Transportation Systems Management & Operations

Managing and Operating for an Efficient Transportation System

Concept of Operations for: ***ITSIQA Intelligent Transportation Systems Integration Quality and Analysis***

Version: *1.1*

Approval date: *11/10/2016*

FDOT

DOCUMENT CONTROL PANEL		
File Name:	ITSIQA - ConOps - V1.0 - 2016-11-09.docx	
File Location:		
Version Number:	1.0	
	Name	**Date**
Created By:	Alex Mousadi, AECOM	8/10/2016
Reviewed By:	Matt Cousins, AECOM	9/1/2016
	Matt Cousins, AECOM	10/3/2016
	Clay Packard, Atkins	10/11/2016
	Alex Mousadi, AECOM	11/9/2016
Modified By:	John Hope, AECOM	9/1/2016
	John Hope, AECOM	10/3/2016
	John Hope, AECOM	10/12/2016
	John Hope, AECOM	11/9/2016
Approved By:		

Table of Contents

List of Tables

List of Figures

List of Acronyms and Abbreviations

API	Application Program Interface
C2C	Center to Center
CFX	Central Florida Expressway Authority
ConOps	Concept of Operations
DIVAS	Data Integration and Video Aggregation System
FDOT	Florida Department of Transportation
FHP CAD	Florida Highway Patrol Computer Aided Dispatch
LOS	Level of Service
MIMS	Maintenance and Inventory Management System
ITS	Intelligent Transportation Systems
ITSIQA	Intelligent Transportation Systems Integration Quality and Analysis
TMC	Traffic Management Center or Traffic Message Channel
TSM&O	Transportation Systems Management and Operations
TSS	Traffic Sensor Subsystem

1. Overview

1.1 Document Overview

The purpose of this document is to identify and outline the Concept of Operations (ConOps) for the Intelligent Traffic Systems Integration Quality and Analysis (ITSIQA) project. This includes describing the current issues, what changes are desired, and how this new system fits into long range plans for a fully integrated traffic management system.

Based on concepts and desired functionality described this document, functional requirements should be developed. Final system testing should reference this ConOps to ensure that the intended goals outlined in this document have been fully realized.

The intended audience of this document includes the end users of the ITSIQA system, including stakeholders who may benefit from this system as well as related engineering staff who seek an understanding of FDOT goals when designing the final system.

1.2 System Overview

The overarching objectives of the ITSIQA system include:

1. Receive real-time traffic information via two interfaces, SunGuide's Databus and the Center-to-Center Software
2. Perform quality checks and analysis on the traffic information
3. Report the cleaned data to multiple systems including the SunGuide Software

Figure 1 depicts a high level description of ITSIQA.

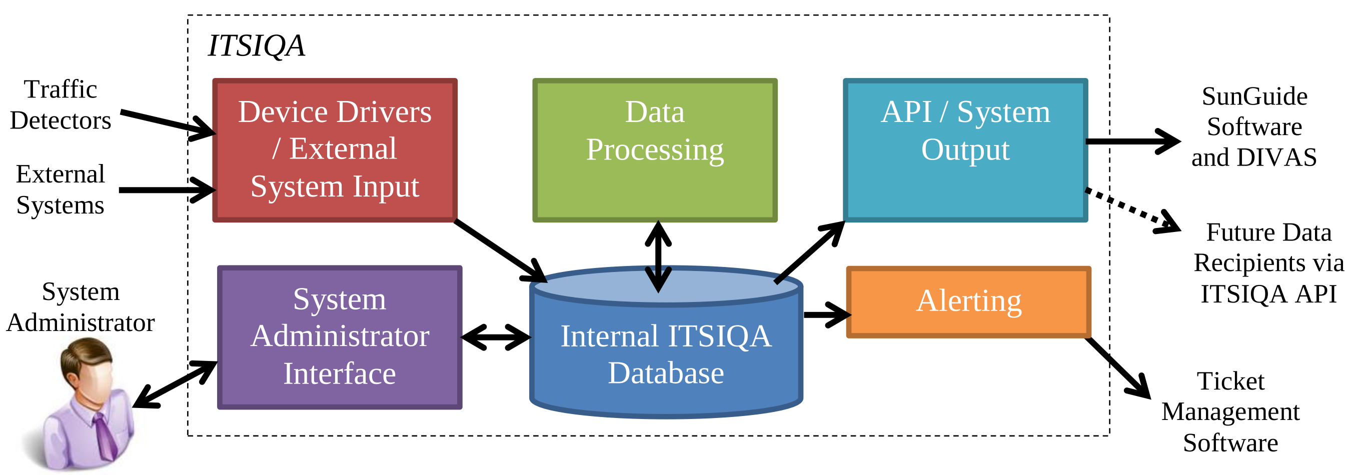

Figure 1: High Level Description of ITSIQA

The traffic detectors encompass all legacy and known future traffic detectors within FDOT District 5's system. Third-party traffic data feeds encompass services that provide real-time traffic information from their own traffic information collection systems. Examples of third party traffic feeds are INRIX and HERE.com. Traffic information encompasses all traffic detectors and traffic data feeds. ITSIQA will house a working database to be used to store raw and processed real-time traffic information for internal data processing and system configuration. This configuration will be handled via a simple System Administration Interface. ITSIQA will provide the SunGuide Software and Data Integration and Video Aggregation System (DIVAS) with consolidated traffic information based on existing algorithms that will best estimate the true traffic conditions. ITSIQA will also establish a standard Application Program Interface (API) that will allow future systems to acquire the same consolidated traffic information. An alerting functionality will be built into the system. This alerting piece will identify potential issues with detectors and external systems and submit this information into an external ticket management software.

Although developed by FDOT District 5, the fully functional ITSIQA can be made available to other FDOT districts and local agencies, including the Central Florida Expressway Authority (CFX).

2. Referenced Documentation

As part of the ITSIQA development, a number of technical documents were reviewed to determine the best approach for addressing the project needs. Each document provides in depth perspectives on various strategies to ingest traffic information from various sources, filter through this data, and fuse it together to form the most accurate picture of current traffic conditions.

Table 1 lists the documents reviewed.

Table 1: List of Documents Reviewed for SIQA Development

Publication	Author / Publisher	Date	Useful Subject Matter
Evaluation of a cellular phone-based system for measurements of traffic speeds and travel times: A case study from Israel	Department of Industrial Engineering and Management, Ben-Gurion University of the Negev, Israel	Jun-2007	Travel Time Verification
Traffic Data Quality Measurement	FHWA, Cambridge Systematics Inc., Texas Transportation Institute	Sep-2004	Data Quality Metrics Data Quality Calculations

Publication	Author / Publisher	Date	Useful Subject Matter
Travel Time Data Collection Handbook	FHWA, Texas Transportation Institute	Mar-1998	Error Checking Data Reduction Reporting
Methods for Floating Car Sampling Period Optimization	Journal of Transportation Systems Engineering and Information Technology ITS Center, Wuhan University of Technology School of Traffic and Transportation, Tongji University	Jun-2007	Data Sample Period
Guide to Establishing Monitoring Programs for Travel Time Reliability	TRB Institute for Transportation Research and Education, North Carolina State University	2014	Data Aggregation
Evaluation of Traffic Data Obtained via GPS-Enabled Mobile Phones: the Mobile Century Field Experiment	UC Berkeley Center for Future Urban Transport	Aug-2009	AVL System Accuracy
Analytical Delay Models for Signalized Intersections	Kirikkale University University of Pittsburgh		Intersection Delay
A Traffic Data Warehousing and Visualization Scheme	University of Minnesota, Thesis Paper	Jul-2004	Data Processing
Integration of Probe Vehicle and Induction Loop Data - Estimation of Travel Times and Automatic Incident Detection	University of Technology, Netherlands	Jan-1996	Data Aggregation Incident Detection
Measuring real-time traffic data quality based on floating car data	ATEC ITS France Congress	Jan-2014	Data Aggregation Data Quality
Quality Management Methods for Real-Time Traffic Information	15th meeting of the EURO Working Group on Transportation University of Federal Armed Forces Munich, Department of Traffic Engineering		Data Quality
Validation and augmentation of Inrix Arterial Travel Time Data using Independent Sources	MDOT State Highway Administration	Feb-2015	Data Aggregation Data Quality Arterial Travel Time
Use of Multiple Data Sources for Monitoring Mobility Performance	FDOT Transportation Statistics Office	Jan-2015	Data Quality TMC segment mapping
Data Fusion Based Hybrid Approach for the Estimation of Urban Arterial Travel Time	Journal of Applied Mathematics	Jul-2012	Arterial Travel Time

