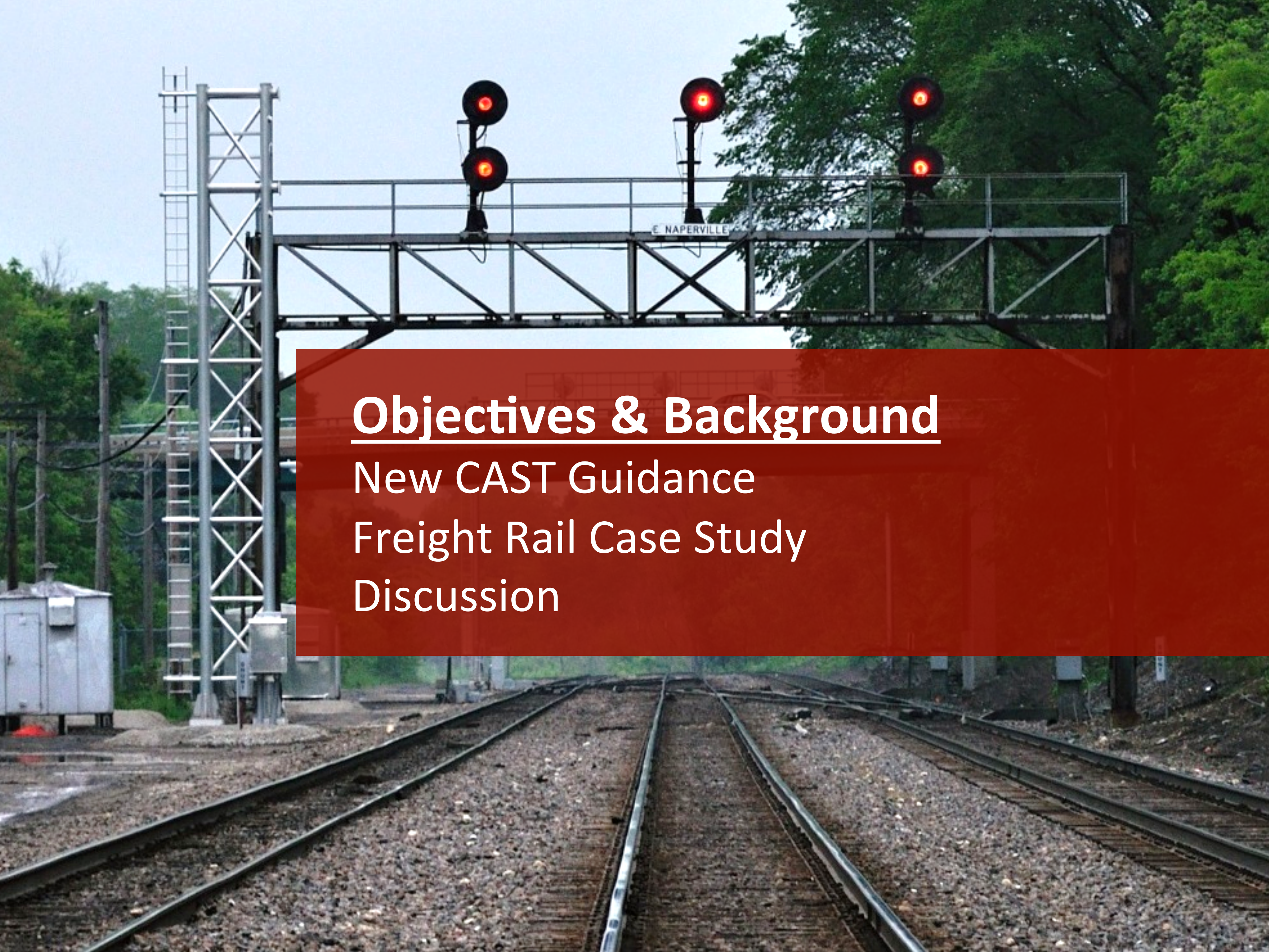
New Guidance for CAST: Case Study of a US Freight Rail Stop Signal Overrun & Collision

Megan France, Jordan Multer, & Hadar Safar, U.S. DOT Volpe Center;
Emilie Roth, Roth Cognitive Engineering

U.S. Department of Transportation
Volpe Center

MIT STAMP Workshop
Cambridge, MA
March 27, 2018



Objectives & Background

New CAST Guidance

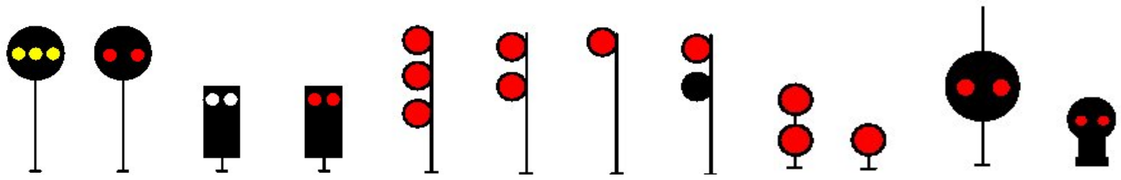
Freight Rail Case Study

Discussion

Objectives

- ❑ Apply CAST to a freight rail case study in order to understand systemic causes of stop signal overruns

- ❑ Suggest additional guidance for CAST to help analysts understand which types of information to include

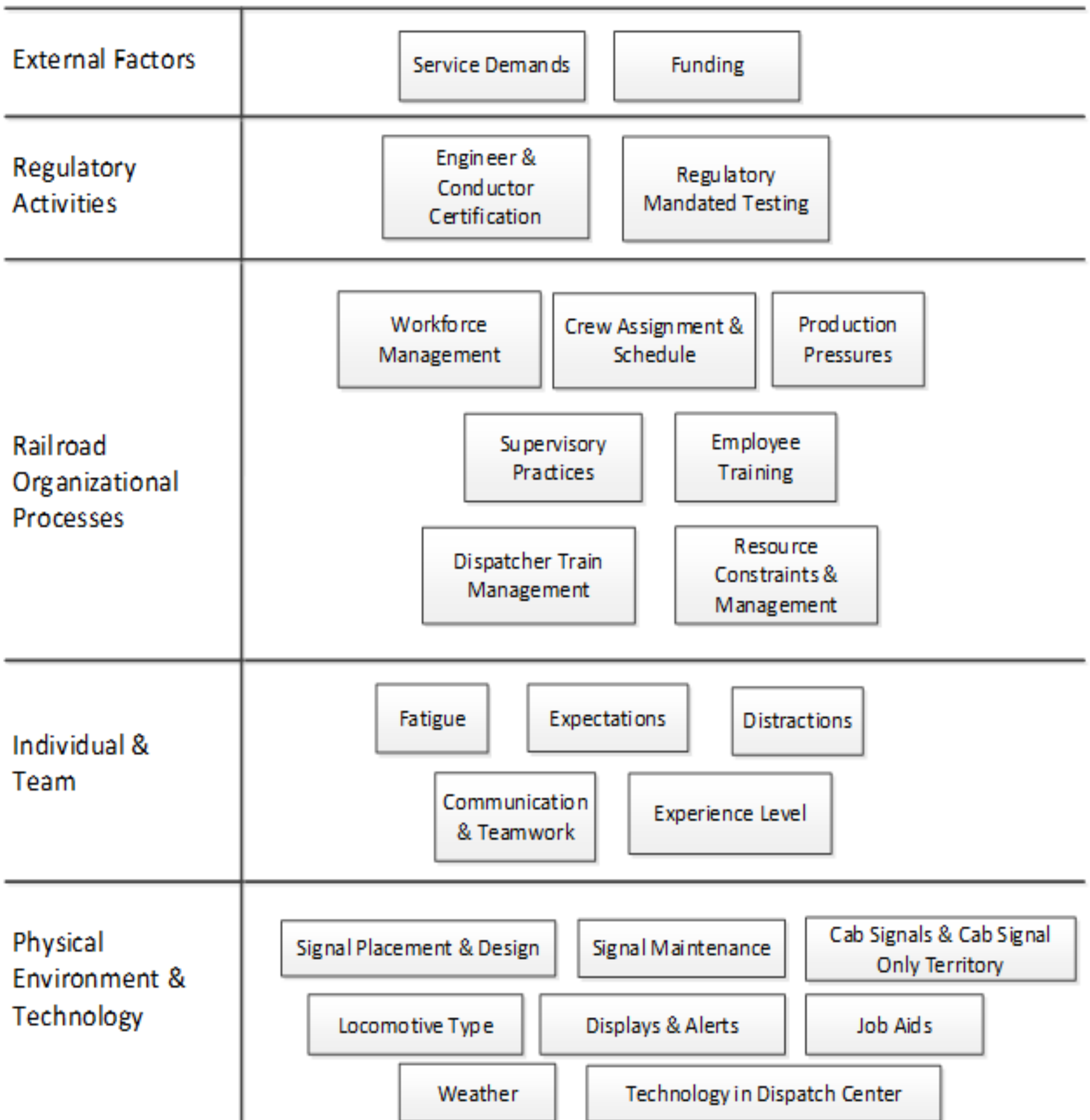


U.S. Department of Transportation
Volpe Center

Background: Stop Signal Overruns (SSOs)

- Consequences can include derailment or collision; may result in injuries, fatalities, and major property damage
- Railroads tend to blame the operators (engineer, conductor), but many factors contribute to these incidents!

Background: Stop Signal Overruns (SSOs)



- 2 prior studies at passenger railroads examining SSOs
- Focus groups, interviews, and observations
- Identified contributing factors at all levels of the system hierarchy!

