STANDARDS ITS TRAINING

WELCOME

U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology

Welcome

Ken Leonard, Director
ITS Joint Program Office
Ken.Leonard@dot.gov

www.pcb.its.dot.gov

Module A315b Part 2:

Specifying Requirements for Actuated Traffic Signal Controllers (ASC) Based on NTCIP 1202 v03 Standard Part 2 of 2

Updated July 2020

Instructor

Kenneth L. Vaughn

President

Trevilon LLC

Learning Objectives

Manage Special Considerations for NTCIP 1202: Infrastructure

Manage Special Considerations for NTCIP 1202: Functionality

Incorporate Requirements Not Supported by Standardized Objects

Testing NTCIP 1202 v03 Conformance

Learning Objective

Manage Special Considerations for NTCIP 1202: Infrastructure

Special Considerations: Infrastructure

Overview

- Origins of NTCIP
- Simple Network Management Protocol (SNMP)
- Simple Transportation Management Protocol (STMP)
- Exception-Based Reporting
- Block Objects
- Infrastructure Limitations
- Communications Loading

Origins of NTCIP

Original NTCIP Constraints and Origins of Design

NTCIP effort originated in 1993 to support remote communication for traffic signal control

- Intended to be the communication protocol for NEMA TS 2 (Traffic Controller Assemblies)
  - Originally intended for signal control
  - Quickly expanded to support other devices
- Different architectures
  - Central control
  - Field masters
  - Distributed control
- Predominant 1200 bps environment
  - Recognition that higher speeds would emerge

NEMA = National Electrical Manufacturers Association

Origins of NTCIP

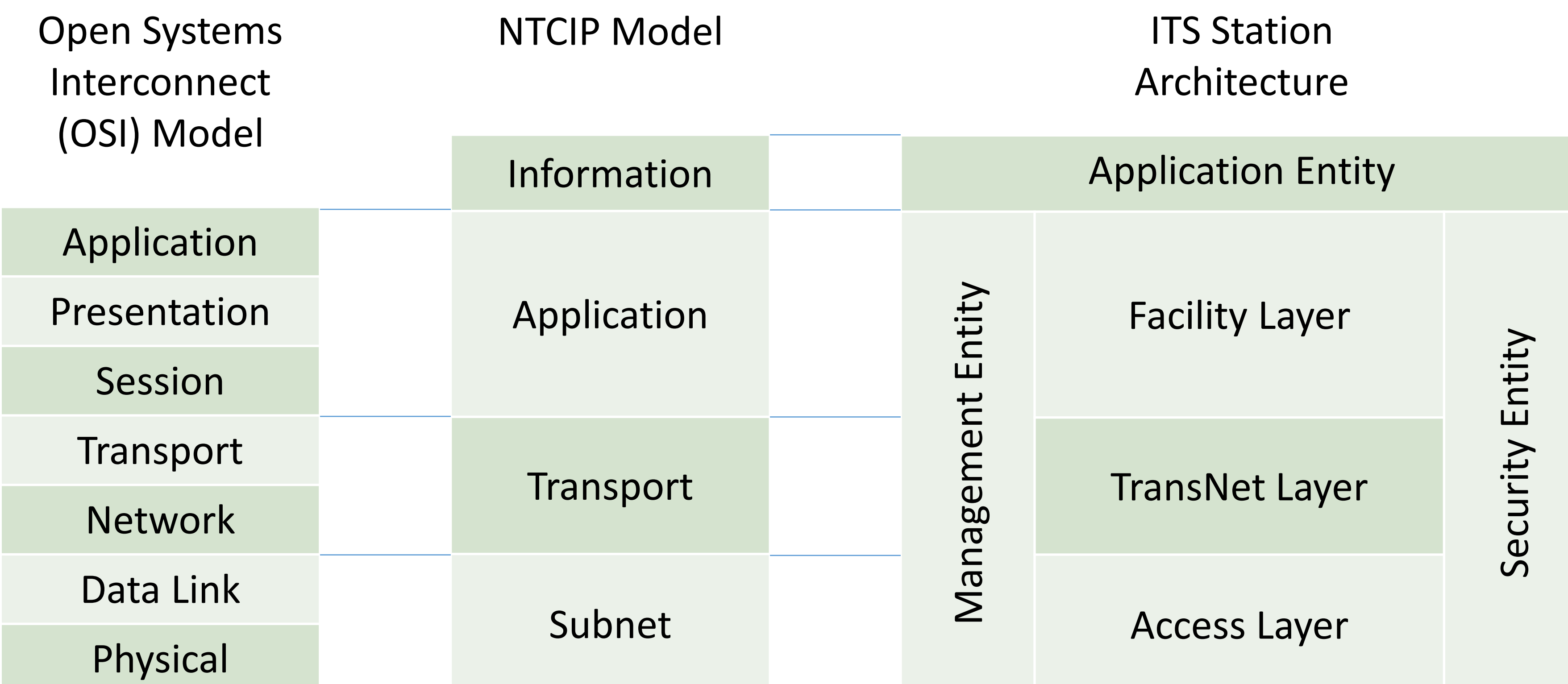
Practical Challenges

- Different needs for:
  - Frequency of command and monitoring messages
  - Content of command and monitoring messages
  - Number of devices sharing communications medium

Origins of NTCIP

A Layered Solution

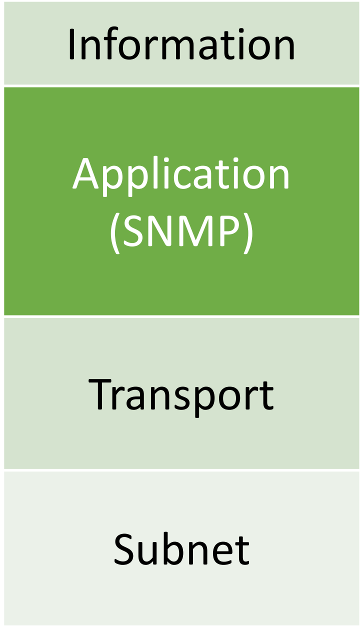
- Adopted layered protocol model to provide flexibility



Origins of NTCIP

Application Layer

- Flexibility: Simple Network Management Protocol (SNMP)
  - Major Internet standard
  - Provides flexible message structure
  - Manager decides when to send each message



Simple Network Management Protocol (SNMP)

SNMP Packet Structure

Each message can contain multiple objects

NTCIP defines standard data objects

Information Layer

Object Name	Value	Object Name	Value
phaseStatusGroupGreens.1	34 (ϕ2, 6)	shortAlarmStatus.0	0 (no error)

NTCIP adopted SNMP

Application Layer

Ver	Name	Type	ID	Err	Index	Information Content
1	admin	Response	1	0	0	Object Name: phaseStatusGroupGreens.1; Value: 34 (ϕ2, 6); Object Name: shortAlarmStatus.0; Value: 0 (no error)

NTCIP allows multiple lower layer solutions

Lower Layers

Header	Application Protocol Data Unit	Footer
Protocol Specific	Ver: 1; Name: admin; Type: Response; ID: 1; Err: 0; Index: 0; Information Content: phaseStatusGroupGreens.1, 34 (ϕ2, 6), shortAlarmStatus.0, 0 (no error)	Protocol Specific

Manager decides when to use each object

Simple Network Management Protocol (SNMP)