Publication	Author / Publisher	Date	Useful Subject Matter
Comparison of Methods for Measuring Travel Time at Florida Freeways and Arterials	FDOT Systems Planning Office	Jul-2014	Roadway Segment Correlation Data Accuracy
REGIONAL TRANSPORTATION DATA WAREHOUSE – Phase I, II, III	Texas Transportation Institute	Aug-2008	Data Aggregation Data Quality Data Filtering Data Fusion Data Warehousing
Classifiers and Distance-Based Evidential Fusion for Road Travel Time Estimation	Laboratoire d'Ingénierie Circulation Transports Laboratoire d'Informatique et d'Automatique de l'Artois	2006	Data Fusion
OOCEA Data Server Travel Time Filtering and Fusion Data Flow	Central Florida Expressway Authority	2005	Data Fusion
Bluetooth Sensor Data and Ground Truth Testing of Reported Travel Times	Department of Civil and Environmental Engineering, University of Maryland	2012	Data Fusion Data Accuracy
Road network spatial segmentation	FDOT, Clay Packard	2016	Spatial Issues

3. Current System Situation

The SunGuide Software is currently positioned at the center of FDOT District 5's Supervisory Control and Data Acquisition (SCADA) system for traffic operations. Owned, customized, and maintained by FDOT Central Office, the SunGuide Software is a suite of services and interfaces intended to accomplish all software ITS control, archiving, and reporting functions required for an FDOT district or local agency to carry out its traffic operations.

Figure 2 depicts a graphical view of the SunGuide Release 6.2 Software.

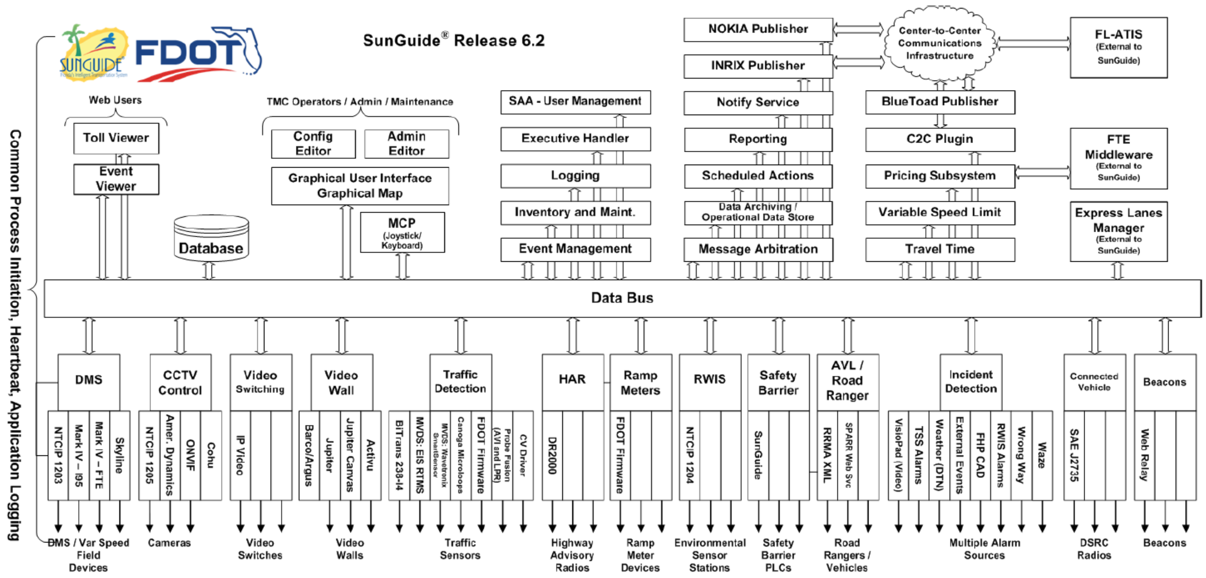

Figure 2: SunGuide Release 6.2 Software Design Diagram

As shown in the diagram above, the SunGuide Software includes a wide range of software drivers that allow FDOT districts and local agencies to view and control their ITS devices using this single suite of software, rather than supporting multiple vendor-specific software packages.

The SunGuide Software is currently deployed district- and agency-owned and maintained equipment throughout the state of Florida, actively used by all FDOT districts, two tolling agencies, and multiple local municipalities. In most cases, it operates 24/7/365 and actively used by operations and engineering staff that is charged to keep the system fully operational with as little downtime as possible.

In addition to interfacing with a district and agency's ITS field equipment, the SunGuide Software also interfaces with external third party and FDOT systems, including the Florida 511 Traveler Information system and the Florida Highway Patrol Computer Aided Dispatch (FHP CAD) system. Each of these interfaces are monitored and maintained by traffic operations and SunGuide system administrative staff.

3.1 Background, Objectives, and Scope

FDOT District 5 has been architecting long range plans for a fully integrated traffic management system. ITSIQA is intended to be an integrated portion of these plans. Figure 3 is FDOT District 5's Transportation Systems Management and Operations (TSM&O) Data Fusion Architecture Road Map, which shows the planned high level data flow of this fully integrated system.

