NASA's Plan for SDLS Testing

Presenter(s):

Brandon Bailey

brandon.t.bailey@nasa.gov

304-629-8992

ivv-itc@lists.nasa.gov

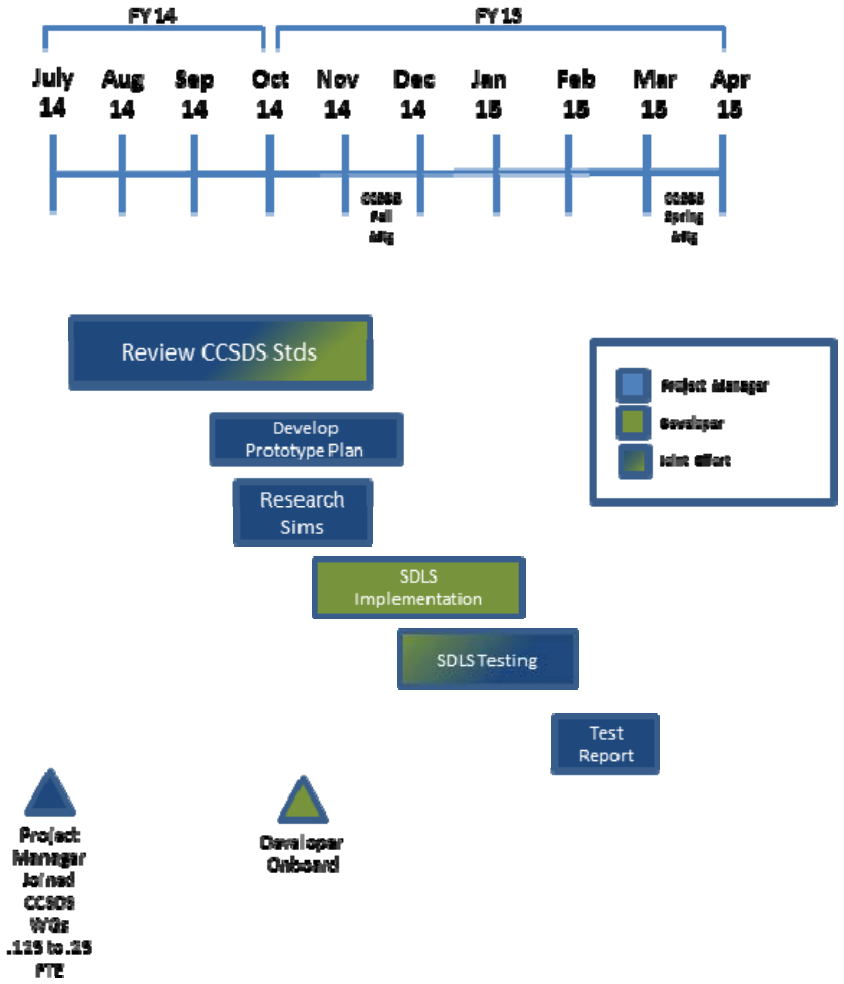
ITC Website: http://www.nasa.gov/centers/ivv/jstar/ITC.html

JSTAR Website: http://www.nasa.gov/centers/ivv/jstar/JSTAR.html

Background

- Joined SEA-SEC Working Group July 2014 at ~.125 FTE
  - Not much experience with CCSDS
  - Spent time learning about CCSDS and SDLS
- Simulation, Testing and Security Background
  - Could perform SDLS testing
- Began developing approach to test SDLS for NASA
  - Complete approach outlined in CCSDS-SDLS-Prototype-Plan document

