implementation needs to incorporate this capability to prevent undesirable behaviour. The word *should* is used to indicate a desirable feature of an implementation that will reduce the potential undesirable behaviour.

H.2.1 GEV Version

The version of the standard referenced in the compilation of this document is 2.0.

H.2.2 Module Addressing

GEV devices selected for implementation *shall* support persistent internet protocol (IP) addresses. This mechanism will allow for rapid start up and is consistent with the fixed configuration that would be typical of an AFV variant.

GEV devices *shall* support address resolution protocol (ARP) check for address conflict. This will prevent a replacement module from disrupting operation of a working system.

The network *shall* neither use nor support DHCP and LLA .

H.2.3 Device Enumeration

[4] Note: an image processing application that enhances or compresses imagery, may be both a sink (from a camera) and a source (to a display)

System *should* implement device enumeration as part of power up built in test (BIT). This ensures that the system configuration is consistent with the expected configuration.

Devices *should* support the user defined name option. This allows identical devices to be assigned a position identifier.

System *should* periodically attempt to enumerate any devices missing from expected configuration. This allows the system to accommodate devices that are slow to power up and devices that may be powered off for part of an operational cycle to conserve power.

H.2.4 Multicast Management

GEV devices can support multicast streams, but provides no management to: announce availability, announce changes in stream content, or manage connections. This must be addressed outside of the GEV protocol.

H.2.5 Packet Resend

GEV allows any application to request a stream packet to be resent. This could cause issues in network saturation – especially in multicast streams where a fault in a route to one application could propagate to other routes. System implementations should limit packet resend requests to a nominal level (< 1 %).

H.2.6 Device Configuration Files

Devices selected for implementation *should* provide local copies of configuration files (embedded in device). System *must* provide access to configuration files for any processor implementing a GEV application (in local file store).

H.2.7 Time Stamps

Implementers should note that GEV time stamps are designed to support inter-frame time measurements rather than assignment of absolute times to images. Where needed a “control application” can access the time stamp counter to develop a mapping between device time stamps and system time or a common time reference such as UTC[5]. It should be noted that due to the way that time stamp requests are handled a “monitoring application” can not access a coherent time stamp value.

---

[5] UTC – Coordinated Universal Time

GEV allows applications that do not have control of the device (monitoring applications) to access some data including the time stamp; however, access by a monitoring application doesn't guarantee coherent data and fragments of the time stamp can be asynchronously updated by the imager during the read.

H.2.8 Control Routing

GEV requires an active control process to be operational for any device to operate (even when streams may be multicast or directed to several destinations). The active control process will typically issue a command to every device under control within a heartbeat timeout interval to maintain control (and continue streams). While the heartbeat requirement can be disabled in the device, retention of the mechanism may simplify fault detection. A GEV implementation *should* ensure that the control process for any source provides a method for other applications to adjust device parameters when required (implementing control precedence rules where required).

H.2.9 Control Transfer

Devices selected should support secondary control channels (monitoring by non-control applications). The implemented system should provide a reversionary application to monitor state of GEV devices and provide for continuity of control if the primary control application fails. It should be noted that transfer of control can (will, by default) cause the GEV device to cease streaming video – any reversionary process will need to re-start all streams.

H.2.10 Unconditionnal Streaming and End of Streaming

The devices selected shall support unconditional streaming (Stream Channel Capability Register bit 30).
If there is a need to prevent the cease of streaming video if the control application fails or during a control tranfer, system should use unconditionnal streaming.
When using multicast, no longer wanted streams should be stopped with IGMP.

H.2.11 Compression Support in GEV versions prior to 2.0

The GEV protocol provides no "native" compression support. The implementer *should* use file transfer mode (indicating compression type in file type – e.g. x.jp2), but may use a device specific mode. Evolution of the GEV protocol is expected to provide more options for native compression in later versions – potentially through the definition of additional pixel types (in GEV version 1.1 only 36 of 4096 currently assigned), or through more complete specification of how file payload types are used to support this functionality.

H.2.12 Metadata Tagging

The GEV protocol does not provide for direct support of metadata tagging of image frames (other than the time stamp). It is possible to incorporate metadata into imagery by using a “chunk” transfer or by defining device specific transfers. For the majority of real-time data transfers envisioned for an AFV video network, metadata tagging is not relevant. It is of greater importance for data that is exported from the vehicle.