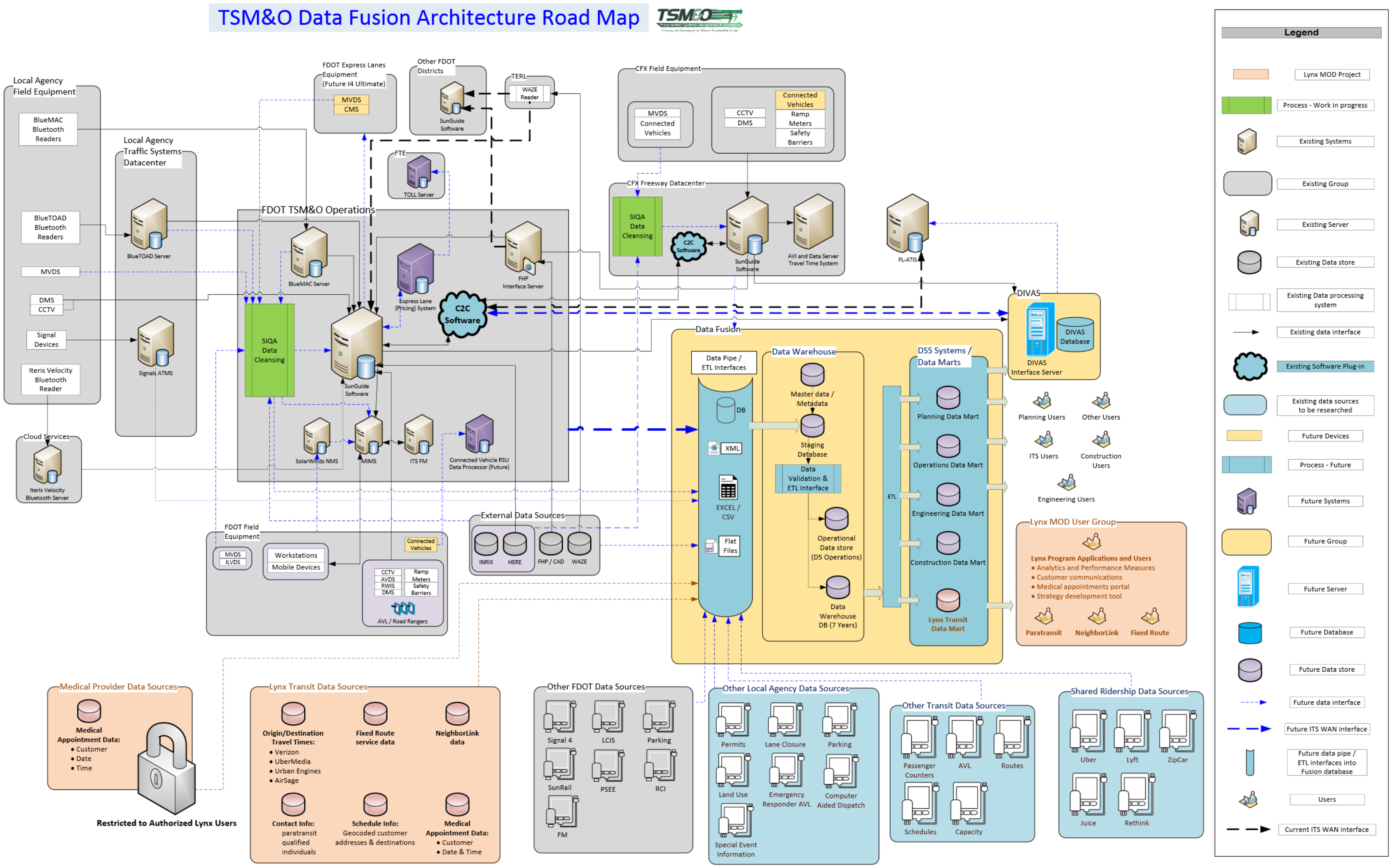

Figure 3: TSM&O Data Fusion Architecture Road Map

Note that the ITSIQA system is showed as the green “SIQA Data Cleansing” boxes. Also note that initially, this system is planned to be deployed within FDOT District’s TSM&O Operations and CFX’s Freeway Data Center. Each deployment will be configured appropriately to acquire data from legacy detectors and systems and provide processed information to the SunGuide Software. Alerting information will also be provided into FDOT District 5’s ticketing management software, called the Maintenance and Inventory Management System (MIMS).

3.2 Operational Constraints

The desired long-range plans involve a large number of data sources from various technologies and outside vendors. Many of these data sources are not standardized, requiring operations staff to interact with a variety of management software packages. Also, traffic data from one source often differs from what’s reported from a different source. Managing this wide array of data that may or may not provide a consistent picture of current traffic conditions has proven to be a burden on traffic operations.

Additionally, maintenance of the traffic detectors has its own challenges. Existing systems and O&M procedures may result in long periods of time when sections of roadway are without adequate instrumentation in order to properly monitor traffic conditions.

Traffic information received from 3rd parties may be useful in determining accurate traffic conditions; however, the agreement in place between FDOT and the data provider may not allow FDOT to transmit traffic conditions derived, even in part, by the vendor’s data feed, to other recipients outside of the internal usages and Florida’s 511 system.

The regional transportation management center (RTMC) operators use lane-specific information for the following usages:

- in order to be able to tell if slow traffic conditions is due to an off-ramp backup, as this would only block certain lanes,
- as an indicator if slow traffic conditions is caused by something on the shoulder, and
- to know which side of the road to look for a traffic issue when visually searching with a closed caption television (CCTV) camera.

3.3 User Profiles

A variety of skill sets are required to maintain and operate traffic management with FDOT District 5. The following user classifications summarize each of these skill sets.

1. ***Traffic Management Center (TMC) Operator***: This user’s focus is monitoring roadways within the TMC’s operational boundaries, responding to traffic events – particularly those involving lane blockage, and coordinating with responders and/or regional partners as necessary. This user interacts directly with the system’s user interface and is likely the first to notice system issues should they occur.

2. ***Traffic Management Center (TMC) Supervisors***: This user assists the duties of a TMC Operator and manages Operator staff. As with TMC Operators, this user interacts directly with the system's user interface and is likely the first to notice system issues should they occur.

3. ***System Administrators***: This user provides system support to ensure its availability to all other users. They also are in responsible for system updates and configuration changes as necessary as additions, removal, or other changes to ITS devices are made over time. Administrators also perform ad hoc testing to troubleshoot and resolve reported issues.

4. ***Software/System Support***: This user supports System Administrators should issues require higher tier support and/or if problems warrant software fixes. They typically coordinate with System Administrators except for specific issues that necessitate different support.

5. ***Traffic Engineering/Management***: This user oversees and provides management support of ITS systems. This user is typically focused on higher level operations as well as system functionality and performance. Consequently, their interaction with the system is limited to directing configuration changes to System Administrators and reviewing system reports.

3.4 Support Environment

The FDOT District 5 ITS system is mostly owned and licensed by FDOT and its partnering agencies. These components operate by and on equipment owned by FDOT and its partnering agencies. For those components owned by third parties, such as the HERE traffic data feed, FDOT has contracts in place to use their reported data as necessary. This architecture allows these ITS systems to operate autonomously with little reliance on Internet Service Providers (ISPs) which typically do not guarantee 100% uptime.

System support is provided by both in-house staff and contracted consultants and contractors through a variety of contracts. The specific staff is identified in Section 3.3 as System Administrators and Software/System Support. ITS equipment is, by in part, also covered by vendor warrantees and other mechanisms to ensure support.

The contract under which the ITSIQA project is being developed includes a six-month support period to support the system.

4. Justification and Nature of the Changes

As identified in Section 3.2, traffic data reported from multiple data sources often differ from each other. Also, existing procedures for handling device failures may result in extended downtime and lack of coverage for corridors that operations staff is required to monitor. This creates mistrust in reported data and makes it difficult for operations staff to determine the actual traffic conditions. FDOT District 5 desires to address these issues with ITSIQA, designed to analyze reported traffic data and automatically make intelligent decisions on what information should be reported and quickly notify appropriate support staff to address system and device issues.

4.1 Description of the Desired Changes

This section should include a summary of the new or modified capabilities, functions, processes, interfaces, and other changes needed to respond to the justifications previously identified. This shall include:

- ***Traffic Detector/Third Party Data Interfaces***: Rather than reporting traffic data to SunGuide or other operations systems directly, traffic data will be routed into ITSIQA.
- ***System Processing Changes***: ITSIQA will provide a new layer of quality controls and algorithms that will determine a truer picture of actual traffic conditions.
- ***Device and Data Source Management***: ITSIQA will depend on the SunGuide software for the configuration of the FDOT detectors. ITSIQA will automatically ingest this configuration information from the SunGuide software in order to facilitate processing of the data. ITSIQA will have a configuration management interface to manage various parameters related to the multiple sets of data retrieved into the ITSIQA system.
- ***Standardized Output Interface***: ITSIQA will provide an Application Program Interface (API) for any future system that requires traffic condition data.
- ***Standardized Reporting***: ITSIQA will report a standardized list of road segments. Although this list will be configurable to allow future changes, it is envisioned to make infrequent changes to the list, to ensure consistent reporting from month to month and year to year. This list will initially use segments defined within the HERE data, which is based on roadway geometry and traffic flows and will not be directly tied to detector locations or reporting standards of third party vendors.
- ***Automatic Detector Issue Reporting***: ITSIQA will flag potential issues with system interfaces and traffic detectors and automatically generate trouble tickets within FDOT District 5's MIMS issue tracking system.

