DOI 10.5162/ETTC2024/A10.2

Network Management of Flight Test Installation equipment

Joaquín Antonio Pablos Palomino[1]
[1] Airbus Defence &Space , San Pablo Sur FTC, Seville, Spain,
joaquin.pablos@airbus.com

Abstract :

Monitoring the status of flight test instrumentation components and networks has been a key element to ensure flight test operations. Originally the monitoring was implemented using the remote acquisition units data format (IENA, Inet-x, ..) but new flight test devices adopted SNMP (Simple Network Management Protocol) to provide network management of ethernet equipment. As a natural evolution acquisition units have improved SNMP capabilities to be managed as standard ethernet devices. Adoption of SNMP provides new functionalities such as control, authentication functions and standardization of objects to be monitored but it requires update of flight test software tools and support of hybrid architectures.

This paper describes the evolution of monitoring capabilities of flight test instrumentation equipment and different options for management of SNMP devices in flight test. Future needs for monitoring and control of FTI equipment and SNMP contribution are also analyzed.

Key words: Flight Test Network Management, SNMP, FTI monitoring.

Introduction

System management of flight test instrumentation in IP networks has been based on monitoring data encapsulated in FTI protocols (IENA, INET-X, CH10) [16] provided by data acquisition systems. With the adoption of Ethernet new equipment such as Ethernet Network recorders, Ethernet switches, or printers appeared in FTI Ethernet data networks that needed to be managed. Commonly this equipment didn't support FTI protocols to report status and the management was initially limited, being difficult to integrate in flight test monitoring displays.

Fortunately, this new flight test instrumentation equipment supported Simple Network Management Protocol. This protocol was introduced in 1988 for supporting the management of Internet Protocol (IP) networks being widely accepted by vendors as a standard.

The support of this standard for monitoring flight test networks has become essential to anticipate to problems and provide new functionalities as configuration setting not covered by standard reporting of acquisition systems.

New scenarios of flight test networks, operating in system-of-systems environments, will make even more critical to provide monitoring of network equipment in different locations.

This paper introduces first how FTI components and networks are currently monitored, why SNMP is relevant, an introduction to SNMP framework, its evolution, and the adoption by TmNS for network management.

Secondly it provides an overview of the current support of SNMP by FTI components and the solutions to integrate SNMP onboard in Airbus DS so far.

Thirdly it describes functions provided by standard network management tools and the software solution developed by Airbus DS to cover flight test activities.

Finally, new FTI scenarios are presented to show how FTI networks will be more complex so the need of tools supporting SNMP to monitor and control the equipment and network will be even more important.

Monitoring of FTI networks

In addition of light indicators and digital outputs for signalling status, most of the remote acquisition units provide internal parameters using FTI protocols as IENA (see Fig. 1) to be easily integrable in standard monitoring displays. Some acquisition systems provide even a dedicated alarm card dedicated to this function.

The number of parameters is dependent of the manufacturer but usually parameters like the following are acquired:

- Out of range input voltage, internal temperature and voltages.
- Communications and synchronization errors.
- Built-in test results.
- Firmware version.
- Detection of connectors.
- Synchronization status.
- Loss of messages.
- General statistics.

The data parameters are configured in the same way of aircraft signals tapped, usually with a low sampling rate of 1 sample per second for most of the them.

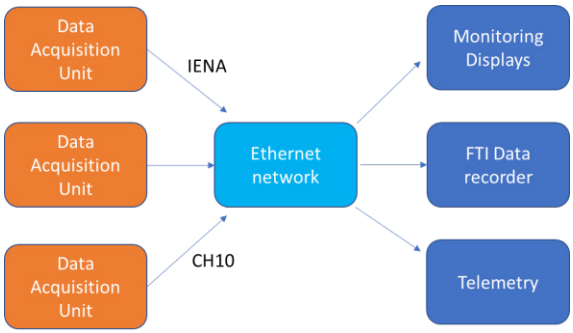

Fig. 1. DAU Internal parameters transmission in IENA / CH10 format to data processing destination.

In addition to status monitoring using FTI protocol, flight test data acquisition systems and data recorders have implemented serial and Ethernet protocols to be configured and controlled. These capabilities are vendor dependent although some of them use standards such as SNMP or IRIG 106 Chapter 6 [1].

The monitoring of other FTI devices is done connecting some of their digital / analogue outputs or serial buses to the FTI acquisition systems that provide standard data using a FTI acquisition protocol (see Fig. 2).