(Safar, Multer & Roth, 2017)


Objectives & Background
New CAST Guidance
Freight Rail Case Study
Discussion

Additional Guidance: Mental Model Flaws

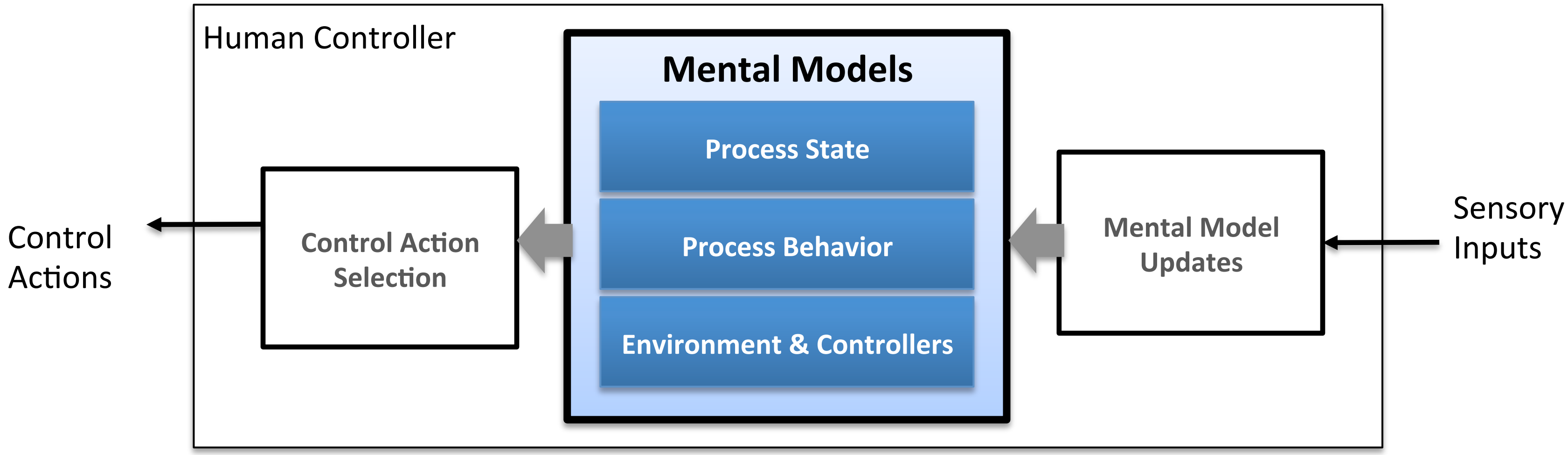
1. Safety Roles & Responsibilities
2. Unsafe Control Actions (UCAs)
3. Mental Model Flaws*
4. Contextual Factors

Recent work (France, 2017) provided additional guidance for mental model flaws in STPA; can be applied to CAST

*This presentation uses *mental model* in place of *process model* when referring to human controllers.

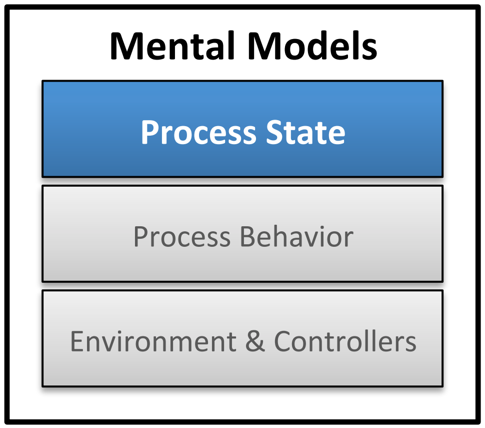
Foundation of Mental Model Guidance

STPA – Engineering for Humans Extension



(Thomas & France, 2016; France, 2017)

Guidance for Mental Models

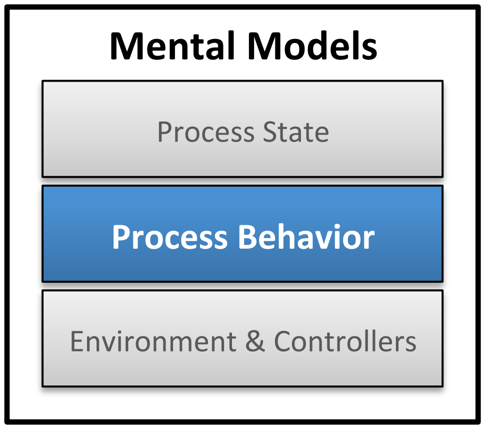


Mental Model of Process State

- Beliefs about modes and mode changes
- Beliefs about the current process stage (for processes with multiple stages)
- Beliefs about system variables (e.g. true/ false, on/off)

(France, 2017)

Guidance for Mental Models

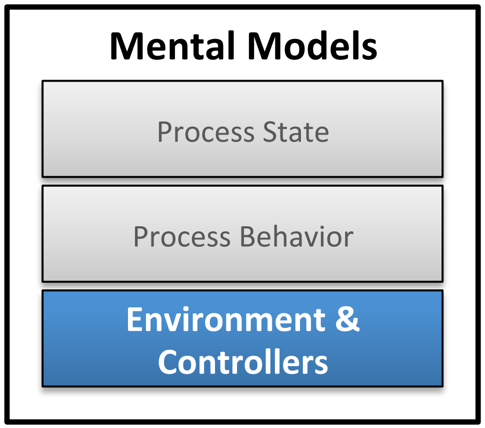


Mental Model of Process Behavior

- ❑ Beliefs about what the system can do
- ❑ Beliefs about how the system will behave in a particular mode or process stage
- ❑ Beliefs about if-then relationships between operator input and system output

(France, 2017)

Guidance for Mental Models



Mental Model of Environment & Controllers

- ❑ Changes to environmental conditions
- ❑ Familiar or unfamiliar environments
- ❑ Other controllers' states and behaviors
- ❑ Social and organizational factors

(France, 2017)

Additional Guidance: Contextual Factors

1. Safety Roles & Responsibilities

2. Unsafe Control Actions (UCAs)

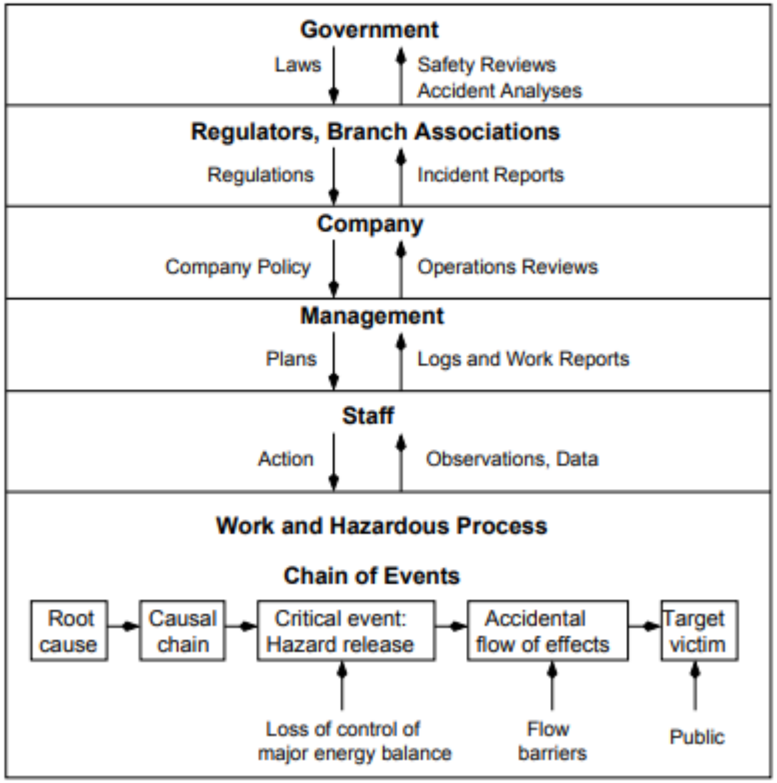
3. Mental Model Flaws

4. Contextual Factors

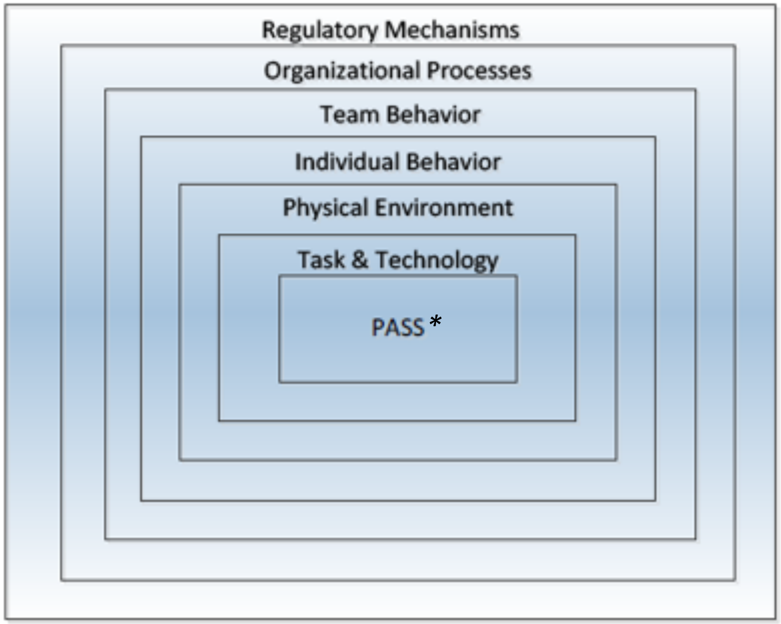
Contextual factors is a broad category, leaving analysts with potential questions:

- ❑ Which types of information belong in "contextual factors"?
- ❑ How should findings listed under "contextual factors" be structured?

