Establishing Wireless Communications Security in Legacy PTC Systems

Philippe Ayrault, PhD

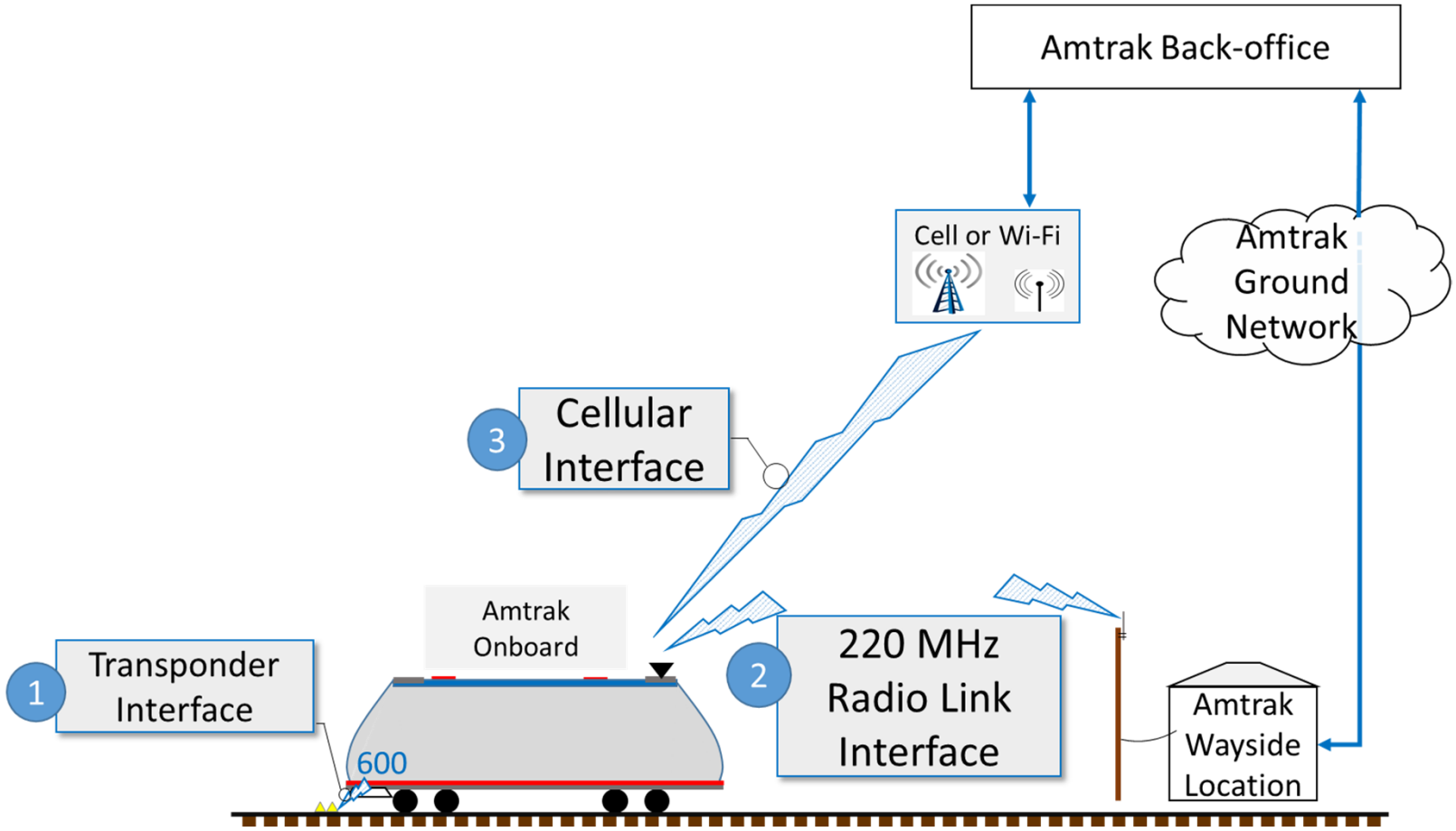
SYSTRA, System Assurance

New York, NY

Key Presentation Take-Aways

- PTC (ACSES II) network security for Amtrak North East Corridor (NEC)
- Security design and demonstration
- Interoperability and smooth cut-over
- Balancing cryptography, performance and operational procedures