4.2 Assumptions and Constraints

ITSIQA will use existing data-producing systems, such as Nokia's HERE, CFX's Data Server, Brevard County's BlueTOAD, and Seminole County's BlueTOAD system, travel time information associated with Waze JAMs, and legacy traffic detectors as data inputs. FDOT D5's SunGuide Software should collect most of this real-time traffic information and make this information available to ITSIQA. ITSIQA will be designed based on the versions of the software and systems FDOT District 5 has in place as of the start of the ITSIQA project. Changes to external systems may warrant changes to ITSIQA.

The server environment hosting ITSIQA will be sized appropriately to handle the processing and availability requirements as tested during system acceptance.

Should changes to the SunGuide Software be warranted, there is typically a considerable delay in getting the changes designed, implemented, and deployed – approximately six to twelve months. This is due to required procedures in place at FDOT Central Office to make such changes. As such, lead time will be required to accommodate changes, should they be needed.

5. Concepts for the Proposed System

5.1 Description of the Proposed System

The ITSIQA system will achieve the intended objectives in an eight step process. Each step achieves a specific goal and, with the exception of the final step, each step is needed before the next step can be achieved.

The following subsections outlines each of these steps.

5.1.1 Step 1 – Acquiring from Data Sources

This step acquires all reported traffic data. Implementing this step will require reusing the existing Traffic Sensor Subsystem (TSS) within the SunGuide Software in order to interface with the legacy detectors and external systems providing traffic data. TSS standardizes detector information into a SunGuide-specific format that is made available to the SunGuide Databus Subsystem. In order to intercept this data, ITSIQA will request TSS data via the Databus Subsystem. The ITSIQA will also receive information from the C2C infrastructure. Once ITSIQA processes the data, ITSIQA will provide consolidated traffic information to SunGuide via the Center-to-Center (C2C) software. Doing this, TSS would not need to be modified. However, this creates a dependency on the TSS subsystem within the SunGuide Software for the ITSIQA system.

Figure 4 depicts how ITSIQA and the SunGuide Software would be tied in together.

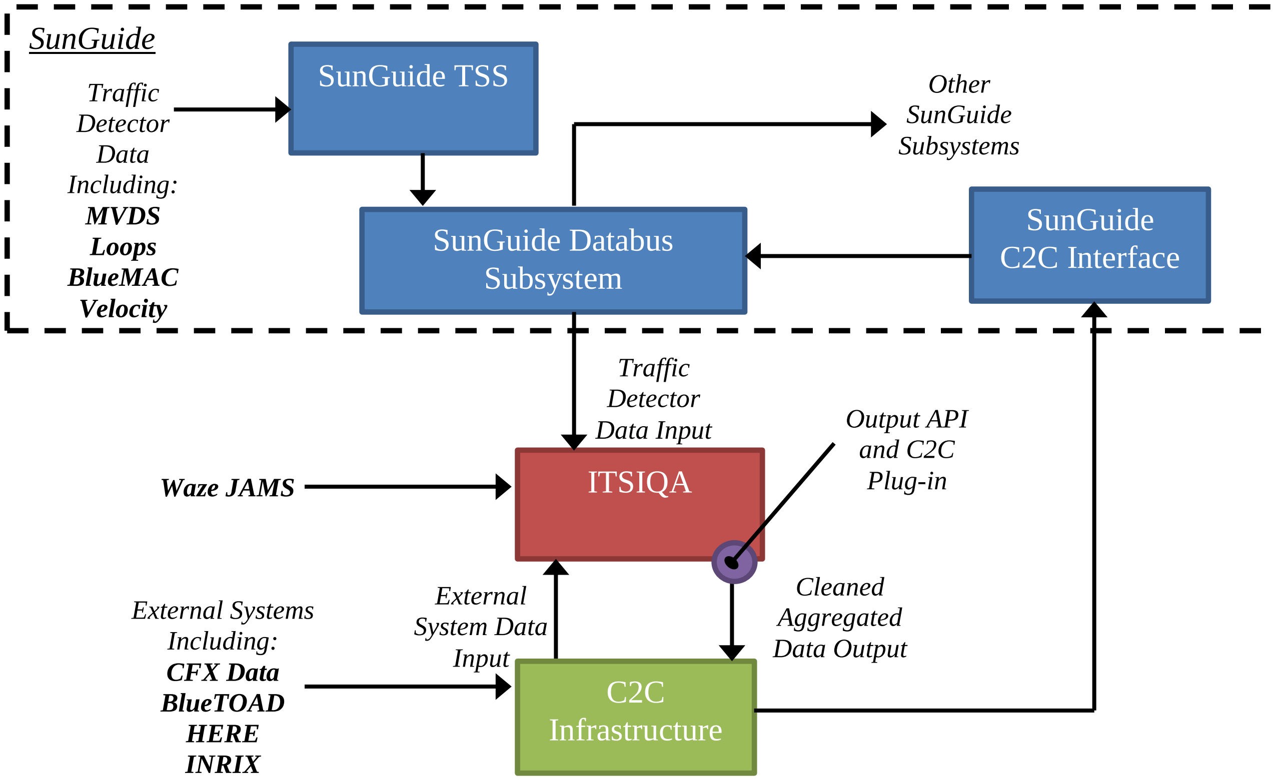

Figure 4: ITSIQA Integration with SunGuide

As shown above, ITSIQA will receive data from two different interfaces. Each interface will include data from different sources. The following lists what data will be acquired from each interface.

- **SunGuide Databus Interface** – This interface requires ITSIQA to send requests to SunGuide via the Databus and receive XML-formatted raw detector data. This data is formatted as TSS links and is accompanied by TSS detector and link information in XML, includes the source device information and the starting and ending and midpoint latitude and longitude. This data also includes C2C Remote TSS links, but ITSIQA will not be using this data. ITSIQA will acquire C2C data directly from a separate C2C interface. As long as the data within Databus is within the SunGuide R6.2 TSS data structure/format, then ITSIQA should be able to ingest this data. For example, ITSIQA will acquire TSS link and TSS detector data through this interface for the following devices:
  - **MVDS** – These detectors include Wavetronix 105, 125, 126 detectors and IssG4 detectors. The Databus should report raw speed, volume, and occupancy data from these detectors.
  - **Loops** – These detectors include the inductive loop detectors. The Databus should report raw speed, volume, and occupancy data from these detectors.

   - **BlueMAC** – These detectors include Bluetooth detectors whose tag read data SunGuide matches to produce travel time data. The Databus should report these travel times.
   - **Velocity** – These detectors include detectors whose tag read data SunGuide matches to produce travel time data. The Databus should report these travel times.

- **Center-to-Center Interface** – This interface requires ITSIQA to subscribe to C2C requests and receive XML-formatted data generated by external systems. This data is formatted as C2C links and nodes, as described in the C2C networkData, which includes starting and ending and midpoints latitude and longitude. For example, ITSIQA will acquire C2C data through this interface for the following data sources:
   - **CFX Data** – This data is generated by the Central Florida Expressway Authority (CFX)'s travel time system based on toll transponder data. Data includes link-based travel times and average speeds.
   - **BlueTOAD** – This data is generated by Seminole County and Brevard County's BlueTOAD travel time systems based on Bluetooth data. Data includes link-based travel times and average speeds.
   - **HERE** – This data is generated by Nokia's HERE average speed system based on variety of data sources, including trucking data. Data includes link-based average speeds.
   - **INRIX** – This data is generated by INRIX's average speed system based on variety of data sources, including trucking data. Data includes link-based average speeds.
- **Waze JAMs Interface** – Separate interface for just the Waze JAMs data feed.
   - **Waze JAMs** – This travel time-related data is generated by the Waze application and is based on a variety of data inputs acquired by Google.