Foundations of Contextual Guidance



(Leveson, 2004; adapted from Rasmussen, 1997 and Rasmussen & Svedung, 2000)



(Safar, Roth, & Multer, 2015)

**Note: "PASS" stands for "passing a stop signal" and is synonymous with "Stop Signal Overrun" or SSO.*

Guidance for Contextual Factors

Five categories of contextual factors to consider:

- ❑ Physical system and technology factors
- ❑ Individual and team factors
- ❑ Organizational factors
- ❑ Regulatory factors
- ❑ External / Environmental factors; “Other”

NOTE: This guidance DOES NOT replace the need to create a safety control structure and examine the control and feedback loops specific to YOUR system and controlled process!

This is NOT a checklist; it’s a recommendation to consider factors at all levels of your system!

Guidance for Contextual Factors

Physical System and Technology Factors

- ❑ Operating environment design
- ❑ Interface design (e.g. displays and alerts)
- ❑ Maintenance/operational status of physical systems
- ❑ Availability or non-availability of job aids
- ❑ Other physical factors (e.g. weather)

Guidance for Contextual Factors

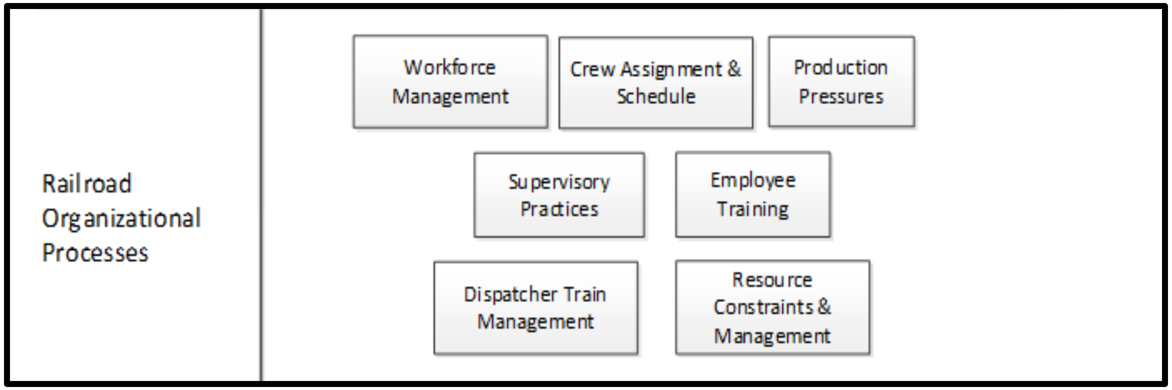
Individual and Team Factors

- ❑ Communication and teamwork; coordination
- ❑ Distractions / competing demands for attention
- ❑ Experience level; qualification and training
- ❑ Fatigue; work schedule
- ❑ Medical fitness for duty
- ❑ Expectations; similar situations encountered

Guidance for Contextual Factors

Organizational Processes

- Supervisory priorities / safety culture
- Resource constraints & production pressures
- Policies and procedures (work schedules, training, discipline, etc.)
- Degree of feedback from employees



Guidance for Contextual Factors

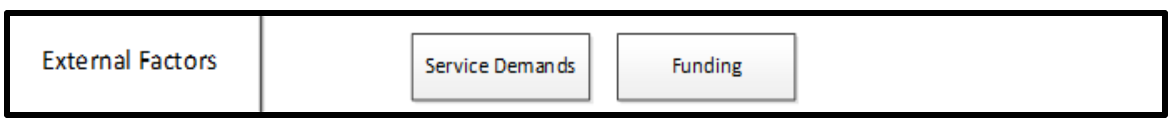
Regulatory Activities

- Degree of support to/control over organizations
- Feedback (data) collected from organizations
- Regulations regarding employees
- Regulations regarding physical systems and technologies

Guidance for Contextual Factors

External Factors

- ❑ High-level societal, governmental, etc. influences
- ❑ Economic context, funding sources
- ❑ Demands for service driving production pressures
- ❑ Political climate's effects on funding, regulation, etc.



<u>REMINDER: </u>These lists are not comprehensive, they are simply a set of examples!

U.S. Department of Transportation
Volpe Center

Complete CAST Controller Guidance

1. Safety Roles & Responsibilities

2. Safety Constraints Violated or Unsafe Control Actions (UCAs)

3. Process Model (Mental Model) Flaws

Explain why Unsafe Control Actions appeared appropriate to the controller.

A. Mental model of process state
B. Mental model of process behavior
C. Mental model of environment

4. Contextual Factors

Systemic factors that influence controllers' mental models and decisions.

A. Physical system and technology factors
B. Individual and team factors
C. Organizational processes
D. Regulatory activities
E. External factors

Objectives & Background

New CAST Guidance

<u>Freight Rail Case Study</u>

Discussion

Head-On Collision of Two Union Pacific Railroad Freight Trains

Goodwell, Oklahoma
June 24, 2012, 10:02 a.m

Photo source: the Guymon Daily Herald courtesy of Marit Edwards

- 3 fatalities
  - Eastbound train's engineer & conductor
  - Westbound engineer
- 1 survivor
  - Westbound conductor
- 5 locomotives and 32 cars derailed
- $14.8 million in estimated damage

(NTSB, 2013)

Accidents and Hazards

ACCIDENT

- A train collides with another train on the same stretch of track

HAZARDS

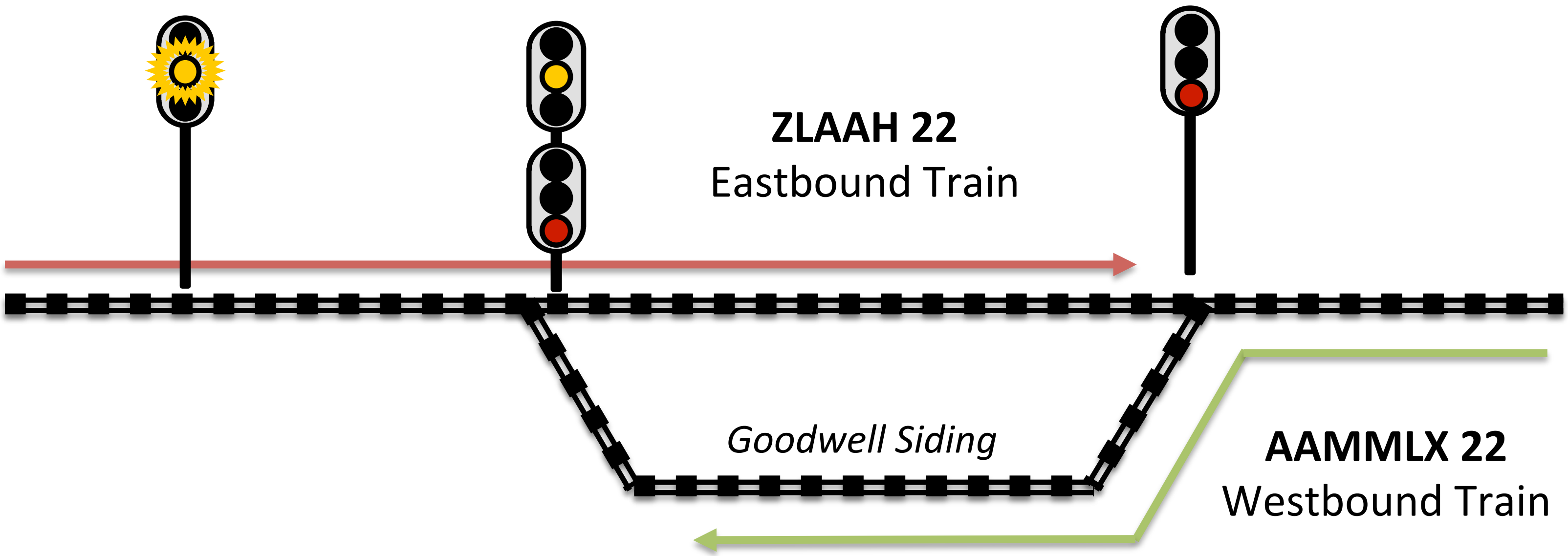
- A train enters an area of track it was not cleared to enter
- A train enters an area of track already occupied by another train

System Safety Constraints

- Dispatchers must use stop and approach signals to alert train crews to areas they do not have clearance to enter
- Train crews must slow down at approach signals and stop at stop signals
- Train crews must have adequate visual acuity and color vision to recognize signal indications
- Railroads must ensure that crews are adequately qualified and medically fit for duty

