

****



##### Consultative Committee for Space Data Systems (CCSDS) Space Data Link Security (SDLS) Protocol

##### Prototype Implementation and Testing Plan

##### 1.0

##### 11/9/14

**Authors:**

Brandon Bailey

Mark Pitts

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version Number | Author(s) | Revision Date | Reason for Revision |
| 1.0 | Brandon Bailey  Mark Pitts | 11/9/14 | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Reference Documents**

|  |  |
| --- | --- |
| Document Number | Document Name |
| CCSDS 355.0-R-4 2014 | CCSDS. “Space Data Link Security Protocol” |
| -- | NASA/GSFC’s Flight Software  Core Flight System (presentation from FSW Workshop 2012) |
|  |  |

**Table of Contents**

[**1.0** **Introduction** 5](#_Toc403214431)

[1.1 Purpose 5](#_Toc403214432)

[1.2 Scope 5](#_Toc403214433)

[1.2.1 Assumptions 5](#_Toc403214434)

[1.2.2 Constraints 5](#_Toc403214435)

[1.3 Organization 6](#_Toc403214436)

[1.4 SDLS Overview 7](#_Toc403214437)

[2.0 Prototype Overview 7](#_Toc403214438)

[2.1 Cross Platform Security Library 8](#_Toc403214439)

[2.2 Flight Software 9](#_Toc403214440)

[2.3 Ground System 11](#_Toc403214441)

[2.4 SDLS Prototype Data Flow 12](#_Toc403214442)

[**3.0** **Test Overview** 12](#_Toc403214443)

[3.1 Entry/Exit Criteria 12](#_Toc403214444)

[3.1.1 Entry Criteria: 12](#_Toc403214445)

[3.1.2 Exit Criteria: 13](#_Toc403214446)

[3.2 Prototype/Test Schedule 13](#_Toc403214447)

[3.3 Resources 14](#_Toc403214448)

[**4.0** **Test Preparations** 15](#_Toc403214449)

[4.1 Test Configuration 15](#_Toc403214450)

[4.2 Hardware Configuration 15](#_Toc403214451)

[4.3 Software Configuration 16](#_Toc403214452)

[4.4 Test Objectives 16](#_Toc403214453)

[**5.0** **Post Test Activities** 17](#_Toc403214454)

[**APPENDIX A: Acronyms** 18](#_Toc403214455)

1. **Introduction**
   1. Purpose

The Space Data Link Security (SDLS) Protocol is a Consultative Committee for Space Data Systems (CCSDS) standard which extends the known Data Link protocols to secure data being sent over a space link by providing confidentiality and integrity services. This plan outlines the approach by National Aeronautics Space Administration (NASA) in performing testing of the SDLS protocol using a prototype based on an existing NASA mission’s simulator.