The PTC (ACSES II) Wireless Communication System



The PTC (ACSES 2) Wireless Communication System

- Transponder Interface

- 220 MHz Radio Link
  - Primary interface delivering dynamic operating status and restrictions
- Cellular Interface
  - Configuration management and log file retrieval only

PTC Security Constraints

- Design must not change the physical network layer design
- No new hardware or modification to existing hardware
- No impact on the Safety of the system
- Design must have no/minimal impact to current message latency and system timing
- Design must be capable of incremental deployment for both host and tenant
- Design must have no/minimal impact on the system reliability
- Design must accommodate all (known) variations in operations and maintenance

General Security Concepts

- Authentication
  - Do I really communicate with the equipment I want to?
- Integrity Assurance
  - Has the received message been tampered?
- Confidentiality
  - Can a third party read part of my message content?

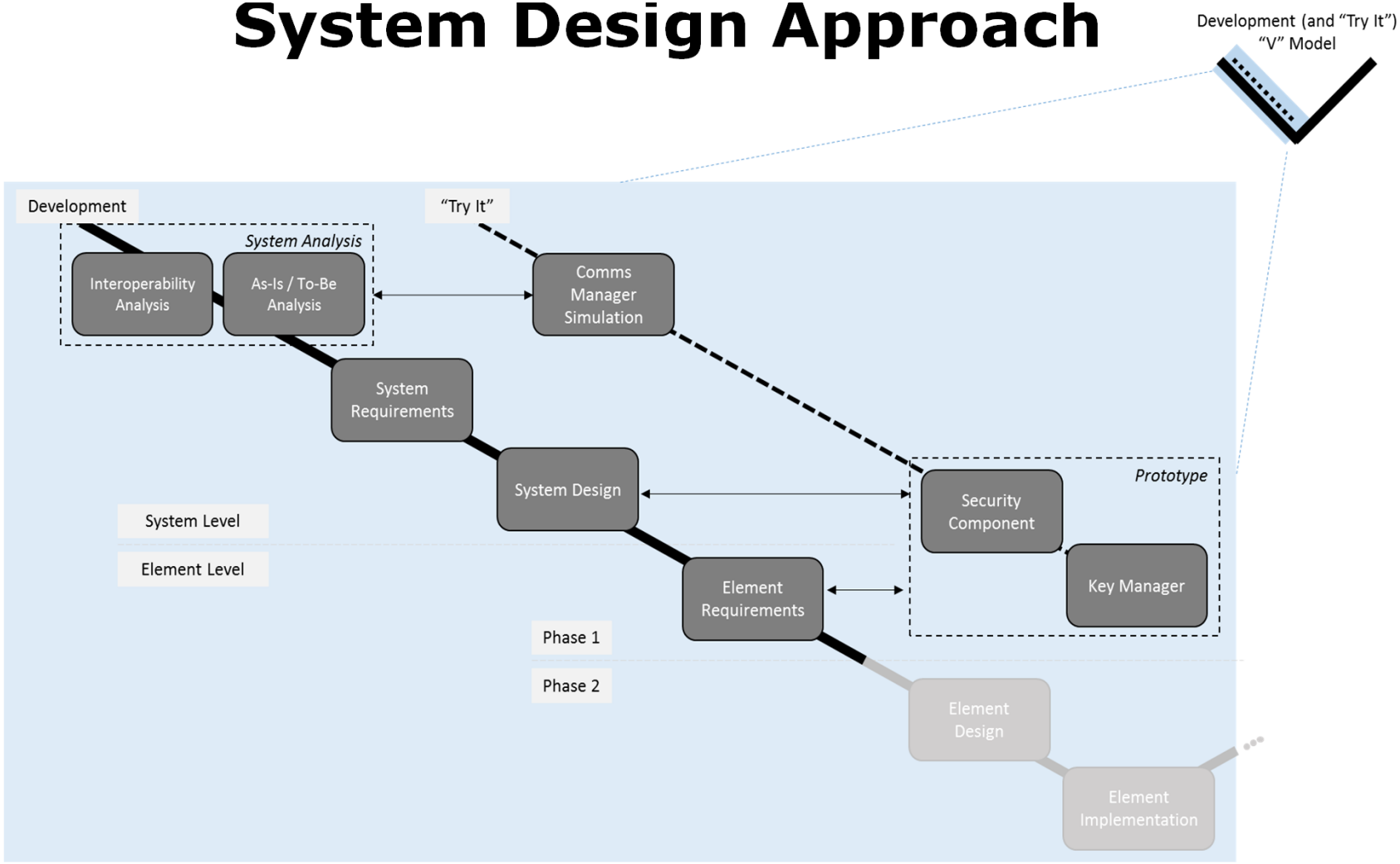
PTC Security Needs

- Defined in the seven clauses of section 1033 of 49 CFR 236
- Message **Authentication** and **Integrity** protection by “approved” cryptographic algorithms
  - Needed on 220 MHz Radio link and Cellular Interface

PTC Security Needs

- Message **Confidentiality** protection by "approved" cryptographic algorithms
  - ➢ Needed on Cellular interface
    - – Key distribution/renewal/revocation
  - ➢ Not needed on 220 MHz radio link
    - – Message information easily retrieved from field status
    - – CPU Load on the equipment for encryption

System Design Approach



System Analysis

- What is the current “as-is” system and what does it do?
- What does the “to-be” user/system need to do?
- What does the current system on other railroads do?
- How much security was enough security for the “to-be” system?

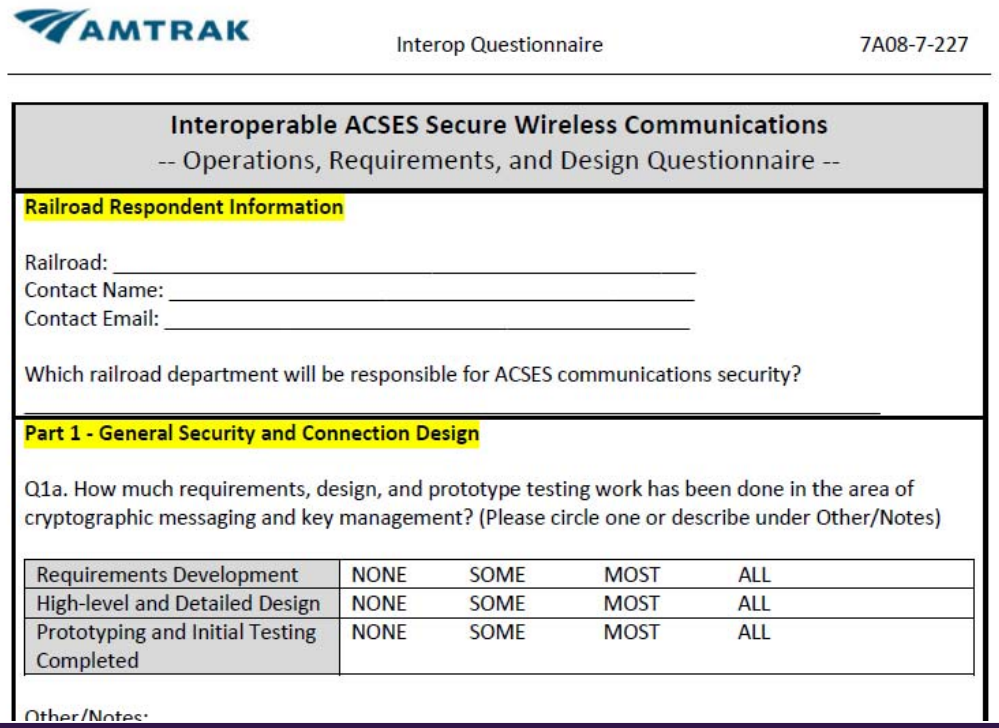
What does the "To-Be" User/System Need to do?