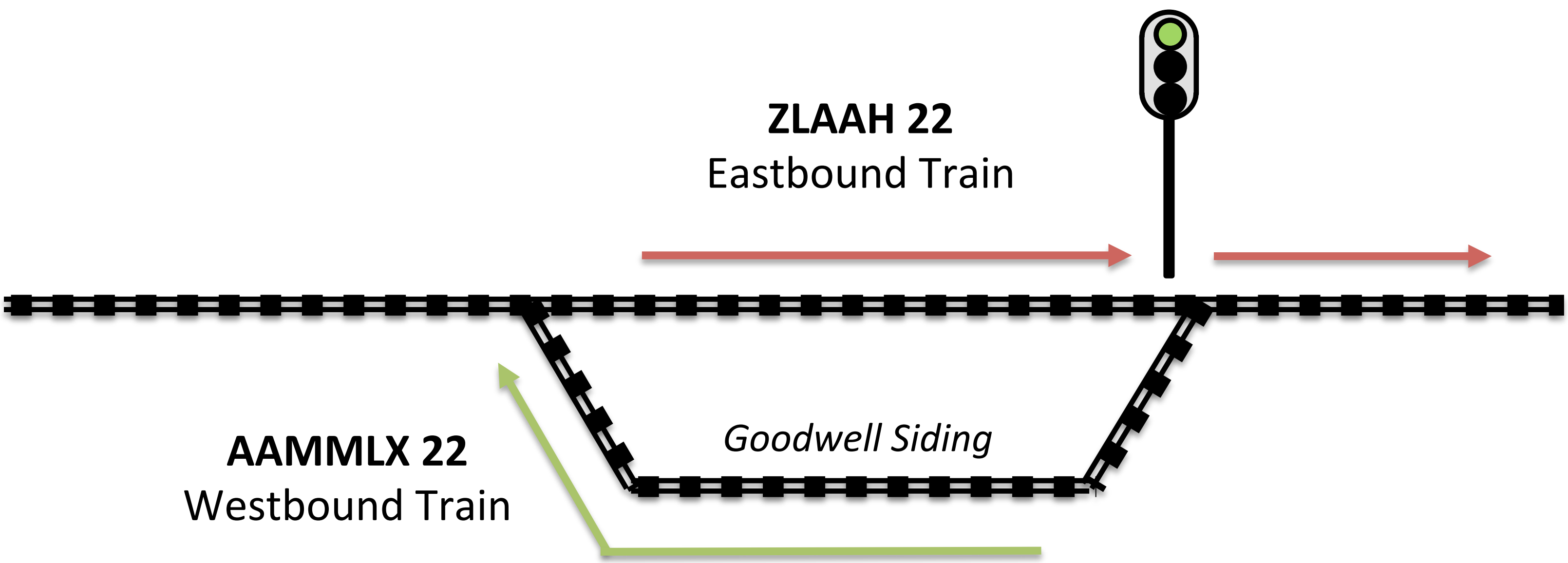
Event Overview: Planned Route

The eastbound train was supposed to wait at the stop signal for the westbound train to enter the siding.



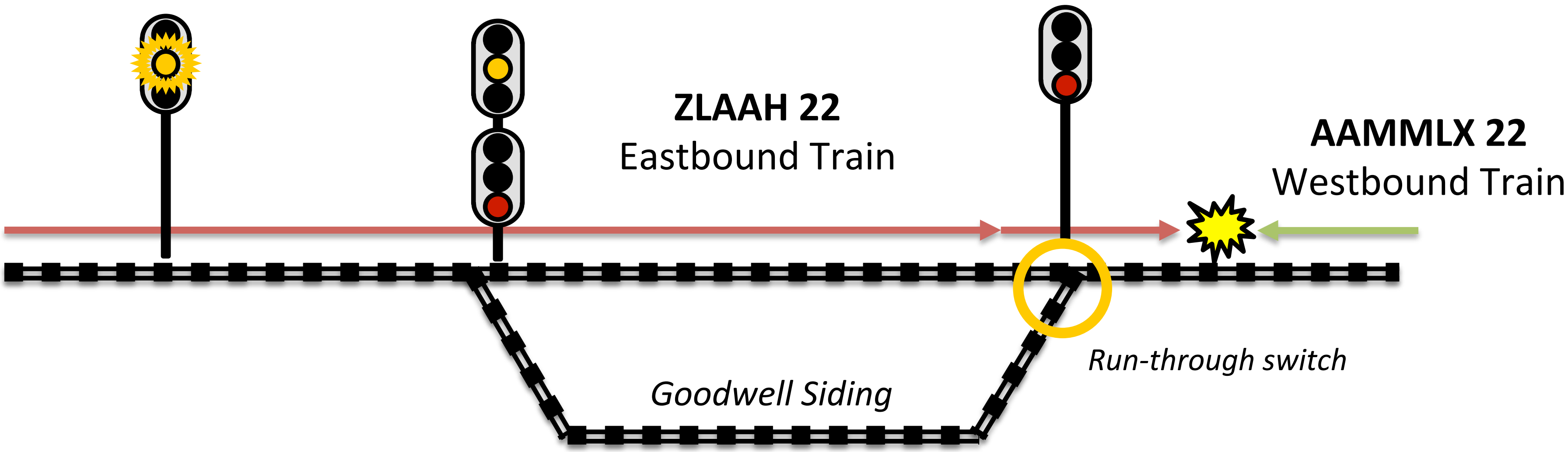
Event Overview: Planned Route

The eastbound train could then proceeded forward safely, followed by the westbound train.



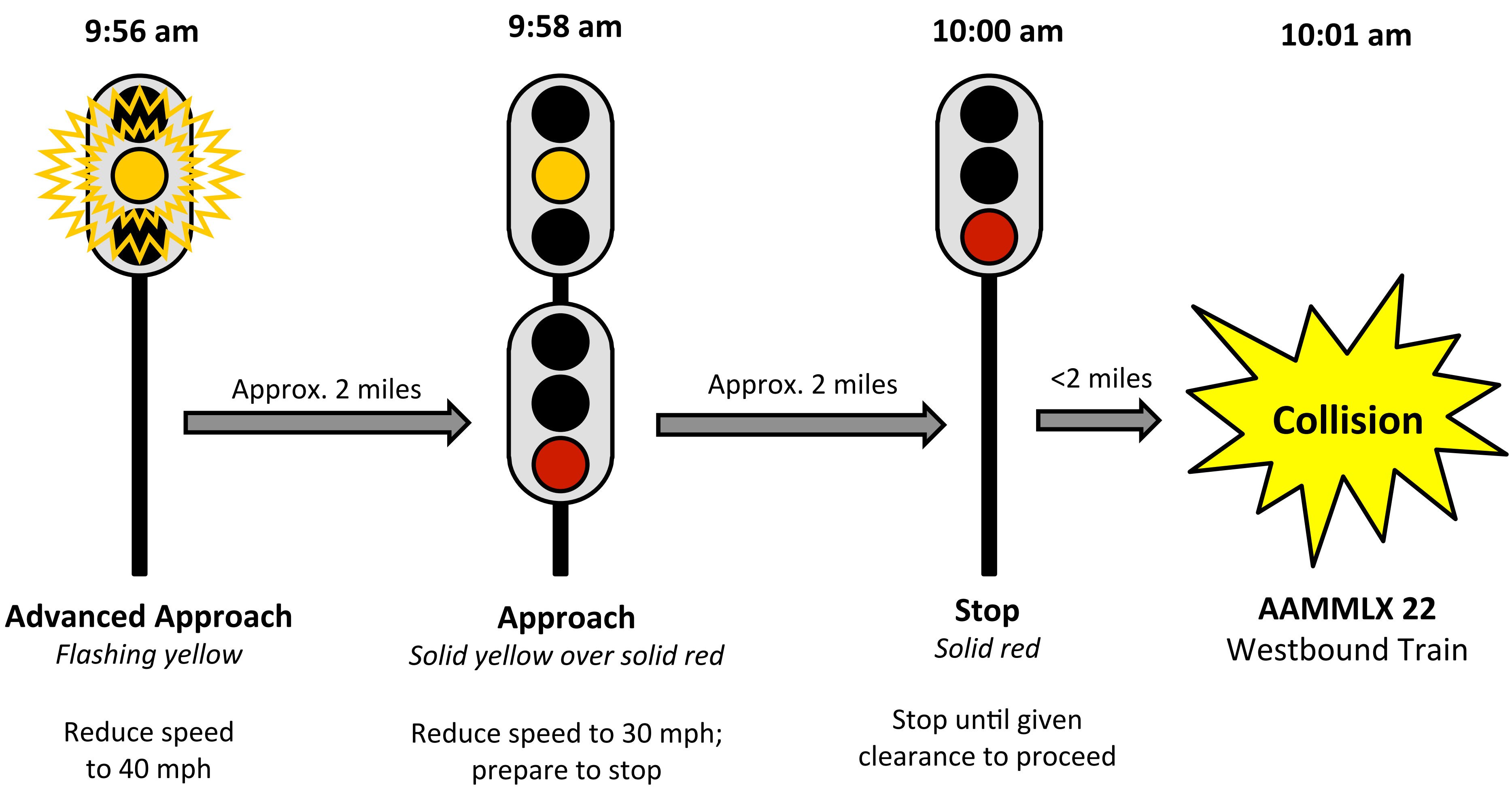
Event Overview: Actual Route

Instead, the eastbound train passed the stop signal and collided with the westbound train before it reached the siding.

