Safety Pilot Security System

Crash Avoidance II: Connected Vehicles
(Session Code: G201)

W L Fehr

Safety Pilot/Model Deployment

- Safety Pilot/Model Deployment is a U.S. DOT research program conducted by the **RITA** and **NHTSA** with **CAMP** to develop technology that will help cars, trucks, buses, and other vehicles avoid crashes.
- The Program has two parts:
  - □ Six **Safety Pilot Driver Acceptance Clinics** to help the Department learn more about how drivers respond to crash-avoidance applications that use connected vehicle communication. The clinics have been held in locations around the country.
  - □ The **Safety Pilot Model Deployment** that includes the installation of wireless devices in up to 3,000 vehicles in one location to evaluate the effectiveness of connected vehicle technology to prevent crashes. The deployment will take place of Ann Arbor, MI from August, 2012 to August, 2013 and will operate in an everyday environment.
- Both the **Driver Acceptance Clinics** and the **Model Deployment** results will contribute to the NHTSA 2013 Agency Decision.

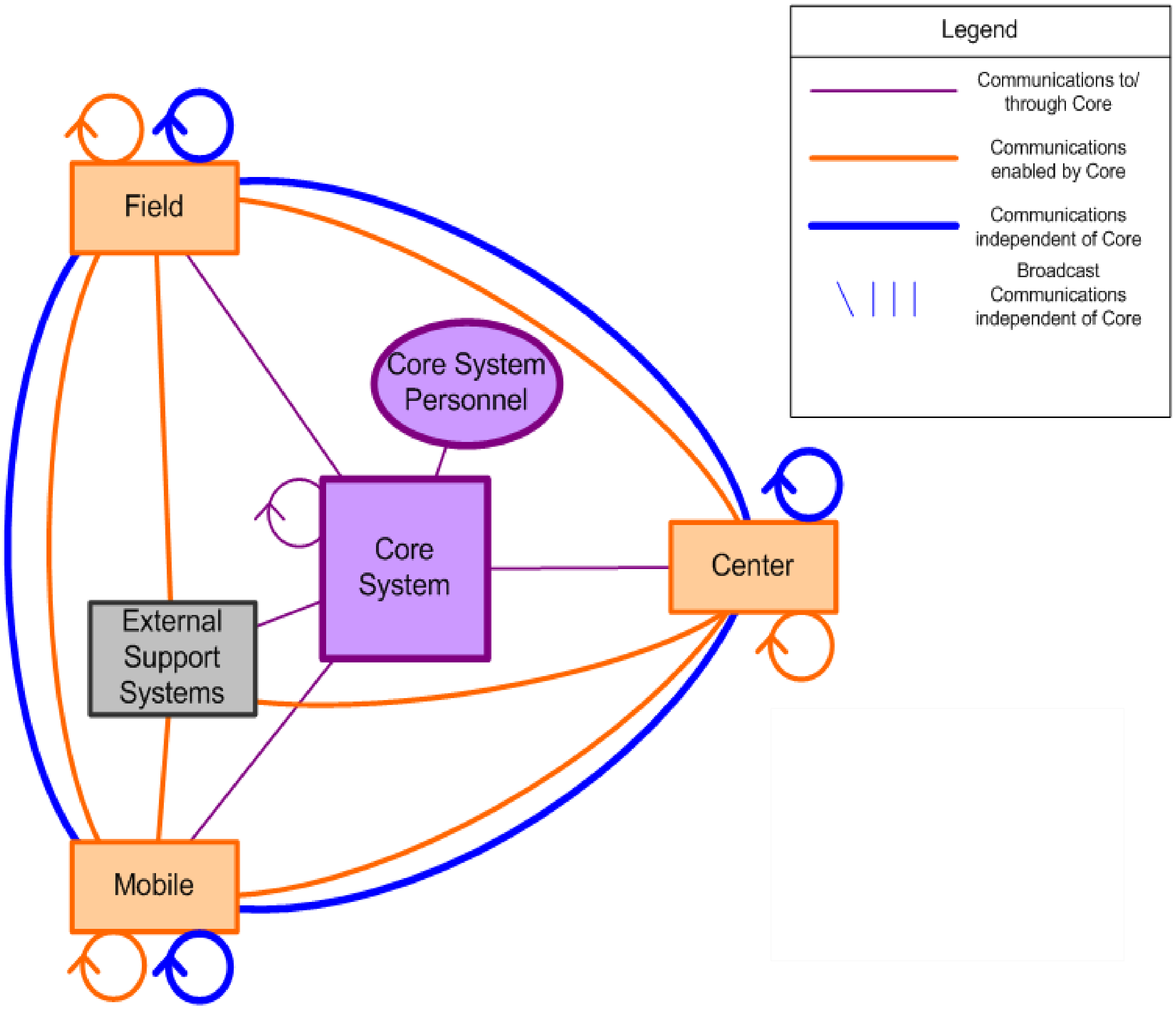
Complete Security Plan

- To be complete, the Safety Pilot/Model Deployment security plan must include all **devices**, **communications**, and **policies** determined by all of the organizations that make up the installation.
  - □ **Devices:** in-vehicle equipment, roadside equipment, Internet-based equipment, support equipment.
  - □ **Communications:** 5.9GHz DSRC communication among vehicles, between vehicles and roadside, IP communication between vehicles, roadside, and the Internet.
  - □ **Policies:** USDOT, CAMP.
- The plan will be embodied in device requirement specifications, experiment operational specifications.

System Design Principles

- **The parts of the system are controlled by a federation of equals**
  - Private industry; government at all levels.
  - An appropriate level of trust is essential: All communications will be signed using a common cryptographic process.
  - Rights of ownership (privacy) are protected.
  - The receiving party of a communication will be responsible for determining the authenticity of any message.
  - An entity trusted by all will establish the root secret that all cryptographic security credentials will be based on.
- **Security solution fits the communication needs**
  - Small data exchanges; rapid exchanges; short, intermittent connections.
  - Devices share situation information (BSM's, SPaT, etc.) in broadcasts with no expectation of a response.
  - Any response to broadcast information, or point-to-point interactions that cause a result to occur in a device (such as a driver alert or file update) will be initiated by the most vulnerable party to the interaction: Onboard equipment will initiate interactions with roadside equipment. Roadside equipment will initiate interactions with Internet-based equipment. (NO push from the Internet)