All incoming data will be subject to a blacklist check. The ITSIQA will allow administrators to configure a list of links and/or detectors to add or delete from a blacklist. All links and detectors included in the blacklist will be immediately ignored by ITSIQA and will not be passed onto subsequent steps beyond the data acquisition step. This will allow administrators to address specific issues with links and/or detectors. This configuration would be done via the ITSIQA Administrative Editor.

Administrators will also have the ability to enable or disable an entire data feed. If a data feed is disabled, ITSIQA will not use any data from that particular data feed until it is re-enabled. This configuration would be done via the ITSIQA Administrative Editor.

5.1.2 Step 2 – Incoming Data Temporal Normalization

The various data sources report information on different intervals and at different times. Table 2 contains various known data sources that will provide data to ITSIQA and the intervals in which this data will be received.

Table 2: Data Source Reporting Intervals

Data Source	Reporting Interval
INRIX	2 Minutes
Nokia HERE	2 Minutes
Waze JAMs	Non-Standard*
Seminole County BlueTOAD	1 Minute
Brevard County BlueTOAD	1 Minute
CFX Data	1 Minute
Velocity Data	1 Minute
FDOT D5 BlueMAC	1 Minute
FDOT D5 Field Devices – MVDS	30 Seconds
FDOT D5 Field Devices – Loops	30 Seconds

* = Waze JAMs will only report travel times and speeds for links when a traffic jam is detected by Waze. ITSIQA will check for queued Waze JAMs data once per Time Slice.

ITSIQA will need to normalize the reported data into Time Slices. A Time Slice is a segment of time in which data is accumulated and reported. Initially, ITSIQA will assume a Time Slice interval of *60 seconds*, but this will be changeable system configuration.

Assuming a 60-second Time Slice interval, ITSIQA will perform normalization on incoming data that does not report on a 60-second interval. Normalizing over time will use the following logic:

1. If a data source reports less frequently than ITSIQA's Time Slice interval, ITSIQA will reuse the last reported data from that source for a Valid Data Time Horizon. A Valid Data Time Horizon is the amount of time in which reported data is valid. ITSIQA will use a 5-minute Valid Data Time Horizon, though this value will be configurable via the Administrative Editor. If the data source fails to report within this time horizon, then ITSIQA will assume no data for the current Time Slice for that data source. Note that according to the reporting intervals of the various data inputs listed in Table 2, all data except for MVDS and Loops report less frequently than ITSIQA's Time Slice interval.

2. Although data is still considered valid between the time it was reported to the Valid Data Time Horizon, as described in the previous step, the confidence of the data will decrease over time. If new data is reported between on Time Slice and the next, then the newly reported data will be given the highest confidence. If by the next Time Slice, new data is not reported, then the previously reported data will be used, but the confidence level will be decreased using the following formula:

   Confidence Level = (Valid Data Time Horizon – Age of Data) / Valid Data Time Horizon

   Note that if the Age of Data is greater than the Valid Data Time Horizon, the data will not be used.

3. If a data source reports more frequently than ITSIQA's Time Slice interval, ITSIQA will aggregate the data reported during that interval. Volume will be summed, speed will be volume-weighted averaged, and occupancy will be averaged.

For example, consider the following time chart in Figure 7.

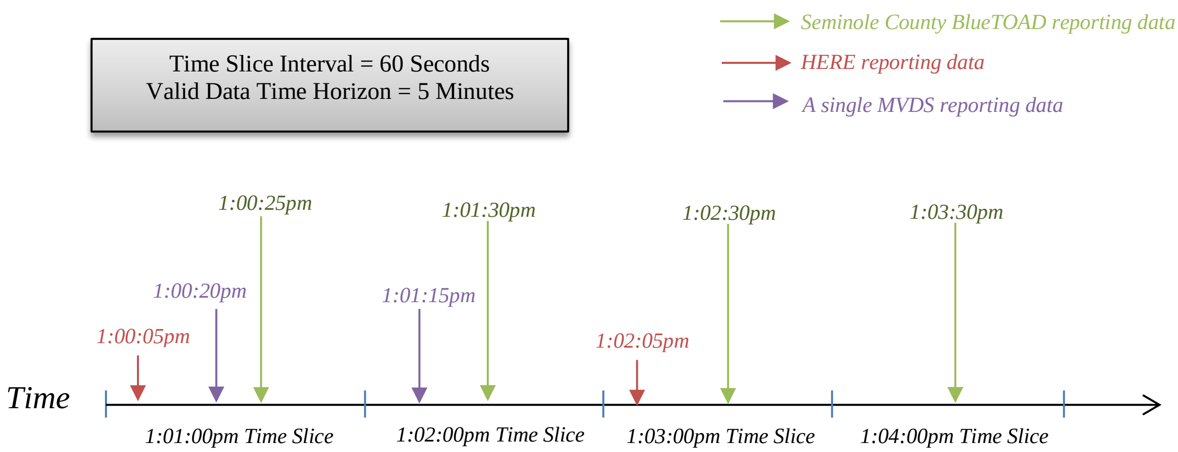

Figure 7: Example for Temporal Data Normalization

In the example above, ITSIQA will process and report data once per 60 seconds at exactly 1:01:00pm, 1:02:00pm, 1:03:00pm, and 1:04:00pm. Each of these reporting times is a Time Slice. Each Time Slice consists of data from the previous 60 seconds. The 1:01:00pm Time Slice consists of data reported from the Seminole County BlueTOAD system, from HERE, and from a single MVDS. During the 1:02:00pm Time Slice, ITSIQA will re-use the HERE data that was reported at 1:00:05pm and the newly-reported MVDS and BlueTOAD data reported at 1:01:15pm and 1:01:30pm, respectively. The 1:03:00pm and 1:04:00pm Time Slices lack data from the MVDS, possibly due to a failed detector. In this case, these Time Slices would use MVDS data from the 1:02:00 Time Slice, but with a lower confidence level.

5.1.3 Step 3 – Incoming Data Spatial Normalization

FDOT District 5 desires to standardize the reporting of traffic information. Part of this standardization involves developing a static list of reportable road segments. The goal of this step is to associate incoming data to a reportable road segment. Consider Figure 5 as an example.

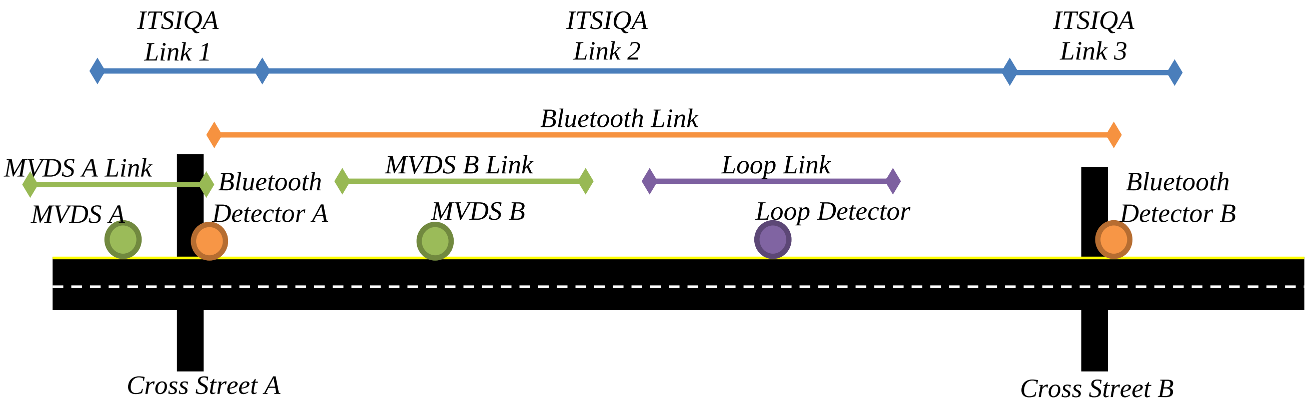

Figure 5: Example of Misaligned Links

In the above example, ITSIQA Links 1, 2, and 3 are what will be reported from ITSIQA. These segments, however, do not match up with the existing detector links, which acquire data from Bluetooth, MVDS, and Loop technologies. This is a very likely scenario throughout FDOT District 5's roadway network. As such, ITSIQA will need to relate the existing detectors to standardized ITSIQA Links.