- Developed 35 system level use cases to explore options and determine functions

Id	UC-SYS-211
Title	**Train Communicates with an Own-Railroad Non-Nested Interlocking**
Description	This scenario describes the establishment of communications by an ACSES onboard-equipped train with an approaching interlocking, where the interlocking is *not* nested with the adjacent interlocking in the direction of train travel.
Background/Review	
RR Personnel	(None Required)
Pre-Condition	1. Train has good communications with the approaching base station on the 220 MHz communications link.
Trigger Event	The ACSES onboard equipment determines (via receipt of transponder data) that it is time to initiate communications with an approaching interlocking.
Main Scenario Steps	1. The ACSES onboard listens for beacon messages from the approaching interlocking, and selects a hailing timeslot to use. 2. The ACSES onboard performs requests an interlocking status update from the ACSES wayside. See UC-SYS-251 for details. 3. The ACSES onboard performs requests a TSR list update from the ACSES office. See UC-SYS-253 for details. a. When hailing, the interlocking status and TSR list requests are typically sent in the same (hailing) timeslot. 4. Until the train enters the interlocking, the ACSES onboard periodically requests interlocking and TSR status updates in the same manner as steps 2 and 3.
Resulting System State if Successful	The train receives all interlocking status changes and TSR list changes as it approaches the interlocking.
Failure Scenarios	1. If the wayside subsystem receives an interlocking status request message with corrupted data – base message payload or security data – it logs the issue and drops the request

What does the Current System on other Railroads do?

- Questionnaires and discussions with AAR NEC PTC Committee



AMTRAK Interop Questionnaire 7A08-7-227

Interoperable ACSES Secure Wireless Communications
-- Operations, Requirements, and Design Questionnaire --

Railroad Respondent Information

Railroad: _____
Contact Name: _____
Contact Email: _____

Which railroad department will be responsible for ACSES communications security?
_____

Part 1 - General Security and Connection Design

Q1a. How much requirements, design, and prototype testing work has been done in the area of cryptographic messaging and key management? (Please circle one or describe under Other/Notes)

Requirements Development	NONE	SOME	MOST	ALL
High-level and Detailed Design	NONE	SOME	MOST	ALL
Prototyping and Initial Testing Completed	NONE	SOME	MOST	ALL