Connected Vehicle Environment

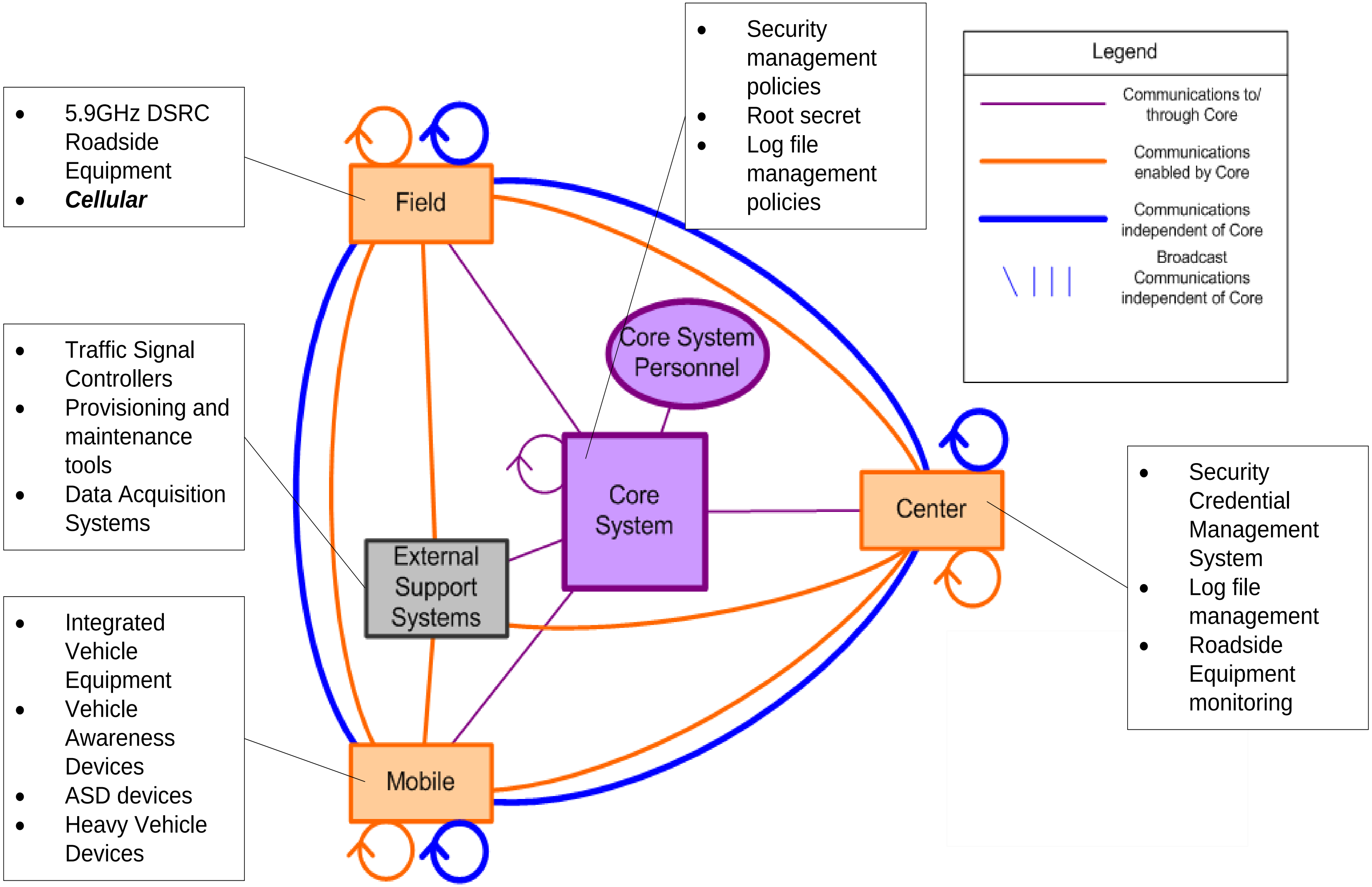

Legend
Communications to/ through Core
Communications enabled by Core
Communications independent of Core
Broadcast Communications independent of Core
Field
Core System Personnel
Core System
Center
External Support Systems
Mobile

Devices

Security processes – either **cryptographic** or **physical** – will be applied to all device interfaces used for **operational** and **maintenance** purposes.

- Mobile (Onboard)
  - Integrated Vehicle Devices
  - Aftermarket Safety Devices
  - Vehicle Awareness Devices
  - Heavy (Truck, Transit) Devices
- Field (Roadside)
  - Roadside Equipment
- Center (Internet)
  - Security Credential Management System
  - Log File Management System

Safety Pilot/Model Deployment Environment


Field
Core System Personnel
Core System
External Support Systems
Center
Mobile
Legend
Communications to/ through Core
Communications enabled by Core
Communications independent of Core
Broadcast Communications independent of Core

- 5.9GHz DSRC Roadside Equipment
- ***Cellular***

- Traffic Signal Controllers
- Provisioning and maintenance tools
- Data Acquisition Systems

- Integrated Vehicle Equipment
- Vehicle Awareness Devices
- ASD devices
- Heavy Vehicle Devices

