OBTAINING AN ATO FOR AN iNET OPERATIONAL DEMONSTRATION

David Hodack
Naval Air Systems Command
Patuxent River, MD USA

ABSTRACT

The integrated Network Enhanced Telemetry (iNET) project was launched to foster network enhanced instrumentation and telemetry. The program is currently implementing an operational demonstration. That will involve installing and using a network enhanced instrumentation system on a helicopter. This demonstration will be used as a learning exercise for the implementation of network technologies. This paper will give a brief description of the operational demonstration. Then it will explore the need for an Authority to Operate (ATO) and describe how one was obtained.

KEY WORDS

Ethernet, iNET, IP, Networking, vNET, Network Security, Information Assurance

PROGRAM BACKGROUND

The Central Test and Evaluation Investment Program (CTEIP) has launched the integrated iNET project to foster advances in networking and telemetry technology to meet emerging needs of major test programs. An iNET architecture has been developed that defines a Telemetry Network System (TmNS) that would utilize traditional telemetry links in conjunction with a network-based telemetry link. The basic approach allows for the integration of network-based systems without significantly affecting traditional telemetry systems. The TmNS (Figure 1) architecture is divided into several elements and contains three key areas: the Radio Frequency Network (rfNET) element, the test Vehicle Network (vNET) element, and the Ground Network Interface (gNET) element. Utilizing this architecture, proposed iNET standards have been developed to allow for the interoperability of the many components of the TmNS. The iNET team is currently in the process of obtaining prototypes to validate the Proposed Standards. To gain insight into existing technologies relative to the Telemetry Network System architecture, demonstrations utilizing Commercial off the Self (COTS) equipment are being implemented. Earlier demonstrations have been conducted to demonstrate a baseline of existing technologies to show potential users the validity and benefits of adding a two-way data connection to the test vehicle, which included a traditional serial streaming telemetry link. The current operational demonstrations are meant to expand on the previous demonstration and to be used as a test bed for incoming prototypes. Additionally the operational demonstration will allow for operational procedures to be developed and validated.

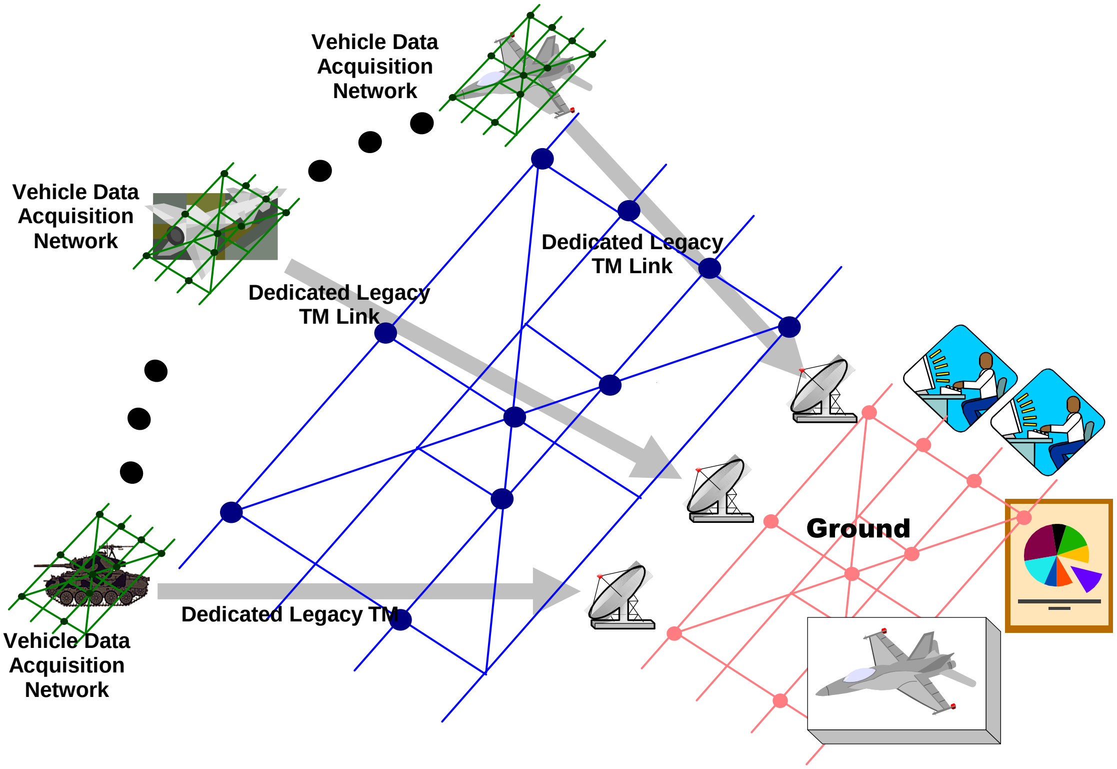
Vehicle Data Acquisition Network
Vehicle Data Acquisition Network
Dedicated Legacy TM Link
Dedicated Legacy TM Link
Vehicle Data Acquisition Network
Dedicated Legacy TM
Ground

