White Paper

Data Loading Cabin Autonomous Systems

(a work in progress for discussion at the CASSI Team Meeting Tuesday, 24 October 2023)

Steven H. Rines

Safran Cabins

[Steven.rines@engenui.com](mailto:Steven.rines@engenui.com)

Ph: +1 (714) 592-9359

CSMIM assumes that cabin network equipment will be installed and commissioned (configured) by the aircraft integrator. The cabin network commissioning process defines the network architecture and centralized network services. During the commissioning process, IP address, hardware identifier, manufacturer, and installation position are assigned for each equipment. Following successful CSMIM cabin network commissioning, network services are available to administer network membership when equipment is replaced. Thereafter, ARINC 615A can be used to accomplish cabin network equipment data loads. CSMIM does not address how ARINC 615A will be used to data load and configure wireless devices on equipment replacement.

CASSI systems are designed to operate autonomously. Autonomous systems require no specific commissioning or other administrative involvement by an aircraft network integrator/administrator during installation. The data load process for autonomous systems should be accomplished by airline maintenance personnel with no specific knowledge of network architecture or security model.

From an airline maintenance perspective, the ideal solution would be for CASSI systems to be data loadable in compliance with ARINC 615A.

This paper addresses the requirements unique to data loading autonomous aircraft systems, proposes an autonomous system approach to satisfy those requirements, documents necessary modifications to the ARINC 615A and ARINC 665 standards and defines the maintenance process steps to enable data loading autonomous aircraft systems and equipment connected to a shared network, independent of network media type.

## ARINC 615A Overview

ARINC 615A is a well-developed, universal solution to onboard data load of avionics and cabin systems.

ARINC 615A defines a data loader as a file server that can be accessed by target equipment via TFTP and UDP. Each equipment is responsible for its own data load, constrained by WoW and Maintenance discrete inputs and a maintenance procedure followed by a trusted actor (maintenance technician) to initiate the data load process.

ARINC 615A utilizes network addressing and specific features of Internet Protocol version 4 (IPv4). ARINC 615A does not any recognize IPv6-specific features.

ARINC 615A assumes each data loadable equipment has a preassigned IPv4 address, typically established by wired mounting location, position hardware discretes or by programming in advance of installation.

ARINC 615A documents a FIND function that the data loader application uses to locate data loader TFTP hosts and clients on the shared network. The FIND function should be executed at least once at the beginning of a data load session. The FIND function registers all available data load TFTP hosts. The data loader application presents the list of registered hosts and clients to the data load operator for selection. The FIND registration process captures the MAC address, the IP address and the identity and functional characteristics of each data load host.

Multiple data loader applications may be accessible on the aircraft network and respond to a FIND request. Multiple target equipments can use the data loader application simultaneously.

The data loader application presents the operator of the data loader with the information necessary to select an available target equipment and an appropriate data load package with which to initiate the data load process.

The ARINC 615A data load process identifies the correct package to data load to a target equipment by MAC address, IP address, hardware identifier, manufacturer, and position in the aircraft. The data structures and parameters for these parameters are documented in ARINC 665.

Target equipment typically utilizes port 59 for data load, although an alternate port (>49152) may be optionally assigned by the ARINC 615A data load protocol to simplify data loading multiple equipments simultaneously.

If any step in the ARINC 615A data load process is interrupted, both the data loader and the target equipment are required to return to a known good state.

ARINC 615A defines file size and (optional) CRC to verify file integrity. ARINC 615A contains no specific methods to cryptographically protect data during the process of data load. However, files to be data loaded to a target equipment may be encrypted in advance for protection during delivery and storage.

## CASSI Data Load Background

When an autonomous system is initially installed in an aircraft, it has no reference as to where its local address(es) fit within the aircraft network’s address space. In fact, a shared network is an autonomous system. Installation of an autonomous system on an aircraft may be the event that initially installs a shared network.

Data load of CASSI systems onboard must be accomplished without knowledge of the network architecture since the network architecture and security boundaries will be established by data loading software and configuration data to network switches and routers.

