

*Communication – Based
Signaling
(as defined by AREMA Section
23)*

2008 IRSE North American Section AGM
Bill Petit
www.BillPetit.com

Background

- Roundtable discussions at 2005 AREMA C&S show generated request for interoperability guidelines for radio-based cab signal systems
- Assigned to Committee 37
- Following Manual Parts were approved for 2009 AREMA C&S Manual

What I'll Talk About

- Background and status of CBS
- Basic Architecture
- ICBS Project
- Safety Evaluation under 236 Subpart H

Section 23.2

- 23.2.1 Recommended Functional Requirements of a CBS System.
 - Define the recommended system functional requirements.
- 23.2.2 Recommended RAMS, Environmental and Other Requirements for Signaling Systems Using CBS Architecture.
 - Define the recommended reliability, availability, maintainability, and safety (RAMS), environmental, electromagnetic compatibility, and quality assurance requirements.

Background and Status

Section 23.3

- 23.3.1 Recommended Design Guidelines for a CBS System
 - Define the recommended system architecture and interfaces based on conventional signaling principles.

Section 23.4

- 23.4.1 Recommended Communications Protocols for a CBS system
 - Define the recommended system communication protocol (based on ATCS addressing and datagram)
- 23.4.2 Recommended Communications Messages for a CBS System
 - Define the recommended standard messages for communications between CBS subsystems

What is CBS?

- Defined Communications Based Signaling as 'a radio-based cab signal system'.
- Operate the same as a conventional Cab Signal System with enforcement. Onboard aspect display instead of wayside signals
 - "Virtual" Block Occupancies used instead of physical track circuits.
 - Train location determination done by on-board equipment (Definition of how to indicate a block is occupied, not how position is determined).
 - Communication, including cab signal aspect transmission from wayside to trains, via a digital data communications network.

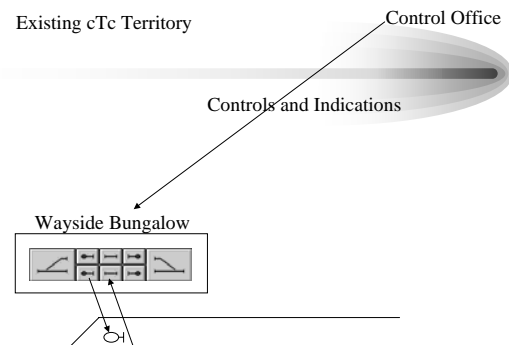
Section 23.5

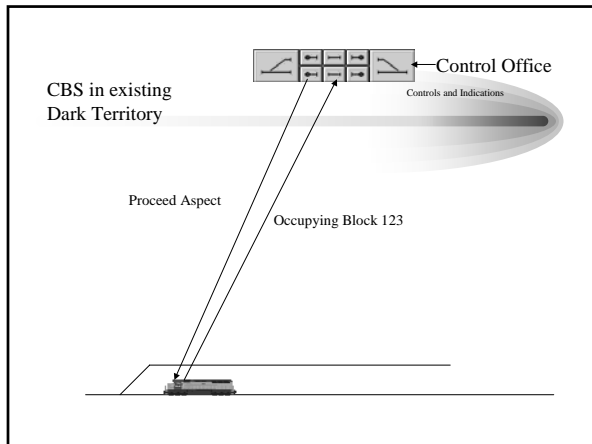
- 23.5.1 Recommended Onboard Database Guidelines for a CBS system
 - Define the recommended structure and content of the onboard database

What is CBS?

- CAD operation (i.e dispatching) is the same as in conventional CTC system.
- Signal Logic Processor (SLP) does all the vital logic and sends controls to wayside appliances and signal aspect info to the On Board Logic Processor (OBLP).
- OBLP provides signal aspect and speed limit info to train operators, and performs vital overspeed protection and signal enforcement.
- SLP also processes Bulletins received from CAD via Form Translator, and communicates them to various OBLPs.
- Interlocking logic is done in SLP or locally at the wayside.
- Communication follows ATCS protocols over a wide variety of transmission media

