CONFLICT MONITOR FOR PLUG-AND-PLAY
DISTRIBUTED SMART SIGNALS AND SENSORS FOR
TRAFFIC CONTROLLERS

Final Report
KLK122
N08-07

National Institute for Advanced Transportation Technology

University of Idaho

Dr. Richard Wall and Dr. Brian Johnson

December 30, 2008 – Revised July 2010
DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the Department of Transportation, University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.
### Abstract:

This report addresses a solution to implementing a safety critical network applied to distribute-control of traffic signals. Conventional approaches to traffic controller conflict or malfunction management is to use an independent electronic device physically placed in the traffic controller cabinet that observes all the signal states controlled by the intersection.

In a distributed processing environment, the direct signal controls are spatially distributed and the conflict monitor is no longer able to observe the status of all lights. The challenge undertaken by this research was to investigate methods of implementing a safety critical distributed processing system suitable for traffic signal controls. The basic approach was to make all distributed operations observable from both time and value perspective. Redundancy is acknowledged as one method of achieving high system reliability. However, the cost and complexity of redundancy will render a distributed control system unaffordable.

We focused on a solution that used expectancy and check back to provide observability of remote operations. The solution that we investigated was implemented on low-cost 8-bit microcontrollers to achieve one millisecond system synchronization. An IEEE 1588 Precision Time Protocol standard was incorporated with the information protocols to implement a time division multiplexing scheme. Using the time precision protocol, each node can be observed and the actions verified.

This report presents the methods and performance characteristics of using the IEEE 1588 standard for providing failure detection on distributed traffic signal systems.
# TABLE OF CONTENTS

Figures................................................................................................................................. ii
Tables...................................................................................................................................... ii
EXECUTIVE SUMMARY .................................................................................................... 1
BACKGROUND ...................................................................................................................... 4
MOTIVATION FOR SMART SIGNALS AND SENSORS ....................................................... 6
  Improved Quality of Service and Access .............................................................................. 6
  Cost Reduction....................................................................................................................... 7
  Traffic Control Fine Tuning ................................................................................................ 8
APPROACH AND METHODOLOGY - DISTRIBUTED TRAFFIC SIGNAL ARCHITECTURE .................................................................................................................. 9
  Hardware Architecture........................................................................................................ 9
  Hardware Description........................................................................................................... 12
  SSN Software Model ......................................................................................................... 12
SYNCHRONIZATION OF SSN DEVICES ............................................................................ 14
  Overview of IEEE 1588 ..................................................................................................... 15
  PTP Clock Source .............................................................................................................. 15
  Synchronization Error ....................................................................................................... 15
  SSN Communication Scheduling ..................................................................................... 16
  Failure Modes .................................................................................................................... 18
FAULT DETECTION AND HANDLING .............................................................................. 18
FINDINGS; CONCLUSIONS; RECOMMENDATIONS .......................................................... 20
ACKNOWLEDGMENT .......................................................................................................... 21
REFERENCES ....................................................................................................................... 22
FIGURES

Figure 1: Diagram of NEMA TS2 traffic controller cabinet equipment. ........................................ 5
Figure 2: Photo of equipment in a NEMA TS2 cabinet (photo courtesy of Econolite Controls). .................................................................................................................. 8
Figure 3: Communication architecture for distributed Smart Pedestrian Traffic Signal System.................................................................................................................. 11
Figure 4: OSI and SSN software models. ....................................................................................... 13
Figure 5: Synchronization error percent frequency distribution plot............................................ 16
Figure 6: SSN communication scheduling scheme ........................................................................ 17
Figure 7: TCID omission failure detection. .................................................................................. 20

TABLES

Table 1: Definitions of Acronyms .................................................................................................. 3
EXECUTIVE SUMMARY

Traffic controllers use standard interfaces that conform to recognized NEMA or ITS standards. Under these standards, the controller uses single function signaling wires to communicate with intersection traffic and pedestrian signals. Modern traffic controllers have far greater capability than are currently utilized because existing interfaces are constrained to one-way communications.