H.3 Summary

The use of the GigE Vision® standard provides a consistent protocol for integrating a wide range of sensors on combat vehicles. In conjunction with the use of Gigabit Ethernet as a transport medium, it provides a flexible and adaptable platform for all classes of vision sensors. While less well supported in the standard definition, the protocol can also be used with generic data streams from other types of sensors such as surveillance radars. Together these two standards form the key elements of a sensor architecture for combat vehicles. Only minor tailoring of how components are selected or the standard is applied is required to adapt to the vehicle environment.

Gigabit Ethernet is widely available and commercial and industrial take up is so high that one can assume support for the underlying components for an extended period. If required, EMI considerations can be fully addressed through selection of fibre implementations of the standard.

The GEV standard has also now achieved a broad level of industrial use and availability. As noted above, it is a creation of the machine vision community which has experience with uncompromising requirements and extended product support cycles. This is well aligned to typical military equipment life cycles.

Once a standardized sensor architecture is adopted the subsequent integration effort to add additional sensors is minimized. A common architecture allows sensors to be replaced with comparatively low levels of engineering effort and qualification, either to exploit higher performance or merely to cope with obsolescence of the original equipment.

ANNEX I AUDIO PROTOCOL

I.1. General

This chapter defines how audio streams should be transmitted on a PLEVID bus.

I.2. Objective

The objective is to define a scheme that is:

- based on open standards;
- simple to implement with a low latency and low CPU overhead
- divided in items (requirements and recommendations) that are individually implementable;
- compatible with the service providers, service users and switches specified by PLEVID in the other PLEVID documents

I.3. Background

The background is defined by the PLEVID Framework document.

I.4. Applicability

Reminder: audio on PLEVID is not mandatory, but if implemented, it shall be implemented as described in this document; hence the usage of "SHALL".

I.5. Presentation

PLEVID profiles for two variants of digital audio at this time; a basic Pulse Coded Modulation (PCM) code known as L16 (mandatory) and MPEG-4 Part 3 (optional), better known as Advanced Audio Coding (AAC).

For both codes, preferred frequency and the duration of the encoded audio (packet length) are given.

I.6. Requirements

[AUDIO_RTP]
When connected on a PLEVID bus for audio streaming, service providers and users SHALL use the RTP/SAP/SDP based protocol defined in the Def Stan 00-82 standard.

[AUDIO_DDS]
Service providers and users MAY use DDS (Data Distribution System) to announce their streams, publish their CODEC capabilities and negotiate CODECs.

[AUDIO_MIB]
Service users should be able to receive streams from audio providers that do not implement a MIB.

Note: even though MIB is a mandatory feature for service providers, service users should accommodate for service provider with a cheap implementation of the standard

[AUDIO_CODEC_L16_MONO]
When connected on a PLEVID bus for audio streaming, service providers and users SHALL implement the L16 audio standard, mono (no channels interleaving).

Notes:
- L16 is intended as described in [RFC3551]/[RFC4856]
- L16 is a signed a basic linear 16bits PCM coding; this allows achieving high audio quality
- with low latency without having a great impact on processing and LAN bandwidth.
- L16 is used in DVD PCM, Microsoft multimedia file formats (WAV, AVI, ASF), TIA 920 (Telecommunications Industry Association), and many others.

[AUDIO_CODEC_L16_STEREO]
When connected on a PLEVID bus for audio streaming, service providers and users MAY implement the L16 audio standard, stereo with channels interleaving.

[AUDIO_SAMPLING_8kHz]
Service provider and users SHALL implement 8 kHz sampling rate.

Notes:
- 8kHz: gives a bandwidth equivalent to analog audio systems currently used in military vehicles.

[AUDIO_SAMPLING_48kHz]
Service provider and users MAY implement 48 kHz sampling rate.

Notes:

- 48 kHz provides better quality than 8kHz
- 48 kHz allows easier voice and speech recognition
- 48 kHz is the emerging standard for consumer computers (some new audio device/driver do not support 8kHz any longer)
- 48 kHz is recommended by the AES/EBU (Audio Engineering Society / European Broadcasting Union) in the AES3 standard
- 48 kHz requires more CPU and network ressources

[AUDIO_CODEC_AAC]
When connected on a PLEVID bus for audio streaming, service providers and users MAY implement the AAC standard.