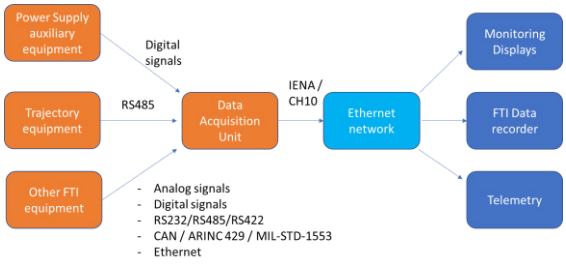

Fig. 2. FTI Status parameters acquisition using DAU.

The FTI monitoring data is processed and shown in monitoring displays dedicated to FTI status. These displays are key to:

- Validate flight test installation.
- Check that FTI is operative, and status in preflights and postflights review.
- Warn flight test engineer about any problem during flight test.

Usually, a general status display is defined for flight test engineer (see Fig. 3), and additional specific displays are defined for operation teams to analyse and detect problems during preflights and verification of installation.

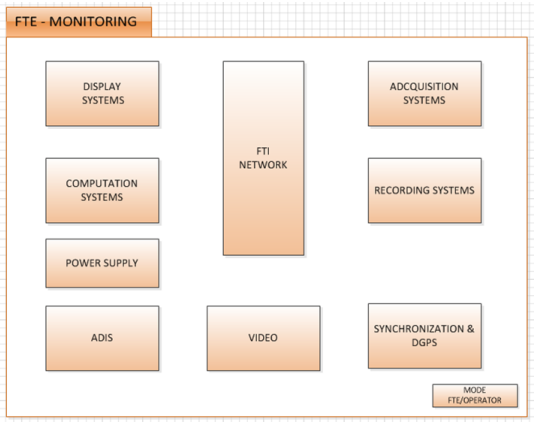

Fig. 3. Global FTI monitoring display for FTE.

If a problem has been detected only during flight, data can be analysed after flight with same tools used by analysis team to check FTI status parameters.

Although this solution has covered successfully the monitoring of data acquisition units, the use of new flight test components with ethernet connectivity but without IENA/Chapter 10 output makes necessary to implement new ways of monitoring. Fortunately, most of them provide plenty of status data using SNMP capabilities, but what are the advantages of SNMP?

Introduction to SNMP

The Simple Network Management Protocol (SNMP) is a full internet standard and was originally focused to manage nodes in the Internet community. The original standard [2] included a description of SNMP architecture and the protocol definition.

The architecture is based in a collection of components (See Fig. 4):

- Network management station, that controls and monitors all the network elements.
- Network elements that include a management agent that performs the

functions required by the network management station.

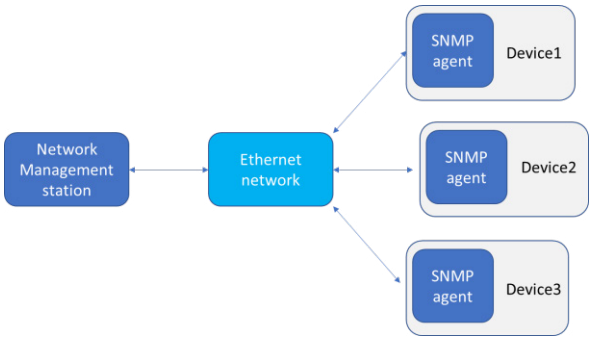

Fig. 4. Components in an SNMP system.

For representation of the management information, it was defined a sub-set of ASN.1 [3] language and created an Internet-standard Structure of Management Information (SMIv1) [4]. It included descriptions of an object information model for network management along with a set of generic types used to describe management information. For identifying objects this standard uses the concept of "OBJECT IDENTIFIER", a sequence of integers which traverse a global tree.

The root node of this tree has at least three children depending of the organization who administers it: ccitt(0), iso(1) and joint-iso-ccitt(2). The internet community has allocated the following one:

internet OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 }

Inside this tree the Internet Activities Board (IAB) has defined the following nodes (see Fig. 5):

directory OBJECT IDENTIFIER ::= { internet 1 }

mgmt OBJECT IDENTIFIER ::= { internet 2 }

experimental OBJECT IDENTIFIER ::= { internet 3 }

private OBJECT IDENTIFIER ::= { internet 4 }

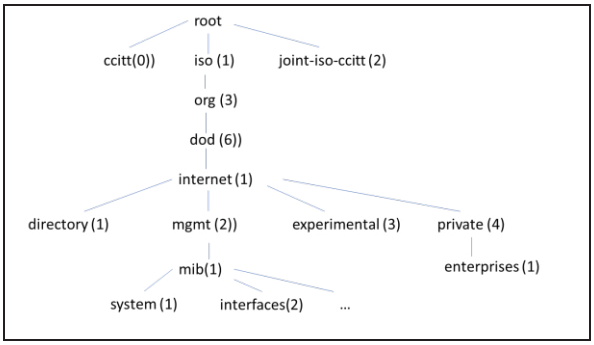

Fig. 5. OID tree.

