EXPLANATIONS AND CAVEATS RE RISK ASSESSMENT OF TA VS. TWC

The preliminary draft risk assessment for Track Access (TA) in comparison with manual Track Warrant Control consists of a set of fault trees for the top level hazards of train collisions with other trains, collisions with roadway work vehicles and collisions with highway vehicles at crossings that are to be flagged. Derailment hazards are not yet included in this analysis, but their contribution to the total risk is expected to be small in comparison to that of collisions.

Fault trees have been developed for both the Base Case (TWC) and for the Proposed Product (TA) Case. The Base Case is the form of operation that was understood to have been used at Marquette Rail (MQR) prior to the introduction of TA, namely, manual (not computer-aided) Track Warrant Control (TWC), in accordance with GCOR. The Proposed Product Case is that of operating the TA system without a dispatcher or other control operator.

Assumptions used in the fault trees regarding the TA application on MQR are:

- Track Plan Infrastructure – all three subdivisions of MQR
- Total Number of Trains and Movement Density – normal mainline operations on MQR; yard/switching operations not included.
- Wayside Train Control Subsystems and Components – None
- Onboard Train Control Subsystems and Components – None, other than a cellphone for the TA case or a radio or cellphone for the TWC case.
- Frequency of Issuing Authorities = 1,429 per year (actual quantity in 2007)
- Frequency of Issuing Bulletins = 879 per year (actual quantity in 2007)
- Probability of Authority Violation per Authority = 6.7e-6 (historical Class 1 data)
- Probability of Human Error when using TA with appropriate training = 2.5e-4 (per NUREGs with shaping factors)
- Probability of Human Error when using manual TWC with appropriate training = 5e-4. This is based on the shaping factor data provided in the SPAR-H NUREG which indicates that system complexity can increase probability of human error by a factor of 2 to 5. Given the additional complexity of TWC over TA, a factor of 2 was applied (2.5e-4 x 2 = 5e-4). This is considered a conservative assumption, given that MQR's TWC form has 13 line items vs. 4 line items in TA's authority form, and TWC includes conditional authorities (TA does not), which are known to increase risk appreciably.
- Probability of Hardware/Software Logic Fault = 10e-6 (hardware supplier quote & adjustments – see explanation below)
- Probability of Undetected Data Corruption = 10e-6 (see explanation below).

TTCI has insufficient insight into the development processes that were applied and therefore no means to assess the software integrity of TA in a way that would yield a quantitative probability of software logic fault for the system. So, for fault tree purposes, the probability of combined software and hardware wrong-side fault has been roughly estimated by simply using the same approach as was used in another PSP developed by a class 1 railroad and approved by FRA. That approach was to obtain the MTBF for the

system hardware from the supplier and to assume that the combined rate of software and hardware wrong-side faults will not exceed 10% thereof. The supplier quote was just over 200,000 hours MTBF. For conservatism, this was de-rated to 100,000 hours, or an overall failure rate of 1e-5 per hour, for all types of failures. Applying the 10% factor yields a failure rate of 1e-6 per hour, just for wrong-side software and hardware faults, which are the only faults of concern to this risk assessment.

This estimate of probability of combined software and hardware wrong-side fault is intended to be replaced by a more accurate, scientifically-obtained value, provided by RailSoft prior to submission of this risk assessment to FRA.

As a sanity check, it is generally accepted that well developed and tested software will attain an appreciably lower probability of error than a human performing the same function. Since the human error probability was determined to be 2.5e-4, an assumption of 1e-6 for TA software failure rate is intuitively reasonable.

The probability of undetected data corruption was estimated based on the logic that both of two events must occur: 1) there must be a data error and 2) the detection mechanism must fail to detect it. Assuming that the initial data error is caused by a logic fault, the probability of that event is 1e-6.

Theoretically, the probability of the data error detection mechanism employed failing to detect a data error is generally better 1e-6. However, the detection algorithm is implemented in software whose integrity is 1e-6, so it seems unreasonable to assume an ability to detect errors beyond that. Consequently, the probability undetected data corruption (for protected data in the TA system) is: 1e-6 x 1e-6 = 1e-12.

Additional caveats regarding these preliminary draft risk assessment results:

- Certain input data is still being awaited from suppliers, e.g., SMS text message error rate/error detection characteristics from Alltel, additional data on TA hardware and software failure rates. Rough estimates had to be made for the time being.
- Risk probabilities for human tasks can vary significantly from person-to-person and situation-to-situation. The risk assessment results will vary accordingly.
- Absolute quantitative results are subject to many uncertainties as discussed here. However, by using the same risk assessment method for the TA Case and the TWC (Base) Case, the relative comparison of risk between the two systems should have a higher level of confidence than the absolute risk presented for either system. So, the primary value of these results is for comparative purposes.
- Combinatorial effects of any possible risks that might appear in more than one place throughout the tree are not taken into account.