The media of the shared aircraft network is undefined. Autonomous systems may be data loaded and configured over either wired or wireless shared networks.

RTCA DO-402/EUROCAE ED-319 defines the hardware requirements for a Secure Computing Platform (SCP) that is capable of being configured as part of a NIST SP.800-207-compliant Zero Trust Architecture.

The ARINC 856 CASSI standard defines the interoperability requirements that enable secure communications between CASSI autonomous systems compliant with NIST SP.800-207 and the above derived requirements.

The security model defined in DO-402/ED-319 and expanded in ARINC 856 utilizes specific features of Internet Protocol version 6 (IPv6) to facilitate secure intersystem communications.

A CASSI system may be a network architectural component (switch, router, bridge, server, etc.), a network subnet, or an autonomous system. Every CASSI system has an SCP as its secure network interface to a shared network. A CASSI system may be data loaded with software and internal configuration provided by the system integrator, or data loaded with network interconnection tables provided by the aircraft integrator.

Consistent with the Zero Trust model, each autonomous system is responsible for maintaining its own security boundary, including external interaction during the data load/configuration process.

A CASSI system could be a system of systems with a single interface to the shared network. To maintain its autonomy and security boundary, the target system must accept responsibility for data loading and managing the configuration of its internal subsystems.

Autonomous system installation and data load depends on the presence of a shared network from which the system can be data loaded. When no shared network initially exists on the aircraft, a minimal shared network could potentially be established by the interconnection of a data loader with the target equipment.

A (potentially wireless) data loader process for autonomous systems must mitigate the security vulnerabilities identified in Appendix A of RTCA DO-402/EUROCAE ED-319 Wireless Avionics Intra-system Communications (WAIC) MOPS.

To enable an autonomous system to interact with an A615A data loader, the autonomous system must be capable of communicating with the A615A data loader using IPv4.

* An empty SCP at the edge of the autonomous system has no predefined shared network address or mounting location. An IPv4-compliant DHCP service is required to provide an address to the target SCP to enable data loading.
* The DHCP service should only be active on-ground and in maintenance mode while under the direct control of a trusted actor.
* The DHCP address pool must not conflict with any existing aircraft addresses.
* To get an IP address, an SCP must broadcast a DHCPDISCOVER message using UDP. This requires use of port 68.
* DHCP options include the ability to authenticate. How can we use this to satisfy DR06?
  + The SCP is responsible for protecting itself, therefore the SCP must authenticate the DHCP service, not vice versa.
  + DHCP Options could be used to define the CASSI Pre-Loader service as the only valid connection for an SCP with a DHCP-assigned IP address.
  + Attestation could be used to enable SCP connection to the CASSI Pre-Loader service.
* Since the CASSI Pre-Loader application is a precursor to connection to A615A, the pre-loader will have to communicate with the SCP using its allocated IPv4 address.
* The CASSI Pre-Loader application enables the trusted actor to define the SCP’s IPv6 address and mounting location.
  + As part of the pre-loader function, the SCP mounting location defined by the trusted actor must be stored in the SCP for use in normal operation. The SCP mounting location will also be used during the A615A data load process.
  + The SCP IPv6 address defined by the trusted actor must be stored in the SCP for normal operation. The DHCP IPv4 address assigned to the SCP will be used throughout the CASSI pre-loader and A615A data load processes.

An autonomous system accepts only IPv6 traffic during normal operation. Only after data loading is an SCP capable of determining on-ground and Maintenance Mode states (using received Aircraft Parameters).

The CASSI pre-loader description below needs to be revisited. As written, the pre-loader assigns an IPv6 address to the SCP. It is therefore not compatible with an A615A data loader.

CASSI Pre-loader

ARINC 615A could conceptually work to data load CASSI systems if methods existed to make CASSI systems compliant with existing ARINC 615A minimum network and security requirements.

When a CASSI system is installed on an aircraft, that system must have a global IP address assigned before it can be accessible to other network entities such as a data loader.