The ITSIQA Links will follow the HERE data reporting scheme in which they are based off of the roadway and not the detector locations. These links alternate between two types of links:

1. **Connecting Links**: These are longer links that span from one interchange to the next downstream interchange
2. **Interchange Links**: These are shorter links that span the length of an interchange

In the Figure 5 example, ITSIQA Link 1 and 3 are Interchange Links, while ITSIQA Link 2 is a Connecting Link.

The ITSIQA Links will be predetermined and configured within ITSIQA. Initially, ITSIQA will be configured using the same Traffic Message Channel (TMC) Codes as defined in the Nokia HERE configuration. ITSIQA will keep a separate configuration database so that changes can be made independently of the Nokia HERE data feed.

Spatial normalization will performed based on a physical comparison of the ITSIQA Links against the reported links received from the various data feeds. The ITSIQA Links will be associated with the incoming links every time the incoming link configuration is updated. The association will use percentages of incoming data depending on how much of incoming link overlaps. Figure 6 shows how spatial normalization will be performed.

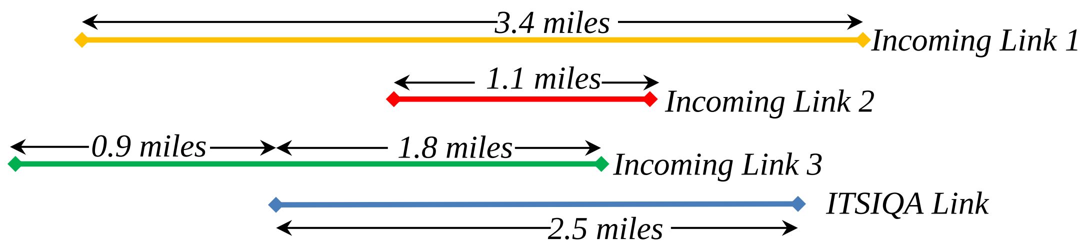

Figure 6: Example of Spatial Data Normalization Method

In the example above, there are three different incoming links, Incoming Link 1 (orange line), Incoming Link 2 (red line), and Incoming Link 3 (green line). These need to be incorporated into the Standard Link (blue line). To do this, three cases should be considered:

- **Case 1, Incorporating Incoming Link 1**: The ITSIQA Link is physically located completely within Incoming Link 1. In this case, 2.5 / 3.4 or 73.5% of Incoming Link 1's travel time should be applied to 100% of ITSIQA Link's travel time.

- **Case 2, Incorporating Incoming Link 2**: Incoming Link 2 is physically located completely within ITSIQA Link. In this case, 100% of Incoming Link 1's travel time should be applied to 1.1 / 2.5 or 44.0% of the ITSIQA Link's travel time.

- **Case 3, Incorporating Incoming Link 3**: A portion of Incoming Link 3 overlaps a portion of the ITSIQA Link. In this case, 1.8 / (0.9 + 1.8) or 66.7% of Incoming Link 3's travel time should be applied to 1.8 / 2.5 or 72.0% of ITSIQA Link's travel time.

5.1.4 Step 4 – Factoring in Level of Service

Each ITSIQA Link will have one or more attributes that indicate the level of service (LOS) of the traffic light(s) that exist within the link. The LOS indicator will affect the Quality Value of reported data for that link. See the Quality Value section of this document for more details of the Quality Value.

There will be six levels of service: A, B, C, D, E, and F. These levels of service correspond with industry standard LOS values in which traffic lights with LOS of A exhibit the lowest vehicle control delay and F exhibit the highest delay.

ITSIQA will allow the configuration of global LOS values. These global values will vary based on time of day.

ITSIQA will allow the configuration one or more LOS values per ITSIQA Link, which will override the global values. Per link values can be configured per time of day. When ITSIQA processes data for a ITSIQA Link, it will average the current LOS values associated with the link to produce a single LOS for the entire link at that time.

As a future enhancement, ITSIQA will update LOS values dynamically from a future interface and/or separate ITSIQA module.

5.1.5 Step 5 – Detector Data Filtering

ITSIQA will initially look for suspicious incoming data and filter as necessary. Note that filtering will only occur at a traffic detector level. Since all detector-level data will be reported via the SunGuide Databus interface, this filtering step only applies to this interface.

This initial filtering will check for expected data ranges and configuration values against what is being reported. ITSIQA will flag issues and automatically generate a MIMS ticket when the data is outside an expected range and meets other criterial indicating device failure or miscalibration – Table 3 dictates which filtering checks will trigger a MIMS ticket. Note that this step will only filter data from raw detector data that ITSIQA will receive via the SunGuide Databus interface. ITSIQA will assume that data received from the C2C data has already been filtered.

Table 3 below lists the initial filtering that ITSIQA will perform during this step, the parameters it will use, and if a MIMS Ticket will be created if the parameter(s) are violated. In all cases, if data will not be used past this step if the parameter(s) are violated.

In order to adjust the sensitivity if too many false alarms are present, the following constants below will changeable from the ITSIQA system administration interface. This also includes the Boolean value of whether to produce a MIMS ticket or not.

All parameters are configurable via the ITSIQA Administrative Editor.

Table 3: Initial Filtering Checks

Filtering Check	Parameter(s)	Action	MIMS Ticket	Learning (Future)
Max Volume	Volume > 50 per 1 Minute per Lane	Flag Lane	Yes	Yes
Max Occupancy	Occupancy > 70% per Lane	Flag Lane	Yes	Yes
Lane Speed Differential	Difference of Speed Between Lanes > 35 MPH Do not flag if volume is zero	Flag if Device Involved 2 Errors	Yes	Yes (interface with EM)
Max Speed	If All Lanes Report Speed ≥ 35, Speed Per Lane > Posted Speed + 25 MPH	Flag Lane	No	No
Min Speed	Speed < 3 MPH for Volumes > 2	Flag Lane	No	No
Inconsistent Values for Volume / Occupancy / Speed	If any of the following are true: Occupancy < 3% and Speed < 45 Speed > 0 and Volume = 0 Speed = 0 and Volume > 0 Occupancy > 70% and Volume = 0	Flag Detector	Yes	No
Sequential Volumes	Same Volume Reported per Lane (i.e. comparing the same Lane's Volume) for 4 Minutes when Volume > 0	Flag Lane	Yes	No

Filtering Check	Parameter(s)	Action	MIMS Ticket	Learning (Future)
Duplicate Values	Same Volume, Speed, or Occupancy for Multiple Lanes (i.e. comparing all Lanes from a single Detector) for 8 Periods (4 Minutes) when Volume > 0	Flag Detector	Yes	No
Directional Checks	This check attempts to determine if a detector's configured direction of traffic is wrong. To do this, ITSIQA will determine the predominate direction of travel by comparing volume of one direction to the volume in the opposite direction at the same location. For example, if direction A > direction B of locations n-1 and n+1, then direction A > direction B of location n. This test fails if the check doesn't pass at least 7 out of 8 times. ITSIQA will need to determine information about the upstream and downstream detectors. Test passes if there is no functional upstream and/or downstream detector.	Flag Detector	Yes	No
Reported Lanes Count	Reported Number of Lanes Don't Match the Configured Number of Lanes	Flag Detector	Yes	No
AADT Checks	Daily Reported Volume for all Lanes at Detector is > or < AADT by 15%	Flag Detector	Yes	No
Communication Down	No data received from a detector for X minutes – Valid Data Time Horizon	Flag Detector	Yes	No

For filtering rules that include "Learning", ITSIQA should automatically adjust the filtering parameters based on historical data. This learning capability should account for reoccurring conditions in order to reduce false alarms. Learning capabilities should be considered a future enhancement to ITSIQA and not included in its initial release.