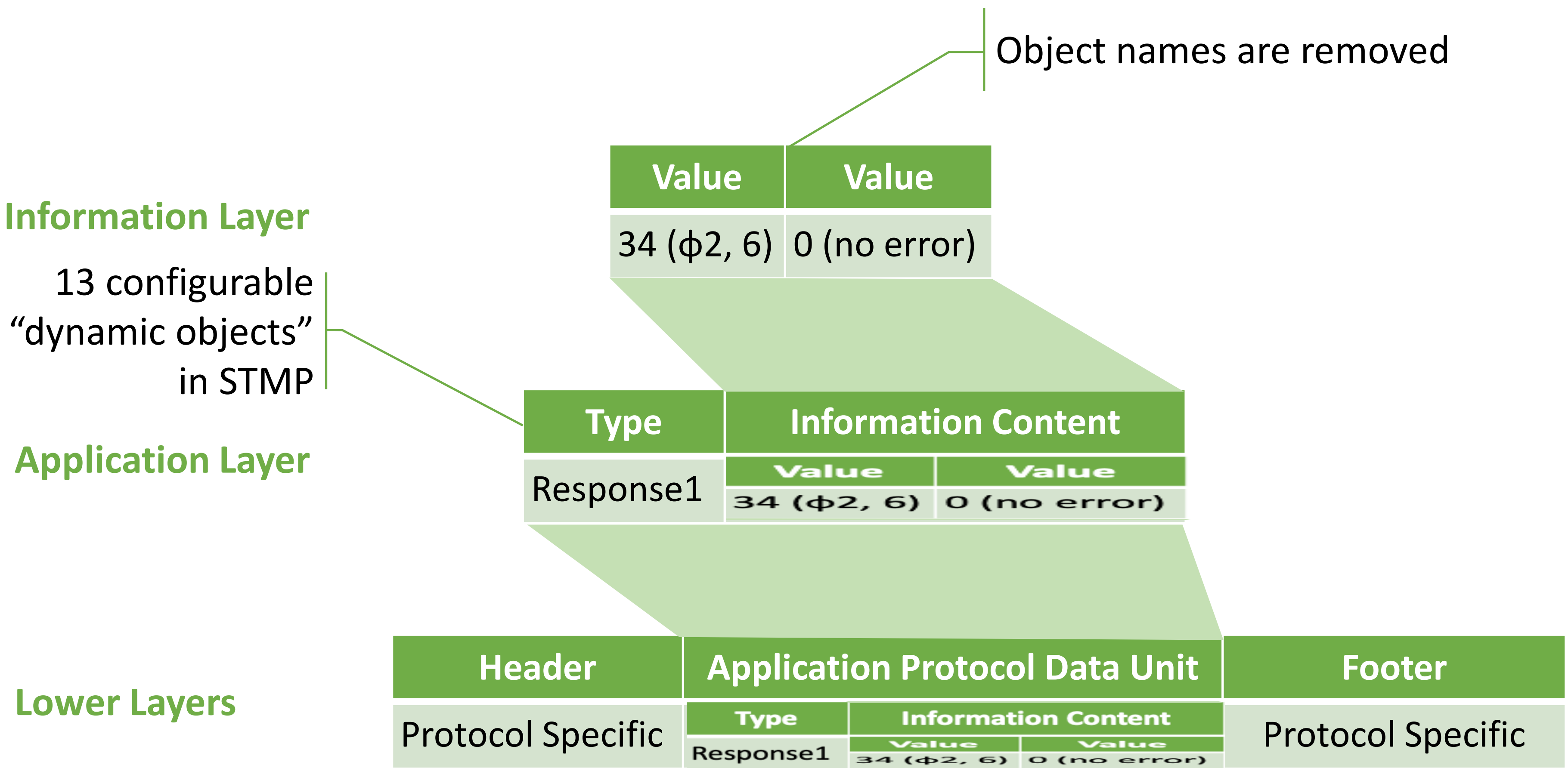
Challenges with SNMP

- SNMP is verbose
  - Request and response are nearly same size
  - Inefficient encoding
  - Example message is ~75 bytes + lower layers
  - One exchange every ~1.6 seconds @ 1200bps
- SNMPv1 does not provide any cybersecurity protection
  - Community name provides access control but not authentication
  - SNMPv3 coupled with (D)TLS provides necessary security
    - See Module CSE 203: Adding Security to NTCIP
- NTCIP developed a configurable protocol
  - Simple Transportation Management Protocol (STMP)
  - Custom design for transportation industry
  - Defined as optional enhancement to base NTCIP

(D)TLS = Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS)

Simple Transportation Management Protocol (STMP)

STMP Packet Structure



Manager decides configuration of and when to use each "dynamic object"

Simple Transportation Management Protocol (STMP)

Predominant 1200 bps Environment

- Simple Transportation Management Protocol
  - GET-Requests and SET-Responses omit data fields
  - Example message is 3 bytes + lower layers
  - Request is only 1 byte + lower layers
  - One exchange every 0.16 seconds @ 1200 bps
- Dynamic objects are configured through SNMP
  - Configure once; use many
  - Each system can configure dynamic objects to meet their needs

Simple Transportation Management Protocol (STMP)

STMP vs SNMP

- Reduced data communication demand
  - Most integer parameters have a 25:1 reduction
- Both provide flexibility
  - STMP only allows 13 dynamic objects
  - STMP requires full support for and use of SNMP
- STMP increases processor/memory/code demands
  - Translating dynamic object number into series of object requests
  - Encoding using different rules
- Niche market of a more complex protocol increases integration costs
  - Custom testing for each configuration

Exception-Based Reporting

A New Approach to Monitoring Equipment

- Traditional Systems Polled Signals Once-per-Second
  - 120-second cycle = 120 requests/replies
- Exception Reporting Allows Signal to Report Changes
  - E.g., send a message each time a signal phase green changes
  - At most, 2 message exchanges per phase per cycle
  - Delay settings can further reduce number of messages
  - Acknowledgements can be suppressed
  - Perhaps a 20:1 reduction in communications demand

Exception-Based Reporting

Other Benefits of Approach

- Can be used to capture transient events
- Based on event-logging logic
  - Most of logic already implemented in many controllers
  - Exceptions can also be stored in local logs
- Standard supports monitoring 65,535 conditions

Exception-Based Reporting

Challenges with Exception-Based Reporting

- Current design (NTCIP 1103) based on SNMPv1
- Upgrade to SNMPv3 required for proper cybersecurity
  - Requires changes to the design
  - ISO 15784-2 defines the use of SNMPv3 within ITS
  - ISO 20684-3 and 20684-4 will define exception reporting within ITS
- Event detection increases processor requirements

Should consider as a part of cybersecurity migration plan

Block Objects

Database Uploads and Downloads

- An ASC configuration can be megabytes
  - Mostly 1-byte INTEGERs
- NTCIP 1202 v03 Defines Standardized "Block Objects"
  - An SNMP object containing a static structure of a set of other objects
  - Similar to dynamic objects, but statically defined in standard
  - Only standardized for upload/download of standardized configuration parameters
  - Manufacturers may define their own block objects
- Reduces time to transfer an entire configuration