The most important nodes are the mgmt and private ones:

- Mgmt: identify objects which are described in IAB-approved documents. The Internet Assigned Numbers Authority assigns object identifiers when a new RFC containing standard Manage Information Base is published.
- Private: is used to identify objects defined unilaterally. Initially, this subtree has at least one child:

enterprises OBJECT IDENTIFIER ::= { private 1 }

This allows to enterprises to receive a subtree where they can define new objects.

In RFC 1155[4] the following objects syntax is defined:

- Primitive types: integer, octet string, object identifier, and null.
- Aggregate types: "sequence" type allows to generate lists and tables.
- Defined types: some application-wide types are defined as NetworkAddress, IpAddress, Counter, Gauge.

The definition of an object should include: object descriptor (textual name), syntax, definition (description), access (read-only, read-write,write-only, not accessible), status (mandatory, optional, obsolete).

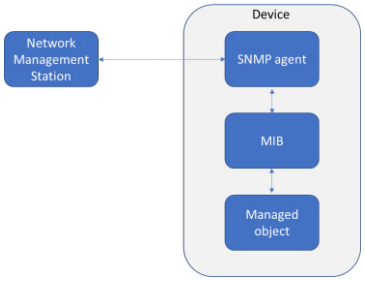

Fig. 6. Components in an SNMP device.

This allows to define MIB databases that will be accessible through SNMP (see Fig. 6), as an example the ifOperStatus of an interface is defined in MIB-II [5]:

```
ifOperStatus OBJECT-TYPE
  SYNTAX  INTEGER {
          up(1),       -- ready to pass packets
          down(2),
          testing(3)   -- in some test mode
        }
  ACCESS  read-only
  STATUS  mandatory
  DESCRIPTION
        "The current operational state of the interface.
        The testing(3) state indicates that no operational
        packets can be passed."
  ::= { ifEntry 8 }
```

SNMPv1 messages include a version identifier, an SNMP community name and a protocol data unit. The protocol entities receive messages at UDP port 161, except for those that report traps that do at port 162. The PDU originally defined were:

- GetRequest-PDU: the receiver will send a GetResponse-PDU with the name and value of the variable requested.
- GetNextRequest-PDU: the receiver will send a GetResponse-PDU with the name and value of the immediate successor of the object requested.
- GetResponse-PDU: it is generated by a protocol entity when receiving a GetRequest-PDU, GetNextRequest-PDU, or SetRequest-PDU.
- SetRequest-PDU: after receiving this message an entity will set the variables with the values sent in the message. A GetResponse-PDU of identical form and error-status field of noError will be generated.
- Trap-PDU: is generated by an SNMP entity and sent to a specific IP address (Network Manager). Includes information of the generic trap type (coldStart, warmStart, linkDown, linkUp, authenticationFailure,egpNeighborLoss , enterpriseSpecific), time stamp and variable list.

The authentication scheme to define administrative relationships is based in SNMP community. Each SNMP community is named by a string of octets, that is called the community's name for said community. This community string is sent in readable text when a query is made, being a security issue.

For any network element, a subset of objects in the MIB that pertain to that element is called a SNMP MIB view. An element of the set { READ-ONLY, READ-WRITE } is called an SNMP access mode. A pairing of a SNMP access mode with a SNMP MIB view is called an SNMP community profile. A SNMP community profile represents specified access privileges to variables in a specified MIB view. A pairing of a SNMP community with a SNMP community profile is called a SNMP access policy.

Finally in addition to object descriptions and protocol definition, a standard Management Information Base (MIB-II) [5] was defined. It contained the definition of essential elements related with the following groups: System, Interfaces, Address Translation, IP, ICMP, TCP, UDP, EGP, Transmission and SNMP. The implementation of them is mandatory for all systems and provide essential information for network management.

Internet equipment vendors adopted this standard and the deployment was fast [2]. In parallel new revisions of SNMP were published to increase security and capabilities.

SNMPv2c and SNMPv3 improvements

A second version of SNMP was defined in RFC 1901, named Community-based SNMPv2 (SNMPv2c) [6]. It defined new protocol operations described in RFC 1905 [7]:

- GetRequest, GetNextRequest, Response, SetRequest with similar function to SNMPv1.
- GetBulkRequest: request the transfer of large amount of data, improving efficiency and performance for transferring large tables.
- SNMPv2-Trap: it includes the objects sysUpTime.0 and snmpTrapOID.0 and following additional optional variable-bindings.
- InformRequest: it allows data transfer between two SNMPv2c entities acting as managers. A response-PDU is sent by the receiver so it is a confirmed event notification.