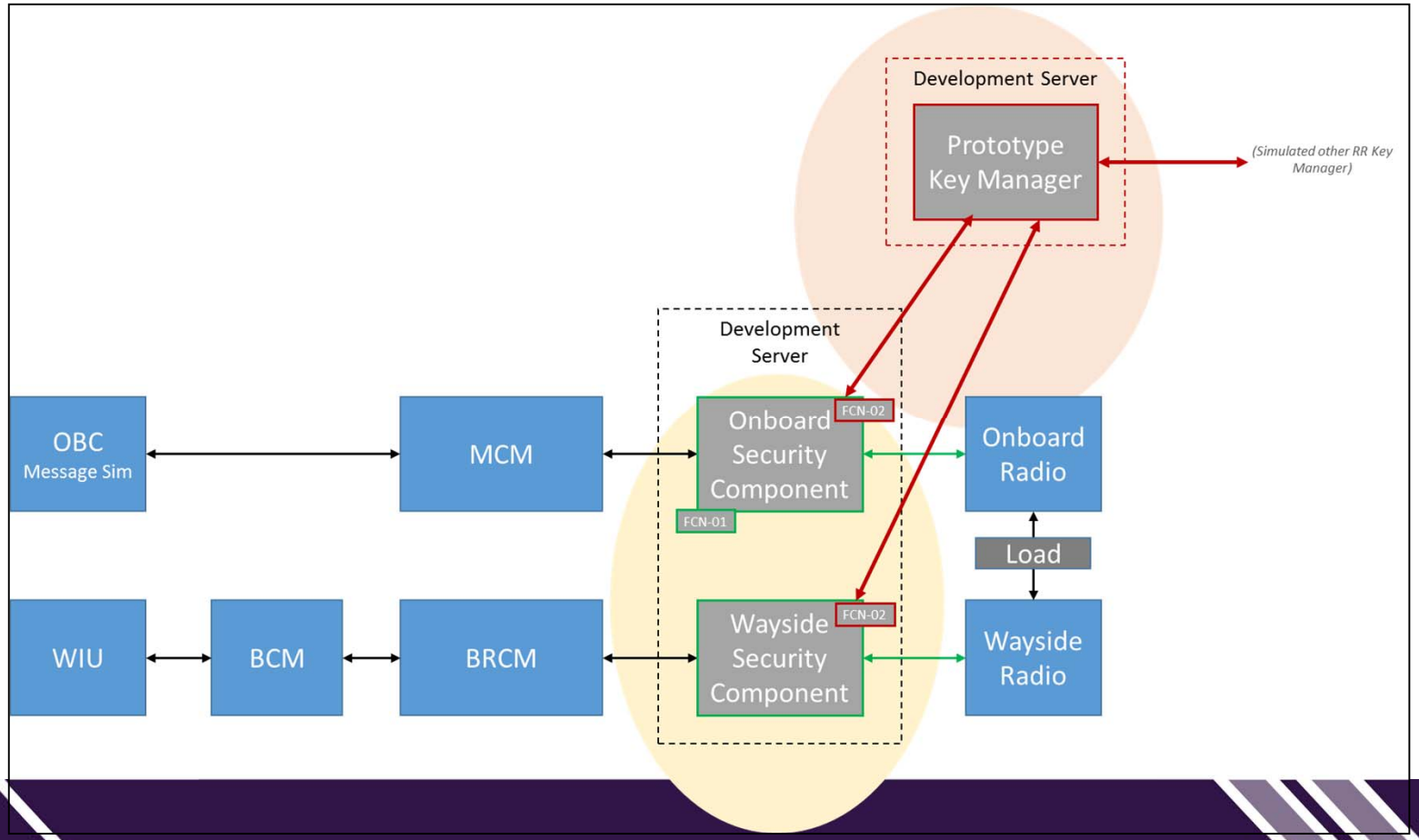
Other/Notes:

How Much Security was Enough Security for the “To-Be” System?

- Threat and Vulnerability Assessment (TVA)
- Threats list is based on the NIST SP 800-30
- 40 Safety constraints on the equipment
- 45 Exported constraints on the railroad organization (maintenance, security process, design…)

Try It Phases

- Proof of Concept and prototype development



Project Status

- Phase 1
  - Functional and security analyses of the current ACSES II
  - System level requirements and design
  - Proof of Concept
- Phase 2
  - Implementation
  - System Verification & Validation
  - Deployment

Phase 1 Outcomes

- A full specification of the security system compliant with FRA requirements and PTC constraints
- A full description of the interoperable interfaces
- Adjustment with other Railroad security systems
- A complete security analysis
- A prototype on Amtrak laboratory equipment

Phase 2 On-Going

- Development of the full scale security system
- Deployment on the NEC for Amtrak - end of December 2018 to meet FRA deadline

Further Works

- Capability for NEC inter-operability assessment
- Methodology reusable for any Railroad wireless system (I-ETMS, CBTC…)

Thank you for your attention