Multiple CASSI systems could be installed on an aircraft, each with identical equipment part numbers, that will differ in functionality based on the software data loaded into them. Aircraft mounting location is used to differentiate one identical system from another for the purpose of data loading. In some implementations, a system’s mounting location may be defined by analog system discretes, but this cannot be assumed for a generic solution.

The purpose of the CASSI pre-loader application is to inform an autonomous target system of

1. its assigned global IP address within the architecture of an aircraft shared network,
2. its aircraft mounting location,
3. the address of the data loader application.

Data load depends on active initiation, control, and verification of the data load process by a trusted actor [DR8]. Aircraft parameters used by autonomous systems to inhibit data load functionality during aircraft operations may in some systems be accessible via analog discretes, but, as a generic implementation, such discretes cannot be assumed to be available to the target system during data load.

Describe how the DR8 requirement for on-ground/maintenance mode will be addressed.

If the trusted actor initiates a data load sequence from the data loader interface, then the target can accept that we are in a correct aircraft state to initiate data loading. My concern is: What happens if the aircraft state changes during the data load process?

Would it be good enough for the target to use a timeout to trigger aborting the TFTP data load?

If not, consider using a CASSI pre-load wrapper that encapsulates the ARINC 615A application in the data loader. That wrapper provides a WoW/Maint heartbeat to the target SCP. If the heartbeat stops then the target SCP knows that the data load process must be aborted.

A CASSI system can only establish a trust relationship with another CASSI-compliant system. Therefore, a data loader application intended for data loading CASSI systems must be hosted on an SCP. (Most laptops and servers manufactured since 2015 can comply with this minimum requirement.) The SCP hosting the data loader application may be part of the installed equipment complement or a portable device.

The CASSI pre-loader application should be installed on the same SCP as the data loader application.

CASSI IP Address Allocation

Assigning a global IP address to a target system is a necessary first step to enable data loading using an ARINC 615A data loader.

A newly installed autonomous system may have pre-defined local internal addresses, but it has no global IP address. The CASSI pre-loader application on the data loader SCP can only communicate with a newly installed autonomous system after the new system has been assigned a global IP address. The typical method to assign a global IP address to a system attempting to become a member of the network is to use the Dynamic Host Configuration Protocol (DHCP).

If the CASSI Aircraft Parameters service is functioning, then the CASSI pre-loader application has Weight-on-Wheels and Maintenance discretes available to verify the aircraft operation state. Otherwise, the maintenance operator (trusted actor) must confirm that the aircraft is on the ground and in maintenance mode prior to launching the CASSI pre-loader application [DR8].

Aircraft shared networks use only fixed predefined IP addresses for communications between systems. The use of DHCP on an aircraft shared network is only appropriate to initially assign an IP address to a newly installed system while under active control by a trusted actor, having first verified that the aircraft is on ground and in maintenance mode [DR8].

Autonomous systems use only IPv6, therefore RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6) should be used for IP address assignment to autonomous systems.

The DHCPv6 service should be hosted on the same SCP as the data loader application, launched from within the CASSI pre-loader application.

The DHCPv6 server should only be enabled by the CASSI pre-loader application following installation or replacement of an autonomous system.

When a newly installed target system first powers up it must first request a temporary IP address to enable communications with the CASSI pre-loader application. The DHCPv6 server allocates a temporary IP address to the target system in the following manner:

The target system sends a UDP Solicit message to the All\_DHCP\_Relay\_Agents\_and\_Servers (link local address FFE0: …) to locate an available DHCPv6 server. The DHCPv6 server responds with an Advertise message to provide its IP address to the target system. The target system then sends a Request message to the server asking for an IP address and other configuration information. The DHCPv6 server responds to the target system with a Reply message that contains its assigned temporary address and configuration.

The temporary IP address assigned by the DHCPv6 server will only be used by the target system to communicate with the CASSI pre-loader application. Once the CASSI pre-loader application has successfully allocated a fixed system IP address to the target system, the CASSI pre-loader application should discontinue the DHCPv6 service. The DHCP server should deny any Renew request from a target system.