Present signal systems are limited as to the type of information and number of predefined messages that can be displayed or devices controlled. A model of Plug and Play (PnP) Distributed Signal Network (DSN) traffic controller architecture was demonstrated to selected representatives of the Federal Highway Administration (FWHA), universities, consultants, and manufacturers of traffic controllers at the Transportation Research Board (TRB) Signals Systems Committee mid-year meeting in Las Vegas, NV (July 10th -13th, 2005). All agreed that existing controller architectures are incapable of providing the fine grained sensing and the degree of control expected to manage today’s transient, automobile, bicycle, and pedestrian use of roadways.

The response was overwhelmingly positive, and feedback identified a critical next step in the development of this technology. The system must ensure safe-fail operations by including a conflict monitor (CM) before there will be acceptance of this new technology by the state and federal department of transportation (DOT) agencies. Since the PnP DSN architecture uses software to a much higher degree to distribute the control information, existing CMs designed for central control hardware based architectures are no longer able to provide safe-fail mode operations. Hence, a distributed approach to conflict monitoring is necessary for this technology to move forward.

Today’s signalized traffic controls represent a closed loop control system that uses rudimentary sensor inputs to signal a request for service. The information reduction to a binary on/off state discards any information that may indicate the need for special service. A distributed approach to road traffic management is capable of providing enhanced services to special need users and can quickly reconfigure traffic lights to comply with operations to accommodate abnormal traffic patterns. However in a distributed control environment, the safety critical monitoring is normally
provided by the Malfunction Management Unit (MMU). In order to compensate for this loss of monitoring capability in a timely fashion, the concept of safety critical network (SCN) operations is introduced to provide the level of reliable operations comparable to today’s conventional traffic signal operations.

The safety critical managed network provides a safe-fail environment for communication of traffic signal light controls using an Ethernet based local area network. Safety critical operation is enforced by validating operating modes using communications that is expected in a timely manner. The SCN management implements a scheduling scheme in which a global time base is divided into mutually exclusive time slots during which a specific device is allowed to access the communication network. This global time base is generated using the IEEE 1588 Precision Time Protocol. In this paper, we present a safety critical network with a communication scheduling scheme that facilitates detection of all critical device failures within the 450 ms required by traffic standards.
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIU</td>
<td>Bus Interface Unit</td>
</tr>
<tr>
<td>BPL</td>
<td>Broadband Power Line</td>
</tr>
<tr>
<td>CGI</td>
<td>Common Gateway Interface</td>
</tr>
<tr>
<td>CM</td>
<td>Conflict Monitor</td>
</tr>
<tr>
<td>DSN</td>
<td>Distributed Signal Network</td>
</tr>
<tr>
<td>EoP</td>
<td>Ethernet over Power Line</td>
</tr>
<tr>
<td>FHWA</td>
<td>Federal Highway Administration</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineers</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transportation Systems</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>MMU</td>
<td>Malfunction Management Unit</td>
</tr>
<tr>
<td>MMUID</td>
<td>MMU Interface Device</td>
</tr>
<tr>
<td>MUTCD</td>
<td>Manual for Uniform Traffic Controller Devices</td>
</tr>
<tr>
<td>NEMA</td>
<td>National Electrical Manufacturers Association</td>
</tr>
<tr>
<td>NIATT</td>
<td>National Institute for Advanced Transportation Technology</td>
</tr>
<tr>
<td>NTCIP</td>
<td>National Transportation Communications for ITS Protocol</td>
</tr>
<tr>
<td>PnP</td>
<td>Plug and Play</td>
</tr>
<tr>
<td>PTP</td>
<td>Precision Time Protocol</td>
</tr>
<tr>
<td>RCM</td>
<td>Rabbit Core Module</td>
</tr>
<tr>
<td>SDLC</td>
<td>Synchronous Data Link Control</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SCN</td>
<td>Safety Critical Network</td>
</tr>
<tr>
<td>SSN</td>
<td>Smart Signals Node</td>
</tr>
<tr>
<td>SPN</td>
<td>Smart Pedestrian Node</td>
</tr>
<tr>
<td>TCID</td>
<td>Traffic Controller Interface Device</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Data Protocol</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
</tbody>
</table>
BACKGROUND