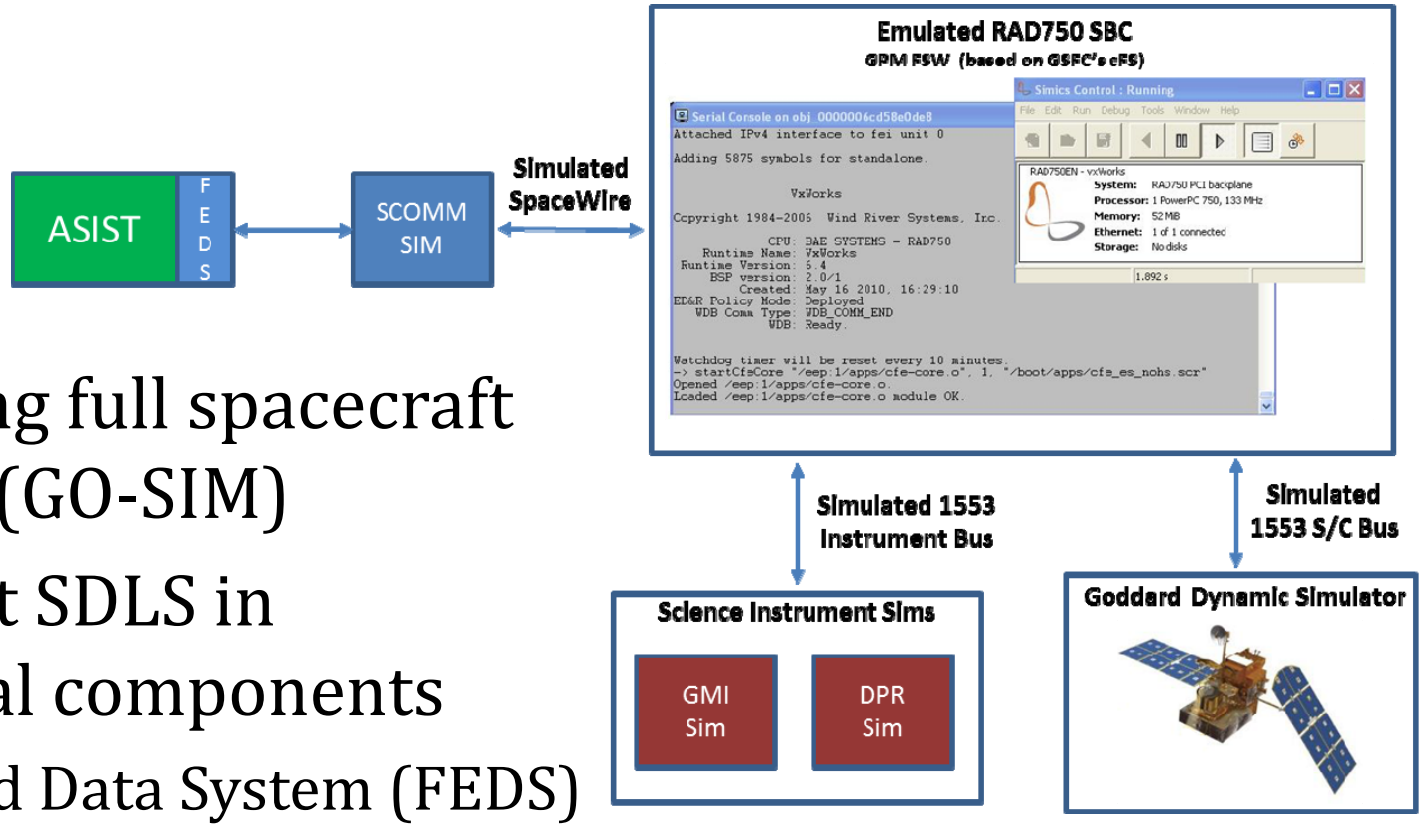
Proposed Schedule



Resources

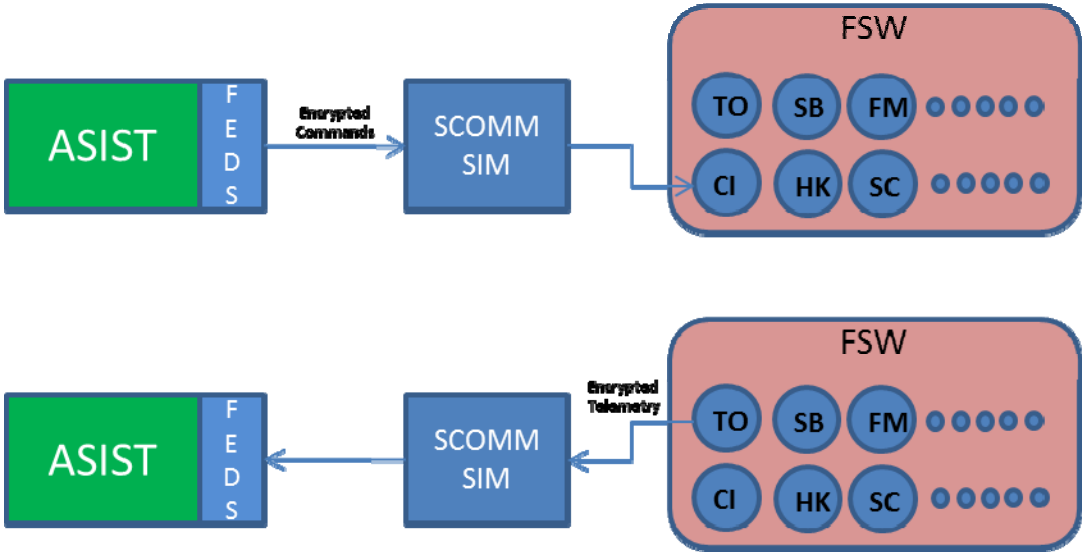
Resource Needed	Type	Details
.125 to .25 FTE Project Manager	Personnel	CCSDS document review, oversight, planning, testing, resource management and reporting
.25 FTE Developer	Personnel	Developer for SDLS implementation on both ground (ASIST/FEDS) and flight (FSW)
.1 FTE SME	Personnel	ASIST/FEDS SME 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

Approach



- Use existing full spacecraft simulator (GO-SIM)
- Implement SDLS in operational components
  - Front End Data System (FEDS)
  - Global Precipitation Measurement (GPM) FSW

Approach (cont.)



The data (telemetry and telecommand) will be exchanged through Telecommand and Advanced Orbiting Systems (AOS) Protocols. 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 and then decrypted by FEDS and passed to the ground station ASIST.

Goals

- To implement the SLDS protocol
- To validate the SDLS protocol
- Perform interoperability testing using AOS Protocol with CNES to complete Yellow Book testing
- To test compatibility of the SDLS protocol in a full operational simulator that includes operational ground software as well as flight software
  - Benefits of using existing NASA operational systems
    - Reduction in time to implement due to software reuse
    - Applicability after prototype is completed
      - Future missions will be able to take the lessons learned from the prototype and apply them to their mission when implementing SDLS (Or even reuse prototype code!)

SLDS Test Objectives

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

Summary

- More detail in document CCSDS-SDLS-Prototype-Plan
  - http://confluence.ivv.nasa.gov:8090/display/IA/SDLS+Prototype+Plan

Backup Slides

NOS Middleware Interception