Baseline conclusions of the FTA-based risk assessment indicate the following potential values of hazard rate and mean time to hazardous event (MTTHE):

- hazard rate for collisions in the TA Case is approximately 2.5e-6/train-operating-hour,
  or a MTTHE of approximately 403,000 train-operating-hours.
- hazard rate for collisions in the Base Case (TWC) is approximately 9.1e-5/train-operating-hour,
  or a MTTHE of approximately 11,000 train-operating-hours.

The risk assessment indicates a potential safety improvement of a factor of approximately 37 when using TA as compared with the base case of manual TWC.

Note that hazard rate is not the same as accident rate. A hazard is defined as a condition that is prerequisite to a mishap (per MIL-STD-882C). Hazards generally occur at a significantly higher rate than accidents (mishaps).

Sensitivity analyses were also performed with regard to key input parameters. The input parameter variations and results are cited below.

Sensitivity Analysis Variation Case #1: The probability of software and hardware wrong-side fault was increased (degraded) by a factor of 10. Conclusions of the FTA-based risk assessment indicate the following potential values of hazard rate and mean time to hazardous event (MTTHE):

- hazard rate for collisions in the TA Case is approximately 4.0e-6/train-operating-hour,
  or a MTTHE of approximately 250,000 train-operating-hours.
- hazard rate for collisions in the Base Case (TWC) is approximately 9.1e-5/train-operating-hour,
  or a MTTHE of approximately 11,000 train-operating-hours.

The risk assessment indicates a potential safety improvement of a factor of approximately 23 when using TA as compared with the base case of manual TWC.

Sensitivity Analysis Variation Case #2: The probability of human error was increased (degraded) by a factor of 10. Conclusions of the FTA-based risk assessment indicate the following potential values of hazard rate and mean time to hazardous event (MTTHE):

- hazard rate for collisions in the TA Case is approximately 1.2e-5/train-operating-hour,
  or a MTTHE of approximately 82,000 train-operating-hours.
- hazard rate for collisions in the Base Case (TWC) is approximately 9.0e-4/train-operating-hour,
  or a MTTHE of approximately 1,100 train-operating-hours.

The risk assessment indicates a potential safety improvement of a factor of approximately 75 when using TA as compared with the base case of manual TWC.

Sensitivity Analysis Variation Case #3: The probability of human error was decreased (improved) by a factor of 10. Conclusions of the FTA-based risk assessment indicate the following potential values of hazard rate and mean time to hazardous event (MTTHE):

- hazard rate for collisions in the TA Case is approximately 1.6e-6/train-operating-hour,
  or a MTTHE of approximately 630,000 train-operating-hours.
- hazard rate for collisions in the Base Case (TWC) is approximately 1.0e-5/train-operating-hour,
  or a MTTHE of approximately 98,000 train-operating-hours.

The risk assessment indicates a potential safety improvement of a factor of approximately 6 when using TA as compared with the base case of manual TWC.

Sensitivity Analysis Variation Case #4: The probability of voice communication error (e.g., by cell-phone for TA and by radio or cell-phone for TWC) was decreased (improved) by a factor of 10. Conclusions of the FTA-based risk assessment indicate the following potential values of hazard rate and mean time to hazardous event (MTTHE):

- hazard rate for collisions in the TA Case is approximately 2.4e-6/train-operating-hour,
  or a MTTHE of approximately 410,000 train-operating-hours.
- hazard rate for collisions in the Base Case (TWC) is approximately 9.1e-5/train-operating-hour,
  or a MTTHE of approximately 11,000 train-operating-hours.

The risk assessment indicates a potential safety improvement of a factor of approximately 37 when using TA as compared with the base case of manual TWC.

Sensitivity Analysis Variation Case #5: The probability of human error for the Base Case (TWC) was decreased (improved) by a factor of 2, to exactly match the rate used in the TA Case. Conclusions of the FTA-based risk assessment indicate the following potential values of hazard rate and mean time to hazardous event (MTTHE):

- hazard rate for collisions in the TA Case is approximately 2.5e-6/train-operating-hour,
  or a MTTHE of approximately 403,000 train-operating-hours.
- hazard rate for collisions in the Base Case (TWC) is approximately 4.6e-5/train-operating-hour,
  or a MTTHE of approximately 22,000 train-operating-hours.

The risk assessment indicates a potential safety improvement of a factor of approximately 18 when using TA as compared with the base case of manual TWC.

Note that the results presented here are considered to be of a preliminary draft nature, for the various reasons cited above. The results are to be refined as more input data becomes available and further assessment is performed.