MANAGEMENT OF NETWORK-BASED FLIGHT TEST SYSTEMS

Michael S. Moore, Evan T. Grim, Ganesh U. Kamat, Myron L. Moodie
Southwest Research Institute®
Communications and Embedded Systems Department
San Antonio, TX
msmoore@swri.org http://commsystems.swri.org/

ABSTRACT

Network-based instrumentation systems are rapidly replacing traditional fixed serial interconnected instrumentation in both commercial and military flight test environments. Modern network-based flight test systems are composed of large numbers of devices including high-speed network switches, data acquisition devices, recorders, telemetry interfaces, and wireless network transceivers, all of which must be managed in a coordinated fashion. Management of the network system includes configuring, controlling, and monitoring the health and status of the various devices. Configuration by hand is not a realistic option, so algorithms for automatic management must be implemented to make these systems economical and practical. This paper describes the issues that must be addressed for managing network-based flight test systems and describes a network management approach that was developed and employed to manage a large-scale network-based flight test system.

KEY WORDS

Networks, Flight Test, Telemetry, Data Acquisition, Network Management, iNET

INTRODUCTION

Networks, both wired and wireless, are beginning to become commonplace as replacements for, or alongside, traditional fixed serial interconnects and telemetry streams in flight test systems. Both commercial and military flight tests will soon rely heavily on networks to interconnect and carry data between the devices on test articles, as well as between the test articles and ground stations.

Network management is an overloaded term; some believe it to include only the configuration, control, and monitoring of the network devices themselves (network switches, their interconnections, telemetry end points, and wireless network transceivers). The end-node devices (data acquisition units, solid state recorders, analysis applications) are often thought of as

being managed separately from the devices that interconnect them. However, having an operational network by itself does not solve the difficult problems that must be addressed in order for a flight test system to function correctly any more than having an Ethernet network in a bank creates a financial accounting system. A flight test system is made up of many devices and applications which, when configured and integrated together, form a complete system for acquisition, recording, and analysis of flight test data. Moreover, the tight timing constraints required of the network by flight test applications make it necessary to utilize appropriate technologies (e.g. IEEE 1588 time synchronization, IGMP snooping, and UDP multicast), and to optimize the integration of the end nodes and the applications that run on them with the network. It is advisable, if not necessary, for the network and the end node devices to be configured, controlled, and monitored together as a whole. A system-level, or holistic approach, toward managing a network-based flight test system is recommended.

The issues that must be addressed in order to manage a network-based flight test system can be categorized into system configuration, and system control and monitoring. The following sections describe the issues in each of these categories and describe recommended approaches that have been developed through experience in developing, integrating, and deploying network-based flight test systems.

SYSTEM CONFIGURATION

Configuration includes network address assignment, network resource assignment for both the wired and wireless portions of the network, network topology and device discovery, end-node device and application configuration, and security administration.

Network Address Assignment

There are two competing methods of network address assignment: static and dynamic. Assignment of fixed IP addresses has become somewhat rare in most networks. Utilizing dynamic IP address assignment (e.g. DHCP) provides a far more flexible network configuration, requires less user intervention when a system is plugged into a network, and allows devices to become more mobile. A major drawback of using dynamic IP network assignment in flight test systems is startup time. A DHCP server must be up and running when the end nodes make requests for addresses. Power losses and resets occur commonly in some flight test environments, and if DHCP is used for address assignment, the transmitting and recording of data will be delayed until the DHCP server is booted and the end nodes have acquired addresses. Assigning fixed IP addresses to all devices a priori allows transmitting and recording of data to begin far more quickly across a power outage or system reset. The tradeoff is that using fixed IP addressing reduces flexibility and drives a test organization to put effort into building up a process for administering the assignment of IP addresses to physical devices. However, if the test application requires that data be acquired and recorded very quickly (e.g. within low tens of seconds) after a power loss or system reset, then the fixed IP address assignment is more prudent. It may be possible to create a dynamic address assignment method that exhibits lower startup times, but the desire to use standard services and protocols along with the need for quick system startup drives some network-based flight test designs toward static IP address assignment.