Researchers at the University of Idaho’s National Institute for Advanced Transportation Technology (NIATT) have been investigating methods of applying networked based distributed control approach for controlling traffic signal lights and detecting requests for service by vehicles and pedestrians since January 2006. We encountered three issues in the process of changing the control approach for improving intersection management: an infrastructure to support the information system, sensors that provide the detection desired, and a control process that can effectively use this information. When the application of a control system affects public safety or high economic risk, there is an additional requirement to ensure safe and reliable operations of the control system. As our research continues to develop sensors, communications, and control processes, we must address the one issue that is necessary for industry and public acceptance: a safety critical control environment. In this paper, we present a safety critical network with a communication scheduling scheme that facilitates detection of all critical device failures within the 450 ms required by traffic standards.

Today, the traffic and pedestrian signal displays that regulate the flow of motor-vehicles, bicycles, and pedestrians in a road traffic intersection are managed by a central traffic controller. The traffic and pedestrian signal displays are switched on and off by the traffic controller based on various inputs and timing plans. Present intersection traffic control systems are designed to provide a safe and efficient flow of motor-vehicles, bicycles, and pedestrians. A simplified block diagram (Error! Reference source not found.) illustrates the major components in a typical NEMA TS2 traffic controller cabinet [1].
Depending on the mode of operation, the microprocessor-based traffic controller, located in the cabinet, makes control decisions based on time, vehicle detector inputs, video detector inputs, pre-emption inputs, and pedestrian button inputs. The output from the traffic controller is sent to the load switch amplifiers that switch the pedestrian and traffic signal lights on or off.

Currently, NEMA TS2 controller cabinets consists of four major components as shown in Error! Reference source not found.. A Synchronous Data Link Control (SDLC) communicates inputs and outputs to other system components via the bus interface unit (BIU). Control of signal lights and detectors that sense vehicles on approaches to the intersection or pedestrians requesting service use point to point wiring with the terminals of the bank of load switches and detector rack respectively.

The traffic controller changes the signal outputs based on either a fixed time basis or actuation calls placed by vehicles and pedestrians. Semi-actuated controller schemes use a combination of both fixed time and actuated control algorithms.

The MMU monitors all outputs from the load switches to ensure that the traffic and pedestrian signal lights are in a non-conflicting state. The MMU operates on the premise that all control
decisions made by the traffic control, and the states of all output signals are observable at the terminals in the controller cabinet. The MMU is required to take over control of the intersection traffic signals and activates a safe-fail mode within 450 ms of fault detection [2]. In this safe-fail state, all red signals within the traffic intersection flash synchronously with the pedestrian signals turned off.

**MOTIVATION FOR SMART SIGNALS AND SENSORS**

A recently proposed enabling technology developed at NIATT known as “Smart Signals” is based on a distributed control system in which the traffic signals are controlled by Ethernet connected spatially distributed microprocessors [3, 4, 5]. Microprocessor-based traffic signal lights enable the system to communicate complex data to provide enhanced services to users. The advantages of such a system are improved quality of service, lower cost, and greater effectiveness. Some of the advantages of the distributed approach to road traffic control systems in these three areas are discussed in the subsections below.