Secure Pre-loader Communications

Communications between the target system and the CASSI pre-loader application must be secured to enable both the target system and the pre-loader application to autonomously maintain their security boundaries. Trust must be established before secure communications can be initiated. Trust between the target system and the pre-loader application is achieved through mutual attestation.

Describe the attestation process that occurs to establish 1) trust and 2) secure communications between target system and pre-loader application. The attestation process should verify the TPM AIK, SCP manufacturer, hardware part number and data load software part number, as well as the EVIM.

CASSI Pre-loader Address Allocation

There will likely be multiple identical SCPs attached to the network. The only way to differentiate one SCP from another and determine the correct IP address of the target system is by its mounting location. The CASSI pre-loader application assigns an IP address to the target system based on the unique identity of the target system’s SCP in combination with that SCP’s unique aircraft mounting location.

Describe mutual attestation here for CASSI pre-loader and target SCP before allowing mounting location and IP address to be assigned.

The CASSI pre-loader application references a table of the systems attached to the shared network on a given aircraft. That table, supplied by the aircraft integrator, must be installed in the data loader prior to use of the CASSI pre-loader application. That table defines the IP address and aircraft mounting location of each system’s SCP network interface, and the EVIM of the SCP.

A newly installed SCP may power up with no mounting location defined. The aircraft mounting location of the target system’s SCP must be designated by the trusted actor performing the installation before the target system’s assigned IPv6 address can be determined by CASSI pre-loader process.

At the end of the CASSI pre-loader sequence, the target system’s mounting location and its global IPv6 address should be saved on the target system so the target system is aware of its location and global address when it powers up.

The target system would be capable of being data loaded and configured using the ARINC 615A data loader after completing the CASSI Pre-loader process –except that the target system has no way to determine if the aircraft is in an operational state in which data load is allowed (e.g., on the ground and in maintenance mode).

At this point in the autonomous system installation, the aircraft is still not in a known good state. While an IP address and a mounting location have been allocated, the target system has not yet been data loaded with the software or the ACLs necessary to enable the system to become an active member of a shared network.

The aircraft operational state was verified by the maintenance operator at the launch of the CASSI pre-loader application. The target system installation and configuration process, managed by the CASSI pre-loader, is still under active control of the maintenance operator. Launching the ARINC 615A data load process on the target system as a final step from within the CASSI pre-loader application confirms to the target system that the aircraft is still in maintenance mode in the absence of other system inputs. Thereafter, the CASSI pre-loader application can be terminated as the data load process will be monitored on the ARINC 615A user interface.

A screenshot of a computer

Description automatically generated

Autonomous system Data Load Sequence

Autonomous systems have no specific sequence in which they are configured, and data loaded. However, during a multi-system installation, some systems may not have access to the data loader SCP until the network architecture has been defined. In this case, it will be necessary to first configure and data load switches, routers and gateways that define the architecture and security boundary of the shared network.

If an onboard data loader is to be attached to the shared network, then, logically, the SCP hosting the data loader function and the aircraft data load packages should be data loaded next to eliminate the necessity for a portable data loader to complete the aircraft configuration sequence.

The Aircraft Parameter service offers common avionics parameters, including aircraft operational state which autonomous systems use to control system behaviors. The autonomous system that offers the Aircraft Parameter Service should be configured and data loaded early in a multi-system installation sequence to limit the number of faults reported as newly installed systems are powered up.

Hierarchical Data Load

Each autonomous system is responsible for managing its internal configuration. An SCP acting as a Gateway for an autonomous subnet is responsible for the configuration and potential data load of every component attached to that subnet. The data load package for an autonomous system should include the data load packages for all internal system components, such that, once data loaded, each autonomous system has all the necessary software and data elements necessary to independently establish and verify its own internal architecture, security boundary and internal communications.