Network Resource Assignment

Wired Network Resources

Network-based flight test systems often have large amounts of data (e.g. many measurements, streaming video) being sent from many sources to more than one recipient. In this case, transporting the data with TCP/IP unicast is non-practical, as that would cause a separate copy of the data to be sent to each recipient. This would be a waste of network resources and would be difficult to manage.

The alternative approach is to use UDP/IP multicast for transmission of data across the network, as it is more efficient for delivering data to many locations on a network. Multicasting creates each recipient's copy of the data at a point as close to that recipient as possible, thus minimizing the extra bandwidth consumed. Multicast is the most prudent approach for transferring high-rate data in flight test networks. Utilizing IGMP and multicast will prevent the data from being transmitted across network links where the data has not been requested, preventing network devices, data acquisition devices, and applications from being overwhelmed with high bandwidth data transmission (hundreds of Mbits/sec). The multicast approach requires that multicast addresses be assigned to data streams in an intelligent manner with the knowledge of the estimated data rates, the network topology, and the source, sinks and routes of the data. Managing the number of multicast addresses is important; too many multicast addresses can cause network switch performance and data sink IP stack performance to degrade. Too few multicast addresses can cause the data on each multicast address to have a higher rate than the data sink applications can handle. The multicast algorithm has to balance the number of addresses and the expected data rates against the network topology, data routes, and data sink properties. We have developed methods to allocate multicast addresses to a large number of data sources in a way that balances the conflicting requirements.

Wireless Network Resources

In addition to the same parameters monitored and controlled for a wired network, the system-level network management approach has to handle a variety of additional parameters when wireless networks of various forms are introduced into the test system. Since wireless networks can take various forms, including short-range sensor networks on the test article up to long-range network-based telemetry links between the ground station and test articles, the network management system should be flexible and extensible to handle these various needs. For sensor networks, the functions required of the network management system likely will only involve initial static configuration of addressing and topology parameters. On the other hand, emerging long-range wireless network telemetry links require significantly more extensive and dynamic capabilities of the network management system to achieve their full potential. Whereas current fixed, one-way, PCM telemetry links only require initial setup and configuration with a predefined operating frequency, waveform, power, etc., fully networked, two-way, shared access telemetry systems, such as that being envisioned by the iNET program, have much more configuration flexibility, complexity, and dynamics.

For such wireless networks, the quantities that must be managed can include the frequency bands, the wireless waveforms, Time Division Multiple Access (TDMA) time slots, CDMA spreading codes, Forward Error Correction (FEC) parameters, and spatial parameters such as direction, beam width, and power. Unlike current fixed telemetry links, all of these parameters can and should be evolved dynamically during test operation to maximize utilization of the network.

Network Topology and Device Discovery

Flight test systems include test articles, telemetry streams, and ground stations. The test article and ground stations are typically wired networks. The test article networks include data acquisition units, solid state recorders, telemetry transmitters, network switches, and wireless network transceivers, among other devices. The ground station networks include telemetry receivers, network switches, wireless network transceivers, and analysis computers. The telemetry endpoints and wireless network transceivers glue the wired test article and ground station networks together wirelessly.

For tests of reasonable scale, the test article and the ground station networks tend to include tens of wired network nodes each. The number of devices that must be managed scales with the number of test articles involved in the test, and in some scenarios, test articles may cross range boundaries during the test. With a large number of devices being managed, and multiple ground stations and test articles involved, the task of coordinating the device and network configuration becomes complex. Methods of automatically determining what devices are present and how they are connected in test article and ground station networks are required to make this task feasible. Algorithms for discovering and keeping track of what devices are currently attached to the wireless network are also required, as test articles may join and leave a test network as they cross range boundaries.

Methods for discovering the devices and network topology in wired networks exist and have been proven in flight test environments. The methods leverage technologies such as TCP/IP sockets and broadcast ping, as well as Simple Network Management Protocol (SNMP). Methods for discovering the wireless network topology are less mature. Ad-hoc networking techniques exist that are based on commercially-available wireless technologies such as Bluetooth (802.15.1) and WiFi (802.11a/b/g). However, the flight test applications have special requirements for wireless link performance (large distances, low azimuth angles, high Doppler effects, and low bit error rate requirements), and for security. These drive the community toward utilization of non-standard wireless protocols for which custom network formation and discovery algorithms must be developed. Research is required in this area to determine a robust method of discovering the topology of the wireless flight test networks with custom links and protocols.