**Improved Quality of Service and Access**

Inductive loop detectors or video cameras are used to sense the presence of vehicles in a specific area of the approaches to an intersection. Pedestrians place requests for service by manually operating mechanical or piezoelectric push buttons. Regardless of the capability of the sensors to measure traveling characteristics of the vehicle or pedestrian, the communications of existing traffic controller systems are constrained to binary presence or absence of information and cannot distinguish an able-bodied pedestrian from a special need pedestrian or a heavily loaded freight truck from a motorcycle.

Using the Smart Signals concepts, the traffic controller can identify pedestrians who are at risk because of a physical or cognitive disability [6, 7]. NIATT researchers are currently developing an architecture for guiding and tracking visually impaired pedestrians using audible and tactile feedback while they cross an intersection [8].

By installing sensors and microprocessors within vehicles and pedestrian signal display equipment or in the vicinity of this equipment, it is possible to communicate pertinent information, such as ambient noise volume, pedestrian types, and vehicle types, to the traffic
controller. The traffic controller then adjusts the pedestrian and vehicle phases to provide additional crossing time when the need arises. The end result is improved quality by providing safer access to the intersection.

**Cost Reduction**

A picture of a modern NEMA TS2 equipment cabinet is shown in Figure 2. Typically, such a cabinet is installed at one of the corners of every signalized intersection. The cabinet represents a safety risk because it can obscure vision for pedestrians and vehicle operators. In metropolitan areas, the cabinets are subject to vandalism and impede pedestrian traffic. In urban areas, the cabinet detracts from the neighborhood aesthetics.

Over 60 percent of cabinet space is allocated to terminal connections to accommodate the point-to-point wiring and the AC load switches that can be seen in the bottom portion of Figure 2. Using microprocessor controlled LED-based signal lights and Ethernet over power line (EOP) for both powering signals and communication eliminates the need for this space.
In theory, using a distributed control approach could reduce the controller to a size that could fit into a pedestrian signal. This results in savings due to reduced equipment, installation and maintenance costs.

**Traffic Control Fine Tuning**

Based upon the Manual for Uniform Traffic Controller Devices (MUTCD), current traffic signal devices display only a limited set of symbols, i.e. walk and don’t walk icons for pedestrians and the common green, red, and yellow balls and arrows for vehicles [9]. Smart traffic signal devices can be used to display a wide range of symbols and information that can change dynamically to reflect current road operations. The difficulty of changing signal lights for temporary traffic patterns makes the information displayed to the driver incorrect, contradicting signage and often confusing drivers, thus generating unsafe intersection operations. With Smart Signals, dynamic
signaling can communicate information about the system such as system failure modes or symbols for redirecting traffic during special events or emergencies.

**APPROACH AND METHODOLOGY - DISTRIBUTED TRAFFIC SIGNAL ARCHITECTURE**

Smart Signals uses distributed intelligence to provide enhanced capability. Information is exchanged with NEMA TS2 controllers using the National Transportation Communications for Intelligent Transportation Systems Protocol (NTCIP) [10]. Signal status and detector calls are communicated using Simple Network Management Protocol objects based on the NTCIP 1201 and 1202 standards [11, 12]. This software interface replaces all direct wire connections between the traffic controller and signal lights and detectors.

Our initial development (January 2006) of the Smart Signals technology explored the benefits of a distributed plug and play traffic signals system. This system demonstrated the advantages of a distributed approach to road traffic signal systems such as dynamic signaling and improved pedestrian countdown signals.

This previous Smart Signals research did not address the loss of capability to detect conflicts in vehicle and pedestrian signal states. This deficit led to the development of a safety critical software architecture for distributed Smart Signals system. The safety critical software architecture is added to the Smart Signals information architecture. It implements a scheduling scheme in which a global time base is divided into mutually exclusive time slots during which each specific device is expected to communicate with a network monitor. In effect, this scheduling implements a time division multiplexing communication scheme to establish the determinism and expectation necessary to ensure that all devices are performing in a correct and timely manner. The global time base is generated using the IEEE 1588 Precision Time Protocol (PTP) [13]. This initial research focused on pedestrian signals because of an inherent limitation to countdown pedestrian signals that caused the signals, on occasion, to display incorrect times.