Basic System Architecture

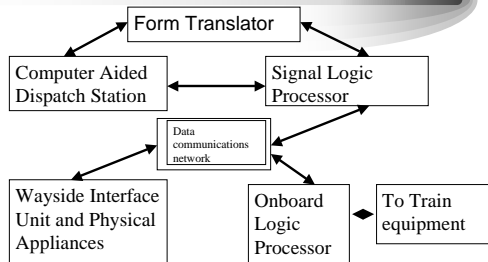




Interoperability Demo Goals

- Verify interoperability MP's and overall system operation
- Alstom, GETS, Safetran and US&S have jointly agreed to support a lab interoperability demo.
 - Each company will modify their own products to demonstrate interoperability
 - 3rd party will be used to develop interoperability simulation and testing
- Funded by FRA through Railroad Research Foundation

Defined CBS Architecture



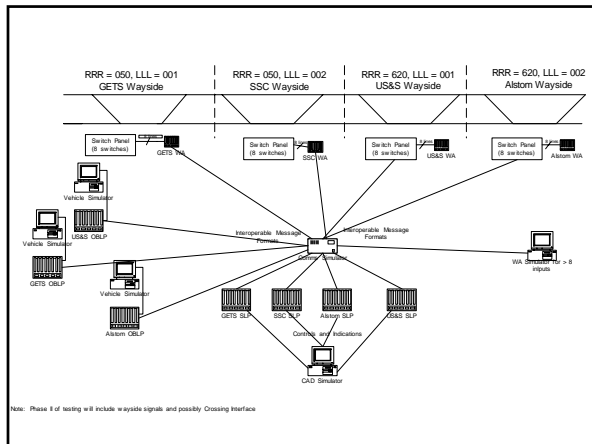
Scope of Work

- Lab Demo
- Each of 4 participating suppliers will modify existing equipment (onboard, logic controller, Wayside Controller) to comply with interfaces
- 3rd Party will develop testing infrastructure (vehicle, office and comms simulation)
- Test Scenarios to be developed for verifying trains move through territory independent of equipment supplier

Interoperability Demo (ICBS)

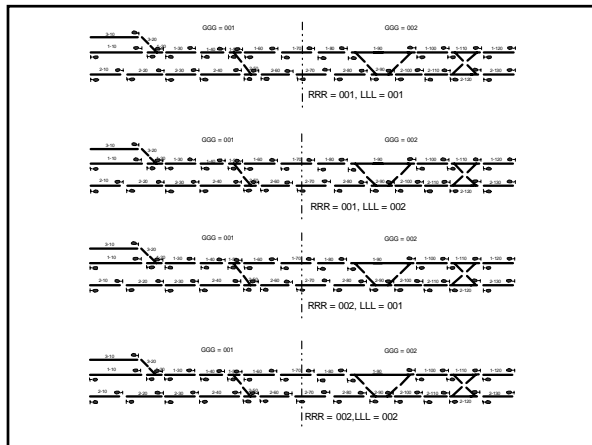
Participants

- Project Management – Bill Petit
- System Integrator – Critical Link
- Equipment Suppliers
 - Alstom
 - GETS
 - Safetran
 - Union Switch and Signal

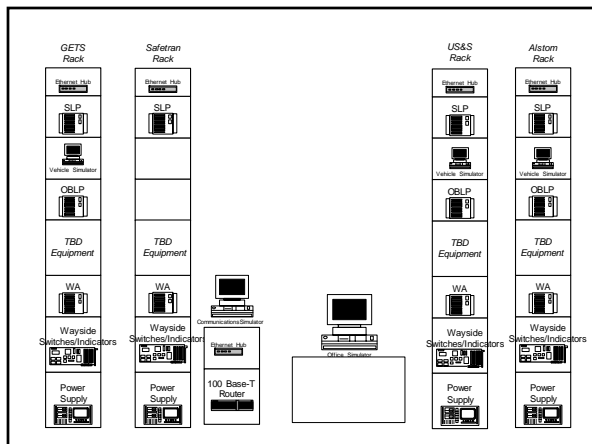


Safety Evaluation

Note that these are my opinions and have not been reviewed by FRA



- ## Existing Part 236 subparts
- A – General
 - B – ABS
 - C – Interlockings
 - D – Train Control Systems (e.g. cTc)
 - E – ATS, Train Control and Cab Signals
 - F – Dragging Equipment, Slide Detectors
 - G – Definitions
 - H – Processor-Based Signal and Train Control



- ## Subpart H
- Basic intent of rule is to verify that new system is at least as safe as system being replaced
 - Measured in accidents per million train miles over a 25 year period.
 - Most of rule spent identifying ways to support safety claims

236 Subpart H

- Railroads required to develop Railroad Safety Program Plan (RSPP)
 - Formal Document identifying strategy for assessing safety hazards and executing that strategy through individual Product Safety Plans
 - Most Class I RR's already have RSPP approved

Use of Signaling Principles and Existing Vital Platforms

- Operations controlled by each railroad
 - Application Logic is written by each railroad according to their own preferences.
 - Minimizes training and rule changes
- Not dependent on underlying method of operation for safety

Product Safety Plan (PSP)

- Basic Components of PSP described, along with comments on how CBS would be justified.