Furthermore, an updated SMIv2 (RFC 2578) was defined with expanded data types (Counter64, bit strings) and how to update MIB modules.

Although a User-based Security Model for SNMPv2 (RFC1910) was developed it was never used, so SNMPv1 and SNMPv2c standards suffered the same security problems.

SNMPv3 added security capabilities providing data integrity, source authenticity and confidentiality. This solved the main weakness of SNMPv1 and SNMPv2c.

An overview of SNMPv3 standard is described in RFC 3410 and is currently STD 62 of IETF containing RFC3411-3415 documents. This new standard supports:

- A new SNMP message format.
- Security for messages.
- Access Control.
- Remote configuration of SNMP parameters.

SNMP and telemetry standard IRIG 106

The telemetry standard IRIG 106 Chapter 21 defines an introduction to The Telemetry Network Standard (TmNS).

IRIG 106 Chapter 21 [9] mention SNMP as one of the core technologies used for system configuration and management. The system management provides a fault, accounting, performance and security configuration information on the network. Other protocols such as FTP, HTTP and ICMP are used for functions of file transfer, discovery and configuration.

The managed devices execute applications called agents that use the TmNS-defined MIB to provide their internal status and to accept controls and configuration.

The other kind of component is the TmNS Manager that manages TmNS-compliant components.

The use of SNMPv3 is recommended for secure communications within a TmNS system to provide authentication and privacy.

In IRIG 106 Chapter 22 [10] it is defined the protocol standards to be supported by TmNS manageable applications (TMA) as well as the RFCs implementation required for supporting SNMPv2c and SNMPv3.

Tab. 1: TmNS RFC requirements

SNMP	SNMPv3	SNMPv2c
RFC 3411	RFC 3410	RFC 1901
RFC 3413	RFC 3412	RFC 2578
RFC 2579	RFC 3414	RFC 3416
	RFC 3415	
	RFC 3417	
	RFC 3826	

Apart of the specific TMNS-MIB, many TMAs will also implement other public standard Internet Engineering Task Force (IETF) Request for Comments (RFC) MIBs. the TMNS-MIB only contains those concepts that are unique to TmNS components reusing MIB standards when possible.

In IRIG 106 Chapter 25 [11] it is defined the TMNS-MIB OID registered with IANA:

Telemetry Network Standard (tmns): iso.org.dod.internet.private.enterprise.31409 (1.3.6.1.4.1.31409)

Documentation for the TMNS-MIB is part of the management resource matrix [11]. All management resources that are TmNS-specific fall under the top-level hierarchy element “tmns” (see Fig. 7).

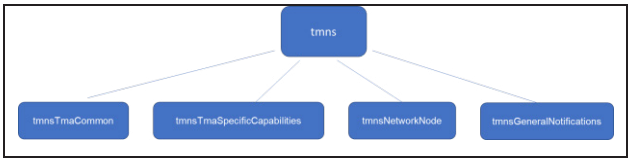

Fig. 7. TmNS tree

The tmnsTmaCommon resource is a container of management resources that shall be available on all TMAs unless otherwise noted. It contains six resource containers (see Fig. 8) referred to identification, fault, configuration, control, status and security.