**Hardware Architecture**

The Smart Signals system consists of four types of network nodes: the traffic controller, the Smart Signals pedestrian signal, the Smart Signals pedestrian button, the MMU Interface Device
(MMUID) and the traffic controller interface device (TCID) (Figure 3). The TCID is required to solicit the object status from the traffic controller. Normally this information is provided by the traffic controller using Simple Network Management Protocol (SNMP) [14] traps, part of the NTCIP 1202 standard, that periodically generate the objects and is distributed to all nodes on the network. However, this feature was not implemented by the controller manufacturer at the time of testing.

Using the Smart Signals distributed environment for actuated traffic intersection, pedestrians send their request for service by actuating a pedestrian button to initiate a pedestrian walk phase. In the Smart Signals architecture, a local pedestrian button interfaces a Smart Pedestrian Node (SPN) using a wire or wireless type communications. A remote pedestrian button currently interfaces with the SPN using wireless IEEE 802.15.4 [15] compliant Xbee communications modem. A remotely operated pedestrian button has access and safety benefits for vision and mobility impaired pedestrians.

In our testing, the SPN interfaces with the NEMA TS2 Type 2 traffic controller and other Smart Signals Node (SSN) devices via a 10baseT Ethernet port. When operating normally, the SPN periodically broadcasts status messages during its appointed time period. This type of message is used to monitor the status of distributed SSN devices. Failure to receive a status message from the scheduled sender node during its pre-assigned time slot is interpreted as device failure by the MMUID.

Upon actuation of a local or a remote pedestrian button, the SPN interfacing with the pedestrian button transmits a pedestrian request for service packet to the traffic controller. This notification packet is sent immediately after transmitting its status packet using SNMP in the form of a management information base (MIB) object, as specified by the NTCIP 1202 standard. The traffic controller appropriately updates the internal variables defining the state of all pedestrian traffic signals, pedestrian countdown displays, and traffic signal lights that are normally used within an actuated intersection based on several inputs.

The TCID requests the control packet from the traffic controller after broadcasting its own status packet. When the TCID receives the SNMP control message from the traffic controller, it rebroadcasts this message to the Safety Critical Network (SCN). On receiving this control
message, the SPN sets the pedestrian signal lights and pedestrian countdown displays to appropriate states.

An SPN controls the display on LED pedestrian traffic signals and countdown signals using low voltage level logic. A pedestrian traffic signal light consists of two symbols—a walking person symbolizing walk and an upraised hand symbolizing don’t walk. A pedestrian countdown signal light consists of two seven-segment displays that show the number of seconds remaining to

Figure 3: Communication architecture for distributed Smart Pedestrian Traffic Signal System.
complete the road crossing, commonly called the pedestrian clearance interval [9]. During this interval, the wait symbol flashes at a one Hz rate.

The MMUID issues PTP sync packets in order to synchronize the clocks on all SSN nodes. The MMUID also ensures that all distributed SSN devices are consistently transmitting status messages during their scheduled interval. On detection of a system failure, the MMUID sets the Smart Signals pedestrian signals into a safe-fail mode where all pedestrian signals are turned off and the red traffic signals for all approaches flash at a one Hz rate. For systems that contain a combination of conventional and Smart Signals devices, the MMUID interfaces with the TS2 cabinet MMU in order to register a fault condition that the MMU otherwise would not detect.

**Hardware Description**

The hardware architecture described above implements spatially distributed Smart Signal nodes using low cost, commercial Rabbit Core Module (RCM) 3000 boards [16] based on the Zilog Z180 architecture operating at 29 MHz. The necessary components of RCM 3000 board used in this architecture are the Rabbit 3000 8-bit processor, the 48-bit real time clock (RTC) counter, parallel I/O ports for controlling pedestrian traffic/countdown displays, and a 10 Mbits/s Ethernet port controlled by Realtake’s RTL8019AS Ethernet controller chip [17].