Figure 1: Telemetry Network System

OPERATIONAL DEMONSTRATION

One of the primary objectives of this operational demonstration is to give flight test engineers, instrumentation engineers, and range engineers the opportunity to get hands on experience with some of the advantages of using network enhanced telemetry. This experience will help foster community use of network based telemetry systems. It will also allow for the discovery of challenges that are associated with implementing and using a network based telemetry system. With this experience, operational procedures will be developed to mitigate some of the risk involved with using networks for flight test.

For this operational demonstration a traditional PCM based telemetry system and a network based telemetry system are going to be installed into a Test Pilot School (TPS)

H-60 helicopter as seen in the top half of figure 2. This dual system approach was done to give TPS confidence that they would have uninterrupted flight test even if issues arose with the network technologies. The dual systems facilitate pushing the limits of the network based telemetry system. Network throughput and the distance at which the RF network can maintain consistent connectivity will also be monitored.

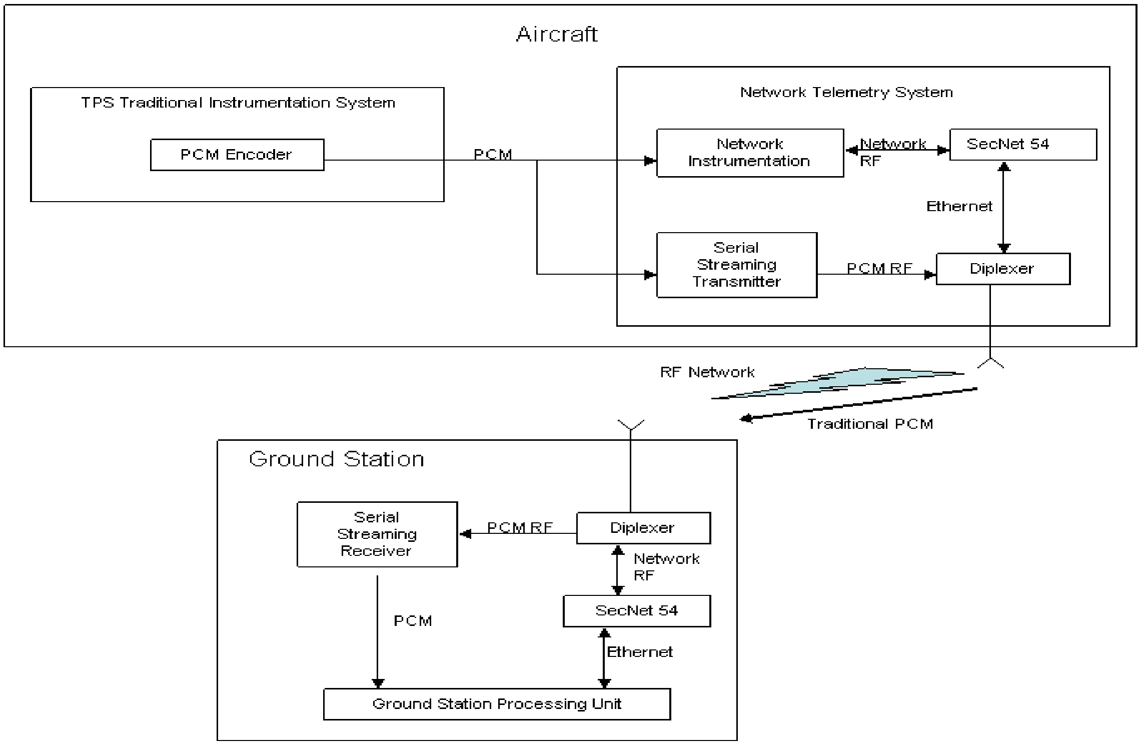

Figure 2: Operational Demonstration System

At the heart of the vNET is a multiplexer with a built in digital recorder. The multiplexer collects PCM data from the traditional instrumentation as well as video data. This unit also performs the data retrieval task. Via the network, it receives a request for time slices of data, fetches them from the recorder and sends them to the ground station. A system diagram is shown in figure 3.