Infrastructure Limitations

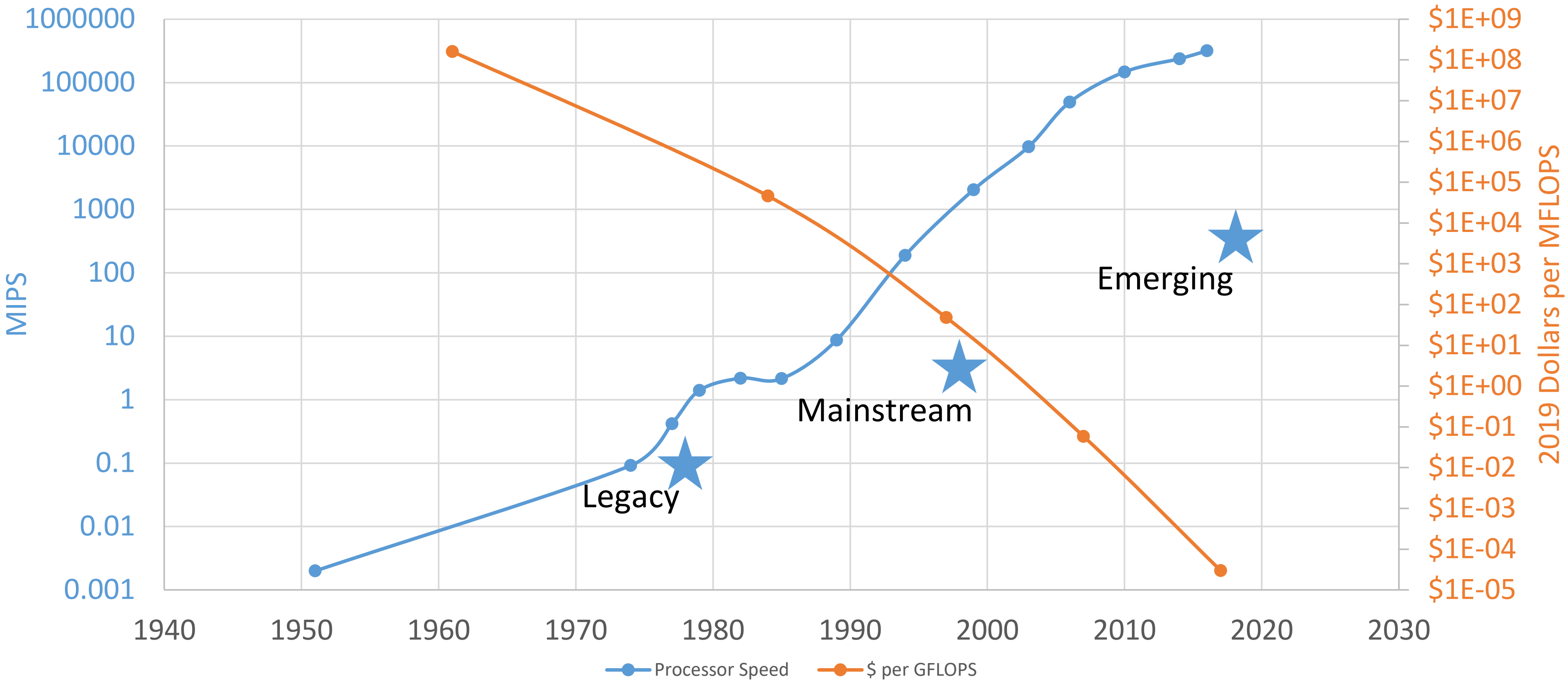
Infrastructure Generations


Capability	Legacy	Mainstream	Emerging
Data Rate	1200 – 9600 bps	10 Mbps	>=50 Mbps
Communications Technology Examples	Multi-drop Copper Wire, Dial-up	Ethernet, LTE	Ethernet, WiFi, 5G
Processor Speed	0 – 4 MIPS	4 – 60 MIPS	>=60 MIPS
OS and API for CV Applications	No	Typically no	Yes
Controller Examples	Type 170 NEMA TS 1	ATC 5202 (2070 L) NEMA TS 2	ATC 5201

SUPPLEMENT

Infrastructure Limitations

Processor Capability Timeline



MIPS = Millions of instructions per second
MFLOPS = Millions of floating point operations per second

Source: https://en.wikipedia.org/wiki/FLOPS, https://en.wikipedia.org/wiki/Instructions_per_second#Millions_of_instructions_per_second_(MIPS)

Infrastructure Limitations

Controller Costs

- The cost of an ASC reflects
  - Processor
  - Other components
  - Software
  - Custom engineering
- As with computers, price point tends to stabilize while
  - Processor speeds increase
  - Memory increases
  - Ports improve speed
  - Each version results in custom engineering
- A 2020 survey indicated that “emerging” controllers cost between $2,000 and $5,500; prices vary based on
  - Required features (processor speed, proprietary features, support)
  - Type of software
  - Purchase quantity
  - Testing requirements

Infrastructure Limitations

Limitations of Legacy Systems for Traffic Signal Control

- Legacy Communication Networks Struggle to Support NTCIP
  - 1200 bps requires STMP or exception reporting
  - No support for any cybersecurity (insufficient bandwidth)
  - Should never be used with connected vehicles
- Legacy Controllers Struggle to Support NTCIP
  - Original processors/memory too limited
  - Limited support with later-model/upgraded legacy controllers
  - No support for any cybersecurity (insufficient processing)
  - Unable to support connected vehicle applications
- Recommendations
  - Upgrade to emerging controllers
  - Consider mainstream/emerging communication alternatives

SUPPLEMENT

Mainstream Systems

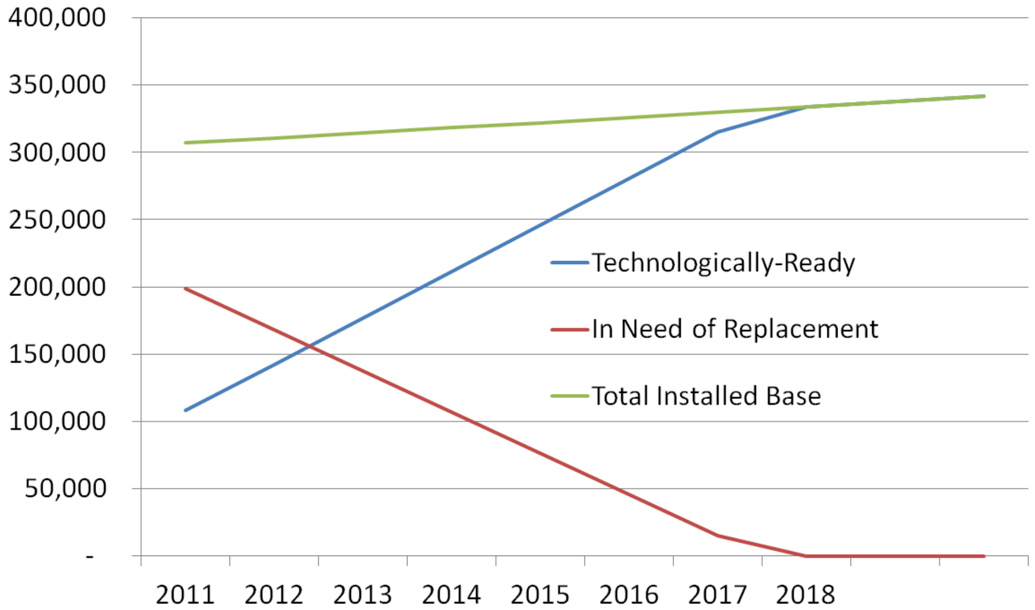
- Mainstream Communication Networks Support NTCIP
  - Supports all NTCIP features
  - Network loading of SNMP generally not an issue
  - Cybersecurity is critical (See Module CSE 203)
- Mainstream Controllers Support Standard NTCIP
  - Ethernet communications can overwhelm early mainstream processors
  - Support possible for most NTCIP functionality
  - Might bump against processing/memory limitations (e.g., complex event reporting, large logs)
  - Cybersecurity will introduce additional processor loads
  - Connected vehicle applications might stress systems
- Recommendations
  - Upgrade to emerging controllers as needed
  - Initiate migration plan to provide cybersecurity

