INFORMATION ASSURANCE (IA) CONSIDERATIONS FOR A TELEMETRY NETWORK SYSTEM (TmNS)

David Hodack
Naval Air Systems Command
Patuxent River, MD USA

ABSTRACT

The integrated Network Enhanced Telemetry (iNET) project was launched by the Central Test and Evaluation Investment Program (CTEIP) to foster network enhanced instrumentation and telemetry. The iNET program is preparing for the TmNS system demonstration. The goal of the demonstration is to prove that the proposed TmNS will meet the Test Capability Requirements Document (TCRD) and validate the iNET standards. One aspect of the preparation is looking at the IA issues and making decisions to ensure that the system will be certified and accredited, meet user needs, and be secure. This paper will explore a few of these considerations.

KEY WORDS

iNET, Information Assurance, TmNS, Network, Security

INTRODUCTION

CTEIP has launched the 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 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 contains four key segments: the Radio Access Network Segment (RANS), Test Article Segment (TAS), the Range Operations Segment (ROS), and the Telemetry Ground Station Segment (TGS). 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 have been 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.

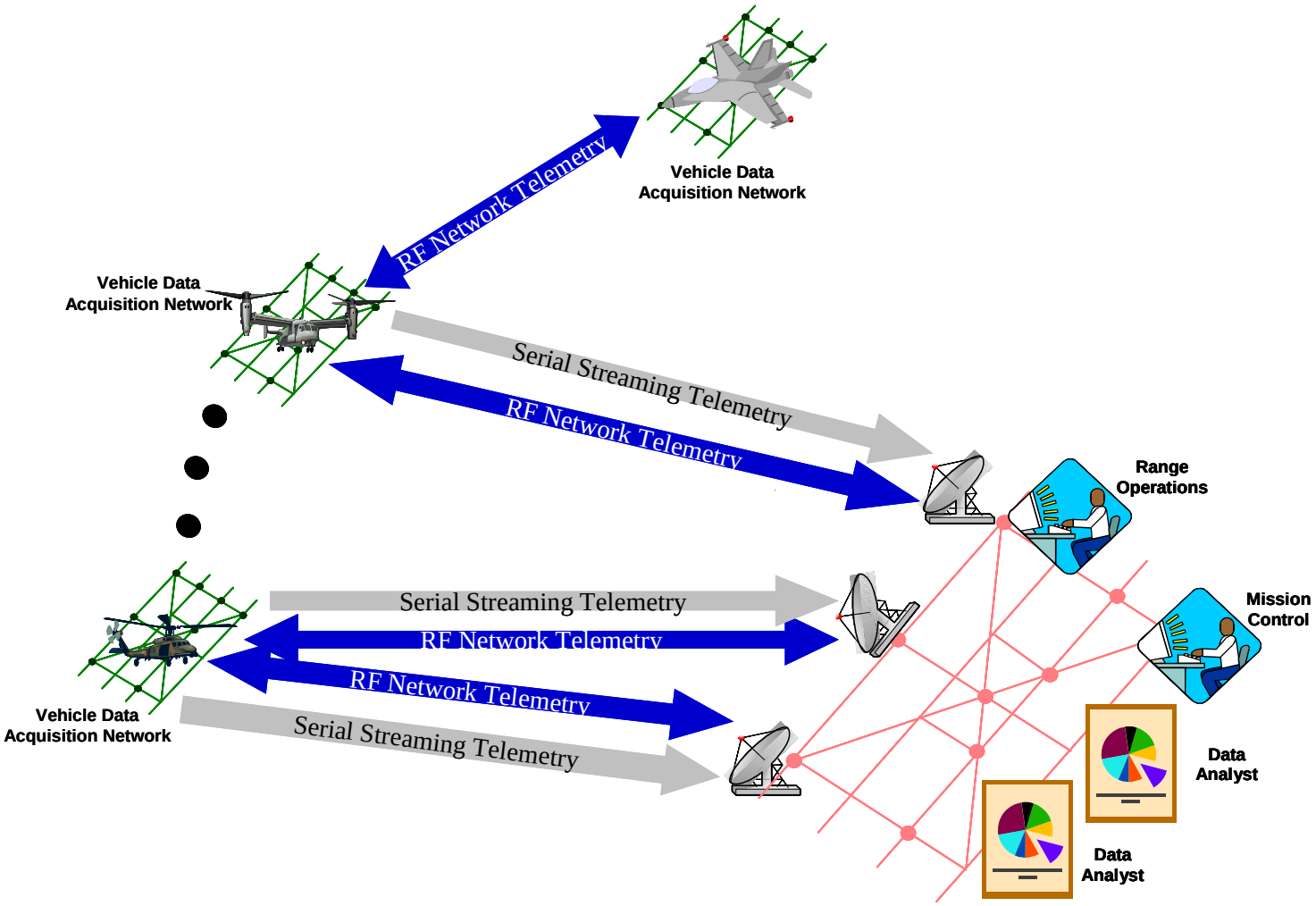

Figure 1: Telemetry Network System