A system will consist of one or more SCPs. In a system with multiple SCPs, the SCP that hosts the system DLA and local data load repository will be the first SCP data loaded and initialized. Thereafter, when other system SCPs send a UDP Solicit message to the All\_DHCP\_Relay\_Agents\_and\_Servers, the system DLA will respond to as a host and provide data load packages to requesting SCPs from its local data load package repository under control of a trusted actor.

The CASSI pre-loader application and ARINC 615A data loader may be useful methodologies for autonomous systems to use to configure and data load their internal components. However, autonomous systems may encapsulate unique architectures, technologies and network media that do not lend themselves to standardized methods for internal configuration. The appropriate manner for data loading, configuring, and managing internal components of an autonomous system will be determined by the system integrator.

We will have to evaluate and address three use cases for data load: 1) an empty SCP that requires an ISO image to set-up its OS, Hypervisor and Endpoints including the Gateway, followed by ACLs to establish network membership; 2) a pre-configured system that only needs ACLs loaded to the Gateway to establish membership on the shared network, and 3) a previous installed and configured autonomous system that requires update.

Keep in mind that the data load method could also be replicated internally to an autonomous system to data load and configure components of the autonomous system. Doing so would make a common model for installing and configuring components whether inside an autonomous system or attached directly to the shared network. (This process might even provide a solution to CSMIM’s current need to commission the cabin network.)

All traffic received via DHCP must be directed to its ARINC 615A data load port (59), at least until its Gateway ACLs have been data loaded. (ACLs are required to define where the installed system’s IP address range fits in the shared network’s global address map.)

How do we force the SCP back to its empty state for retry if the data load process breaks?

Each autonomous system is responsible for configuring and managing its internal network and components.

The Core CASSI secure network interface utilizes pre-established mutual trust relationships between Endpoints. Source and destination information used for messages exchanges between trusted Endpoints is stored in the path and defined in ACLs of the Gateway Endpoint on each SCP.

When an SCP is first installed on aircraft, it has no path or routing tables.

An installed SCP that has previously been data loaded is required to protect itself from modification during normal operation. The SCP requires access to WoW and Maintenance discrete messages with which to enable or disable its interaction with the data loader application. From this we can derive a requirement for an aircraft parameter service that generates WoW and Maintenance discrete messages.

An empty SCP has no OS, Hypervisor, Gateway or other applications. When a newly installed SCP is powered up, it should execute its secure boot process, perform UEFI on inbuilt device firmware, verify overall platform integrity and then launch its data load client application.

The types of data load differ, depending on what is being data loaded. 1) A data load to an empty SCP is a transfer of the ISO image of the OS, Hypervisor, and all the applications running in all the SCP’s Endpoint VMs. 2) A data load to or from a VM is information specifically associated with the application within that VM.

Data loading an empty SCP with an ISO image creates an operational computing platform in the configuration defined by the system integrator. After an SCP has initially been data loaded, it still lacks the IP addresses defined by the aircraft integrator to become a member of the shared network and enable external communications. The system as configured can communicate internally, but no IP traffic or communications is allowed across its shared network boundary.

All Endpoints require Access Control Lists that enable their Secure Messaging Clients to associate accessible parameters with incoming and outgoing messages.

Access Control Lists defined by the system integrator specify which Endpoints in a system are allowed to exchange information with other Endpoints within the system.

Access Control Lists defined by the aircraft integrator specify which Endpoints in a system are allowed to exchange information with Endpoints in other systems.

After an SCP has been data loaded with its ISO image, its Gateway ACL includes network paths to internal Endpoints authorized for internal and external communications, however, the entries in the Gateway ACL still lack IP addresses for external Endpoints.

An SCP Gateway controls all the traffic in or out of a system. The Gateway’s router and firewall functions reside within the Gateway Endpoint. ACLs used by an SCP’s Gateway functions are only valid and accessible within the scope of the Gateway Endpoint.

Every Endpoint has a CASID entry that defines its exposed input and output interfaces. The CASID entry for an SCP (the secure network interface for a system) documents which parameters from which Endpoints are accessible externally via its shared network interface. The aircraft network integrator defines ACLs by linking source parameters from Endpoint CASID entries exposed in the CASID entry for a system with corresponding destination parameters from Endpoint CASID entries exposed in the CASID entries of other systems.

