Technical Memorandum

SunGuide® Software System

SunGuide-TR-AAC-1.0 Draft

Authentication & Authorization Concept of Operations

Version 1.0

October 31, 2012

Prepared for:

Florida Department of Transportation
Intelligent Transportation Systems Program
605 Suwannee Street, M.S. 90
Tallahassee, Florida 32399-0450
(850) 410-5600

DOCUMENT CONTROL PANEL		
File Name:	SunGuide-TR-AAC-1.0.0.docx	
File Location:		
Version Number:	1.0 DRAFT	
Name		**Date**
Created By:	Robert Heller, SwRI	2012-10-30
Reviewed By:	Roger Strain, SwRI	2012-10-30
	Tucker Brown, SwRI	2012-10-30
Modified By:		

Table of Contents

List of Figures

List of Acronyms and Abbreviations

ConOps ..... Concept of Operations
FDOT ..... Florida Department of Transportation
ITS..... Intelligent Transportation Systems
IV&V .....Independent Verification and Validation

1 Introduction

The SunGuide contains a simple Authentication and Authorization model; users either have permission to perform a task on all members of a device type or they do not have permission to do so on any members of that device type. As districts have gained experience using the SunGuide software, they have developed operational strategies that require more granular permission models; i.e. the districts want to be able to allow users to control subsets of devices. This CONOPS describes a change to the Authentication and Authorization model that addresses these strategies.

1.1 Document Identification

This document is the Authentication & Authorization Concept of Operations identified as SunGuide-TR-AAC-1.0 and describes the operation of a new SunGuide application or subsystem named the System Authentication Application (SAA)

1.2 Document Purpose

This document is organized into the following sections.

- The document presents a description of the current implementation of the SunGuide Authorization and Authentication model and the requirements it addresses.
- The document summarizes limitations imposed by the model and the effect those limitations have on district operational paradigms.
- The document provides a proposed modification to the existing system, how it will be implemented and the advantages of the modification.
- The document describes an operational scenario that takes advantage of the proposed modification.

1.3 System Overview

The Florida Department of Transportation (FDOT) SunGuide® Support, Maintenance, and Development Contract, contract number BDQ69, addresses the necessity of supporting, maintaining, and performing enhancement development to the SunGuide software. The SunGuide software was developed by FDOT through a contract from October 2003 and ongoing as of 2012. The SunGuide software is a set of intelligent transportation systems (ITS) software that allows control of roadway devices as well as information exchange across a variety of transportation agencies; it is deployed throughout the state of Florida. The SunGuide software is based on ITS software available from the state of Texas with significant customization and development of new software modules to meet FDOT's needs. Figure 1 provides a graphical view of the SunGuide software.