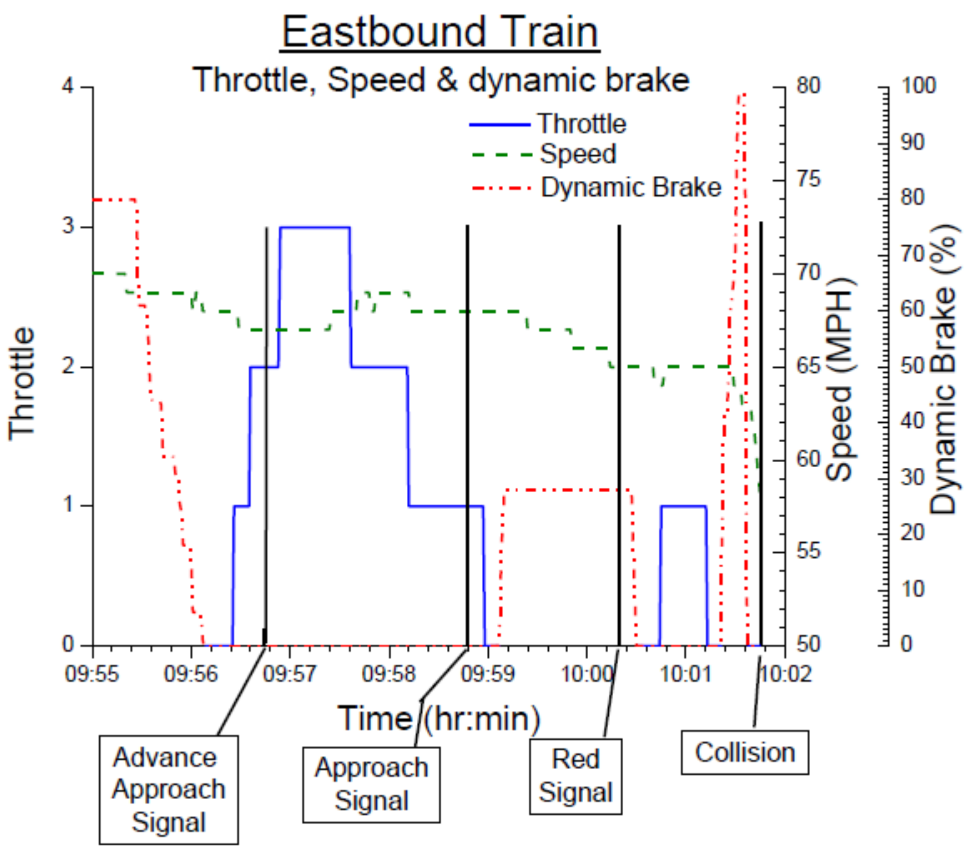


U.S. Department of Transportation Volpe Center

Event Timeline: Eastbound ZLAAH 22



Event Timeline: Eastbound ZLAAH 22



*"...the engineer appeared to make **throttle** and **dynamic brake** adjustments that maintained **train speed close to the 70 mph limit**, as would be expected for a train operating on a clear signal"*

(NTSB, 2013)

U.S. Department of Transportation Volpe Center

Physical System Analysis

(NTSB, 2013)

Safety Controls and Equipment

- Stop signals indicate where trains must not go
- "Approach" signals warn of upcoming stop or speed restrictions
- Sidings allow trains to pass safely on single track

Safety Constraints Violated

- Two trains moving opposite directions were allowed on a single track

Physical System Analysis

(NTSB, 2013)

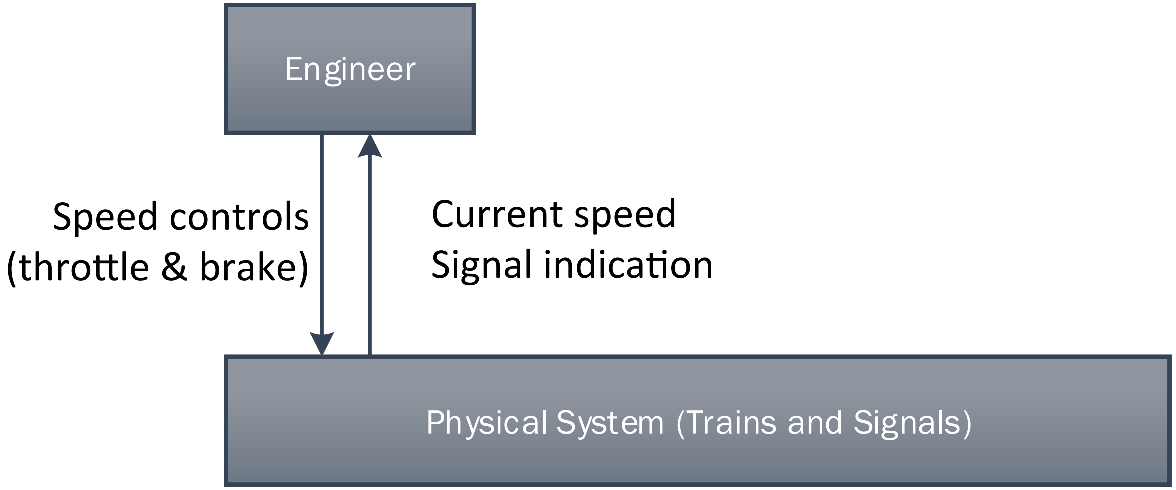
Failures and Unsafe Interactions

- ❑ Signals functioned as intended, but the eastbound train did not obey them
- ❑ No Positive Train Control (PTC) present

Contextual Factors and Additional Questions

- ❑ <u>Individual:</u> If signals were properly functioning, why did the engineer pass a stop signal?
- ❑ <u>Organizational:</u> Why wasn't positive train control installed?

Controller Analysis: Engineer



Controller Analysis: Engineer

Roles and Responsibilities

- Control train speed in accordance with posted signals; call out signal indication to conductor
- Be medically fit to operate a locomotive

Unsafe Control Actions

- Did not slow down as required by approach signals or stop at the stop signal
- Operated while knowing he had inconsistent color vision and diminished visual acuity

Controller Analysis: Engineer

Mental Model Flaws

Model of Process State:

- Incorrectly believed signals were "clear" (green)

Model of Process Behavior:

- *N/A – understood meaning of signals & required actions*

Model of Environment & Controllers:

- May have incorrectly believed conductor would intervene
- Likely unaware of the presence of another train

U.S. Department of Transportation Volpe Center

Controller Analysis: Engineer

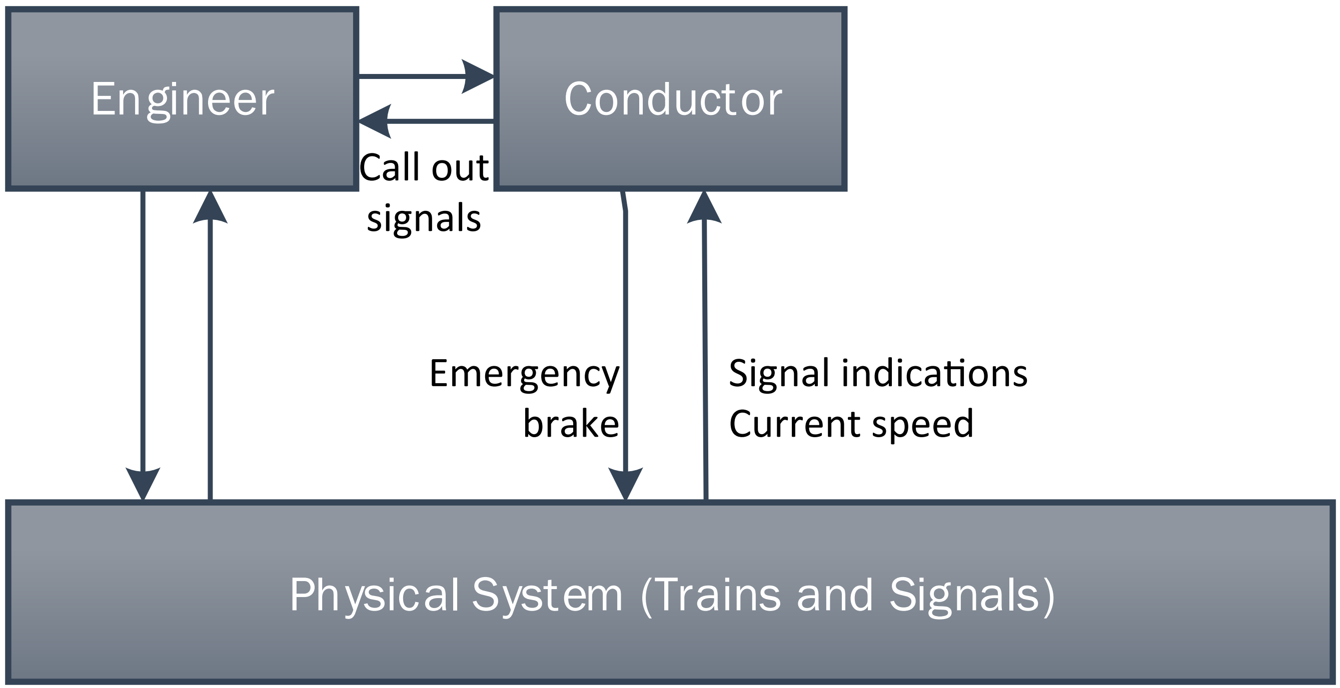
Individual Contextual Factors:

- Perceptual limitations: engineer had severe visual impairments from multiple conditions; had failed a color vision test in 2009
- Coordination: should have been coordinating with conductor to call out signals and ensure proper speed; what was conductor doing?
- Expectations: signals may be typically clear, high-visibility
- Fatigue: fatigue possible based on irregular work schedule

Organizational Contextual Factors:

- What organizational factors allowed (or incentivized) operating despite severe visual severe limitations?