* 1. Scope

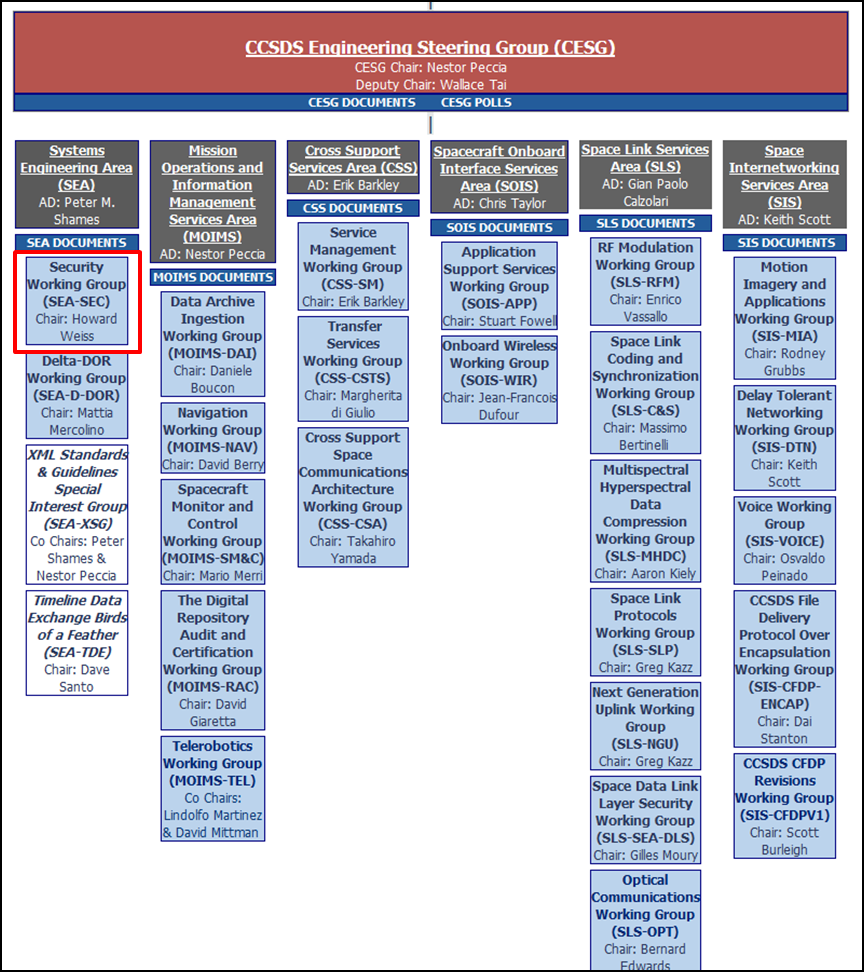
A new standard has been defined by the CCSDS to protect the communications between the ground station and the spacecraft: Space Data Link Security Protocol.

For now, this standard is in draft mode (red book), the scope of the document will outline the implementation plan for the simulation as well as the testing of the SDLS protocol. The main goals are:

* To implement this new protocol
* To validate this new protocol
* To test compatibility of this new protocol in full operational simulator that includes ground station software as well as flight software
  + 1. Assumptions
* Source code from the Global Precipitation Measurement (GPM) mission will be available for use within the test environment
* Source code from the Advanced Spacecraft Integration & System Test Software (ASIST) ground station and the Front End Data System (FEDS) will be available for use within the test environment
  + 1. Constraints
* The simulator being used for the prototype does not use the Advanced Orbiting Systems (AOS) protocol
* Testing and implementation will not include encryption without authentication as mentioned in section 2.3.3 of CCSDS 355.0-R-4 2014
  + - Encryption without authentication can provide a false sense of security and is not recommended
* Implementers and testers are not full-time on task which results in stretched schedule
  1. Organization

The implementation and testing will be performed by a group within NASA’s Independent Verification and Validation (IV&V) Program. The Independent Test Capability (ITC) team will implement the protocol in Flight Software (FSW) and Ground Software (GSW) as well as perform the testing. The ITC team will utilize resources within the Jon McBride Software Testing and Research (JSTAR) Laboratory in Fairmont, West Virginia.

NASA IV&V is Code 180 within the Goddard Space Flight Center (GSFC) organizational structure. Members from NASA’s IV&V Program are currently supporting the Security Working Group (SEA-SEC) and Space Data Link Layer Security Working Group (SLS-SEA-DLS) which falls under the Systems Engineering (SEA) Areas of the CCSDS organization.



**Figure 1-1: CCSDS Technical Organization**

* 1. SDLS Overview

The purpose of the recommended standard is to specify the Space Data Link Security Protocol for CCSDS data links. The SDLS protocol provides a security header and trailer along with associated procedures that may be used with the CCSDS Telemetry, Telecommand, and Advanced Orbiting Systems Space Data Link Protocols to provide a structured method for applying data authentication and/or data confidentiality at the Data Link Layer.