Emerging Systems for Traffic Signal Control

- Emerging Communication Networks Support NTCIP
  - Supports all NTCIP features
  - Network loading of SNMP generally not an issue
  - Cybersecurity is even more critical (See Module CSE 203)
- Emerging Controllers Support NTCIP
  - Can handle current requirements for connected vehicles
  - Cybersecurity is critical
- Recommendations
  - Initiate migration plan to provide cybersecurity
  - Buy more than enough processing power

Infrastructure Limitations

Processor Capability Timeline



2012 Projection of Deployment

- Actual Statistics – 2019 Minnesota
    - Legacy: 5%
    - Mainstream: 65%
    - Emerging 35%

SUPPLEMENT

MNDOT data extrapolated from data in https://www.dot.state.mn.us/research/reports/2019/201935.pdf

Communications Loading

Communications Demand Versus Capacity

- System Design Should Consider Communications Loading
  - Too little capacity limits capabilities
  - Too much capacity opens security vulnerabilities and might increase costs
- Determine how much data per second from all devices sharing the communications medium
  - Double estimate for “collision detection” and peaks
- Mainstream/Emerging Systems Often Incorporate Video
  - Video requires 1,500-4,000 kbps* per feed
  - SNMP requires 1.5-4 kbps per signal
  - Mainstream communications support 1,000 SNMP signals/channel
  - One video link per 100 signals will dominate design

*https://support.google.com/youtube/answer/2853702?hl=en for 720p resolution

Communications Loading

Legacy Communications

- Costs of Maintaining Legacy Communications
  - No cybersecurity
  - Increased equipment costs due to custom code
  - Increased testing/integration costs
  - Fading industry support in future
- If you have a legacy communications system, consider:
  - Upgrading (wireless solutions are often viable)
  - Using exception-based reporting
- View STMP as a last-resort

SUPPLEMENT

ACTIVITY

Question

Which of the below is a waning technology that is not recommended for most new deployments?

Answer Choices

a) Exception reporting
b) Block objects
c) STMP
d) None of the above

Review of Answers

a) Exception reporting

Incorrect. Exception reporting is a fairly new feature that has been added to NTCIP to reduce overhead in communications.

b) Block objects

Incorrect. Block objects are used to speed the upload and download of large portions of an ASC database.

c) STMP

Correct! STMP is a protocol specific to the transportation industry that requires custom code, extra testing, and integration expenses.

d) None of the above

Incorrect. STMP is a waning technology that is no longer recommended due to its niche market and cost implications.

Learning Objective

Manage Special Considerations for NTCIP 1202: Functionality

Special Considerations: Functionality

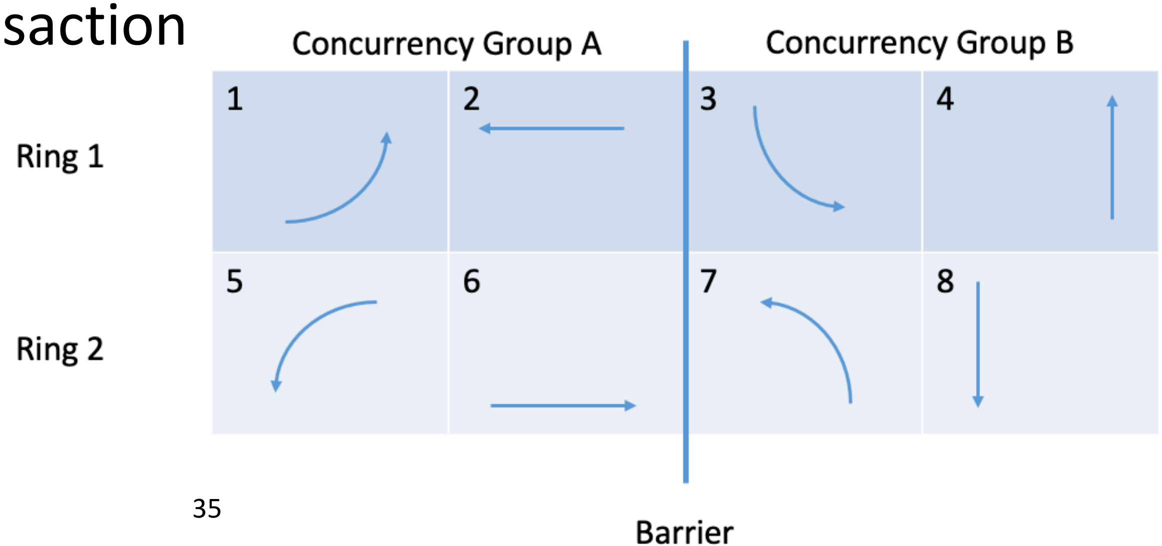
Overview

- Database Transaction Sets
- Consistency Checks and Rules
- Connected Vehicle Support
- Clock Coordination
- Managing Expectations for Off-The-Shelf Interoperability

Database Transaction Sets

Need for Complex Transactions

- Traffic signals are safety-critical devices
- Many configuration parameters are inter-related
- Changing configuration of some parameters need to happen in single step
- Size of each SNMP message is limited
- Database transaction mode interprets multiple SNMP messages as one transaction



Database Transaction Sets

Impact on operations

- When in transaction mode, some operations are buffered
  - Get requests return “live” values (not buffered)
  - Set requests for control objects are implemented immediately
    - E.g., setting force off or current timing pattern
  - Set requests for database parameters are buffered
    - E.g., setting minimum green time
  - Some database parameters can only be set in transaction mode
    - E.g., phase concurrency
- Designation of parameter type was omitted from NTCIP 1202v03
  - WG has been notified of ambiguity
  - NTCIP 1202v02 provides designation for most objects