End-node Device and Application Configuration

The end-node devices and applications should be configured in coordination with the network devices. For instance, suppose a test configuration specifies that a set of measurements be recorded and monitored. The measurements are generated from data acquired from multiple data sources that are connected to different locations on the test article wired network. The configuration information describes many aspects of the measurements: which data is to be acquired, which devices will acquire the data, at what rate the data will be acquired, any

transformations that may be applied to the data (e.g. gains and offsets), how measurement values are to be calculated from the data, the identifiers for the measurements, how the data is to be either placed in a data stream or packetized, and to which devices the data is to be routed. The configuration information may also describe the physical interconnections of the acquisition devices to the network and network topology.

The task at hand is to ensure that the devices that acquire, record, telemeter, and analyze the measurements all have the same information and have coordinated configuration such that the data is captured, converted to measurements, and routed through the network to the appropriate devices and applications, and that the devices and applications are received in the correct format and with the required timing. The journey of measurements from sources to sinks includes many transitions and transformations, and the devices along the path need to be configured with the same notion of the measurements to make it happen.

System management should consider the configuration of source, network, and sink devices and applications from a centralized mechanism and from a common test database. This requires a common test configuration language (sometimes referred to as meta-data) be developed and standardized, and that this language include the notion of acquired data elements, the transformations that are performed to create measurements, the network formats (telemetry streams and packet structures), the details of the physical devices, the network topology, and also aspects of the various applications that will be used to analyze the data. Previous work in flight test has shown that such languages can be crucial to success in system integration, particularly in configuration. This experience can now be leveraged to create standards and common applications for configuration of network-based flight test systems.

Security Administration

Flight test applications often require the use of various security measures to guard system data and control channels. Data can be protected by various encryption methods (along with any applicable key management), while strong multi-factor user authentication and role-based authorization can shore up control channels. Effective management of security components such as encryption devices and security keys, as well as providing for network-level authorization and authentication, has proven extremely tedious and cumbersome. Indeed, many programs (e.g the Joint Tactical Radio Systems program) have struggled with crafting a security strategy that is effective without being unwieldy.

In light of this, systems wishing to deploy security measures can significantly benefit from a centralized and automated configuration strategy similar to that discussed throughout this paper. But the specific problem set of handling security administration has many unique considerations that make it difficult to sufficiently automate without reducing the efficacy of the security measures. Achieving success in this arena requires careful planning and cunning execution in linking together existing technologies with deployment and administrative strategies. Key to this is the use of standard interfaces, common APIs, and technologies that have been proven effective and have been thoroughly vetted by experts in the security community at large. Further research in this area is needed.

SYSTEM CONTROL AND MONITORING

Control includes enabling and disabling of data acquisition, recording, and network devices, as well as starting and stopping the recording of data. It also includes wireless network control (control of frequency, modulation, and transmit power, pointing antennas, etc). In order for this to be successful, the control of the wired and wireless devices must be centrally coordinated, along with the health and status monitoring functions such that the system can be reconfigured and continue to operate (perhaps in a degraded fashion) in the event of point failures.

Health and Status Monitoring

It is crucial for an effective management system to be able to monitor the health and status of a network. This requires a management strategy to not only have access to detailed information on all system components, but also to collect, organize, and display this information in a clear and effective manner. In all but the most trivial of systems, the amount of status information that is required to allow for necessary status monitoring and system troubleshooting would be overwhelming if dumped en masse to an operator. In most cases, this requires creating display screens that rely upon hierarchical relationships of data to provide an intuitive and concise information system. Furthermore, it is often desirable for the management system to facilitate a method for recording this digested system health and status information alongside the data so that it is available when post-processing the results.

Our experience shows that developing an integrated approach toward monitoring the health and status of the network and the devices attached to it is beneficial to the successful integration and deployment of large-scale network-based flight test systems. This should include both the wired and wireless networks. Hierarchy in the monitoring view is mandatory, as these complex networks can overwhelm even experienced users with the level of health and status information that can be made available. The system should show what is important so the information at the various hierarchical layers can be digested for quick understanding.