The goals of the recommended standard are to:

* Provide a standard method of applying security at the Data Link Layer, independent of the underlying cryptographic algorithms employed by any particular space mission;
* Preserve compatibility with existing CCSDS Space Data Link Protocol Transfer Frame Header and Trailer formats and frame processing implementations so that, where appropriate, legacy frame processing infrastructure may continue to be used without modification;
* Preserve compatibility with the CCSDS Space Link Extension (SLE) forward and return services; and
* Facilitate the development of common commercial implementations to improve interoperability across agencies.

1. Prototype Overview

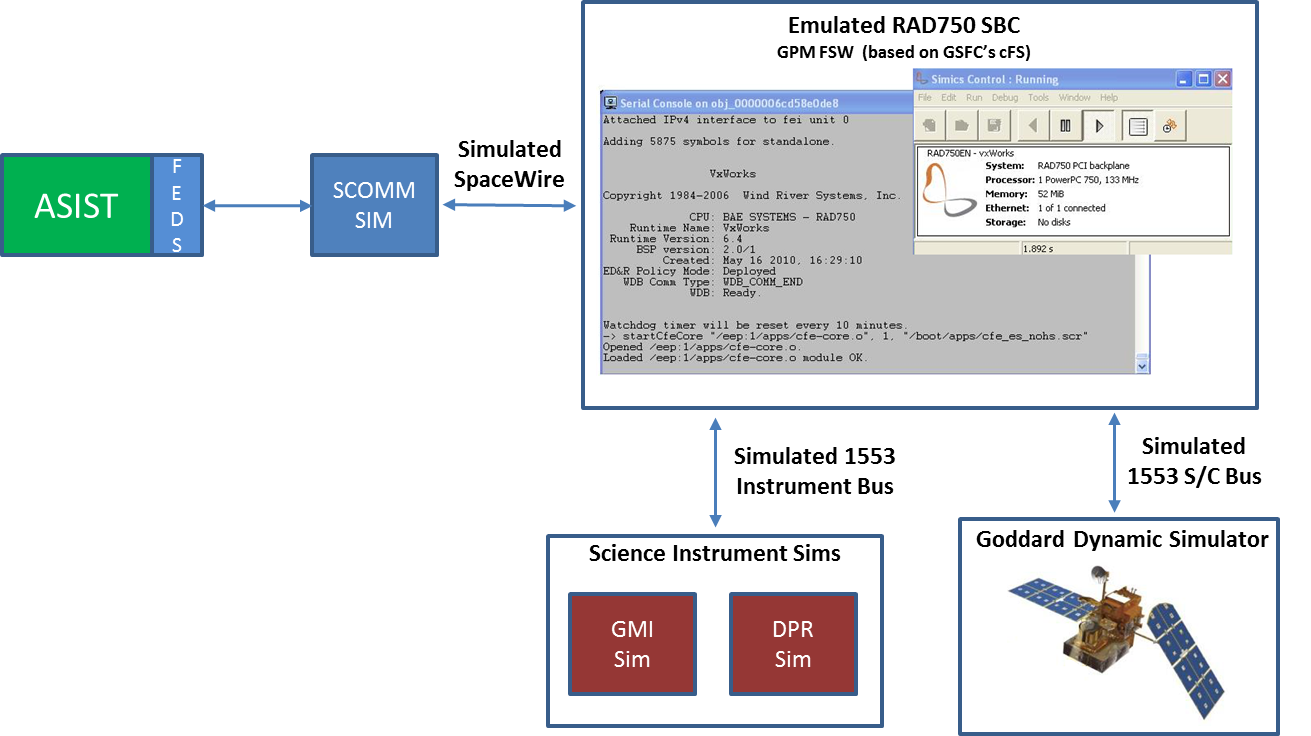
The prototype for testing the SDLS protocol will be developed by the ITC team within the IV&V Program. Limited support will be provided by GSFC’s development organizations: the FSW branch and Ground Systems branch. The approach taken with developing the prototype is to utilize existing NASA operational systems (ASIST, FEDS, and GPM FSW). Using existing systems will provide two benefits: reduction in time to implement (due to software reuse) and applicability after prototype is completed. Upon completion of the prototype, future missions will be able to take the lessons learned from the prototype and apply them to their mission when implementing SDLS.