Consistency Checks and Rules

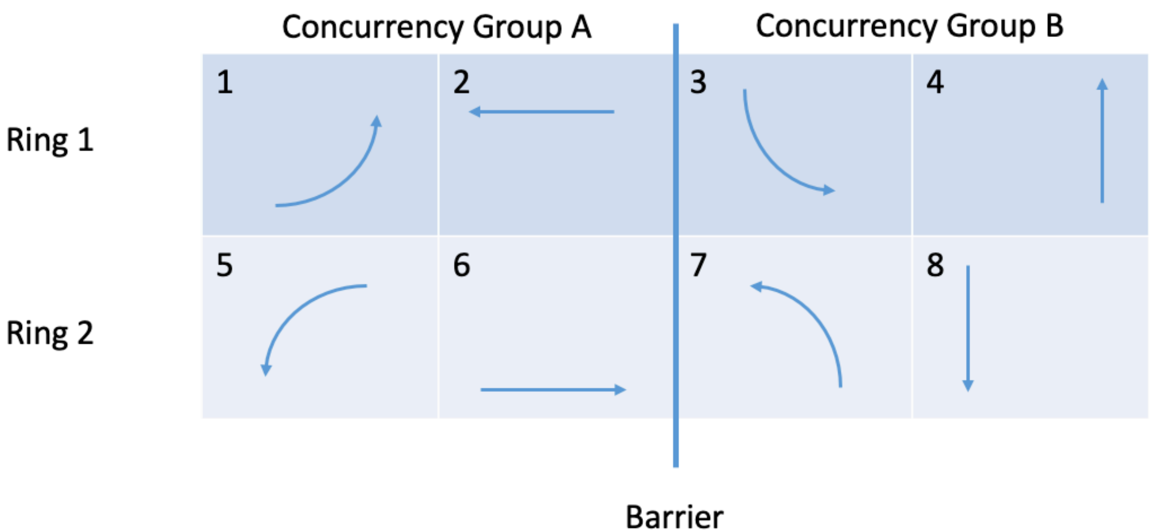
Need for Consistency Checks

- Critical configuration parameters can only be changed using the transaction mode
- 17 standardized consistency checks are required
  - Prevent implementation of controller settings with internal conflicts
  - Require additional time
  - Are performed at end of transaction mode process
- Manufacturer may impose additional restrictions
- Failure of any rule results in transaction set failing

Consistency Checks and Rules

Example Consistency Check

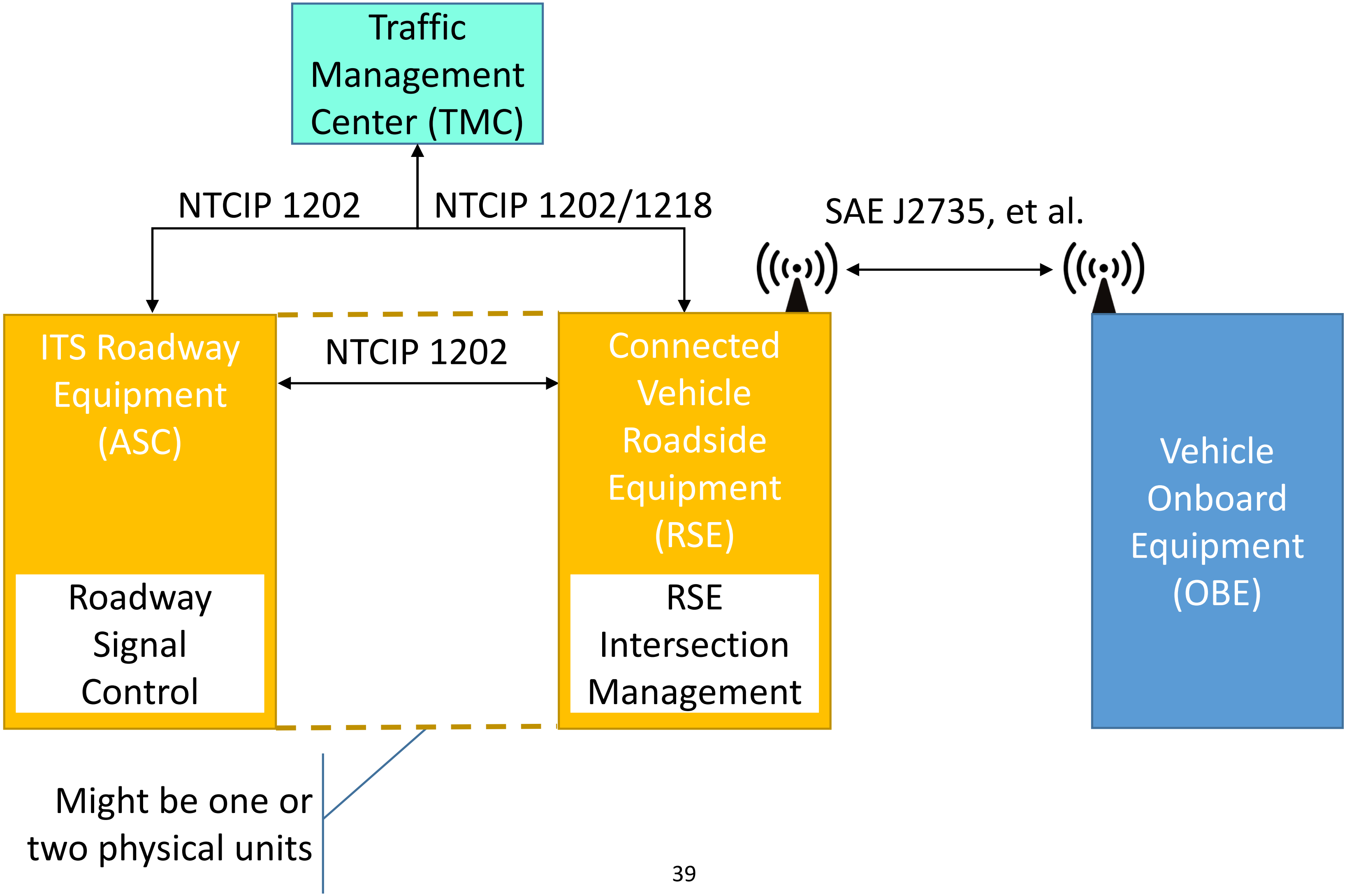
- Concurrent phases must be in different rings
  - Example: Phase 1 must not be concurrent with Phases 2, 3, or 4



Phase	1	2	3	4	5	6	7	8
Ring	1	1	1	1	2	2	2	2
Concurrency	5,6	5,6	7,8	7,8	1,2	1,2	3,4	3,4

Connected Vehicle Support

Signal Controllers and the Connected Vehicle Environment



Connected Vehicle Support

Connected Vehicles

New Features for Connected Vehicles

- TMC–ASC
  - Manage data exchanged between the ASC and RSE
- TMC–RSE
  - Manage map information
  - Manage transformation of ASC timing data to Signal Phase and Timing (SPaT) message
  - Manage data collected from basic/personal safety messages (BSM/PSMs)
- ASC–RSE
  - ASC provides
    - Current/next movement information
    - Expected start/end times of each phase
  - ASC selects
    - Current geometry
    - Current transformation of ASC timing data to SPaT message
  - RSU reports presence of vehicles and vulnerable road users (VRUs)