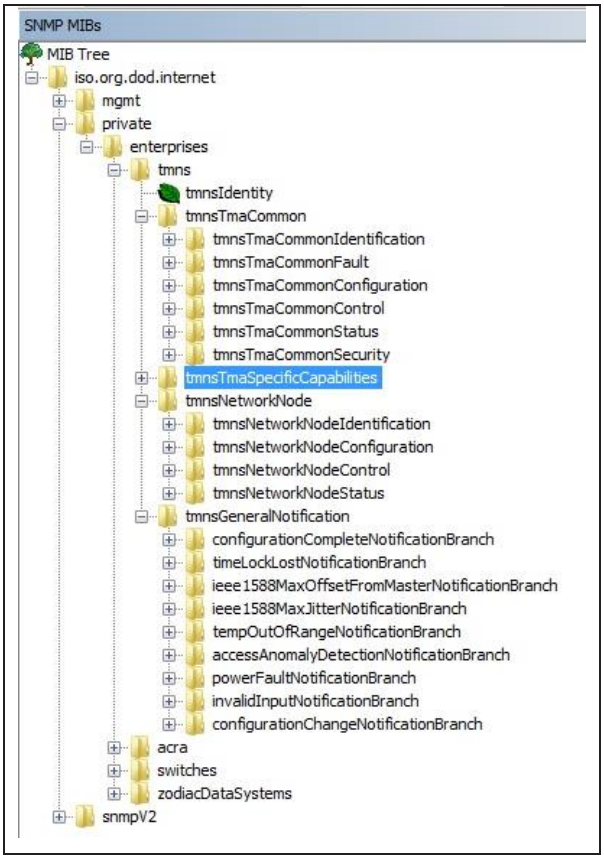

Fig. 8. TmNS MIB tree

The tmnsTmaSpecificCapabilities resource is a container of management resources for application-specific capabilities. Some examples are: tmnsNetworkFabricDevice, tmnsACU, tmnsDAU, tmnsRecorder, tmnsMasterClock, tmnsSSTTx or tmnsSSTRx.

The tmnsNetworkNode resource is a container of management resources that provide status and control capabilities that are specific to the host machine.

All TMAs shall be capable of generating event-based notifications. Management resources regarding general notifications are contained within the tmnsGeneralNotifications container

resource. This container resource contains the nine resource containers that are shown in Fig. 8.

Although this standardization work was done in IRIG 106 [17] it has not been implemented in real devices as it is described in next chapter. But it should be the starting point to be used in future standardization initiatives.

SNMP readiness of FTI equipment

Although IRIG 106 MIBs have not been implemented, there are more than 100 standard MIB modules to support network and system management published in "Internet Official Protocol Standards" list and even a greater number of MIBs defined by enterprises.

FTI equipment support both types of MIBs:

- Standard MIBs: for interfaces [5], routing, .. defined by IETF
- Enterprise MIBs: most of FTI system provides specific MIBs to define the parameters that can be monitored or controlled using SNMP.

Most of current FTI systems support only SNMPv2c standard but some of them are starting to support SNMPv3.

Manufacturers of data acquisition systems for FTI support SNMP[19] and have developed their own MIB definitions. The desired solution for final users would be to have a standardized MIB, as IRIG 106, for definition of similar equipment. If needed any manufacturer could extend this definition in the enterprise tree with additional objects. This is a common practice in other sectors that use intensively SNMP.

More even, existing standard MIBs for certain FTI functions are not adopted yet by FTI manufacturers [15]. This is the case of “Precision Time Protocol Version 2 (PTPv2) Management Information Base” defined in RFC 8173 [8]. The information is available but in specific manufacturer OIDs.

This situation makes complex the task to manage the same function with different manufacturers and should be fixed in the future. Using standard MIBs makes simpler for standard network management applications to discover and detect systems and process standard alarms.

The following table shows the monitoring capabilities of FTI components in a standard instrumented aircraft. It describes if they are capable of being monitored and controlled using SNMP, IENA or any other method, the SNMP version they support and if they support standard and enterprises MIBs:

Tab. 2: FTI device monitoring capabilities

FTI device	SNMP mon/cont	IENA	Other mon	SNMP version	MIB std/ent
RDAU1	Low/No	High	No	SNMPv2c	Yes/Yes
RDAU2	Low/No	High	No	SNMPv2c	Yes/Yes
RDAU3	High/Low	High	Yes	SNMPv2c	Yes/Yes
Recorder	High/High	No	Yes	SNMPv2c	Yes/Yes
Switch	High/High	No	Yes	SNMPv2c	Yes/Yes
Video	High/low	No	Yes	SNMPv2c/v3	Yes/No
Cameras	No/No	No	Yes	No	No
Telemetry	High/High	No	Yes	SNMPv2c	Yes/Yes
Computer	High/Low	No	No	SNMPv2c	Yes/No
Control	High/High	No	Yes	SNMPv2c	Yes/Yes

As it is shown most of the DAU support IENA and SNMP but the recorder only supports SNMP. Majority of the devices only support SNMPv2c and support of SNMPv3 is weak so far (only 2 systems are capable).

Reviewing this table, it can be seen that IENA should be complemented with SNMP monitoring to have a full picture of the flight test installation.

Adopting SNMP monitoring we will benefit from the following capabilities to monitor:

- Recorder: remaining time, disk space, recording bit rate, BIT, system health information, synchronization status
- Ethernet switches: status and statistics of interfaces, synchronization status, health information
- Video IP encoder: resolution and status of video input, system health information.
- Rugged PC: system health information, disk space, CPU usage,
- Telemetry equipment: output power, frequency selection, system health information.