The current TmNS demonstration will be used to prove that the proposed TmNS will meet the TCRD and validate the iNET standards. It is the iNET team's goal that this demonstration will give flight test programs the confidence to use network enhanced telemetry systems. Demonstrations will take place at Edwards Air Force Base (AFB) and Patuxent River Naval Air Station (NAS). The goal at Edwards will be to test the radio frequency (RF) network link and at Patuxent River the system will be tested end-to-end. A data flow diagram of the demonstration system is shown below in figure 2.

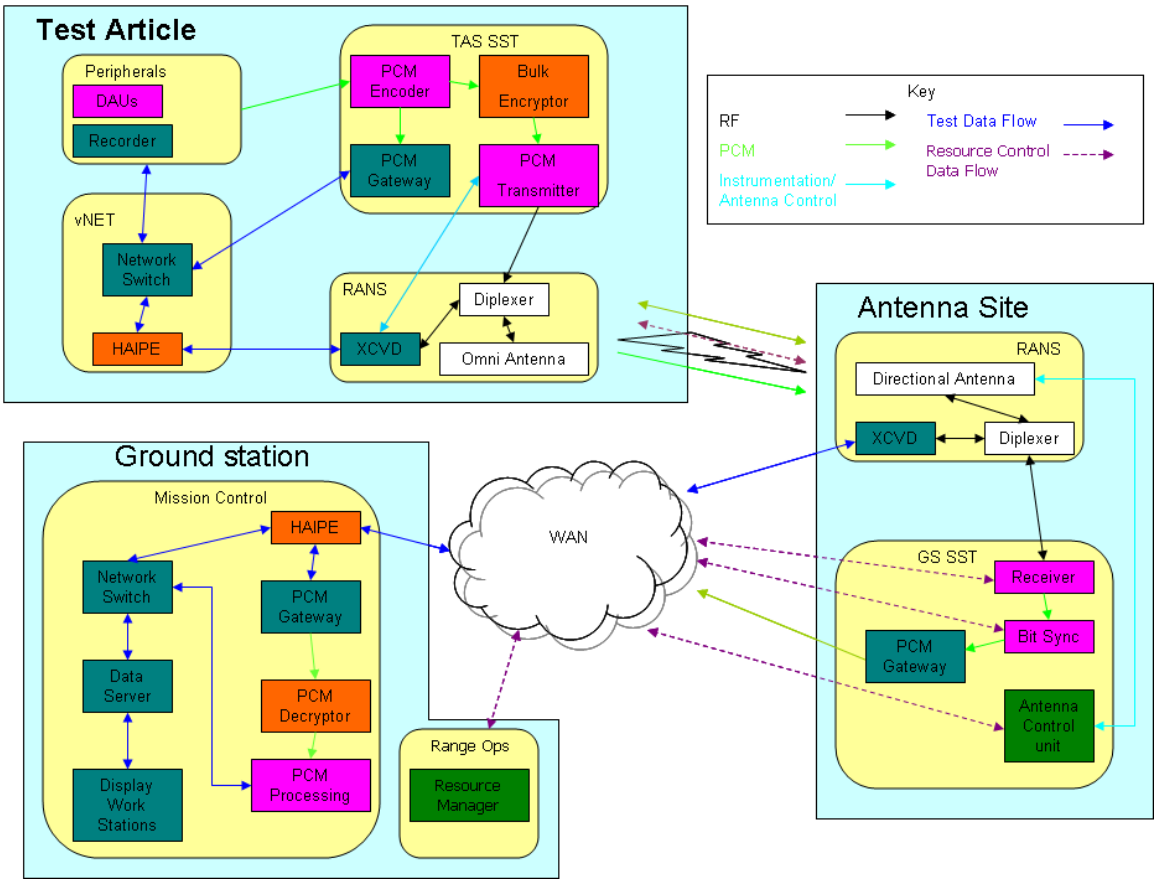

Figure 2: TmNS Demonstration System

IA decisions will need to be made that will allow for the system to receive an authority to operate (ATO). The Department of Defense (DoD) requires all IT systems to be designed with IA in mind. DoD ensures this happens by requiring a certification and accreditation for these systems. Most available documentation is geared towards corporate office networks and 802.11 wireless networks. Aircraft instrumentation provides its own challenges with the need for real time ruggedized equipment. IA decisions currently being made will affect the usability, maintainability, level of security, and the ability for future iNET deployments to receive an ATO. The three most challenging security considerations are:

- Is Data at Rest (DAR) encryption needed?
- Is National Information Assurance Partnership (NIAP) approval needed?
- Are Federal Information Processing Standards (FIPS) 140-2 certified transceivers required?