Controller Analysis: Conductor



Controller Analysis: Conductor

Roles and Responsibilities

- Call out signal indications; ensure engineer obeys signals; use emergency brake if necessary

Unsafe Control Actions

- Apparently did not call out the approach and stop signals; did not warn engineer
- Did not pull the emergency brake

Controller Analysis: Conductor

Process Model Flaws

Model of Process State:

- Was likely unaware that signals were in a restrictive state

Model of Process Behavior:

- *N/A – would have understood meaning of signals*

Model of Environment & Controllers:

- Was likely unaware that the engineer was not responding to signals; likely believed engineer could read the signals

Controller Analysis: Conductor

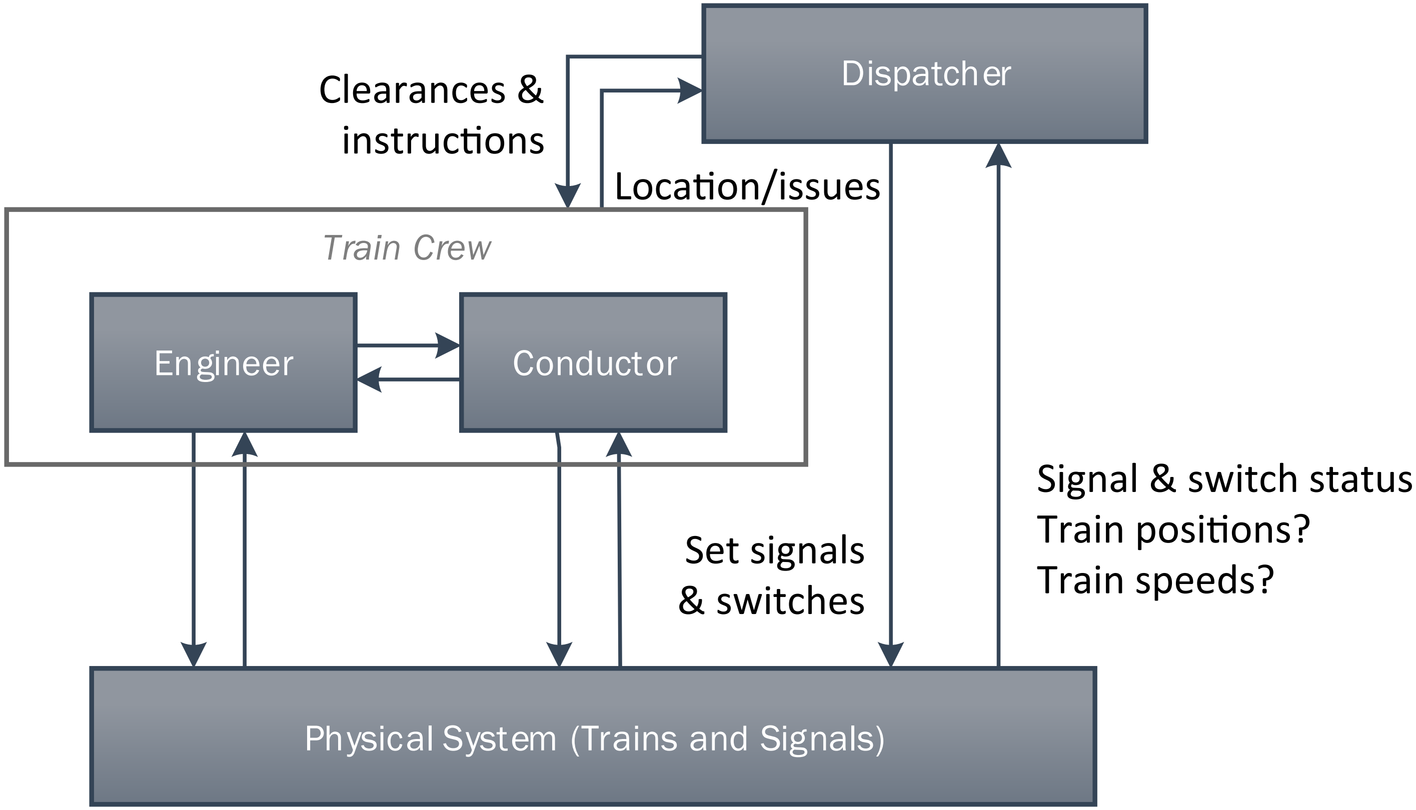
Individual Contextual Factors:

- Distraction / inattention: conductor may have been asleep or absent
- Expectations: signals may be typically clear, high-visibility conditions, may have believed engineer was capable of recognizing signals
- Fatigue: fatigue possible based on irregular work schedule
- Coordination: engineer may have allowed conductor to rest

Organizational Contextual Factors:

- What organizational factors contributed to lack of required coordination between the engineer and conductor?

Controller Analysis: Dispatcher



Controller Analysis: Dispatcher

Roles and Responsibilities

- Set signals and switches for safe routing of trains
- Communicate route information to train crews

Unsafe Control Actions

- Apparently did not warn eastbound train crew about the upcoming stop signal & other train

Controller Analysis: Dispatcher

Process Model Flaws

Model of Process State:

- Did not realize eastbound train had passed the signals

Model of Process Behavior:

- May have believed that if crews passed a signal, he would be alerted and have time to intervene

Model of Environment & Controllers:

- Assumed crew would obey signals even if not given warning

Controller Analysis: Dispatcher

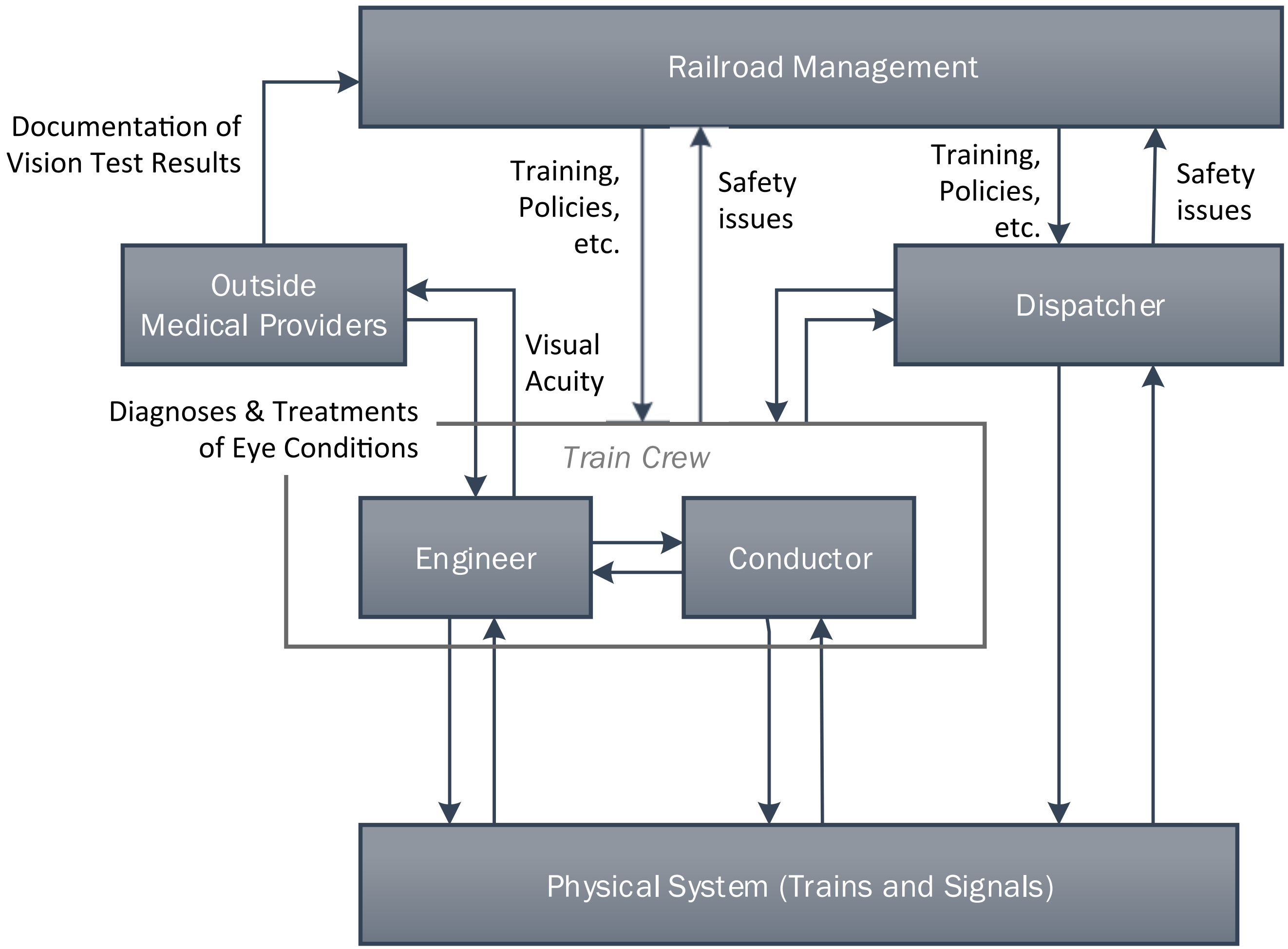
Physical System Contextual Factors:

- Dispatcher was not notified that the train was over the speed limit
- Dispatcher was only notified once the switch at the end of the siding was pushed out of alignment by the eastbound train

Individual Contextual Factors:

- <u>Expectations</u>: did not expect crews to pass a stop signal (very rare)
- <u>Coordination</u>: dispatcher was responsible for 10-12 crews
- <u>Timing</u>: accident occurred approx. 5 mins after first missed signal, and less than 2 minutes after the dispatcher received an alert

Controller Analysis: UP Management



Controller Analysis: UP Management

Roles and Responsibilities

- Ensure that employees are medically fit for duty and adequately trained on job tasks, including coordination
- Ensure that physical system complies with regulations

Unsafe Control Actions

- Did not have PTC installed on the route
- Did not provide training on crew resource management
- Did not require documentation of engineer's visual acuity results; did not require follow-up testing
- Used a color vision test of unknown validity / reliability

Controller Analysis: UP Management

Mental Model Flaws

- May have incorrectly believed engineer's vision was okay
- May have believed that engineer's vision would not be a problem with the conductor assisting by calling out signals
- May have believed resources were not available to implement safety measures, or that safety measures were not as urgent as other priorities (CRM, PTC)