Connected Vehicle Support

Connected Vehicles

Challenges with Interface to RSE Intersection Management

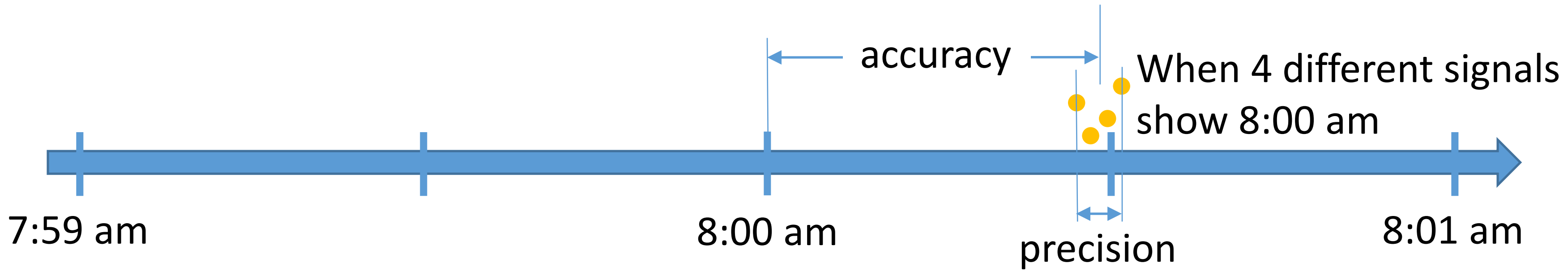
- Connected Vehicle environment is safety critical
  - Integrity of data must be maintained
  - Messages must be properly authenticated
  - Access to data must be controlled
  - Roadside Unit (RSU) Specification v4.1 only allows secure protocols
  - NTCIP 1202 v03 designed for SNMPv1, which is not secure
  - Required Security and Credentials Management System (SCMS) is still being established
- Connected Vehicle features of NTCIP 1202 v03 should only be used in a fully secure environment
  - Secure communications (e.g., SNMPv3 with TLS)
  - Proper maintenance of SCMS certificates

TLS = Transport Layer Security

Clock Coordination

Need for Clock Coordination

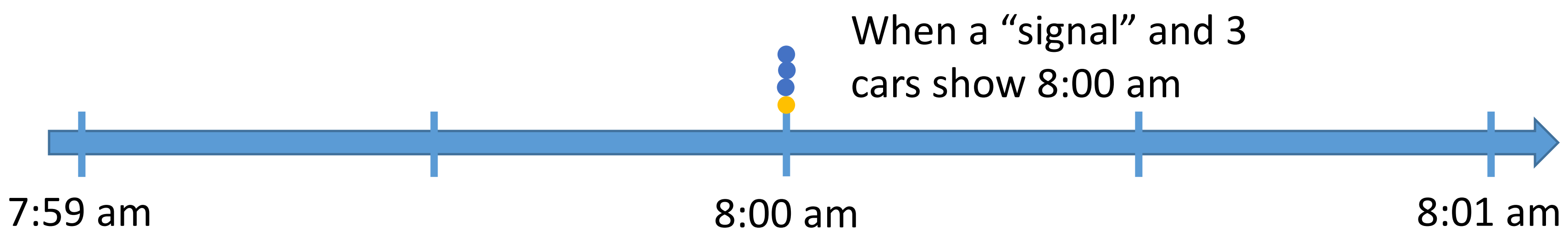
- Traffic signals need to coordinate timing with
  - Adjacent signals
  - Connected vehicles
- Inter-signal coordination requires:
  - Precision ± 2 seconds (green waves approach when expected)
  - Accuracy ± 5 minutes (morning timing pattern starts on time)
  - Any synchronization technology (each system can be different)



Clock Coordination

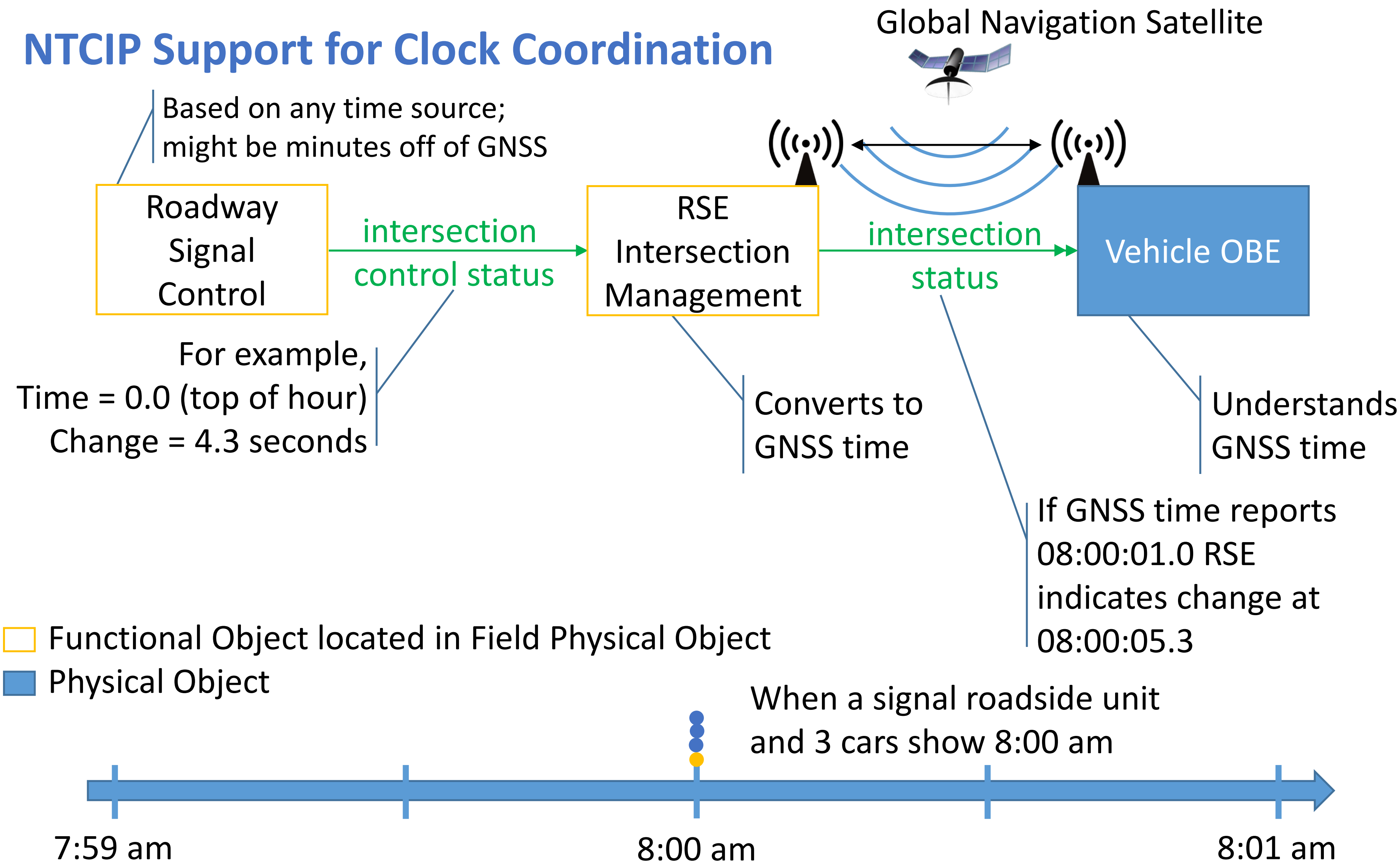
Need for Clock Coordination

- Coordination with connected vehicles requires
  - ± 50 millisecond precision (consistency of signal displays)
  - A single, reliable, national standard to synchronize
- Selected synchronization technology is based on Global Navigation Satellite System (GNSS) time
  - Assuming satellites are accurate, accuracy = precision



Clock Coordination

NTCIP Support for Clock Coordination



Managing Expectations for Off-the-Shelf Interoperability

Signal Controllers Have Most Complex Interface

- Signal controllers have many more configurable parameters than other field devices
- Many agencies continue to require specialized functionality
  - Results in customized extensions
- Some details are manufacturer-specific
  - Shortway, Add-only, and Subtract-only Coordination Correction:
    - *This operation is performed in a device specific manner*
- NTCIP designed to improve interoperability and interchangeability

NTCIP 1202 v03 is a step in the right direction

ACTIVITY

STANDARDS ITS TRAINING TRANSIT

U.S. Department of Transportation
Office of the Assistant Secretary for
Research and Technology

Question

Which of the following most accurately expresses the state of connected vehicle (CV) support in the standard?