In order to limit the amount of effort to implement a prototype of the SDLS protocol, the ITC team chose to leverage existing resources/simulations. To support independent testing of the GPM mission, the ITC team developed the GPM Operational Simulator (GO-SIM).

GO-SIM is a pure software based simulator that uses the GPM ground system, ground system command and telemetry databases, emulated RAD750 Single Board Computer (SBC), and unmodified flight software binaries.

GO-SIM is not a wall clock “real time” model. There is no hardware (e.g., SpaceWire, MIL-STD1553) in the loop. The flight software communicates over a simulated SpaceWire network and MIL-STD-1553 busses. Even though events are marked and seem to be running from the model in “real time,” the simulation may run faster or slower (depending on the level of activity) relative to wall clock real time.

Figure 2-1 depicts a system diagram of the GO-SIM architecture.



**Figure 2-1: GO-SIM System Diagram**

The development plan for the SDLS prototype is broken into three different components: a cross-platform security library, GPM FSW modifications, and GSW modifications.

* 1. Cross Platform Security Library

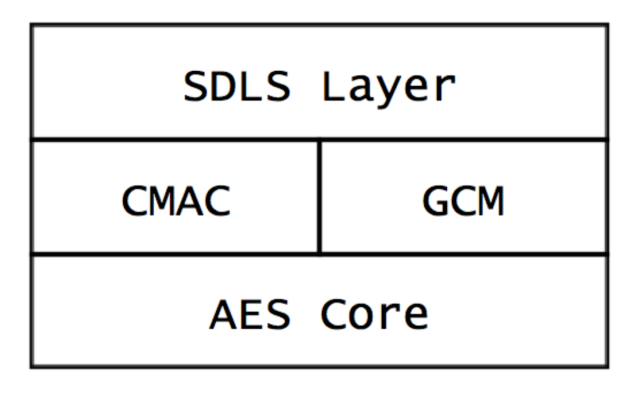
In an effort to reduce code duplication, a simple cross-platform security library will be developed for both use in the ground system and flight software. Due to limited memory on the flight system hardware, the library will be kept as compact as possible.

Based on Annex E of CCSDS 355.0-R-4, Baseline Implementation Mode, the library will support the following capabilities to support the modes for each of the Space Data Link Protocols:

* Advanced Encryption Standard (AES) algorithm
* Cipher-Based Message Authentication Code (CMAC) for authentication
  + Based on AES algorithm with 128-bit keys
  + 32-bit Anti-Replay Sequence Number
  + 128-bit output Message Authentication Code (MAC)
* Galois Counter Mode (GCM) for authenticated encryption
  + Based on AES algorithm with 128-bit keys
  + 96-bit Initialization Vector
  + 128-bit output MAC

The base library will be composed of three layers:

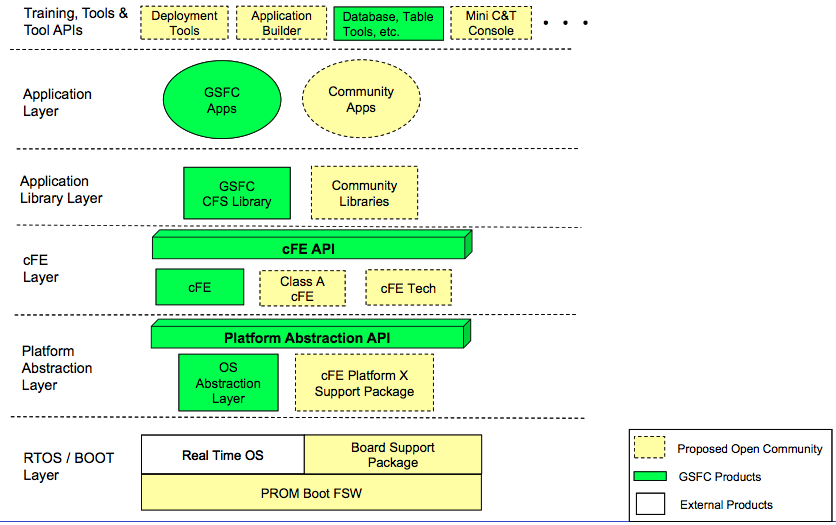
* **AES Core**The AES Core layer will provide the forward and reverse encryption procedures, supporting 128-bit keys
* **CMAC and GCM Layers**
* **SDLS Layer**Contains support for SDLS-related constructs (e.g., Security Association (SA), Authentication Masks)