Make sure there is a common process for generating and data loading ACLs to Endpoints for both system and aircraft integrators.

But how do the external ACLs get loaded into individual Endpoints?

Two problems (at least) need to be addressed to data load individual VMs:

1) The VMs lack knowledge of aircraft operational state with which to control/inhibit data load; 2) the VMs lack external access to the shared network to initiate interaction with the data loader.

Second problem first: Data loading ACLs to the SCP’s Gateway manager Endpoint would open a network path from the data loader function of each SCP internal Endpoint to an ARINC 665 data loader on the shared network.

* That is not really a solution since we have not defined how Gateway ACLs get data loaded. There should be only one Endpoint data load process for any sort of Endpoint.

Data loads for all SCP Endpoints could be done as single Data Load to the SCP Gateway Manager. In this case, after downloading the SCP’s combined data load package, the Gateway Manager would become the data loader for all SCP Endpoints.

* This is not really a solution either since it doesn’t define how the first step (data loading the SCP combined data load package to the Gateway) would be accomplished.

Using the Gateway to distribute data loads to internal Endpoints is probably the faster and more robust approach for getting a system up and running. On the other hand, some Endpoints will likely need content uploaded or downloaded outside of the installation/configuration process, which would not work well with a combined data load managed by the aircraft integrator.

About a page back, I stated that the SCP’s IP address and mounting location had to be stored on the SCP before rebooting to initiate the data load sequence. Where exactly were the SCP global IP address and mounting location stored? The Gateway Endpoint does not exist yet since there is no OS or Hypervisor installed.

The reason I ask is that we could transfer additional information to the SCP when we load the IP address and mounting location to facilitate making Endpoints data loadable. I do not yet know what that info might be.

If we passed an IP range to the SCP rather than just a single IP address, then we might be able to allocate a local system address or a pointer that every Endpoint would know to use for the local data loading function...

Should the SCP’s IP address and mounting location be stored in NVM in the TEE? If so, then another option might be for each Endpoint to retrieve the local data loader Endpoint’s address from the TEE.

16 August 2023 – We have defined a way to data load an ISO image to an SCP. That image will include OS, Hypervisor and some number of Endpoints. The data load image for each Endpoint will include its Access Control Lists (ACLs) that define the internal network architecture and the Endpoints that are allowed to communicate with each other.

One of the Endpoints data loaded as part of the ISO image hosts the system local version of the data loader application (DLA). The ACL for each Endpoint that was part of the data loaded ISO image includes the network path to the system’s data loader Endpoint. After an SCP’s ISO image has been successfully data loaded, control of data load functionality is passed to the system DLA within its dedicated Endpoint.

The system DLA can access an ARINC 615A data loader as an external service. The system data loader application evaluates an Endpoint’s data load request to determine if it can be satisfied from the local data load package repository or requires external access to a remote data loader.

The local data load repository is part of the ISO image created by the system integrator and reflects only system software and internal ACLs. The local data load repository will be used to data load system components following component replacement.

Aircraft intersystem ACLs are created by the aircraft network integrator. Aircraft intersystem ACLs are aircraft specific, have a different data load package part number, and must therefore be data loaded as a separate process step from a system’s ISO image.

Aircraft intersystem ACLs should be data loaded by the system DLA to its local data load repository to enable the system to locally restore a known good state following equipment replacement.

Following the SCP ISO image data load, an Endpoint recognizes that its ACLs are incomplete and initiates a data load request to the system DLA which delivers the ACLs from the local data load repository.

Endpoint External Data Load

Some Endpoint applications are expected to collect or utilize ephemeral content that is not included in the scope of the system software and configuration packages stored in the local data load repository. Those applications require interaction with an external data loader.

The system DLA maintains the system security boundary with the ARINC 615A data loader. The system DLA is the only Endpoint capable of interaction with an external data loader. Endpoint applications that require interaction with an external data loader do so indirectly, through the system DLA.