[AUDIO_CODEC_20ms]
Service provider and users MUST implement 20ms/packet.

Note: this is required by RFC3551

[AUDIO_CODEC_16ms]
Service provider and users MAY implement 16ms/packet.

Note: a power of two samples packets this is required to use some OTS low latency audio software but is not very common in communication systems (8 kHz x 16 ms = 128 = 2^7 samples)

[AUDIO_CODEC_10ms]
Service provider and users MAY implement 10ms/packet.

Note: this allows lower audio latencies and is fairly common in communication systems.

[AUDIO_CODEC_8ms]
Service provider and users MAY implement 8ms/packet.
Note: a power of two samples packets is required to use some OTS low latency audio software but is not very common in communications system (8 kHz x 8ms = 64 =2^6 samples)

[AUDIO_CODEC_10.667ms]
Service provider and users MAY implement 10.667ms/packet.

Note: a power of two samples packets is required to use some OTS low latency audio software but is not very common in communication systems (48 kHz x 10.667ms = 512 = 2^9 samples).

ANNEX J AUDIO CODING

I.1. Overview

The following sections detail SAP/SDP announcements for the PLEVID preferred formats:

- L16
- MPEG-4 Part 3

I.2. L16

L16 denotes uncompressed audio data samples, using 16-bit signed representation with 65,535 equally divided steps between minimum and maximum signal level, ranging from -32,768 to 32,767. The value is represented in two's complement notation and transmitted in network byte order (most significant byte first).

I.2.1. L16 payload header

The format of the RTP header is specified in RFC 3550, with guidance on its use provided in RFC 3551, RTP Profile for Audio and Video Conferences with Minimal Control. The Payload Type is fixed at 8 and the encoding name is defined as L16.

I.2.2. SDP announcement for L16

The format for the SDP announcements for this audio RTP profile are defined in RFC 4566 Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences. An example SDP announcement for a service provider transmitting L16 encoded audio on multicast address 239.192.1.100 is shown below. This example SDP announcement would be announced using SAP on multicast address 224.2.127.254 and UDP port 9875.

```
v=0
o=-3394362021 3394362021 IN IP4 192.168.204.100
s=Ch1
c=IN IP4 239.192.1.100/15
t=0 0
m=audio 5004 RTP/AVP 97
a=rtpmap:97 L16/8000/1
```

The audio media is transmitted using RTP with a payload assignment of 97 selected from the dynamic allocation. The “rtpmap” attribute then maps this assignment to the

L16 profile with a sampling rate of 8 kHz. The “/1” attribute specifies that no channels are interleaved (mono).

I.3. MPEG-4 Part 3

This standard may support MPEG-4 Part 3, better known as Advanced Audio Coding (AAC), and standardised in ISO/IEC 14496 3:1999. The AAC audio frames may be interleaved within the RTP packets to reduce the perception of errors due to packet loss.

I.3.1. MPEG-4 Part 2 RTP header

The format of the RTP header is specified in RFC 3550, with guidance on its use provided in RFC 3016, RTP Payload Format for MPEG-4 Audio/Visual Streams, which specifies how the streams are fragmented and mapped into RTP packets. This profile does not have a separate payload header. The section therefore just provides a guide to using the main RTP header with this video format.

I.3.2. SDP announcement for MPEG-4 Part 3

The SDP announcement for a source node transmitting MPEG-4 Part 3 64 kbps AAC LC stereo bitstreams with an audio sampling rate of 24 kHz on multicast address 239.192.3.101 is shown below. This example SDP announcement would be announced using SAP on multicast address 224.2.127.254 and UDP port 9875.

```
v=0
o=- 3394362021 3394362021 IN IP4 192.168.204.101
s=AcousticCh3
c=IN IP4 239.192.3.101/15
t=0 0
m=audio 5004 RTP/AVP 96
a=rtpmap:96 MP4A-LATM/24000
a=fmtp:96 bitrate=64000; config=9122620000
```

The audio media is transmitted using RTP with a payload assignment of 96 selected from the dynamic allocation.

AEP-79(A)(1)