The rfNET consists of a RF power splitter, phase shifter, serial streaming transmitter, and a serial streaming receiver. It also has two of each of the following, one on the aircraft and one at the ground station; Harris SecNet 54 wireless network transceiver, transverter, diplexer, and phase shift processor. The SecNet 54 links the RF network to both the vehicle network and the ground network. The transverter shifts the frequency and amplifies the signal of the 802.11 based SecNet 54 to the telemetry L-Band. The serial streaming transmitter, serial streaming receiver, and RF power splitter are parts of the traditional PCM based telemetry system. It is planned to work in partnership with a science and technology effort to perform testing, using the phase shifter and phase shift processor for the future capability of steering the serial streaming telemetry antenna pattern. The airborne phase shift processor receives feedback from the ground phase shift processor about the serial streaming telemetry signal strength through the network and uses the phase shifter to add a delay to the aircraft's upper serial streaming telemetry signal. This delay will change the antenna pattern so that the signal strength at the ground station will remain strong. The diplexer is used to combine the aircraft's lower serial streaming telemetry signal with the RF network signal. This can be seen in figure 3.

The gNET is built around a telemetry processing unit. This unit receives both a network link and a PCM feed. The processing unit decodes the PCM and fills in drop outs by making a request for time slices of data from the onboard recorder through the network. Also part of gNET is another phase shift processor that is used to send feedback to the onboard phase shift processor for beam steering. This can be seen in figure 3.

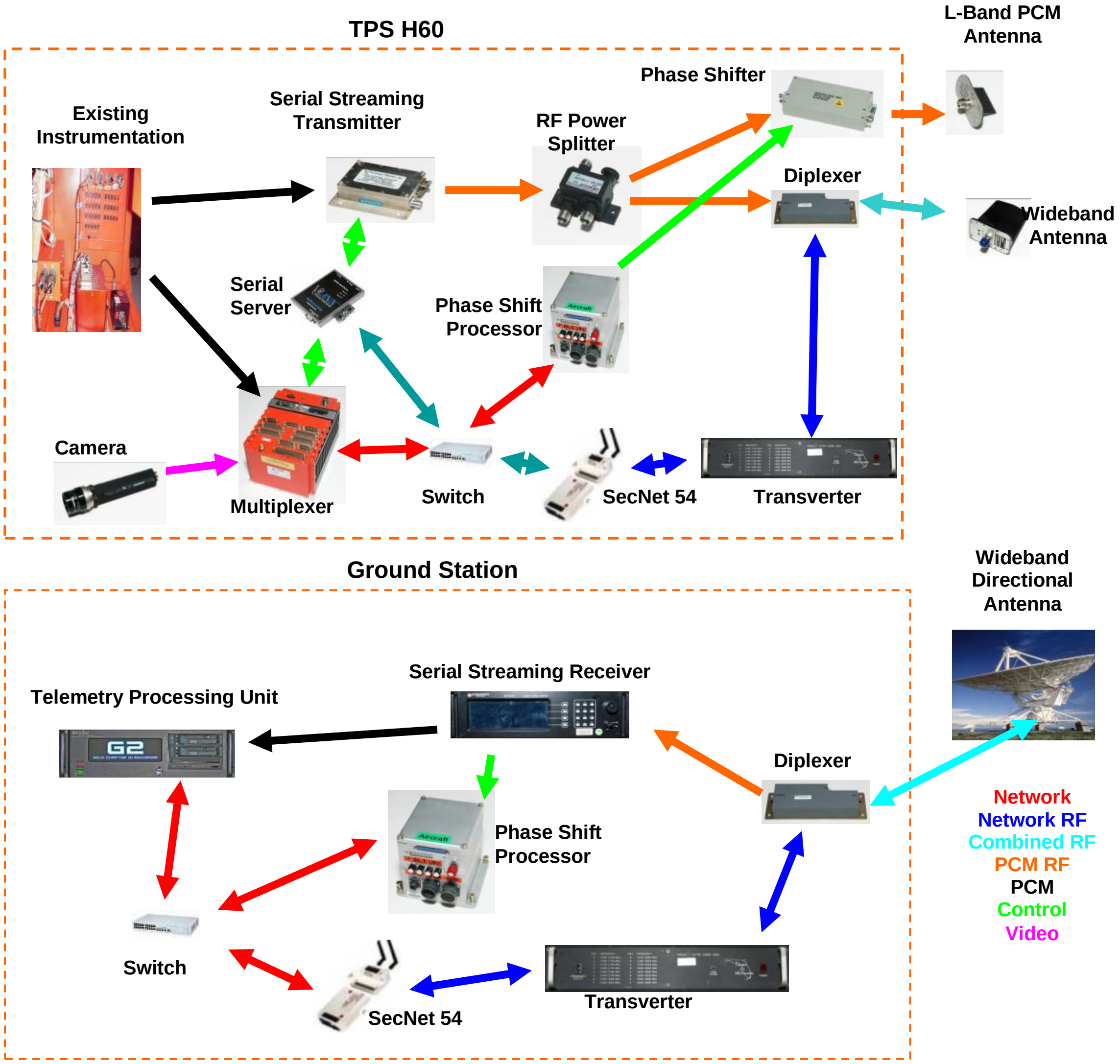

Figure 3: Detailed Block Diagram

This system will demonstrate three major iNET objectives; data retrieval from the onboard recorder during flight, the ability to fill in telemetry drop outs during flight, and in-flight instrumentation control from the ground station. To use this system and be able to demonstrate these tools to the telemetry community it was necessary to acquire an ATO from the Patuxent River Designated Approving Authority (DAA).