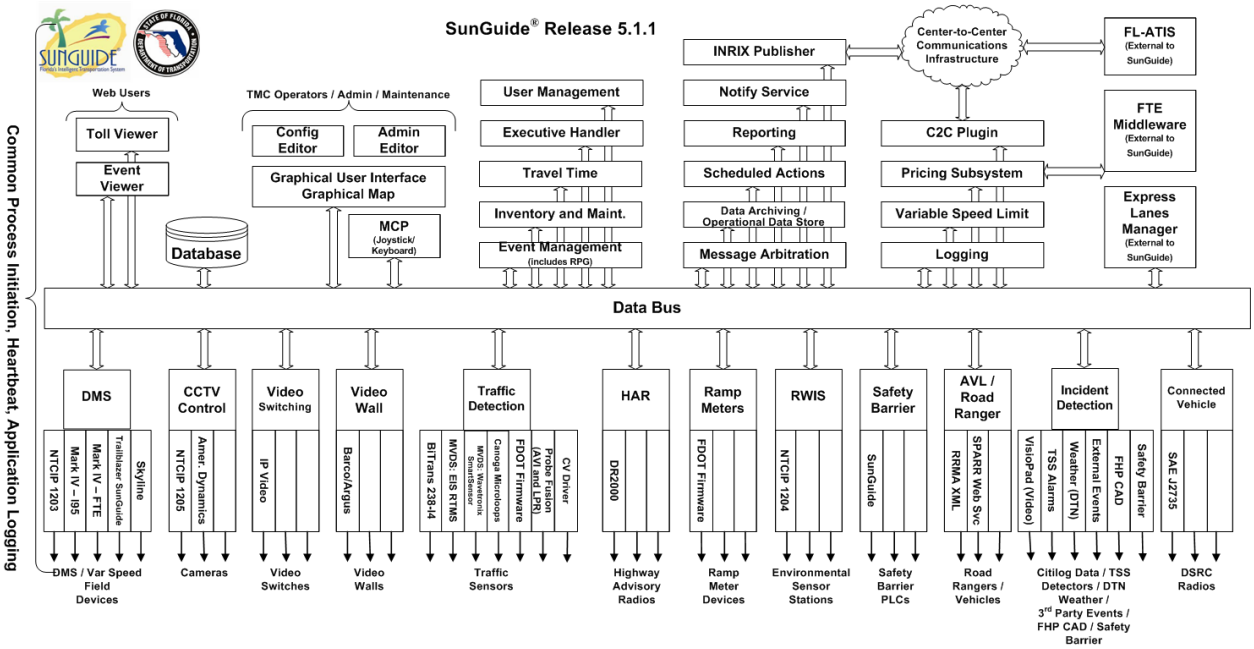

Figure 1.1 – High-Level Architectural Concept

The SunGuide software development effort began in October 2003; several major releases have been developed and this document addresses an incremental update of the most recent release. After development, the software will be deployed to a number of regional and local transportation management centers throughout Florida and support activities will be performed.

2 References

The documents provided in this section were used in preparation of this document or are useful reference documents.

2.1 Related Documents

The documents listed below form a part of this document to the extent specified herein. In the event of a conflict between the documents referenced herein and the contents of this document, this document shall be considered the superseding document.

> Statewide Transportation Management Center Software Library System: Scope of Services. Florida Department of Transportation, September 23, 2003. Contract BD826.
>
> Software Administration Application Concept of Operations, SAA-COO-2.0.0, Texas Department of Transportation, May 9, 2012.
>
> Presentation Slides, SunGuide Configuration Management Board Meeting, Florida Department of Transportation, August 15, 2012.

These documents are available from the document library on the SunGuide project web site at http://sunguidesoftware.com.

Alternatively, they can be obtained by request to:

Florida Department of Transportation Traffic Engineering and Operations Office
605 Suwannee Street, M.S. 90
Tallahassee, Florida 32399-0450
(850) 410-5600

2.2 Contacts

The following is a list of contacts for the SunGuide software project:

- Elizabeth Birriel, ITS Section, Traffic Engineering and Operations Office, elizabeth.birriel@dot.state.fl.us, 850-410-5606
- Arun Krishnamurthy, FDOT SunGuide Project Manager, arun.krishnamurthy@dot.state.fl.us, 850-410-5615
- Clay Packard, Atkins Project Manager, clay.packard@dot.state.fl.us, 850-410-5623
- David Chang, Atkins Project Advisor, David.Chang@dot.state.fl.us, 850-410-5622
- Robert Heller, SwRI Project Manager, rheller@swri.org, 210-522-3824
- Tucker Brown, SwRI Software Project Manager, tbrown@swri.com, 210-522-3035

3 SunGuide Permissions

The SunGuide permissions model provides a large number of permissions that may be granted to a user or template. If one or more templates of permissions exist, then a template may be applied to a user and the user inherits permissions from the template at the time the template was applied.

3.1 Background, Objectives, and Scope

The SunGuide permission model was developed in consultation with the FDOT especially FDOT district ITS engineers and representatives of the ITS Central Office. The original requirements provided scant requirements for the permission model; those requirements are provided below.

Requirement Number	Requirement Text
UT002	The STMCSLS shall allow users with proper security permissions to update database tables from the GUI workstations.
WS001	The workstation security function shall provide the capability to assign specific users and groups to categories that have specific access to levels of the software functionality.
WS002	The workstation security function shall use encrypted passwords to identify which users or groups can access what levels of software functionality.
WS003	Each user added to a group shall inherit the functionality of the group.

Requirement Number	Requirement Text
WS004	In the event of a workstation failure, users shall be able to log into other workstations and have the same functionality they would if they were at their own workstation.

3.2 SunGuide Permissions Model

As noted above, the SunGuide software contains a large number of permissions that may be granted to an individual user or template. Templates containing permissions may be applied to users and the user inherit permissions from the template at the time the template is applied. Changes to the template are not automatically inherited by the user.

Permissions are grouped by subsystem or application and a user may have a single set of permissions that apply to all resources or devices controlled or implemented by a subsystem. E.g. a user has a single set of permissions for the CCTV subsystem; if a user can control one camera defined within the system, the user can control all cameras. Other characteristics of the permission model include:

- Usernames and passwords are stored within the SunGuide database; passwords are encrypted in the database.
- The permissions model is implemented within SunGuide in the ITS Generic framework.
- The system permissions are stored within the SunGuide database.
- User permissions (permission granted to users) are stored within the SunGuide database.
- Subsystems have associated usernames and passwords which are stored within the SunGuide database. The encrypted passwords also appear in the SunGuide Config.xml file.