Fault Handling

Going hand-in-hand with health and status monitoring is the handling of various fault conditions that can arise during system operation. Not only should a management system be able to collect system information, it should also be capable of interpreting the data in order to ascertain when an anomaly has occurred or the system needs attention. When these events are observed, the management system should, at a minimum, display the error condition in its monitoring displays. Such detected anomalies could be included in a critical system monitor display that shows the most crucial run-time status information for a system. Depending on the system type and possible error conditions, the management system can also have the capability to automatically take an appropriate action (i.e. issue control commands that will correct the fault, or reconfigure portions of the network to allow continued operations in spite of the failure).

SYSTEM MANAGEMENT APPROACH

SwRI has demonstrated the capability to create a network-based data acquisition and telemetry system for the testing and evaluation of aircraft. SwRI has worked as the system integrator on a multi-vendor project that designed and developed a vehicle network to collect data from various data acquisition units (DAUs), distribute the collected data to solid state recording devices and analysis systems, and telemeter data to a ground network. The system records all acquired data and provides for the dynamic data selection of data of interest for analysis. An analogous data acquisition and telemetry architecture is being developed in the emerging integrated Network-Enhanced Telemetry (iNET) program, which will also provide network links to the ground station and develop architectural standards for network-based flight test. Our experience in integrating and managing network-based flight test systems provides a unique perspective for how best to manage these systems. What we have learned is that in order to make the coordinated management of large-scale flight test systems feasible, a holistic approach is required.

Figure 1 shows a representative layout of a medium scale test article network that is part of a flight test system. A centralized application, the "system manager," performs system management and discovers, configures, controls, and monitors the devices on the test article. The application utilizes TCP/IP broadcast ping and SNMP interfaces in these tasks. The "system status display" is an application that provides user interfaces for viewing test data and status information as well as for configuring and controlling the network system. The test data collected from the DAU devices is transported across the network and captured by the recorder. A subset of the data is encrypted and telemetered to a ground station.

Figure 2 shows an abstract view of the types of services that run on the system manager. The "Network Discovery Service" identifies devices attached to the test network and determines their type, configuration, and function in the test being performed. The "Multicast Configuration Service" executes the constraint balancing algorithm and allocates multicast addresses to the data streams. The IEEE 1588 "Time Sync Service" synchronizes the System Manager with network time. The "Network Configuration Service" configures the network devices, as well as the DAU, solid state recorder, and telemetry devices. The "Status Monitoring Service" collects health and status data from the various devices, manages faults in the system, and reports the overall status of the system.