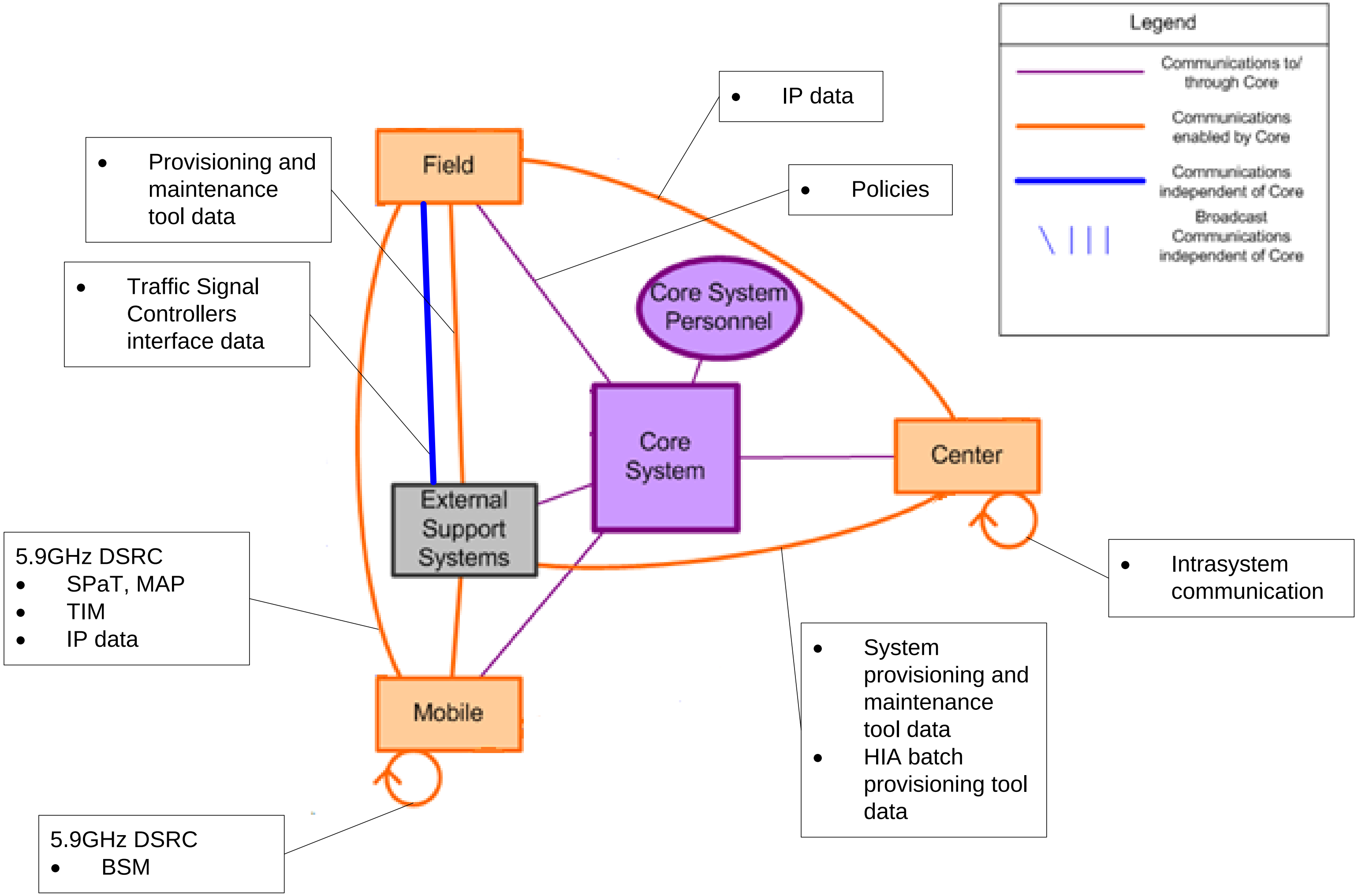
- Security management policies
- Root secret
- Log file management policies

- Security Credential Management System
- Log file management
- Roadside Equipment monitoring

Communications

- Operational Communication
  - WSMP over 5.9GHz DSRC for V-V between mobile devices.
  - WSMP over 5.9GHz DSRC for V-I between mobile devices and roadside devices.
  - IP over 5.9GHz DSRC for point-to-point between mobile devices and roadside devices.
  - IP over Internet for point-to-point between roadside devices and Internet-based devices.
- Provisioning and Maintenance Communication
  - IP over Serial medium (Ethernet, USB) between all devices and temporarily-attached tools.
  - File content in removable medium (SD, USB) in certain mobile devices.
  - **NO** mobile device or field device provisioning from Internet-based devices

Safety Pilot/Model Deployment Communications


Legend
Communications to/ through Core
Communications enabled by Core
Communications independent of Core
Broadcast Communications independent of Core
Field
Core System Personnel
Core System
Center
External Support Systems
Mobile