An Econolite ASC3 traffic controller was used for testing but was not installed in a traffic controller cabinet [18]. The traffic controller was modified by the manufacturer for our research to provide a MIB object for the pedestrian phase time intervals.

Two different Ethernet hubs were tested. A Netgear Model EN104TP four port hub and a Netgear Model FS608 eight port switch. The results of testing revealed that there were no difference in test results between using a hub and switch.

**SSN Software Model**

In a safety critical traffic control communication system, we are more concerned with determinism rather than with speed. Various communication technologies could be used for data transmissions, i.e. LonTalk, SmartDistributedSystem, ControlNet, InfiniBand, BlueTooth, and Ethernet. In our system, SSN devices use 10baseT Ethernet for data communications due to its low cost and rich library to support development. It is not possible to ensure a deterministic
communication system using the Ethernet 803.2 standard [19] due to possibilities of data collisions and retransmissions after collisions. SSN devices use custom software in order to realize 10baseT “time triggered” deterministic Ethernet communications. The SCN ensures that only one SSN device transmits data over the network during a given time interval using custom software developed for distributed traffic control systems. The SCN allows for detection of failed nodes within a SSN cluster. Figure 4 represents an abstract software model for a distributed traffic control environment that is based on the Open Systems Interconnection Basic Reference (OSI) model [20]. The physical (PHY) layer consists of a hardware connection to the other network devices using 10baseT Ethernet CAT 5 cable. Each SSN has a unique 48-bit physical Media Access Control (MAC) address. The SSN MAC layer uses this address for identifying the source and destination nodes for the data being transmitted.

![OSI model and SSN model diagram](image)

**Figure 4: OSI and SSN software models.**

The SSN Internet Protocol (IP) layer provides data fragmentation and re-assembly services for SSN devices. Each SSN device is assigned a unique 32-bit logical IP address. The User Datagram Protocol (UDP) layer transfers data to and from the application layer. Unlike most applications that use Transmission Control Protocol (TCP/IP), we use UDP/IP because this protocol supports broadcast/multicast messaging and does not require verification from the recipient. Although this protocol does not provide guaranteed reception of data, it is still suitable
for our application because the scheduling layer of the SSN network model handles status message omissions.

The session layer in the OSI model is replaced with a synchronization layer in the SSN software model. The PTP layer ensures synchronization of SSN cluster devices using PTP. The presentation layer in the OSI model is replaced with a SSN layer that handles communication scheduling of distributed nodes. The distributed traffic control systems application layer handles the issuing of SSN cluster messages and contains necessary software functions for various types of SSN devices.

Various types of messages shown are routed through the same *physical* Ethernet port (Figure 3). However, different *logical* connections are made for communication of different types of packets. Only three *logical* ports are currently used in the Smart Signals architecture: PTP event port, SSN port, and SNMP port. PTP packets are routed through the PTP event port and similarly SSN status packets are routed through the SSN port. The SNMP port is used to communicate packets in the traffic control application layer of the SSN software model.

**SYNCHRONIZATION OF SSN DEVICES**

Although various protocols that manage clock synchronization in distributed systems are available, we chose the IEEE 1588 PTP standard for SSN clock synchronization because it requires a relatively small amount of computational burden and utilizes only a few network messages. This protocol utilizes a master-slave communication scheme that required little programming effort to incorporate into the traffic controller management environment. The implementation of PTP time synchronization protocol does not require a Global Positioning System (GPS) or other global time receiver to be installed in all nodes. Since absolute time synchronization is not required, we use the traffic controller’s time clock as the system time reference. PTP facilitates high synchronization accuracy with relatively low cost and can be implemented on commercially available hardware components. The IEEE 1588 time synchronization protocol is suitable for distributed systems that support broadcast/multicast messaging schemes and it supports systems with various types of clocks.
Overview of IEEE 1588