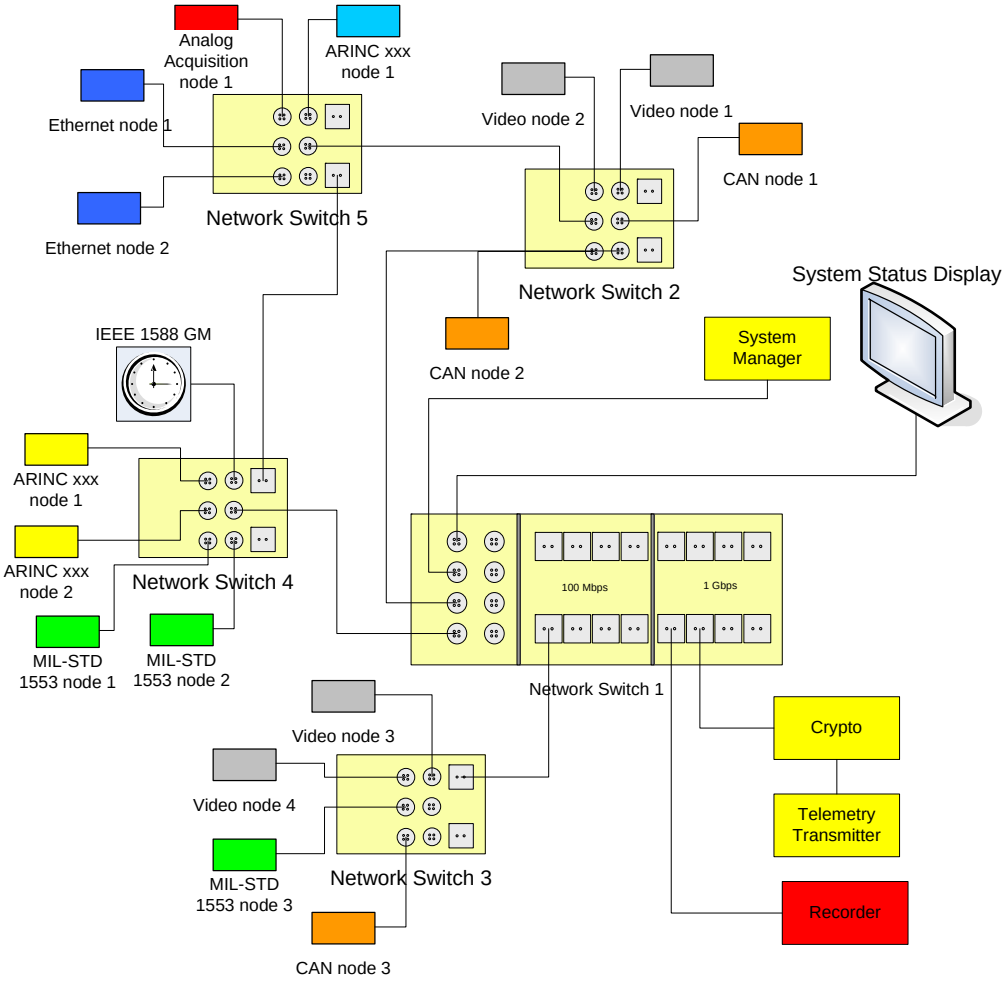

Figure 1: Management View of a Test Article Network

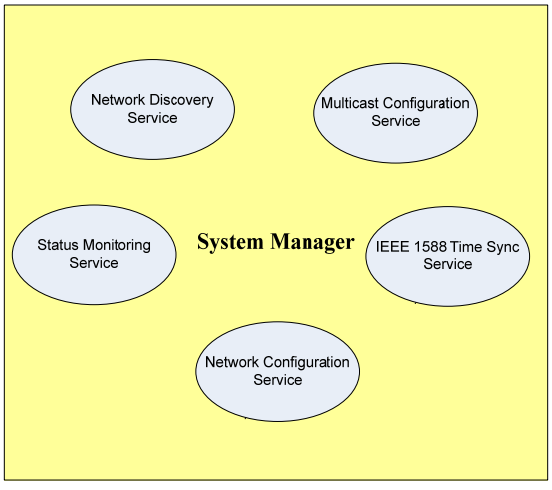

Figure 2: Services Required for System Manager

In order to implement the integrated and holistic system management approach described, there are many factors that must be addressed. To make it economically feasible and viable over the long-term, standard interfaces to devices and a common metadata language are required. To be successful, it is important for the flight test organization and the various vendors to work together to develop standards appropriate for the application, and our experience has shown this can be done. In the broader military flight test world, developing standards for interfaces and metadata languages may be challenging, but we believe it is absolutely critical to the successful deployment of networking into military flight test.

CONCLUSIONS

Network-based technology is the future for flight test systems. Both wired and wireless networks will become commonplace in commercial and military flight test. Management of network-based flight test systems requires more than simply configuring the network devices such as switches and wireless modems. The complexity of these systems requires an integrated approach toward system management that includes the network devices and the end-node devices that acquire, record, and analyze data. If the large-scale deployment of networking technologies is to be cost effective and feasible across the variety of flight test applications, an integrated approach toward management is needed. This approach must include standards for device interfaces and test configuration information, as well as common applications that can be used for configuration, control, and monitoring of the system as a whole. We have described some of the technical issues that we have addressed in prior efforts, as well as some that are yet to be addressed, and have recommended a path forward that will include an effort to develop standards and common applications for network-based flight test system management. We are currently active in the network-based flight test environment, and plan to continue supporting this industry by aiding the development of architectural standards, developing system management applications, and by integrating flight test systems.