5.1.6 Step 6 – Quality Value Evaluation

Filtering rules will affect Quality Values the incoming data. ITSIQA will use the Quality Values listed in Table 4.

Table 4: ITSIQA Quality Values

Quality Value Level	Quality Value Range
Good	10 to 7
Medium	6 to 4
Bad	Less than 4
Unknown	N/A

By default, all incoming detectors will have a Quality Value of 10. Each filter in Table 3 has the potential of decreasing the Quality Value if filtering conditions are triggered. The amount that a filter decreases the Quality Value will be configurable.

For data streams that report a Quality Value, the values will be standardized to match ITSIQA's Quality Value ranges. Table 5 maps the Quality Values reported from various data streams to ITSIQA Quality Values. Note that ITSIQA will use the numeric values in the parenthesis. For example, for all data with a "Good" Quality Value, a value of 10 will be assigned.

Table 5: Quality Value Mapping[1]

ITSIQA Quality Value	INRIX	HERE	Waze JAMs[2]	CFX[3]	BlueTOAD[4]
Good (10)	30	>= 0.94	N/A	TBD	TBD
Medium (5)	20	0.94 to 0.7	N/A	TBD	TBD
Bad (1)	10	< 0.7 to 0.0	N/A	TBD	TBD
Unknown (N/A) [5]	*Default*	< 0.0	All Data	*Default*	All Data

Notes:

1. Each of these data streams will be available via the C2C Software, which currently does not support the reporting of a Quality Value. The C2C schema is planned to be updated to support this in a future release of the C2C Software.

2. Waze JAMs has no plans for reporting a Quality Value indicator. As such, this data will be flagged with an unknown Quality Value. Testing should be done during the development of the ITSIQA system to determine possible default Quality Values for this data. Otherwise, see note #5 for unknown values.

3. CFX's travel time system has Quality Value indicators, but does not currently have a single number that indicates the quality of the data. CFX is currently investigating an update to report a single Quality Value. However, the previously-mentioned C2C Software enhancement is required to support the reporting of this value.

4. BlueTOAD has statistical information, such as the number of matches used to produce the reported travel times. This information is not currently reported via the BlueTOAD interface. An enhancement is being considered to report this information.

5. ITSIQA will attempt to resolve all data reported with an Unknown Quality Value. If a data stream is reported with an unknown Quality Value, ITSIQA will compare reported

data with reported data that has a known Quality Value in order to extrapolate a Quality Value. The extrapolated value will be based on differences between the report data.

During the Data Streams Generation step, Quality Values will be averaged to report a single Quality Value per ITSIQA Link. If a Quality Value cannot be determined for a data stream, the data stream will not be used.

5.1.7 Step 7 – MIMS Ticket Generation and Rules

MIMS tickets will be automatically generated based on the filtering rules noted in Table 3. ITSIQA will not generate a ticket unless a rule is violated X out of Y consecutive data reads, where X and Y are configurable. This would need to be reset once it is flagged.

Each filtering rule will be assigned a MIMS priority level. By default, tickets will be set to a Priority 1: Urgent priority level. The priority level will be automatically adjusted based on if there is overlapping data present at a flagged detector location. No overlapping data would increase the priority level. An increased priority level will be set to Priority 2: Emergency. This priority level will be transmitted to MIMS when the ticket is created or updated. If incoming data violates multiple filtering rules, the highest priority level will be used in the MIMS ticket.

ITSIQA will evaluate if one or more MIMS tickets should be generated once per ITSIQA Time Slice. ITSIQA will group MIMS tickets based on the source of the data and roadway. If multiple violations occur per data source and roadway for a single TimeSlice, ITSIQA will generate only one MIMS ticket. If the state of a detector or group of detectors that was included in a MIMS ticket changes in subsequent Time Slices, the previously-generated MIMS ticket will be automatically updated with the most current information about that detector(s). ITSIQA will cap updates after X minutes if the same update is sent

5.1.8 Step 8 – Data Streams Generation

ITSIQA will support multiple data streams. Each stream will use or not use specific data sources depending on agreements with input data providers. Metadata will be configured within ITSIQA to generate outgoing data. Each data stream will be available via the ITSIQA API.

All data streams will be averaged together on a per ITSIQA Link basis, weighed by the Quality Values. ITSIQA will allow configurable adjustments, to weighing the incoming data. These adjustments will allow giving preference to certain data streams over others.

A single Quality Data value will be reported per ITSIQA Link. Quality Data values for all used data streams will be averaged together to determine the reported Quality Data value.

Future enhancements will include a more elaborate algorithm that will identify clustered data to help smooth rising and falling slopes of final reported data.

If there is no valid data available for an ITSIQA Link, the system will flag that link as having no data using a specific attribute. That attribute will indicate a Boolean value of whether there is no data or if there is data. When no data is flagged, systems and users receiving this data should ignore all other data, such as speed, volume, occupancy, and travel time, reported for the ITSIQA

5.1.9 Step 9 – Data Archiving

This step will archive raw and processed data into the ITSIQA database. Raw and processed data will be stored separately. ITSIQA will only archive a month of raw data, which includes all incoming data streams prior to processing. Processed data will reference what raw data was used to generate the data and will be used for data filtering. Future enhancements may use archived processed data to identify trends and/or other data analysis in order to best determine true speed and travel time data.

ITSIQA's database will be designed to optimize system performance.

5.1.10 Step 10 – Output Interfaces

This step involves making processed data available to external systems including the SunGuide Software. For SunGuide and other external systems that desire traffic information, ITSIQA will establish an Application Programming Interface (API) that will allow external systems to request desired data. For the initial deployment of ITSIQA, a plug-in will also be used to interface between the ITSIQA API and the C2C Software.

The ITSIQA API will contain a variety of functions that will provide processed information to external systems in XML format. Initially, this information will include the following two functions:

- **Roadway Network Configuration**: This includes configuration information similar to HERE roadway segments. This information will not change often and will only change if ITSIQA's configuration is altered due to changes in roadway networks. It is recommended that external systems request this information once per day. This function will require input parameters and will deliver a list of output parameters. These include:
    - **Input Parameters**
        - User Credentials
    - **Output Parameters**
        - Roadways
        - Links and Link Definitions

- **Reported Traffic Information**: This includes processed speed, volume, occupancy, and/or travel time information. This information will update within ITSIQA based on its configured Time Slice interval. As such, it is recommended that external systems request this information once per Time Slice interval. This function will require input parameters and will deliver a list of output parameters. These include:
    - **Input Parameters**

    - User Credentials
    - Selected Roadway (or all)
    - Minimum Quality Value
    - Requested TimeSlice
- **Output Parameters**
    - Reported TimeSlice
    - Speed
    - Volume
    - Occupancy (if available)
    - Travel Time
    - Quality Value

For future deployments of ITSIQA, the ITSIQA API can be expanded to include additional value-added information.

A separate interface will be available to MIMS, FDOT D5's ITS ticketing system. Based on specific filtering rules discussed in this document, ITSIQA will automatically generate MIMS tickets.

Figure 8 depicts the flow of data from ITSIQA and SunGuide software, as well as other external systems.