At the time of writing this paper final decisions have not been reached. The following paragraphs discuss rationale that will inform the decisions, and this information is NOT meant to base design decisions on for equipment that may require ATO.

DAR ENCRYPTION

The requirement for DAR encryption comes from the DoD memorandum "Encryption of Sensitive Unclassified Data at Rest." This memorandum states that all DoD information that is stored on a removable media device shall be treated as sensitive and encrypted using a commercially available encryption technology that is FIPS 140-2 compliant. While this is the stated policy it is not clear that it is applicable to flight test recorders. These are special purpose, ruggedized, airborne recorders. The media itself has the physical security of being located on the aircraft in the same way the other sensitive pieces of the aircraft are protected while it is on the ground. While the aircraft is in flight there is a very slim chance of the media falling into enemy hands through a crash. Even in the event of a crash it is likely that the aircraft will be on US property. It is estimated that adding encryption to the onboard recorder would cause the performance to decrease by a factor of four, cost to increase by 25% and severally complicate in-flight data retrieval. It is for these reasons that the iNET team hopes on board DAR encryption is not needed.

NIAP APPROVAL

NIAP is operated by the National Security Agency (NSA) to ensure IT products meet a certain level of trust and security. Using NIAP approved products will increase the level of trust consumers have in their information systems and promote the development and use of evaluated IT products and systems. The requirement for NIAP approved systems comes from DoD directive 8500.01E, but this directive also states that this requirement can be waived by the Designated Approving Authority (DAA). It is anticipated that systems at the ground station will meet this requirement but that some systems in the aircraft will not. The devices that may be exempt are the ones that boot from internal memory and cannot boot from an external device. These devices are special purpose ruggedized airborne equipment that are not mass produced making the approval process somewhat cumbersome. It is the view of the iNET team that the cost for receiving NIAP approval for instrumentation airborne devices that boot from internal memory is not warranted due to the low probability of corruption since the boot process is self contained.

LAYER 2 RF NETWORK ENCRPTION

To encrypt the RF network at layer 2 a FIPS 140-2 device would need to be used. The Nation Institute of Standards (NIST) Publication "Establishing Wireless Robust Security Networks" states that "Organizations should ensure that all WLAN components use Federal Information Processing Standards (FIPS)-approved cryptographic algorithms to protect the confidentiality and integrity of WLAN communications." As can be seen in figure 2 all aircraft test data is protected using a network encryption device. Some network control information may not be encrypted for transmission. The other reason to use FIPS 140-2 encryption would be to protect the WAN from an attack. There will be

many layers of protection built into the system to prevent this. The intruder would physically need to be in the narrow beam of the ground station antenna which is constantly moving to track the test article during flight. The transceiver at the ground station will be programmed to only talk to the transceiver on the aircraft with the proper electronic ID. The transceiver will also implement port filtering, protocol filtering, and access control lists. It is estimated that to receive a FIPS 140-2 certification for iNET transceivers it would cost 60% of the unit. Because of the great cost increase, the unimportance of control messages, and the built in security measures that protect the WAN it is the hope of the iNET team that FIPS 140-2 encryption will not be needed.

CONCLUSION

The iNET team is still working with the DAA's in anticipation of a decision regarding all three questions posed in this paper. But currently the team is leaning towards not encrypting the Data at Rest. We are also planning on not requiring NIAP approval for the airborne pieces of hardware that can only boot from internal memory. It is anticipated that the transceivers will not need to be FIPS 140-2 certified. Implementing proper security measures has been made easier by working with the DAA early in the design process to ensure there will be no surprises when accrediting the system.

REFERENCES

1. Hodack, David; “Obtaining an ATO for an iNET Operational Demonstration”, Proceedings of the International Telemetering Conference, Les Vegas, Nevada, October 2009.
2. DoD Directive 8000.01, “Management of the Department of Defense Information Enterprise,” February 10, 2009
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