**Figure 2-2: Security Library Structure**

* 1. Flight Software

The GPM FSW utilizes the Core Flight Software (CFS) framework developed at the NASA Goddard Space Flight Center (GSFC). CFS has a multi-layered architecture that provides abstractions of the operating system and hardware, resulting in a platform-agnostic framework for development. See Figure 2-3 for the CFS architecture.



**Figure 2-3: CFS Architecture**

At the Application Layer, GSFC has developed a set of applications that provide common used services that can be re-used on multiple missions. Of particular interest for the SDLS prototype are the Command Ingest (CI) and Telemetry Output (TO) applications. These two applications contain all the logic related to handling the different Space Data Link Protocols.

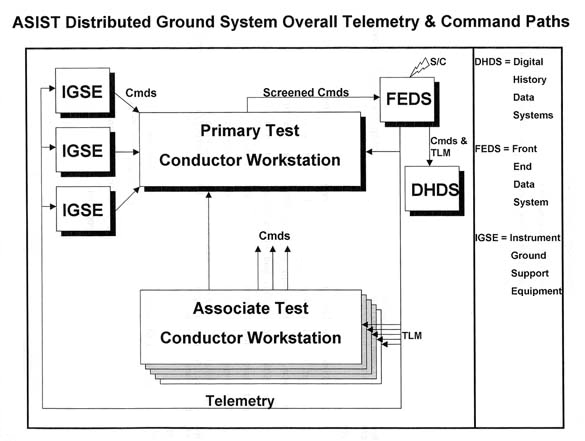
To implement the SDLS Protocol extensions, these two applications will be modified. The security library mentioned in the previous section will be built as a CFS Application Library. This will permit both the CI and TO applications to share the same library, reducing the size of the flight software binaries compared to duplicated code.

Another feature of CFS is the Table Services provided by the core Flight Executive (cFE). The Table Services provide ground operators the ability to update constants/resources used by the flight software during normal operation without the need for patching the software. The Table Services will be used to store configurations for the security associations, namely the cryptographic keys. This will provide the flexibility needed for updating the keys over the operational lifetime of the spacecraft.

* 1. Ground System

The ASIST ground system supports multiple workstations and Instrument Ground Support and Equipment (IGSEs). Spacecraft communications, both uplink and downlink, are channeled through FEDS. The modifications for the SDLS Protocol extensions will be made in the FEDS component, where all of the Data Link Layer logic for the Telecommand (TC) and Telemetry (TM) Protocols is handled.

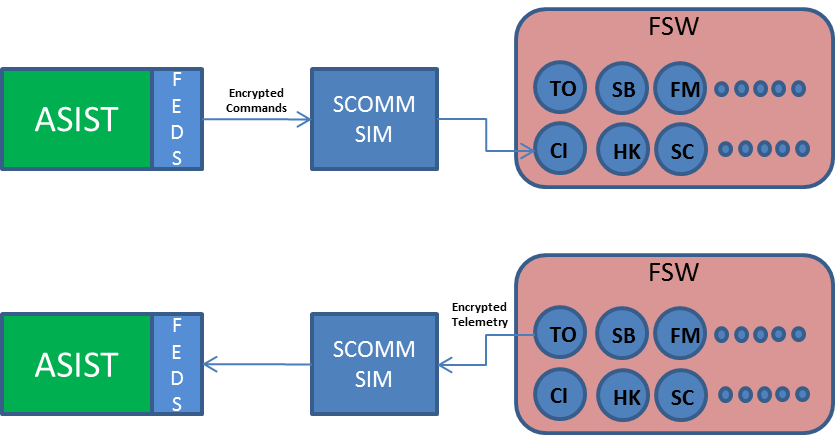
The command and telemetry databases used by ASIST will be augmented to enable configuration of the security services.