It can also be controlled many functions: start/stop recording, enable/disable video streaming, modifying telemetry parameters (frequency, power), …

Integration of SNMP in Airbus DS

As we have seen in many cases SNMP is the only way to monitor systems. In the past the solution has been to implement ad-hoc solutions to cover the urgent monitoring need as no standard solution was easily integrable in FTI monitoring displays.

The usual case is to use a small IENA proxy-server that can generate IENA streams with data acquired using snmp requests to a certain

equipment. In this way data is recorded and available as usual FTI data for monitoring but the solutions are program or even aircraft dependent.

This solution may require a software package to be installed in an existing rugged PC (see Fig. 9) or a new equipment designed to perform this function as the Enhanced Cockpit Control Unit (ECCU) developed for a new fighter prototype [14].

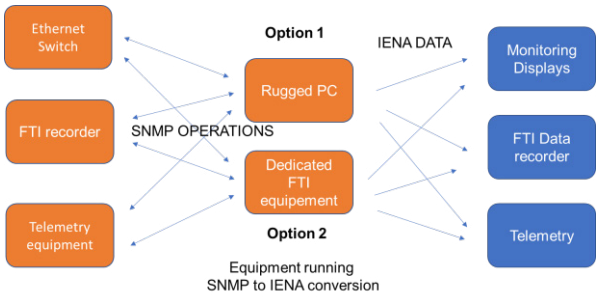

Fig. 9. SNMP to IENA scenarios

Other use case is when FTI data has to be provided to an external system. In this case an SNMP agent is used to receive IENA data from FTI and provide to the external SNMP manager the information through an agreed MIB (see Fig. 10).

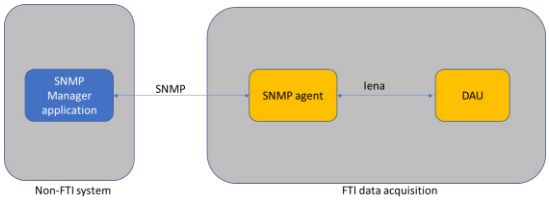

Fig. 10. IENA to SNMP scenario

The objective is to provide a standard solution for FTI and this requires to analyze the tools commonly used for SNMP monitoring in network operators or internet service providers.

SNMP standard monitoring tools

From the beginning of internet, the need of network management was a requirement to ensure a good service level. Most of the network management tools used SNMP as main protocol to acquire data from the systems to be monitored. Some of these historical tools were HP Network Node Manager or IBM Tivoli that have evolved to cover new needs as cloud services or IoT [12].

These powerful tools are used in Network Operating Centres to manage and monitor services, networks and systems. They are capable of discovering the network topology and give visibility of traffic and load of the network using SNMP and managing events providing an alarms console.

The main features of these tools are [13]:

- Discovery of networks: using ICMP and SNMP, the networks that are connected to any device accessible by the network management station are visible.
- Provide preconfigured Device Profiles for known sysObjectID configuring automatically settings.
- Creation of groups of nodes automatically with predefined groups (routers, switches, virtual machines, …)
- Monitor network health, polling critical devices more frequently than non critical devices to reduce the amount of traffic generated. Configuration of alarms with thresholds and rearm values.
- Definition of user groups for access to visualisation of alarms.
- Advanced features to reduce alarms generation: e.g., if a switch is down, all the interfaces connected to it will also be down, generating excessive alarms for an event.

The cost of these tools is high and would require an additional console to monitor events, new administration and configuration efforts and hardware for supporting the network management software. In addition, some DAU has low implementation of SNMP support. So, it seems not practical to integrate it for onboard FTI monitoring.

Developing a solution capable of providing features included in these standard monitoring tools will provide improvements to take the most out of SNMP.

New FTI alarms console in Airbus DS

As part of network management improvement, a new GUI for monitoring FTI alarms has been designed. It is capable of presenting an alarms history view that will reduce the overload for the operator.

The definition of the alarms requires the following data:

- Define to which system type, system group and message group the alarm will be assigned to.
- Description of the alarm thresholds, parameters calculation related with the alarm (up to three), the severity, the message to be shown to operator and a suggested action if needed.

For simplifying the view, alarms can be filtered depending on:

- A specific system as alarm source
- Severity of alarms (critical, major, minor, warning, normal, unknown).
- System group: DAU, Video, Network, Power, Data servers and Recorders.
- Message group: Network, System performance (CPU, hard disk free space,...), synchronization, environmental (temperature), hardware (BIT, ..)

The console will also allow easily to disable monitoring of a system until a problem is solved to avoid excessive alarms from it.