The system DLA is a termination Endpoint for end-to-end secure communications with other Endpoints. The system DLA acts as a protocol translator converting between Endpoint secure messages and ARINC 615A protocols to deliver packaged content.

The empty SCP data load function could be functionally partitioned off and retained after the SCP ISO image is loaded. This would provide a method of resetting the SCP to empty SCP functionality.

CASSI data load use cases:

1. SCP requires BIOS (boot loader) update.
2. SCP requires ISO image of OS, Hypervisor plus all VMs and local ACLs to reproduce integrated, as-tested configuration.
3. SCP with as-tested image installed, requires ACLs to enable aircraft-specific external communications.
4. SCP with as-tested image installed and all necessary ACLs, Endpoint requires content transfer in support of intended function.
5. Data loading nested autonomous systems

The ARINC 615A standard implements a different security model than CASSI zero-trust. The only method defined for communicating with an Endpoint application within the zero-trust environment is via its secure messaging client. An Endpoint required to upload or download content via ARINC 615A will have to do so through the system DLA. The local data loader Endpoint treats communications with an ARINC 615A data loader in the same manner as connecting to another network of unknown provenance. The data loader Endpoint is the termination for end-to-end secure messages at the edge of the CASSI security boundary. The data loader Endpoint acts as the Gateway for data loading and is responsible for adhering to the security model defined in ARINC 615A. This architectural model is the same as is used for the protocol translator or a network bridge. The data loader Endpoint utilizes the same NIC as the SCP Gateway Endpoint since the ARINC 615A data loader Endpoint utilizes the same shared network.

[insert picture of Data Loader Endpoint with Gateway parallel connection to NIC here…]

Following CASSI pre-load and ARINC 615A data load of the SCP’s ISO image, the IPv6 address and mounting location uses to data load the SCP must be transferred to the OS.

Data load should be inhibited by the target system except when weight-on-wheels and maintenance mode discretes are both true. WoW and Maintenance Mode discretes may only be available from an Aircraft Parameter Service, which might reside within a system Endpoint, but might only be externally accessible.

Relying on the parameters supplied by the Aircraft Parameter Service to enable or disable data load functionality creates a catch22 when the system hosting the Aircraft Parameter Service fails or that system has not yet been installed.

Finish thought on how to verify flight phase/operating mode without Aircraft Parameter Service…

DR01 Communications over the WAIC network shall include a mechanism to verify identity of the transmitting node.

A615A makes a TFTP server available and identifies target equipment to operator. Each target equipment is responsible for managing its own data load. SDL FIND function broadcasts UDP message requesting target equipments to identify themselves. FIND assumes network IP addressing is predefined.

Target equipment cannot unequivocally discern identity of node broadcasting a UDP message.

Target equipment is responsible for inhibiting data load during normal operation, typically based on analog discretes for weight-on-wheels and maintenance mode.

For off-loading data from target equipment, target equipment makes downloadable files available using TFTP.

A615A makes downloadable files available to target equipment using TFTP.

Trusted actor defines target equipment and direction of data transfer from list created by FIND function.

FIND uses UDP to broadcast. UDP uses port number 1001.

TFTP server uses control port number 59, but port number can be reassigned as part of protocol to support multiple simultaneous data load sessions.

All communications between the SDL function and the target equipment are in the form of either file transfers or an error packet.

DR02 Communications over the WAIC network shall be cryptographically protected to protect against unauthorized nodes intercepting transmitted messages or illicitly transmitting valid messages.

A615A uses the Tiny File Transfer Protocol (TFTP). The contents of the files transferred are undefined. The files transferred could be encrypted to support CASSI security requirements.

Define CASSI data load package requirements here.

A615A FIND function uses (unprotected) UDP messaging to establish target equipment available to data load.

DR03 Communications over the shared network shall provide a mechanism for the receiving node to identify temporally or sequentially relevant (stale) messages.

TFTP includes sequential numbered packets.