Answer Choices

a) Does not address any CV functionality

b) Does not define sufficient security for ASCs in a CV environment

c) Defines a secure solution for intersection maps

d) Defines a secure solution for signal timing

Review of Answers

a) Does not address any CV functionality

Incorrect. NTCIP 1202 v03 defines the data to support CV applications, including map and signal timing information.

b) Does not define sufficient security for ASCs in a CV environment

Correct! NTCIP 1202 v03 assumes SNMPv1, which is not secure. For CV operation, NTCIP 1202 v03 must only be deployed over a secure protocol (e.g., SNMPv3 with TLS).

c) Defines a secure solution for intersection maps

Incorrect. SNMPv1 does not provide for secure communications.

d) Defines a secure solution for signal timing

Incorrect. SNMPv1 does not provide for secure communications.

Learning Objective

Incorporating Requirements Not Supported by Standardized Objects

Incorporating Requirements Not Supported by Standardized Objects

Overview

- Conditions and Context for Extending the Standard
  - Example: Dilemma Zone Protection
- Specifying Requirements Not Covered by the Standard (Extensions)

What is a Custom Extension

- Standard defines
  - Mandatory and optional user needs
  - Mandatory, optional, and conditional requirements for each need
  - Mandatory dialogs and objects for each requirement
- Custom extensions define
  - Objects (and dialogs) for user needs and requirements that are not addressed by the standard
- Extensions are allowed by NTCIP

Conditions and Context for Extending the Standard

Reasons to Specify a Custom Extension

- Standard does not define every traffic signal control feature
  - Standard only addresses features in wide use
- Customization allows for market innovations
- Might eventually be incorporated into standard
- Example:
  - Purdue University developed a high-resolution data logger
  - Implemented by multiple manufacturers
  - Added to draft of NTCIP 1103v03 in 2015
  - Approved in NTCIP 1103v03 in 2016

Conditions and Context for Extending the Standard

Costs Associated with a Custom Extension

- Custom features might be proprietary
  - Documentation might be limited or cryptic
  - Rights to distribute documentation might be limited
- Custom features might reduce bidders for device
- Custom features increase costs of management system
- Custom features complicate testing
  - Developing and implementing custom test procedures is expensive
  - Documentation might not reflect as-built product if untested
- Custom features complicate maintenance
  - Potentially limited to one vendor/model/version
  - A single product might be discontinued

Example of Extending the Standard

Connected Vehicles

Connected Vehicle Dilemma Zone Protection: User Need

- Minimize drivers being caught in dilemma zone
  - Use Basic Safety Message (BSM) for advanced detection
  - Provides ~19-second advanced detection at 35 mph
  - Continuously track each vehicle's path on approach
  - Identify individualized dilemma zones based on speed, acceleration, etc.
  - Optimize when to gap out

Connected Vehicle Dilemma Zone Protection: Requirements

- Within 0.1 second of its receipt, the RSU shall forward the following data to the signal controller for each BSM received that reports a vehicle on one of the approaches of the intersection:
  - Temporary ID
  - DSecond (i.e., the millisecond within the minute)
  - Latitude
  - Longitude
  - Speed
  - Heading
  - Longitudinal Acceleration
  - Vehicle Length
- Upon request from a manager, the RSU shall enable or disable its BSM reporting.

EXAMPLE

Example of Extending the Standard

Connected Vehicles

Connected Vehicle Dilemma Zone Protection: Design

- Some data already exists
  - The RSU has a copy of the intersection map
- Some data needs to be transformed
  - Definitions of BSM data need to be mapped to SNMP
- Some data is new
  - Object to toggle the reporting of the BSM data

Example of Extending the Standard

Connected Vehicles

Connected Vehicle Dilemma Zone Protection: Procurement

- Option 1: (Potentially Closed) Proprietary Solution
  - Explain the user need and define validation testing
  - Validate operation of delivered product
- Likely to result in **vendor lock-in**
  - Requires manager and controller from same vendor

Example of Extending the Standard

Connected Vehicles

Connected Vehicle Dilemma Zone Protection: Procurement

- Option 2: Integrable Solution
  - Explain the user need and define validation testing
  - Require delivery of systems engineering documentation
  - Obtain rights to distribute documentation to those with a need
  - Obtain rights for others to develop products to implement design
  - Verify that delivered product implements design
  - Validate operation of delivered product

- Might result in **limited marketplace**
  - Distribution of documentation is based on need-to-know

Example of Extending the Standard

Connected Vehicles

Connected Vehicle Dilemma Zone Protection: Procurement

- Option 3: Open Solution
  - Explain the user need and define validation testing
  - Produce/Reference systems engineering (SE) documentation in public domain
    - Without patents
    - Developed by agency, manufacturer, system developer, consultant, etc.
  - Verify that delivered product implements design
  - Validate operation of delivered product

- Provides best competition
  - Might **increase initial costs**

ACTIVITY

STANDARDS ITS TRAINING
TRANSIT

U.S. Department of Transportation
Office of the Assistant Secretary for
Research and Technology

Question

Which of the following is NOT true regarding an extension based on an open solution?

Answer Choices

a) Documentation is made public

b) Cost of initial deployment may be higher

c) Delivered product needs to be tested against requirements

d) Likely to result in vendor lock-in

Review of Answers

a) Documentation is made public

Incorrect. The defining characteristic of an open solution is that the documentation is public.

b) Cost of initial deployment may be higher

Incorrect. Vendors are less able to recover costs in subsequent deployments thereby increasing costs for initial deployment.

c) Delivered product needs to be tested against requirements

Incorrect. To obtain the interoperability enabled by an open solution, the product should be tested against the requirements.

d) Likely to result in vendor lock-in

Correct! An open solution prevents true vendor lock-in by ensuring that the design is publicly available.