The IEEE 1588 protocol uses four types of messages: sync, follow-up, delay request, and delay response. PTP sync and delay request messages are transmitted and received on the PTP event port and PTP follow up and delay response messages are transmitted and received on PTP general port. PTP sync messages contain the master clock time sampled in the PTP layer before it is transmitted to the PTP slave devices. These time samples are used by PTP slave devices to synchronize their individual clocks. The PTP follow-up message can be used for applications that require higher precision synchronization. PTP follow-up messages contain more precise estimates of sync message send time that is captured near the physical layer. This type of message is not currently utilized in our system. Delay request messages are used along with corresponding delay response messages in order to determine one way communication delay from PTP master node to PTP slave node. We use a slightly different messaging scheme with similar principles in order to determine a nominal communication delay value. Our system only uses PTP sync messages during normal operation.

PTP Clock Source

Each Rabbit Semiconductor RCM 3000 based SSN is equipped with a 48-bit real time clock (RTC) counter that uses a 32.768 kHz quartz crystal oscillator. The 32.768 kHz is the time base for a 48 bit counter that is capable of counting up to 272 years without rolling over. While copying the counter value into program variables, the most significant bit of the counter is ignored as entire counter bits are shifted left by one. This reduces the capability of the counter by half. The RTC counter values are divided into two segments. RTC bits 46 through 15 are stored in a variable named time_seconds and RTC bits 14 through 0 are stored in a variable named time_ticks. The SSN RTC counter is used as a clock source for PTP synchronization.

Synchronization Error

Factors such as clock drift, clock resolution, clock variance, communication latency, and communication delay fluctuations must be taken into account in order to synchronize clocks across the network. Each of these factors can contribute to synchronization errors. It is important to minimize this error in order to develop a communication scheduling scheme with mutually exclusive time slots.
Figure 5 shows a frequency distribution plot for the synchronization error observed in our system. This plot was obtained by running a synchronization test for 12 hours. During this test, samples were taken from the PTP master and the slave clocks every 500 ms. Clock samples were then compared to generate the data for the plot in Figure 5. Figure 5 illustrates that during the majority of the test period interval, the synchronization error was limited to ±100 µs. The worst case synchronization error for this 12-hour test period was 808 µs.

![Frequency Distribution of Synchronization Error](image)

**Figure 5: Synchronization error percent frequency distribution plot.**

**SSN Communication Scheduling**

A global time base generated using PTP synchronization is divided into mutually exclusive time slots dedicated for SSN cluster data transmission. In our application, we use 15 time slots allocated to ten spatially distributed SSN devices. Figure 6 shows the communication scheduling scheme [21] used for distributed traffic control system applications. The non-idle slots are 15.625 ms long and idle slots are 7.813 ms long. Idle slots are used to allow SSN devices to process MMUID sync messages and TCID control messages. Therefore each scheduling cluster
cycle is 203.125 ms. Using this scheme, the MMUID can detect critical and non-critical faults within a span of 203 ms.

Slot number zero is dedicated to the MMUID/PTP master. This slot is used to broadcast PTP sync messages to the network devices and contains necessary information for synchronizing PTP slave clocks. Slots numbered three through ten are allocated to spatially distributed SPNs. During these time slots, the SPNs broadcast their status messages on the SSN port. If a request for service is initiated from a local or remote pedestrian button, a pedestrian request for service message is sent directly to the traffic controller within the same slot interval. Slot number 12 is allocated to the TCID for broadcasting its status messages to MMUID. After sending the status message, the TCID sends a SNMP control request message to the traffic controller and rebroadcasts the received controller packet to the remaining SSN devices. Slot number 11 is allocated to the MMUID to transmit status messages to all nodes on the Smart Signals network to indicate the health of the system.