In case that no data is received for a defined alarm, a message will be shown to warn the operator that is not being processed.

For reducing overload only current status of an alarm is shown in console (see Fig.11) but all alarms are stored and can be consulted. This will allow to detect possible failures in a post-flight check.

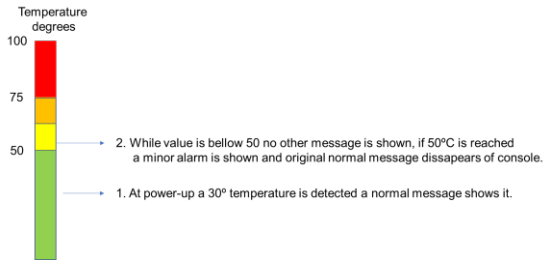

Fig. 11. Alarm message generation.

This software application for alarms visualization (see Fig. 12) receives information from a data server and is independent if this data comes from an IENA or SNMP source.

Fig. 12. FTI monitoring History display

This console is fully operative currently and will integrate SNMP data using an SNMP-IENA application (see Fig. 13) that will do the conversion between SNMP OID's and IENA parameter, poll at defined intervals for SNMP parameters and generate IENA data.

This approach will have the following advantages:

- Monitoring software is independent of data source (SNMP and IENA data can generate alarms).
- Data is recorded in standard FTI format and can be consulted with standard analysis tools.
- SNMP data can be sent over telemetry link in the standard way (IENA).

The architecture will support in addition the reception of SNMP traps in the "IENA-SNMP application" and conversion of this data to IENA format.

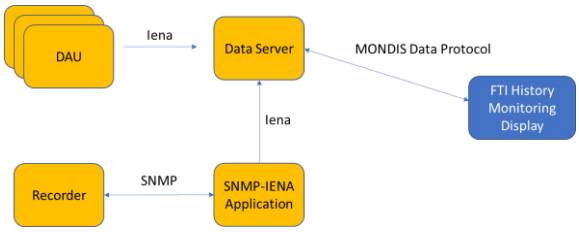

Fig. 13. Architecture for SNMP polling.

For supporting SNMP configuration, a configuration protocol will be used to set SNMP parameters using the SNMP-IENA application. This configuration protocol (see Fig.14) is already used for configuration of FTI devices

using HTTP or sockets applications for video system equipment.

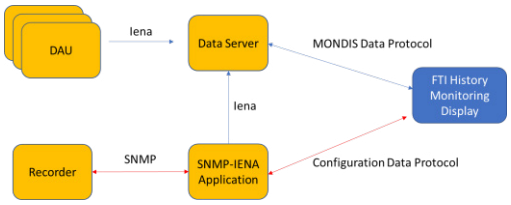

Fig. 14. FTI configuration using SNMP.

The configuration of SNMP-IENA application will be automatically generated from the programming generation tool once the SNMP parameters configuration has been defined.

New monitoring capabilities for new scenarios

Monitoring current FTI architectures can be a difficult task as they include many Ethernet switches, remote acquisition units, recorders and specific equipment for flight test. The new capabilities provided by supporting SNMP will improve the detection of problems of existing flight test installation but will enable also to manage more complex networks.

The development of bidirectional telemetry and mesh networks will allow communication between test articles having FTI installed and ground stations (see Fig.15). This will allow even to monitor and control FTI devices in other test articles if tools are operative.

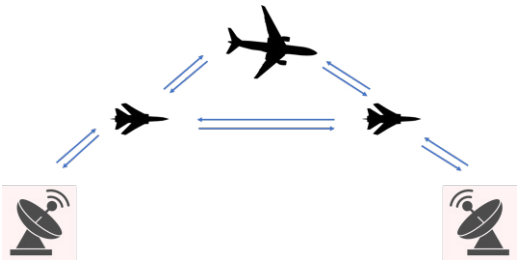

Fig. 15. FTI telemetry mesh network.

SNMP support will be important in these future scenarios [19] utilizing version 3 of the protocol, adding authentication and encryption to the SNMP message exchange. The use of standard TmNS MIBs should be encouraged to simplify monitoring configuration.

The figure 16 shows a FTI architecture in which the flight test engineer of a military transport aircraft could be monitoring FTI data received from drones checking that all parameters are right before launching a flight test, or modifying configuration of drone equipment to prepare the test. This will be possible with bidirectional telemetry if monitoring & control capabilities are ready.