NEED FOR NETWORK SECUITY

With the introduction of networks into aircraft instrumentation and of wireless networks into telemetry it becomes a requirement for all DoD owned or controlled information systems to become certified and accredited. This requirement comes from the DoD directives 8100.02; “Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)” and 8500.1; “Information Assurance (IA).” It is stated that an accreditation is required even if the data being transmitted is unclassified and that the data being transmitted wirelessly must be encrypted. It is also stated that regardless of Mission Assurance Category an accreditation is required. These requirements are not only about protecting the data that is transmitted but also about protecting the Global Information Grid (GIG). This comes from the notion that a vulnerability for one is a vulnerability to all. Some of these requirements were more relaxed because the iNET Operational Demonstration is a stand alone system so it will not introduce vulnerabilities to the GIG but none the less an accreditation is still required. Another part of the accreditation is to assess whether the system availability will meet the mission needs. For the iNET team to move forward with its operational demonstration an Information Assurance (IA) accreditation was required that would give the team ATO.

ACQUIRING ATO

For the iNET operational demonstration to receive an ATO it followed DoD instruction 8510.01; “DoD Information Assurance Certification and Accreditation Process (DIACAP).” This process is used for authorizing the operation of DoD Information Systems (IS). This is accomplished by using baseline Information Assurance (IA) controls to ensure that the system meets the standards set forth by the DoD. These controls can be found in DoD instruction 8500.2; “Information Assurance (IA) Implementation.” Each year a review of the IS must be completed to ensure that the IA posture of the IS is still acceptable. This review must include a validation of the applicable controls and be documented in writing.

A few key players in this process are the DAA, Program Manager (PM), and the User Representative (UR). The DAA is tasked with ensuring the DIACAP package is initiated and completed. Then he ensures that the IS complies with the applicable IA controls. Once he has completed these tasks he grants the IS an ATO. The PM needs to plan and budget for the implementations of IA controls and sustain the IA posture of the IS. He is also responsible for developing, tracking, resolving, and maintaining the DIACAP implementation plan. The user community is represented by a UR that ensures the IS will fulfill their needs once an ATO is granted.

The specific steps that the iNET team needed to complete to receive an ATO are as follows. The first was to complete a Customer Requirements Brief (CRQ). This brief asked questions about the types of systems that would be used in the IS and needed a description of the overall IS that is being considered for an ATO. Once the brief was complete the iNET team had a meeting with one of the Information Assurance specialist that work for the DAA. In this meeting we discussed changes required to our planned system and the need for a System Administrator (SA) and Information Assurance Officer (IAO). One of the changes was to use a wireless network transceiver that is on the National Information Assurance Partnership (NIAP) approval list. This wireless transceiver also needed to have the proper encryption built into it. The transceiver that was chosen by the iNET team was the Harris SecNet 54 because it already had approval from the National Security Agency (NSA). The SA and the IAO for this project each needed to be a CompTIA Security+ certified professional. This required two team members to get the required training. After it was determined that our IS (the iNET Operational Demonstration System) was ready the iNET team proceeded to fill out the TEMPEST Requirements Questionnaire. This gave a description of the physical security that our system would utilize. A list of all system assets and software loaded on these assets was complied to ensure that they meet DoD standards. The operational demonstration system then had to undergo system hardening steps before it could receive an ATO. Once these steps were complete an Authority to Operate was granted by the DAA.

CONCLUSION

One of the lessons learned from completing this operational demonstration is that Network Security needs to be addressed from the start of designing a network enhanced telemetry system. It has been stated in both DoD directives and instructions that when contracting for systems, services, and programs that cover information systems that clauses need to be included to comply with IA and that failure to include these clauses is not justification for non-compliance. As iNET moves forward with deploying network enhanced telemetry systems at the ranges they will become more integrated with the GIG, making the accreditation process more complicated. But with proper planning and working with the DAA and his team of security professionals these hurdles can be overcome.

REFERENCES

1. Hodack, David; "Implementing iNET and the Operational Issues Involved", Proceedings of the International Telemetering Conference (ITC 2007)
2. DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
3. DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
4. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
5. DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007