Product Safety Plan

- Complete description of the product, including a list of all product components and their physical relationship in the system
 - Safety-critical functions reviewed to determine whether they are designed on the fail-safe principle
- *System Architecture as Described in AREMA. Use of Signaling Principles enforces fail-safe principle.*

Basic Ideas to Keep in Mind

- Based on proven and accepted signaling principles
 - Architecture accepted by Professional Organization (AREMA)
- Based on proven and accepted safety-critical platforms
- Use of existing principles reduces HF issues
- Builds on existing knowledge base of S&C employees
- Familiarity with operation.

Product Safety Plan

- Description of the railroad operation on which the product is designed to be used, including train movement density, etc
- *Signaling Principles applicable for all types of operation and movement density*

Product Safety Plan

- Operational concepts document
- *Defined in AREMA Manual Parts, based on signaling concepts*
- Safety requirements document
- *Standard System Documentation, based on signaling concepts. AREMA MP 17 describes safety process.*

Product Safety Plan

- Hazard mitigation analysis
- *Standard System Documentation. Most hazards mitigated through use of signaling principles; other hazards as mentioned on previous slide need to be addressed.*
- *Use of existing safety-critical product architectures have this analysis in place (needs to be updated to reflect any added functionality)*

Product Safety Plan

- Description how product architecture satisfies safety requirements
- *Use of Signaling Principles*
- Hazard log
- *Standard System Documentation, Hazards addressed through well-accepted signaling principles*

Product Safety Plan

- Description of the safety assessment and validation and verification processes applied to the product and the results of these processes, describing how Appendix C subject areas are addressed directly, addressed using other safety criteria, or not applicable
- *Built in accordance with AREMA Part 17 using vital techniques such as described in Appendix C*

Product Safety Plan

- Risk assessment, as prescribed in § 236.909 and Appendix B
- *Need to consider additional hazards or changed risk due to use of communication-based system.*
 - *Failure to detect occupancy on-board, or error in detection.*
 - *Failure to report occupancy*
 - *Communications Error*
 - *Communications Latency*

Product Safety Plan

- Description of the safety assurance concepts used in the product design, including an explanation of the design principles and assumptions;
- *Built in accordance with AREMA Part 17*

Product Safety Plan

- Human factors analysis
- *Same as Conventional Signal Operation*
- *Use of Aspect-Based Displays minimize confusion*

Product Safety Plan

- Analysis of the applicability of the requirements of subparts A-G to the product that may no longer apply or are satisfied by the product using an alternative method, and a complete explanation of the manner in which those requirements are otherwise fulfilled
- *Majority of existing A-G principles are satisfied by use of signaling principles*

Product Safety Plan

- Description of the specific training necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product
- *OK, much of the operation is identical to conventional signal operations.*

Product Safety Plan

- Description of the necessary security measures for the product over its life-cycle;
- *OK*
- Description of each warning to be placed in the Operations and Maintenance Manual and of all warning labels required to be placed on equipment as necessary to ensure safety
- *OK*

Product Safety Plan

- Description of the specific procedures and test equipment necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product.
- *OK*

Product Safety Plan

- Description of all initial implementation testing procedures necessary to establish that safety-functional requirements are met and safety-critical hazards are appropriately mitigated;
- *OK*

Product Safety Plan

- Description of:
 - All post-implementation testing (validation) and monitoring procedures, including the intervals necessary
 - Each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, tests, repairs, replacements, adjustments, and the system's resulting conditions
- *OK*

Product Safety Plan

- Description of any safety-critical assumptions regarding availability of the product, and a complete description of all backup methods of operation; and
- *OK*
- Description of all incremental and predefined changes
- *Application Logic Modifications and Database modifications comprise possible changes*

Questions ?

Bill.Petit@ieee.org
www.billpetit.com