3.3 Operational Constraints

The primary limitation of the current model is lack of ability to grant different sets of permissions for a single subsystem to a single user. A user is granted a single set of permissions for a subsystem and those apply to all resources managed by the subsystem.

4 Justification and Nature of the Changes

The FDOT SSUG has discussed the permission model more than once and there is an active "forum" on the SunGuide Software website (www.sunguidesoftware.com).

4.1 Justification for Changes

Some FDOT districts divide operational responsibility for their managed roadways among their operational staff. They have expressed the desire to be able to subset their devices (cameras, DMS, HAR, RWIS, TSS, etc.) and grant control of different subsets to different users.

4.2 Proposed Change

The SunGuide permissions model will be modified to provide the ability to assign a user two sets of permissions for each subsystem:

- A set of permissions that apply to a single resource subset. These permissions apply only to the resources in the single defined subset.
- A default set of permissions for each subsystem. These permissions will apply to all resources that do not fall into subset (see above).

Example: A user may have a set of permissions that allows the user to view content and status of all DMS within a SunGuide configuration. The same user may have a set of permissions that allows the user to post messages to the DMS in a subset where the subset contains all the DMS on a specific roadway.

4.3 Proposed Limitation

A single alternative was discussed but is not included in this CONOPS. There was discussion of providing the ability to grant a user different permissions for multiple subsets without limitation on the number of subsets. This was abandoned as unnecessary at this time and the estimated cost to implement this was significantly more (double) than the proposed solution.

Example: A TMC manages cameras on I-10, I-95 and I-295 (not an exhaustive list). The operations manager wants to grant permission to a user to view the cameras on I-295, control the cameras on I-95 and control and override locks on camera on I-10. This is not supported because it involves three subsets of the cameras with different permission sets.

4.4 Assumptions and Constraints

Describe assumptions or constraints applicable to the changes and new system features.

5 Implementation of the Proposed System

5.1 Current Implementation

The SunGuide permissions model is implemented within the SunGuide subsystems.

- Each subsystem reads user permissions from the SunGuide database and caches a local copy of those permissions.
- When a user logs into the system, the user authenticates to each subsystem to which the user requests a connection. Each subsystem verifies the provided credentials against those in the database. The status of this authentication can be seen on the start-up splash screen if it is displaying connection details.
- When a user makes a request to a subsystem the subsystem compares the request to the cached user permissions to determine if the user is authorized to perform the requested operations.
- When a change to the user permission is performed, all subsystems must re-read the database to update their permissions table for all users.

5.2 Proposed Implementation

The proposed implementation removes the permission model from the individual subsystems and replaces it with a single application responsible for authentication and authorization.

- The authentication and authorization application will read user permissions from the database and cache a local copy.
- When a user logs into the system, the user authenticates to each subsystem to which the user requests a connection. Each subsystem sends the provided credentials to the authentication and authorization application to be verified. User permissions are transmitted to the subsystem at this time. The status of this authentication can be seen on the start-up splash screen if it is displaying connection details.
- When a user makes a request to a subsystem the subsystem checks that user's permissions as reported from the authentication and authorization application. If a user's permissions change during a session, the authentication and authorization application will send updated permission information to subsystems.

5.3 Implementation Advantages

The introduction of an additional application would seem to complicate an already complex system, SunGuide. But in fact, centralizing the authentication and authorization in a single place does simplify the system.

- More closely resembles the TxDOT Lonestar implementation (a stated goal of FDOT and TxDOT respective PMs), i.e. Lonestar uses System Administration Application (SAA) to perform similar functions.
- While implemented in the C# ITS generic, it also appears as separate implementations legacy Java subsystems.
- Only the authentication and authorization application will read, cache, and process permissions. This will reduce effort and complexity of system maintenance.

6 Operational Scenario

The operations manager in the District 3 TMC has developed an operator development plan for new operators. The development plan includes the following steps:

1. Josephine, a new operator, successfully completes a SunGuide operators' training course that teaches her operation of the system including device control of cameras and signs and ability to view traffic conditions of TSS detectors.
2. Josephine is assigned to watch and operate SunGuide on a small segment of roadway that has light congestion and very few incidents.
    - The SunGuide administrator defines a subset of CCTV devices, CCTV-J, consisting of CCTVs on that roadway.
    - The SunGuide administrator defines a subset of DMS devices, DMS-J, consisting of DMSs on that roadway.
    - The SunGuide administrator grants Josephine the ability to control the CCTV-J and post messages to the DMS-J and ability to "see" other DMS and CCTV in the system.

3. Josephine demonstrates ability to manage the small section or roadway and before long she is granted access to all DMS and CCTV within the system.

7 Summary of Impacts

The complexity of the SunGuide permission model will increase significantly. However, the system should continue to operate as it is with no action taken by administrators unless they choose to make use of the new capabilities.