**Figure 2-4: ASIST TM/TC Paths**

* 1. SDLS Prototype Data Flow

The data (telemetry and telecommand) will be exchanged through the SLE services in real time. Encrypted telecommands will be sent to the FSW via FEDS and an SCOMM simulator. The incoming data can then be decrypted by the CI application within the FSW. Telemetry, sent from the spacecraft to the ground, functions the same way but in reverse. The TO application within the FSW encrypts the telemetry and downlinks via the SCOMM simulator to FEDS, which is then decrypted by FEDS and passed to the ASIST ground station.



**Figure 2-5: SDLS Data Flow**

1. **Test Overview**

The testing of the SDLS protocol will be performed by members of the ITC team within NASA’s IV&V Program. The tests will be performed within the JSTAR Laboratory in Fairmont, West Virginia

* 1. Entry/Exit Criteria
     1. Entry Criteria:

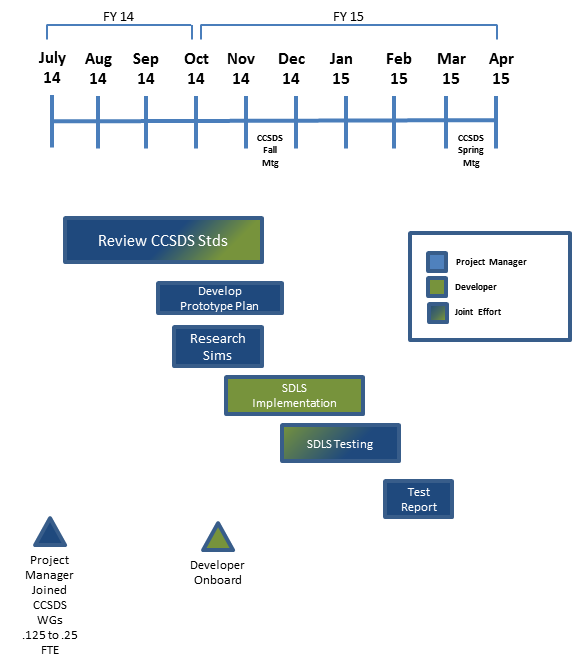
Successful entry into the testing requires the following:

* Review and concurrence of this plan by Security Working Group (SEA-SEC) and Space Data Link Layer Security Working Group (SLS-SEA-DLS) Leads or their designee
* Implementation of SDLS protocol within GO-SIM
  + 1. Exit Criteria:

Successful completion of the testing requires the following:

* All primary test objectives have been completed successfully
  1. Prototype/Test Schedule

Below is a schedule for prototype development and SDLS testing. The beginning part of the project consisted of reviewing several CCSDS standards while developing a plan to implement the protocol in a simulation environment. The later part consists of testing and reporting on the results.