DR04 Communications over the shared network shall enable the receiving node to verify the integrity of the communicating node.

A615A does not check the integrity of the target equipment (communicating mode).

Trusted actor selects data load package source and destination.

Target verifies integrity of data load package. (It doesn’t matter how the data load package was routed, only that it is correct for the target and has not been modified in route.)

DR05 The receiving node shall only accept messages that have been verified for authenticity and integrity.

A615A relies on the trusted agent to select which equipment will communicate and to monitor the data load process, based on a fixed IP address scheme for known equipment locations.

A615A TFTP supports SHA-256 to enable receiver to verify that package has not been modified in transit (integrity).

How target can verify sender’s authenticity still needs to be addressed. “Sender” in this case can have multiple meanings: Sender could be the originator of the data load package or the SDL as it regards the UDP FIND request or TFTP error messages.

The originator of the data load package could embed a signed certificate in the DL package to enable authentication by the target with no change to ARINC 615A.

Target initially has no known IP address, no known aircraft mounting location, and has no method to establish if the aircraft operational state is on-ground and in maintenance mode.

An empty target equipment is normally only installed in an aircraft as part of a maintenance action initiated by a trusted actor while the aircraft is in maintenance mode. The aircraft will not be in a known good state until the empty target equipment has been data loaded and verified to be operational.

An empty target requires access to a DHCP server to be allocated a temporary IP address. For an empty target equipment, requesting and being assigned a DHCP address is not, on its own, a vulnerability. One potential exposure is if a malicious actor launches a fake DHCP service that the target responds to when the aircraft is not on the ground and in maintenance mode. Still, the only security impact is that the empty target is assigned a temporary IP address. (What is the risk that a fake DHCP service could repeatedly interact with the target to intentionally use up network bandwidth?)

If, as part of the DHCP IP address assignment, the target is provided the IP address of a CASSI pre-loader application, then the target could use attestation to verify the integrity of the SCP host and the CASSI pre-loader application.

The CASSI pre-loader application will establish secure communications using TLS with the target equipment. The CASSI pre-loader application includes active interaction with a trusted actor to assign an aircraft mounting location to the target equipment. The assignment of an aircraft mounting location also assigns a fixed network IPv6 address to the target equipment.

Once the target receives and stores its location and IPv6 address, the target should continue to use the assigned IPv4 DHCP address for interaction with the A615A data loader.

Can the active participation of the trusted actor in the assignment of the empty target’s location and IP address substitute for the target’s lack of aircraft state info?

DR06 The software/firmware update mechanism for the WAIC node(s) SCP shall incorporate authentication.

See DR05 response above.

DR07 The software/firmware update mechanism for the WAIC node(s) SCP shall incorporate integrity checks.

A615A TFTP supports SHA-256 to enable receiver to verify that package has not been modified in transit (integrity).

DR08 Mechanisms shall be put in to prevent any changes to the WAIC node configuration onboard except under control of a trusted actor, on the ground with aircraft maintenance mode enabled.

A615A FIND function enables trusted actor to select target for data load.

In an operational network, the Aircraft Parameter Service provides WoW and Maintenance Mode discretes. Those parameters are not available to a replaced target equipment until after the target equipment has been data loaded –a Catch-22.

DR09 WAIC equipment shall verify the authenticity of the sending nodes.

See the DR05 response. We can verify the authenticity of the CASSI pre-loader application at the beginning of the installation process. Thereafter, the ARINC 615A process does not need to be authenticated since it is simply part of the package delivery process (untrusted).

DR10: Reliability of wireless is inherently prone to disruption. Intended functions that require specific reliability should consider the use of redundant communications paths.

Not applicable to the data load process.

DR11: It is the responsibility of the integrator to determine if the need for receipt validation is required and incorporate it accordingly.

Not applicable to the data load process.

DR12 Every Endpoint shall report detected security events.

An empty target does not know the IP address of the network security event logging application, so it is unable to report detected security events. The target equipment should internally log security events and report any such events after data load is complete and a trusted relationship has been established with the network security event logging application.