Learning Objective

Testing NTCIP 1202 v03 Conformance

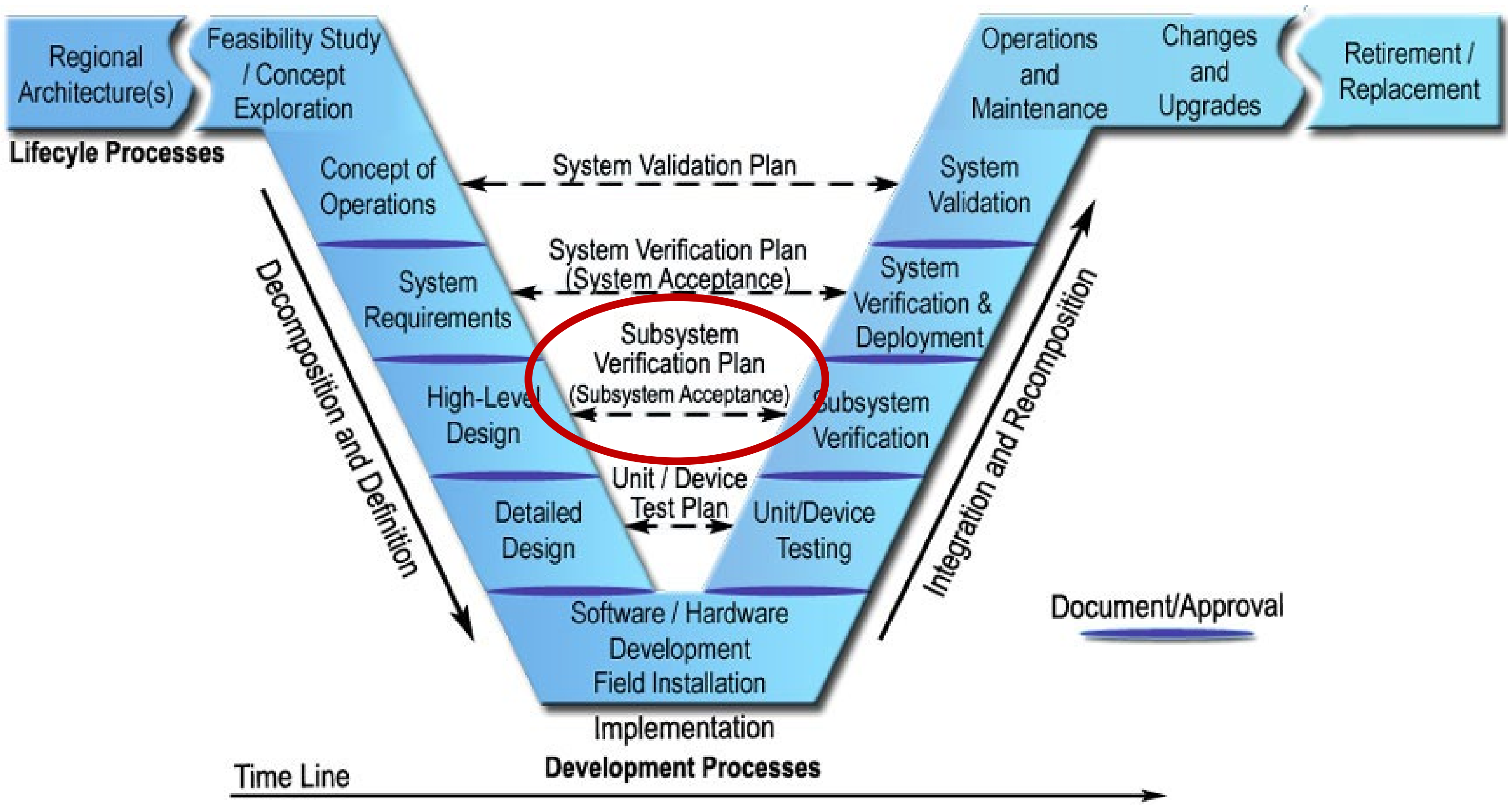
Testing NTCIP 1202 v03 Conformance

Overview

- Systems Engineering Documentation and NTCIP
- Anaheim Case Study
- Interim Guidance

Systems Engineering Documentation and NTCIP

Systems Engineering Vee-Diagram



Systems Engineering Documentation and NTCIP

Standard Outline for NTCIP 1200 Series

1. General
2. Concept of Operations
3. Functional Requirements
4. Dialogs
5. Management Information Base (MIB)
6. <Other Design Elements>

A. Requirements Traceability Matrix
B. Object Tree
C. Test Procedures
D. Documentation of Revisions
E. <Other Annexes>

NTCIP 1202 Test Procedures

It is anticipated that Test Procedures may be developed as part of a future revision of NTCIP 1202 v03. Annex C is a placeholder, at present.

– NTCIP 1203 v03

CASE STUDY

STANDARDS ITS TRAINING TRANSIT

U.S. Department of Transportation
ITS Joint Program Office
Image Source: Thinkstock USDOT

Anaheim Case Study

Connected Vehicles

NTCIP 1202 Standard Testing Project

- Request for Proposals (RFP) Closed February 26, 2020
- Project will:
  - Develop test procedures for all NTCIP 1202 v03 requirements
    - Part 1: All features included in NTCIP 1202 v02
    - Part 2: All additional features
  - Test three vendors
  - Provide public domain test software
  - Produce a final report

Interim Guidance

NTCIP 1202 Standard Testing Project

- Develop a project PRL based on NTCIP 1202 v03 PRL
  - See Modules A315a and A315b Part 1
  - Make sure to extend with any customizations (e.g., dialogs)
- Require compliance to the project PRL
- Require testing per test procedures being developed by Anaheim
  - Should identify a time limit for waiting on the Anaheim deliverables
- Testing should be performed independently from manufacturer
  - Agency
  - Consultant
  - Another agency

ACTIVITY

U.S. Department of Transportation
Office of the Assistant Secretary for
Research and Technology

Question

Which of the below is an appropriate way to test an ASC for conformance to NTCIP 1202 v03?

Answer Choices

a) Using test procedures contained in Annex C of the standard

b) Using Anaheim test procedures (when available)

c) Connecting to system and see if it works

d) Trusting the vendor

Review of Answers

a) Using test procedures contained in Annex C of the standard

Incorrect. Annex C of NTCIP 1202 v03 is currently a placeholder that does not contain any test procedures

b) Using Anaheim test procedures (when available)

Correct! The Anaheim project aims to develop procedures for all NTCIP 1202 v03 requirements

c) Connecting to system and see if it works

Incorrect. While this might provide some insights as whether the device will work under normal conditions, it will omit major tests

d) Trusting the vendor

Incorrect. Trust does not equate to testing

Summary

Module A315b Part 1

Concepts taught in previous Part 1:

1) Identify NTCIP 1202 v03 Standard Requirements
2) Explain the Purpose and Benefits of the RTM
3) Prepare a Project-Level RTM
4) Prepare an ASC Specification

Module Summary

Manage Special Considerations for NTCIP 1202: Infrastructure

Manage Special Considerations for NTCIP 1202: Functionality

Incorporate Requirements Not Supported by Standardized Objects

Testing NTCIP 1202 v03 Conformance

The ASC Curriculum

- **MODULE 31. A315a**: Understanding **User Needs** for Actuated Traffic Signal Controllers (ASC) Based on NTCIP 1202 v03 Standard
- **Module 32: A315b Part 1**: Specifying **Requirements** for ASC Based on NTCIP 1202 Standard v03 – Part 1 of 2
- **Module 42: A315b Part 2**: Specifying **Requirements** for ASC Based on NTCIP 1202 v03 Standard – Part 2 of 2

Module 35: T315: Applying Your **Test Plan** to the NTCIP 1202 v03 ASC Standard

Next Course Module

Module T315: Applying Your Test Plan to the NTCIP 1202v03 ASC Standard

Concepts taught in next module (Learning Objectives):

1) Recognize the importance of testing ASCs
2) Apply the rules for developing a sample ASC test plan
3) List rules for developing test case specifications and procedures
4) Develop sample test case specifications and procedures
5) Understand testing results for NTCIP 1202v03

Thank you for completing this module.

Feedback

Please use the Feedback link below to provide us with your thoughts and comments about the value of the training.

Thank you!