**Figure 3-1: SDLS Implementation/Test Schedule**

* 1. Resources

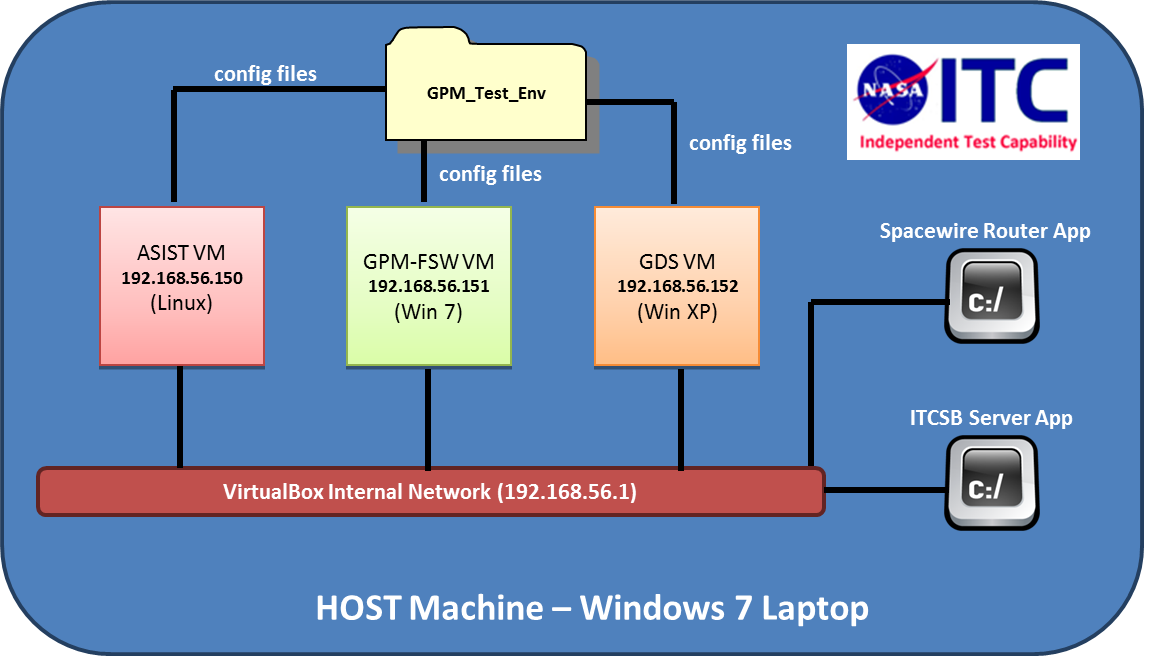
The table below depicts the resources needed to implement and test SDLS as outlined in this plan.

| **Resource Needed** | **Type** | **Details** |
| --- | --- | --- |
| .125 to .25 FTE Project Manager | Personnel | CCSDS document review, oversight, planning, testing, resource management and reporting |
| .25 FTE Developer | Personnel | Developer for SDLS implementation on both ground (ASIST/FEDS) and flight (FSW) |
| .1 FTE SME | Personnel | ASIST/FEDS SME to help with building/implementing ground side of SDLS protocol |
| CCSDS Standards | Documentation | Published as well as draft documents (i.e. SDLS Protocol) will be used |
| JSTAR Laboratory | Hardware | JSTAR lab consists of all the necessary computing resources to implement and test SDLS. Laptops, PCs, virtual servers, etc. |
| GO-SIM 3.7 | Software | Consists of 3 virtual machines with the latest GO-SIM baseline to include ground station (ASIST), flight software (GPM FSW), and Goddard Dynamics Simulator (GDS) |
| ASIST Source Code | Software | Version 9.7.g |
| FEDS Source Code | Software | Version 10.2 |
| GPM FSW | Software | Version 4.7.2 |

**Table 3-1: Resources**

1. **Test Preparations**
   1. Test Configuration

Hardware assets within the JSTAR laboratory will be used for testing. The test configuration is depicted in Figure 4-1.



**Figure 4-1: Test Configuration**

* 1. Hardware Configuration

|  |  |
| --- | --- |
| **Model** | **Specifications** |
| Dell Precision M6700 | * i7-3840QM @ 2.8 GHz (8 cores) * 16 GBs RAM |

**Table 4-1: Hardware Configuration**

* 1. Software Configuration

| **Software Module** | **Comments** |
| --- | --- |
| Windows | * 7 Service Pack 1 (64bit) |
| Virtualbox | * 4.3.12 |
| GO-SIM 3.7 | * Will contain 3.7 baseline with the appropriate modifications to FEDS and FSW. See Table 4-3 for GO-SIM specific version information. |