![Figure 6: SSN communication scheduling scheme](image-url)

- non idle slot interval = 15.625 ms
- idle slot interval = 7.813 ms
- cycle interval = 203.125 ms
Failure Modes

Failures occur when a component fails to meet system data integrity or time response requirements. Hardware or software failures within a distributed SSN device that inhibit reliable operation of the overall system cause critical faults. Some of the common types of failures that occur in a distributed traffic control system are: data omission/loss failure, node crash failure, communication scheduling failure, and SSN state failure [22].

Data omission/loss failure occurs when SSN nodes fail to receive status messages from the scheduled sender node. Node crash failure occurs when a distributed node hardware component fails, i.e. failure of a power supply, a processor, an Ethernet chip failure, a communication bus, or a RTC counter. This type of failure generally manifests into an omission failure.

Communication scheduling failures occur when a scheduled sender node delays a transmission status message or transmits a status message within time slots of other SSN nodes. When a SSN node transmits data during an invalid time slot, it may interfere with the data being transmitted by a valid SSN. This type of failure can cause data collisions during which critical data may be lost. The error can be caused by hardware/software errors within the synchronization layer. SSN state failure occurs when a pedestrian display unit does not conform to the state specified by the traffic controller control message.

FAULT DETECTION AND HANDLING

Detection of status message omission helps the system to identify faulty SSN nodes. A SSN device in an active state is responsible for consistently transmitting status messages during its allocated time slot. Faults within the TCID or the MMUID are considered to be critical faults. Occurrence of a critical fault triggers the system to enter safe-fail mode. In this mode, all vehicle traffic signals flash red. A failed SPN is treated as a non-critical fault as long as it can be determined that the pedestrian signal is not displaying the walk light. When non-critical faults occur, the system still operates; however it loses some of its functionalities. Figure 7 illustrates what happens when the system detects a critical TCID fault that was generated by disconnecting the Ethernet cable connected to the TCID.
Figure 7 is an oscilloscope capture that demonstrates the functional operation of the SSN. The MMUID slot interval signal represents the MMUID time slots. As mentioned earlier, time slot number zero is allocated for transmission of a sync message and slot number eleven is allocated for transmission of a MMUID status messages. In Figure 7, the pulse during on the TCID trace represents the TCID time slots and the pulse on the SPN trace represents the SPN time slots.

The TCID loses its time slot after its Ethernet cable is removed. The rising edge of the MMUID failure detect signal represents TCID omission failure detection by the MMUID. The MMUID detects the TCID omission fault within 203 ms in worst cases. On detecting the TCID omission failure, the MMUID puts the SPNs into a safe-fail mode of operation. The communication scheduling scheme presented in this paper allows only up to eight SPN devices to be connected to the SCN. However, future distributed traffic control applications that require more SPN devices could use multiple MMUIDs for handling multiple SPN clusters without increasing fault detection time.
**FINDINGS; CONCLUSIONS; RECOMMENDATIONS**

This report discusses a distributed traffic control system with enhanced capabilities that implements a communication scheduling scheme to detect failures within spatially distributed SSN devices using low cost, commercially available hardware. Using the scheduling scheme, it is possible to detect critical faults within 203 ms in the worst cases. This worst cast fault detection interval is within the 450 ms specified in NEMA TS1 standard.

In our system, a worst case synchronization error of 808 μs was observed using the IEEE 1588 PTP standard. Reducing synchronization error facilitates developing an efficient communication scheduling scheme with mutually exclusive time slots.
ACKNOWLEDGMENT

Funding for this research was provided to the NIATT by the U. S. Department of Transportation, Research and Innovative Technology Administration, Grant No. DTRS98-G-0027. Equipment and engineering support was provided by Econolite Control Products, Inc. 3360 East La Palma Ave. Anaheim, CA, 92806 and Campbell Company, 450 McGregor, Boise, ID 83705.
REFERENCES