Controller Analysis: UP Management

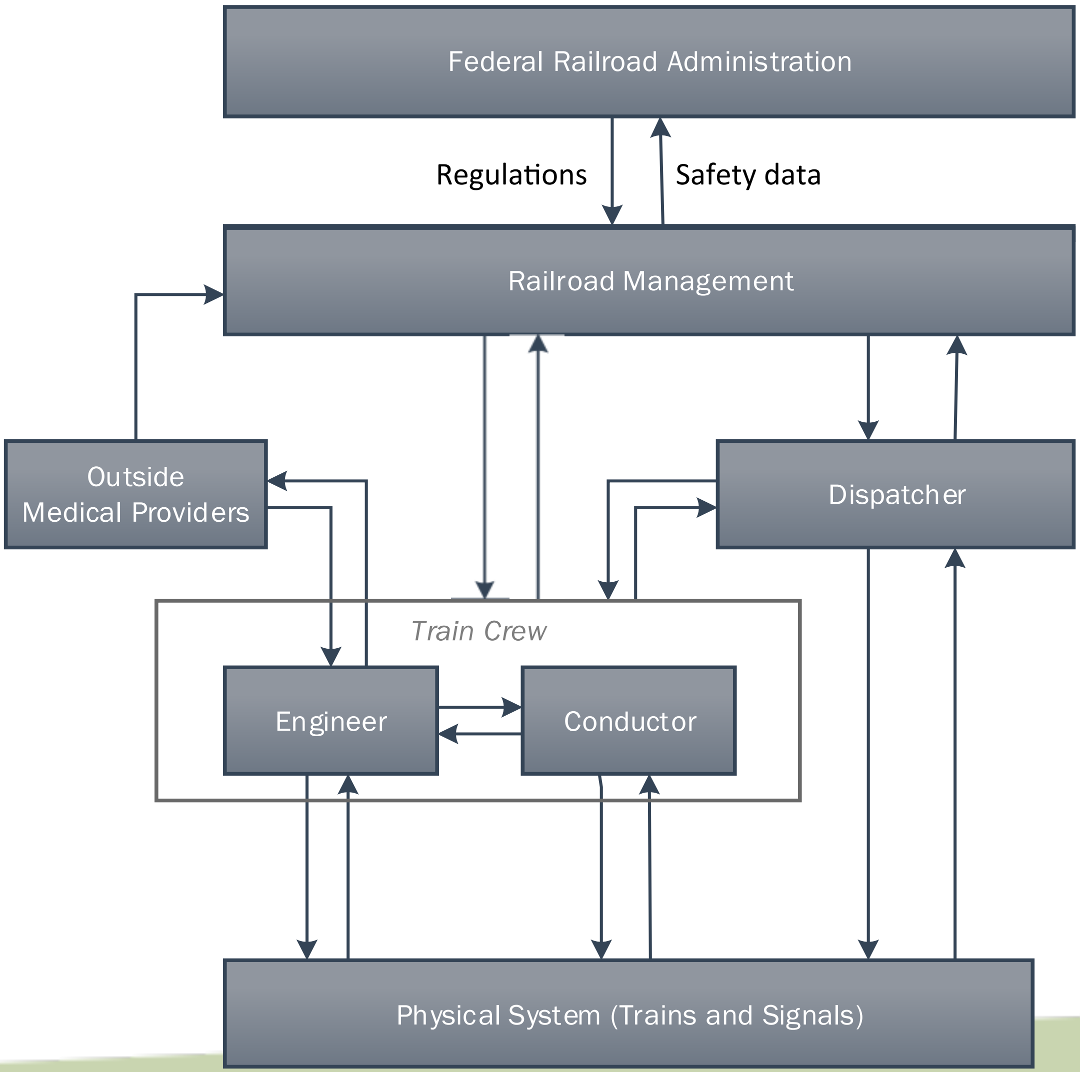
Organizational Contextual Factors:

- Resource constraints: PTC / CRM require large amount of resources
- Staffing constraints: may have needed engineers badly, decided to keep the engineer despite visual limitations
- Policies: did not uniformly apply policy for verifying visual acuity was to obtain written documentation
- Scheduling practices: irregular schedules are common in rail industry; may contribute to fatigue despite hours of service limitations

Regulatory Contextual Factors:

- Was UP in violation of regulations, or were regulations inadequate?

Controller Analysis: FRA



Controller Analysis: FRA

Roles and Responsibilities

- Regulate railroads to ensure safety standards

Unsafe Control Actions

- Allowed retaking vision tests without validating railroad's testing methods
- Did not mandate PTC installation sooner
- Did not mandate CRM trainings

Controller Analysis: FRA

Process Model Flaws

- Believed timeline for PTC implementation was appropriate
- Believed railroads had adequate resources for CRM
- Believed railroads would use a valid vision testing method

Regulatory Contextual Factors:

- FRA already required implementation of PTC by 2015
- FRA conducted research into CRM, provided railroads with funding for pilot programs

External Factors

- Desire to maintain positive relationships with railroads & work within their resource constraints (e.g. PTC regulation timing)


E NAPERVILLE
Objectives & Background
New CAST Guidance
Freight Rail Case Study
Discussion

Enhanced CAST Controller Guidance

1. Safety Roles & Responsibilities

2. Unsafe Control Actions (UCAs)

3. Process Model (Mental Model) Flaws

A. Mental model of process state
B. Mental model of process behavior
C. Mental model of environment

4. Contextual Factors

A. Physical system and technology factors
B. Individual and team factors
C. Organizational factors
D. Regulatory factors
E. External / environmental factors; “other”

- Provides additional guidance on what types of content to include
- Useful for new practitioners of CAST
- Revealed interesting results in our freight case study

U.S. Department of Transportation Volpe Center

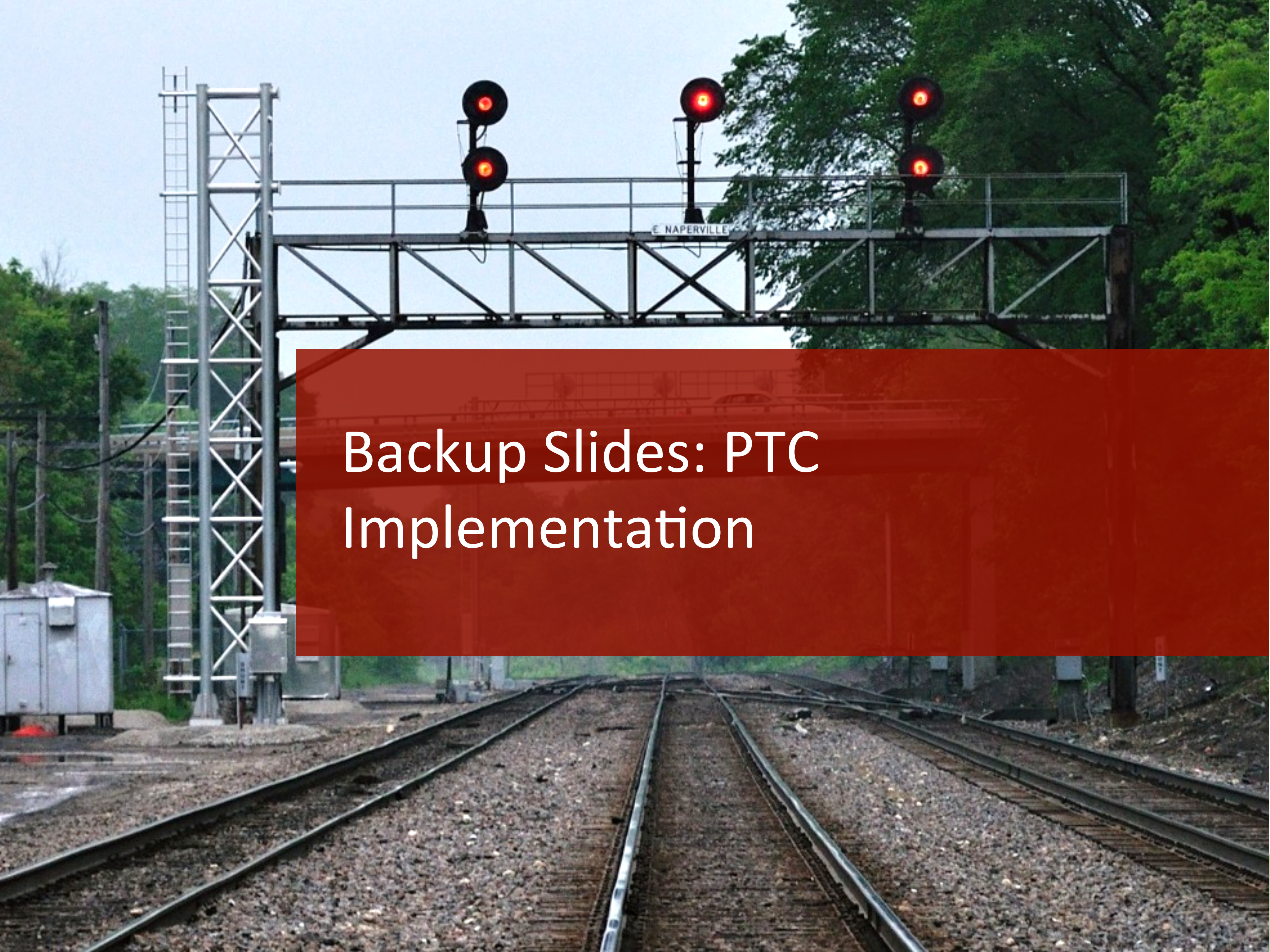
References

- France, M., “Engineering for Humans: A New Extension to STPA,” Master’s Thesis, Massachusetts Institute of Technology, 2017.
- France, M., “Engineering for Humans: Human-Automation Interaction in STPA,” presented at the 6th Annual MIT STAMP Workshop, 2017.
- Leveson, N. G. “A New Accident Model for Engineering Safer Systems.” Safety Science, vol. 42, no. 4, pp. 237-270, 2004.
- Leveson, N. G., “Engineering a Safer World: Systems Thinking Applied to Safety.” The MIT Press, 2012.
- National Transportation Safety Board, “Head on Collision of Two Union Pacific Railroad Freight Trains Near Goodwell, Oklahoma, June 24, 2012.” NTSB/RAR-13/02. Washington, DC: NTSB, 2013.
- Rasmussen, J., “Risk Management in a Dynamic Society: A Modelling Problem,” Safety Science, Vol. 27, No. 2/3, pp. 183-213, 1997.
- Rasmussen, J. & Svedung, I. “Proactive Risk Management in a Dynamic Society.” Swedish Rescue Services Agency, 2000.
- Safar. H., Multer, J,. & Roth, E. “An Investigation of Passing Stop Signals at a Passenger Railroad” Washington, DC: Federal Railroad Administration, 2015.
- Safar. H., Multer, J,. & Roth, E. “Why do passenger trains pass stop signals? A systems view” Washington, DC: Federal Railroad Administration, 2017.
- Thomas, J. and M. France. “Engineering for Humans: STPA Analysis of an Automated Parking System,” presented at the 5th annual MIT STAMP Workshop, 2016.