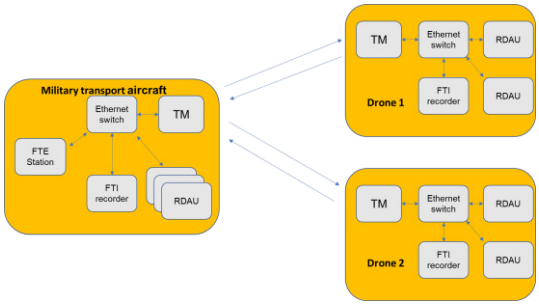

Fig. 16. FTI architecture for MTA and drones.

Conclusions

Network management of FTI requires the adoption of SNMP to be able to monitor most of the components of a flight test network. This is encouraged by the Telemetry Network Standard (TmNS) that adopt SNMP as standard for monitoring, configuration and control and has defined standard MIBs for telemetry components.

The adoption of SNMP requires the use of new software applications to receive the data and to visualize the information received without overloading the operators. The software architecture has also to provide capability to control the systems using SNMP. Airbus DS is developing the flight test software solutions that will allow the management of SNMP devices easily in a multi-program environment.

Finally, the improvement of network management with SNMP support and new software tools is a previous step to cover future needs of flight test activities as System of Systems (SoS) where bidirectional telemetry with mesh networks is expected to be used.

References

[1] Telemetry Standards, RCC Standard 106-23 Chapter 6 - Recorder & Reproducer Command and Control, July2023 - https://www.trmc.osd.mil/wiki/display/publicRCC/106+Telemetry+Standards?preview=/168165620/168165605/chapter6.pdf

[2] RFC 1157 - A Simple Network Management Protocol (SNMP) - https://www.ietf.org/rfc/rfc1157.txt

[3] Information processing systems - Open Systems Interconnection, "Specification of Abstract Syntax Notation One (ASN.1)", International Organization for Standardization, International Standard 8824, December 1987.

[4] RFC 1155 - Structure and Identification of Management Information for TCP/IP-based Internets - https://www.ietf.org/rfc/rfc1155.txt

[5] RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II - https://www.ietf.org/rfc/rfc1213.txt

[6] RFC 1901 - Introduction to Community-based SNMPv2 - https://datatracker.ietf.org/doc/html/rfc1901

[7] RFC 1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2) - https://datatracker.ietf.org/doc/html/rfc1905

[8] RFC 8173 - Precision Time Protocol Version 2 (PTPv2) Management Information Base: https://datatracker.ietf.org/doc/html/rfc8173

[9] Telemetry Standards, IRIG Standard 106-23 Chapter 21 - Telemetry Network Standard Introduction : https://www.trmc.osd.mil/wiki/display/publicRCC/106+Telemetry+Standards?preview=/168165620/168165599/Chapter21.pdf

[10] Telemetry Standards, IRIG Standard 106-23 Chapter 22, July2023 - Network-Based Protocol Suite https://www.trmc.osd.mil/wiki/display/publicRCC/106+Telemetry+Standards?preview=/168165620/168165603/Chapter22.pdf

[11] Telemetry Standards, IRIG Standard 106-23 Chapter 25, July2023 - Management Resources https://www.trmc.osd.mil/wiki/display/publicRCC/106+Telemetry+Standards?preview=/168165620/168165596/Chapter25.pdf

[12] What happened to Tivoli? – Ingo Averdrunk 2016 - https://web.archive.org/web/20180224143553/https://www.ibm.com/blogs/cloud-computing/2016/08/what-happened-to-tivoli/

[13] HP Network Node Manager i Software 10.0 - Online Help: Help for Administrators – https://support.microfocus.com/kb/kmdoc.php?id=KM00838328&fileName=hp_man_nnmi_Help_Administrators_10.00_pdf.pdf

[14] G. Martínez Morán, “Intelligent Networked Flight Test Instrumentation for a new Fighter Prototype”, ETTC 2018; doi:10.5162/ettc2018/11.1

[15] O. Holmeide, M. Schmitzr ,“PTP version 3 in FTI“, ETTC 2016: doi: 10.5162/etc2016/1.1

[16] P. Quinn , “Addressing the Babel’s Tower of FTI Standards in a Network Environment”, ETTC 2020; doi: 10.5162/ettc2020/2.5

[17] Grace, Thomas B., Bertrand, Allison R., Newton, Todd A. , “Applying the iNET System Management Standard”, International Telemetering Conference Proceedings 2019

[18] N.Cranley , D.Corry, “Networked Flight Test Instrumentation Data Recording Solutions”, International Telemetering Conference Proceedings 2009

[19] Pingfan Guo, Ming Liu, Hong Li, Hongxiang Zhu ,” Telemetry System Based on MESH Network and Its Application” , International Telemetering Conference Proceedings 2018