**Table 4-2: Software Configuration**

| **Software Module** | **Comments** |
| --- | --- |
|  |  |
|  |  |
|  |  |

**Table 4-3: GO-SIM Version Information**

* 1. Test Objectives

See Table 4-4 for the test objectives for SDLS testing using the SDLS prototype.

| **Objectives** | **Auth**  **Only** | **Auth**  **Enc.** |
| --- | --- | --- |
| Confirm a security association can be statically preloaded | X | X |
| Confirm a security association can be dynamically loaded \*\* | X | X |
| Confirm the sequence number is appropriately communicated and incremented during transmission and processing | X | X |
| Confirm if the sequence number verification fails, a failure is detected, communicated, and the transfer frame is not processed by the receiver and the sequence counter does not increment | X | X |
| Confirm the data area of the transfer frames can be encrypted using the AES algorithm using the security association authenticated encryption and entire transfer frame can be communicated |  | X |
| Confirm after receipt of the transfer frame, the data area of the transfer frames can be decrypted using when using the security association authenticated encryption |  | X |
| Confirm that when the Security Parameter Index (SPI) verification fails, a failure is detected, communicated, and the transfer frame is not processed by the receiver and the sequence counter does not increment | X | X |
| Confirm that when the MAC verification fails, a failure is detected, communicated, and the transfer frame is not processed by the receiver and the sequence counter does not increment | X | X |
| Confirm that when the Global Multiplexer Access Point ID (GVCID) verification fails, a failure is detected, communicated, and the transfer frame is not decrypted by the receiver and the sequence counter does not increment | X | X |
| Confirm that when the sequence number rolls over, the cryptographic key is reported as expired and the key can be replaced to resume operations \*\* | X | X |
| Confirm that when the transfer frames between ground and spacecraft are intercepted the data area of the frame is encrypted and cannot be deciphered without the encryption key |  | X |

**Table 4-4: Test Objectives**

\*\* Secondary objective – functionality may not be implemented in prototype but will be implemented if time permits

1. **Post Test Activities**

Post test activities consist of the following:

* Archiving log files and test scripts
* Archiving the updated GO-SIM virtual machines
* Ensuring all code developed is committed to ITC’s SVN server
* Reporting any issues discovered with the CCSDS SDLS standard to the SDLS Working Group Lead
* Generating a final report documenting all results

**APPENDIX A: Acronyms**

The following table provides acronyms relevant to this document.

|  |  |
| --- | --- |
| AES | Advanced Encryption Standard |
| AOS | Advanced Orbiting Systems |
| ASIST | Advanced Spacecraft Integration & System Test Software |
| CCSDS | Consultative Committee for Space Data Systems |
| cFE | Core Flight Executive |
| CFS | Core Flight Software |
| CI | Command Ingest |
| CMAC | Cipher-Based Message Authentication Code |
| FEDS | Front End Data System |
| FSW | Flight Software |
| GCM | Galois Counter Mode |
| GDS | Goddard Dynamics Simulator |
| GMAP\_ID | Global Multiplexer Access Point ID |
| GO-SIM | GPM Operational Simulator |
| GPM | Global Precipitation Measurement |
| GSFC | Goddard Space Flight Center |
| GSW | Ground Software |
| GVCID | Global Virtual Channel ID |
| IGSEs | Instrument Ground Support and Equipment |
| ITC | Independent Test Capability |
| IV&V | Independent Verification and Validation |
| JSTAR | Jon McBride Software Testing and Research |
| MAC | Message Authentication Code |
| NASA | National Aeronautics Space Administration |
| SA | Security Association |
| SBC | Single Board C5 omputer |
| SDLS | Space Data Link Security |
| SEA | Systems Engineering |
| SEA-SEC | Security Working Group |
| SLS-SEA-DLS | Space Data Link Layer Security Working Group |
| SPI | Security Parameter Index |
| TC | Telecommand |
| TM | Telemetry |
| TO | Telemetry Output |
| VC | Virtual Channel |

**Table A-1: Acronyms**