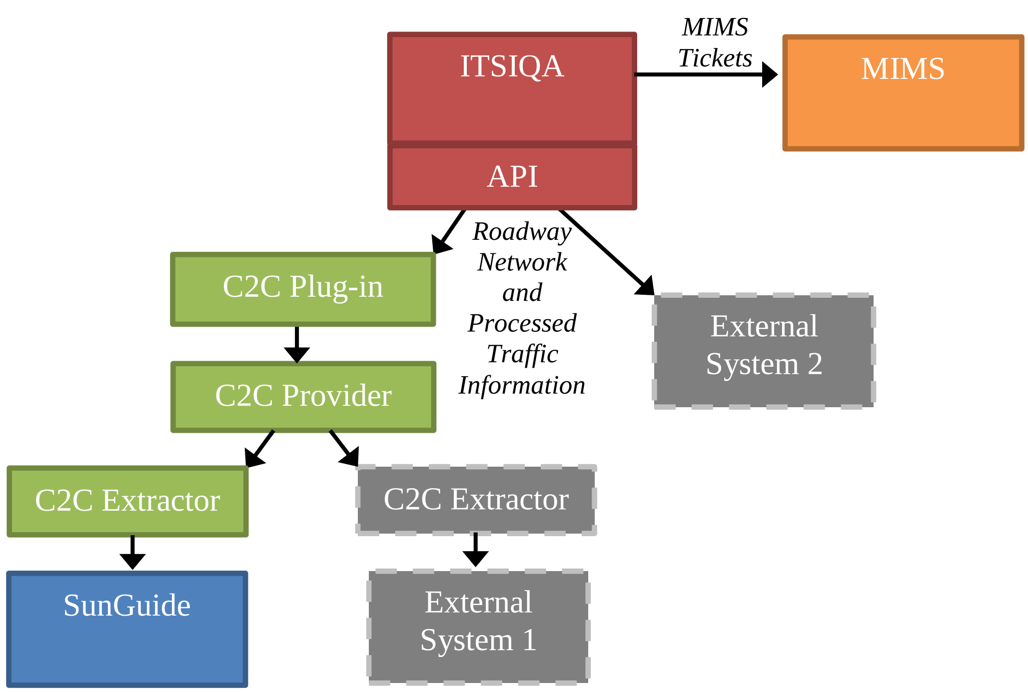

Figure 8: Output ITSIQA Data to Various Systems

As shown in Figure 8, a C2C plug-in will be created to provide ITSIQA Roadway Network Configuration and Reported Traffic Information in C2C-formatted XML data. The C2C plug-in will generate two C2C XML files, networkData and trafficCondData – both are C2C XML Schema elements that SunGuide requires to use traffic information from external systems. This C2C data will be available to SunGuide and other external systems via a C2C Provider, in which SunGuide and other systems will acquire using a C2C Extractor. Alternatively, external systems could interface with the ITSIQA API directly instead of going through the C2C infrastructure. A direct interface will allow requesting information that may not be available in the C2C Schemas.

Note that metadata within the outgoing ITSIQA API data will dictate if information used data that should not be resold, i.e. data from INRIX and/or HERE. It would be the responsibility of the systems receiving data from ITSIQA to filter based on the metadata as necessary. The C2C plug-in will not filter out this data.

5.2 Modes of Operation

This section describes the three modes of operation that ITSIQA will support.

1. **Standard Mode**: In this mode of operation, ITSIQA will receive traffic information from its data inputs, process, filter, and consolidate the data according to the configured metadata, and output processed data. This mode also includes performing checks on the incoming data to identify potential issues and alert external systems like MIMS.

2. **Degraded Mode**: This mode of operation will function just like Standard, except a system interface will be flagged as failed. If an external system does not provide data by a configured timeout period or if ITSIQA cannot successfully connect to the system, that interface will be flagged as being failed. This failed state will be logged and an alert will be sent, if possible. However, the system will continue to process whatever data is can without the data associated with the failed interface.

3. **Test Mode**: This mode of operation will be used during system integration testing. In this mode, data will not be processed as normal. Instead, ITSIQA will establish a connection with selected interfaces and log data being received and/or sent, depending on the interface. Connection errors will be logged for troubleshooting purposes.

5.3 User Involvement and Interaction

System Administrators will need to initially configure connectivity information of all external systems and traffic detectors. ITSIQA will initially use HERE.com segments for its standard reporting list of roadway segments. However, changes to this list will need to be reflected in ITSIQA’s configuration.

Once all configurations are completed, ITSIQA should operate without day to day human interaction. However, ITSIQA logs should be monitored to ensure no major issues are being reported.

5.4 System Support

Once ITSIQA has been fully accepted, this system will be supported using the existing ITS operations and support structure.

5.5 Support Environment

ITSIQA will be hosted on dedicated hardware within FDOT District 5's virtual server farm. FDOT District 5 staff will provide the necessary server allocations to support the operational needs of ITSIQA. These needs will be determined during the detailed system design phase of the project.

6. Operational Scenarios

The ITSIQA will be operational 24/7/365, automatically making decisions of incoming data without human interference. As such, ITSIQA will need to handle a number of scenarios that are likely to occur. The following are some of these scenarios.

6.1 Evaluate Multiple Incoming Closely-Related Data

ITSIQA will receive data from multiple data sources. ITSIQA's weighed averages will consolidate multiple incoming closely-related data into a single set data on a link by link basis..

6.2 Evaluate Multiple Incoming Disparate Data

There may be cases when multiple data sources will report very different traffic information for the same section of roadway. ITSIQA's weighed averages will consolidate multiple incoming closely-related data into a single set data on a link by link basis.

6.3 Evaluate Multiple Incoming Closely-Related and Disparate Data

There may be cases when similar traffic information will be reported from some data sources, but not others. ITSIQA's weighed averages will consolidate multiple incoming closely-related data into a single set data on a link by link basis.

6.4 Evaluate Single Incoming Data

There may be cases when only one data source may be available for a single section of roadway. In this case, ITSIQA will need to rely on other means to evaluate the validity of the data, such as archived data or configured expected values. ITSIQA will lean on existing methods as described in the following documents:

- Guide to Establishing Monitoring Programs for Travel Time Reliability
- Use of Multiple Data Sources for Monitoring Performance Final Report
- Regional Transportation Data Warehouse

The ITSIQA algorithms will dedicate the actual calculations to be used for the reported data.

6.5 Detect Missing or Abnormally Reporting Incoming Data

Through the course of maintaining hundreds of traffic detectors throughout the district, there may be a number of cases when a detector may report falsely. Examples may include a detector not reporting all configured lanes, or reporting the wrong direction of travel, or reporting lane by lane information where lanes are configured in the incorrect order. ITSIQA will flag these detectors and automatically generate a MIMS ticket to alert O&M contractors to respond and troubleshoot accordingly. The checks for these cases are handled in the detector filtering stage of the ITSIQA process.

6.6 Detect Failed Interfaces

This scenario captures the case when an interface fails. ITSIQA will be receiving data from multiple interfaces and providing processed data and alerts to multiple interfaces. Each interface relies on external systems that are outside of ITSIQA’s control. The failure of an external system, including silent failures where the system just stops reporting beyond the Valid Data Time Horizon interval, should not cause ITSIQA to fail. Instead, the interface should be flagged, logged, and continue to operate in a Degraded mode of operation.

7. Summary of Impacts

The overall intended impact of ITSIQA is to greatly improve the traffic information reporting of the district’s ITS, improve the awareness of O&M issues, and generate high-quality traffic information that will be used by district traffic operations and the traveling public.

There will be an extremely large volume of data archived by the system for the purposes of data comparison. This should be architected carefully to ensure appropriate resources are provided and other resources and assets are not affected.