- IP data

- Policies

- Provisioning and maintenance tool data

- Traffic Signal Controllers interface data

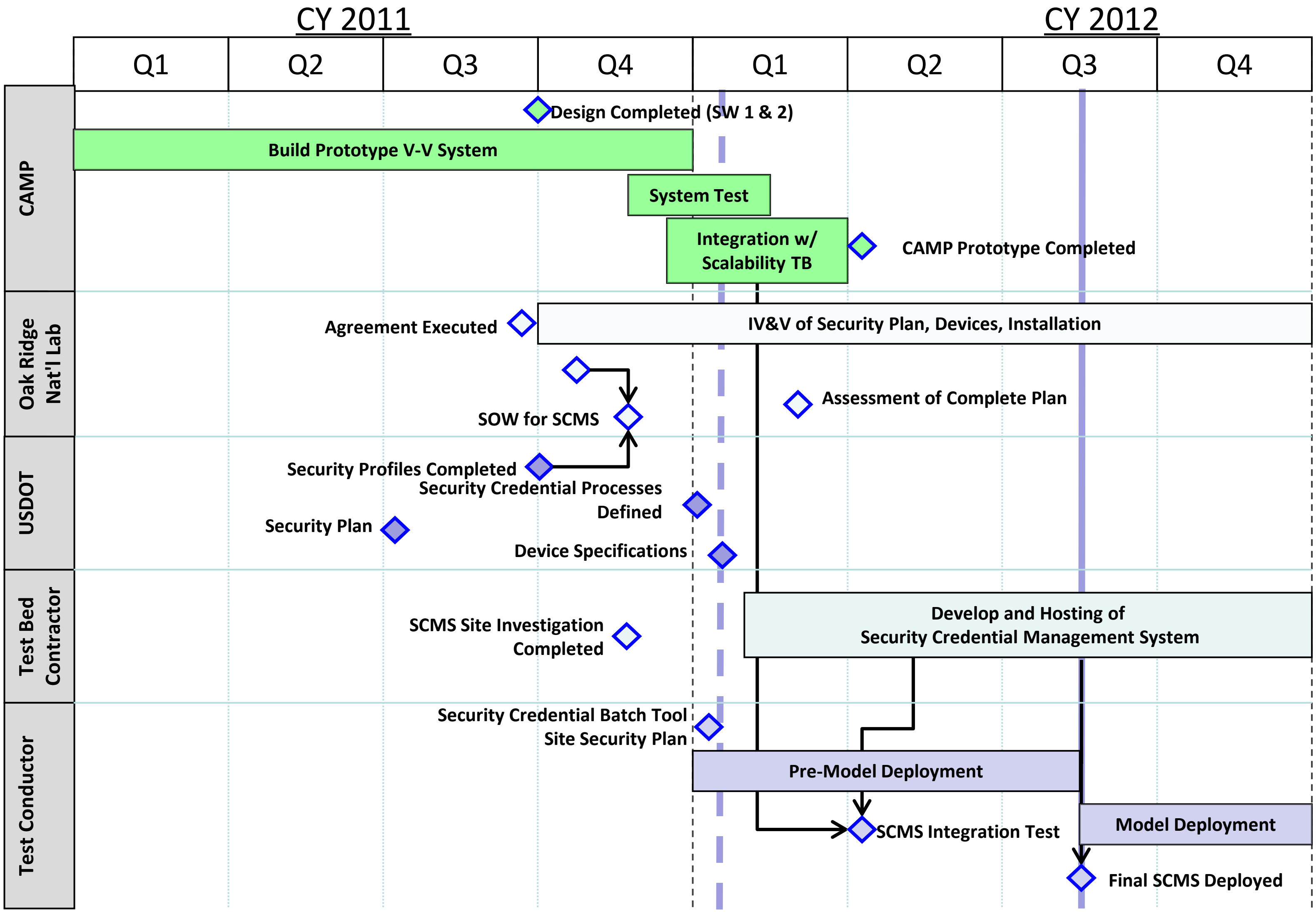
5.9GHz DSRC
- SPaT, MAP
- TIM
- IP data

- Intrasystem communication

- System provisioning and maintenance tool data
- HIA batch provisioning tool data

5.9GHz DSRC
- BSM

Security Plan Roadmap v5


CY 2011
CY 2012
Q1
Q2
Q3
Q4
Q1
Q2
Q3
Q4
CAMP
Oak Ridge Nat'l Lab
USDOT
Test Bed Contractor
Test Conductor
Design Completed (SW 1 & 2)
Build Prototype V-V System
System Test
Integration w/ Scalability TB
CAMP Prototype Completed
Agreement Executed
IV&V of Security Plan, Devices, Installation
SOW for SCMS
Assessment of Complete Plan
Security Profiles Completed
Security Credential Processes Defined
Security Plan
Device Specifications
SCMS Site Investigation Completed
Develop and Hosting of Security Credential Management System
Security Credential Batch Tool
Site Security Plan
Pre-Model Deployment
SCMS Integration Test
Model Deployment
Final SCMS Deployed