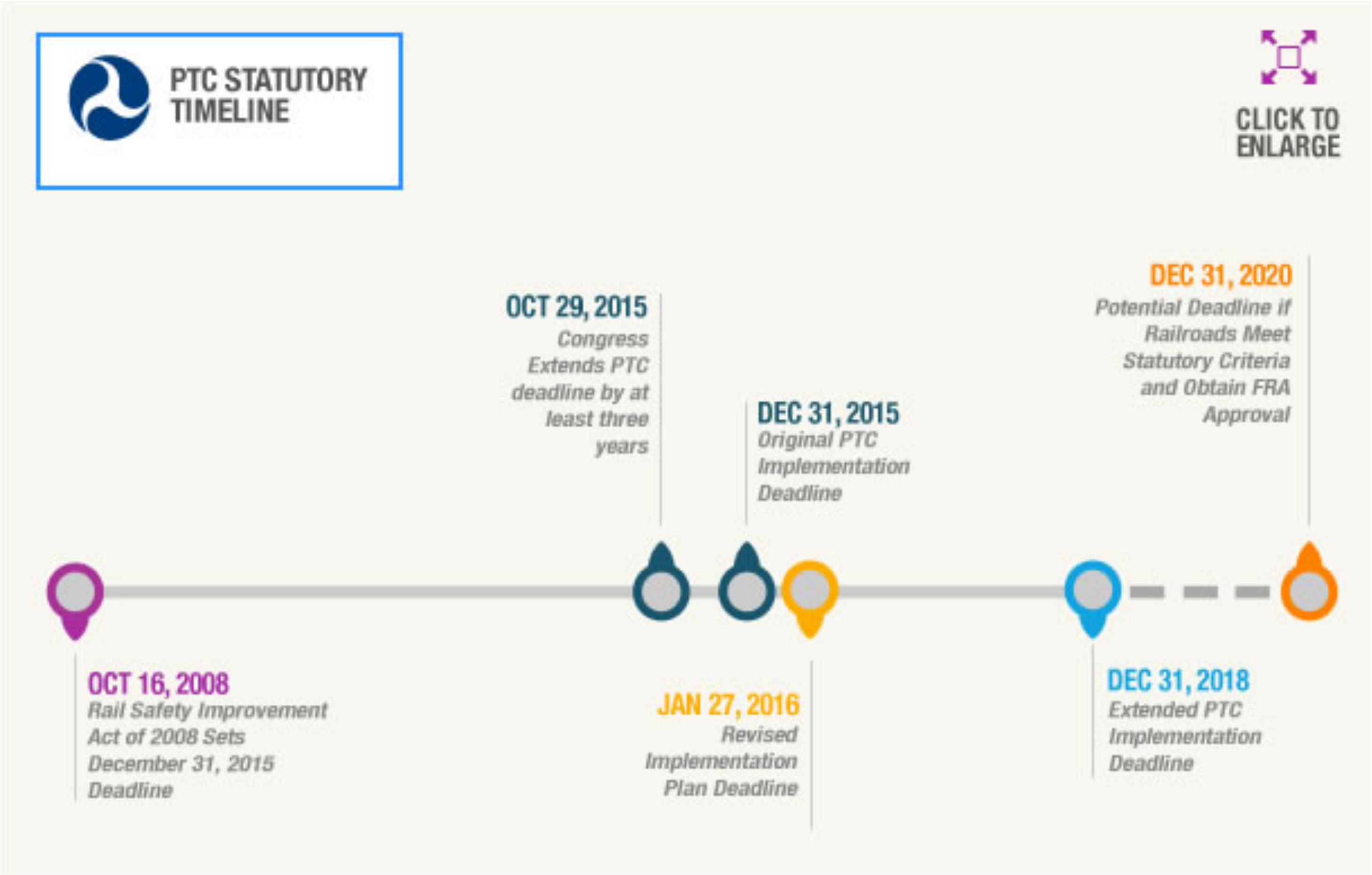
Thank you for your attention!

Contact:
Megan France, US DOT Volpe Center
megan.france@dot.gov

Backup Slides: PTC Implementation

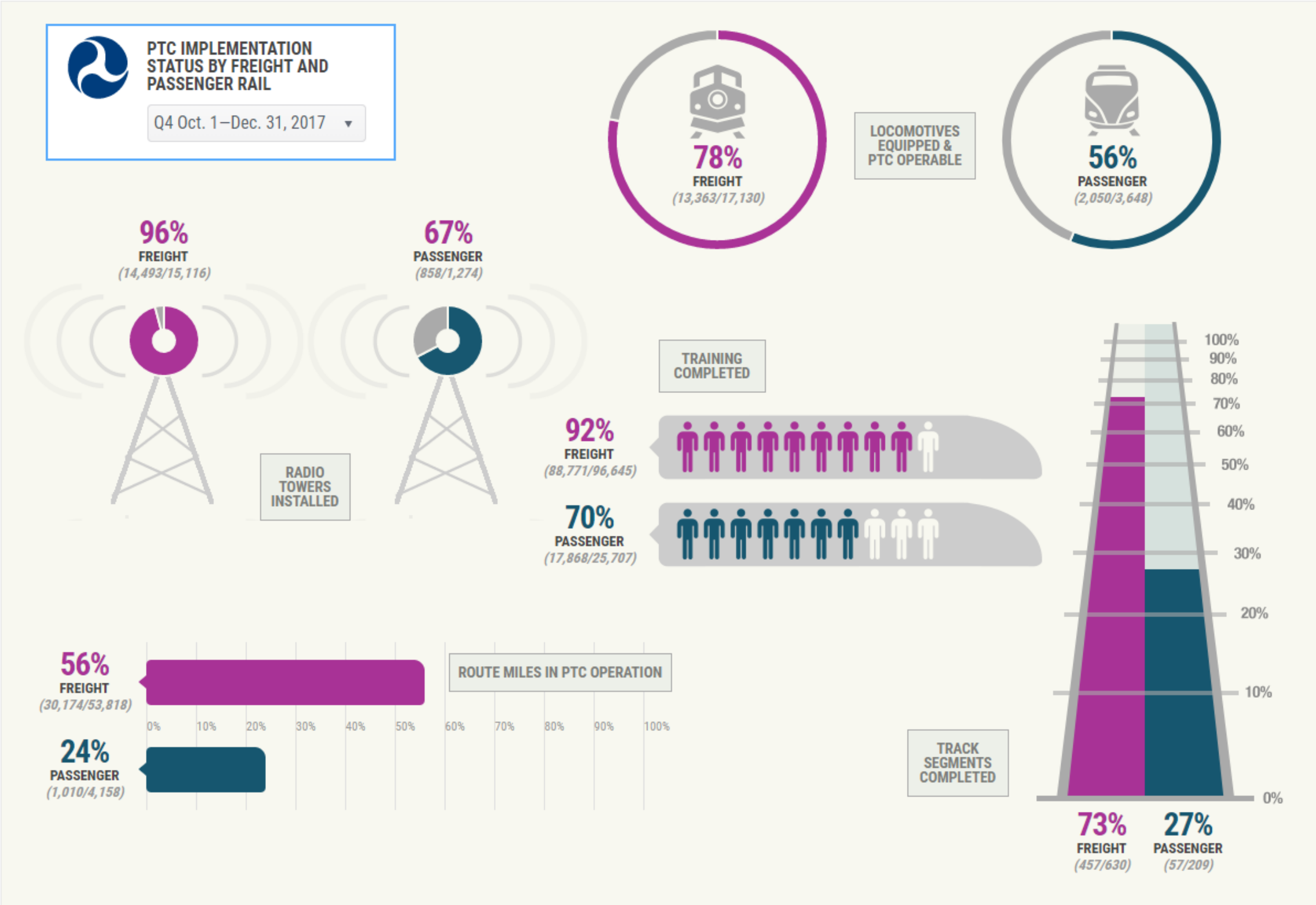


Positive Train Control Timeline



Source: https://www.fra.dot.gov/ptc

PTC Implementation in Freight RRs



Source: https://www.fra.dot.gov/ptc

PTC Implementation at UP

As of December 31, 2017

Source: https://www.fra.dot.gov/ptc

Ongoing/Future Work on SSOs

- Current study focuses on freight environment
  - CAST analyses are a preliminary step
  - Follow-up with interviews, focus groups, etc. and briefing to railroad management
- Other ongoing work
  - Improving SSO data collection using a common form template
  - Communicating findings to railroads in a “Good Practice Guide”