4005 20th Avenue W, Suite 111
Seattle, WA 98199
1-206-781-4475
jniles@alum.mit.edu
October 4, 2002

Mr. Harry Saporta, Director
Office of Safety and Security
Federal Transit Administration
Washington, DC
(e-mail transmission)

Dear Harry:

In re: Hazards in the Design of the Seattle Regional Light Rail System

I have reviewed the draft Handbook for Transit Safety and Security Certification you sent me Sept. 12 as a resource for understanding how the design of the Link Light Rail mixed-mode operation in the downtown bus tunnel would be certified. The Handbook looks to be a very professional product. Thank you for sharing.

This is my reaction to the Handbook in the context of Seattle's light rail line. As you suggested, the Handbook draft bears on my concerns about the Seattle Central Link LRT project. What follows is very detailed. I am sending this letter additionally to Ted Uyeno at FTA Region 10 where staff are reportedly reviewing the Seattle FFGA application, because I am raising fundamental concerns about the viability of the Seattle Central Link Light Rail design. I am also sending copies to Hamid Qaasim at Sound Transit, and Greg Hull at APTA, both of whom I have spoken with earlier.

Page 10-11 of the Certification draft Handbook teaches me:

QUOTE
The system safety and security discipline manages hazards and vulnerabilities throughout the life cycle of a project, program, or activity through a committed approach to risk management, where:

- A hazard is a condition or circumstance that could lead to an unplanned or undesired event;
- A vulnerability is a characteristic of the system that increases the probability of occurrence of a security incident; and
- Risk is an expression of the impact of an undesired event or security incident in terms of severity and likelihood.

Certification for safety and security verifies application of this discipline for transit projects. Through this process, hazards and vulnerabilities are translated into risks,

which are then analyzed, assessed, prioritized, and resolved, accepted or tracked. Figure 1 presents this process as a continuous loop, providing for validation of decisions and on-going evaluation to support further action. This iterative process supports the consideration of safety and security objectives during all activities of the dynamic and evolving project management process.
UNQUOTE

In Seattle, a key LRT hazard needing to be translated into risk is the potential circumstance of road vehicles such as buses, trucks, cars, or even bicycles being on the tracks, being struck by rail vehicles, and people killed or injured. This is of greatest concern in the Downtown Tunnel where buses and trains travel along the same guideway, and also in the Rainier Valley south of Seattle where there are 18 grade crossings of the tracks. The historical record indicates that there were times in the development of the design of Link Light Rail that the tracks were separated from the surfaces where vehicles travel, and thus collisions would be impossible. For example, the system level EIS in 1993 specified that the rapid rail that set the design parameters for what emerged as Link Light Rail was to be completely grade-separated.

However, the opportunity for such collisions was reintroduced as the design evolved. Now, before the resulting design decisions are accepted for Federal funding, I recommend that the resulting design decisions be analyzed for the degree to which this collision hazard manifests, and then translated into risks which are resolved, accepted, or tracked, just like the draft Handbook states.

As I look at the Project Development Safety and Security Activities in Figure 3 of the draft guidelines, it seems to me that what needs to be done about the collision hazard I have identified lies somewhere within this list of tasks extracted from that Figure (I have edited out "vulnerability" and "security" since intentional harm is not my concern in this message):

- Identify Safety Certifiable Elements & Items
- Perform Preliminary Hazard Analysis
- Prepare Safety Design Criteria
- Develop Design Criteria Conformance Checklists
- Perform Safety Design Reviews
- Perform Additional Hazard Analyses (as applicable)
- Implement Hazard Resolution and Tracking

These are all tasks in the Preliminary Engineering and Final Design stage of project development. FTA as of August 21 has authorized Link Light Rail for Final Design.

Let me jump to the last item, hazard resolution and tracking. It seems to me that one requirement of safety certification for Link Light Rail is to resolve the hazard of fatal collision at all points in the Link Light Rail Alignment Design and Operations Plan to an expectation of fewer than one fatality per million operating hours. I obtained this criterion from the FTA Hazard Analysis Guidelines referenced on page 28 of the draft manual.

This gets the Hazard Risk Index from the unacceptable condition of IB or IC to the undesirable (but conditionally acceptable by management decision) condition of ID

Then the FTA Hazard Analysis Guidelines say what to do next. I will quote extensively:

QUOTE
Hazard Analysis and Corrective Action

Corrective action for the elimination or control of unacceptable and undesirable hazards will include the following order of precedence:

1. Design for Minimum Risk. Design, redesign or retrofit to eliminate (i.e., design out) the hazards through design selection. If an identified hazard cannot be eliminated, reduce the severity and/or probability of occurrence to an acceptable level. This may be accomplished, for example, through the use of fail-safe devices and principles in design, the incorporation of high-reliability systems and components and use of redundancy in hardware and software design.

2. Safety Device. Hazards that cannot be eliminated or controlled through design selection will be controlled to an acceptable level through the use of fixed, automatic or other protective safety design features or devices. Examples of safety devices include interlock switches, protective enclosures and safety pins. Care must be taken to ascertain that the operation of the safety device reduces the loss or risk and does not introduce an additional hazard. Safety devices will also permit the system to continue to operate in a limited manner. Provisions will be made for periodic functional checks of safety devices.

3. Warning Devices. When neither design nor safety devices can effectively eliminate or control an identified hazard, devices will be used to detect the condition and to generate an adequate warning signal to correct the hazard or provide for personnel remedial action. Warning signals and their application will be designed to minimize the probability of incorrect personnel reaction to the signals and will be standardized within like types of systems.

4. Procedures and Training. Where it is not possible to eliminate or adequately control a hazard through design selection or use of safety and warning devices, procedures and training will be used to control the hazard. Special equipment operating procedures can be implemented to reduce the probability of a hazardous event and a training program can be conducted. The level of training, required will be based on the complexity of the task and minimum trainee qualifications contained in training requirements specified for the subject system element and element subsystem. Procedures may include the use of personal protective equipment. Precautionary notations in manuals will be standardized. Safety critical tasks, duties and activities related to the system element/subsystem will require certification of personnel proficiency. However, without specific written approval, no warning, caution or other form of written advisory will be used as the only risk reduction method for Category I and II hazards.

Hazards identified as having an unacceptable and undesirable risk will be analyzed using logic network analyses (such as fault tree) to determine effectiveness of corrective action. Unacceptable and undesirable risk will be reduced to an acceptable level before design acceptance, or a decision must be made to dispose of the system.
UNQUOTE

It appears to me that the remainder of the draft guidelines is about making sure that the corrective actions identified as necessary to make an unacceptable risk acceptable are actually implemented. That would be important too, but my main concern at this early stage of certification is the identification of the right action so that the design of Link Light Rail can be certified. So I turn away from the Handbook at this point and conclude.

My latest revised calculations indicate that to achieve certification per the FTA guidelines (one or fewer fatalities in one million operating hours for a certifiable element, assuming track sharing with road vehicles is a certifiable design element), the Link Initial Segment would have to be shown to have an expected fatality rate from collisions of trains with vehicles of one death or less in the first 20 years of operation (!) with the operating schedule shown in Appendix C of the February 2002 Environmental Assessment for the Link Initial Segment.

Here is my concern if the design is not so certified -- that the six minute planned peak headways for the trains will not be possible because the light rail system design is not safe with this many trains moving at the required speed. However, the planned peak hour headways and associated speeds are the basis for the ridership forecasts that support the cost-effectiveness claims of this multi-billion dollar investment. If these headways are not possible, the entire New Starts justification for Federal funding support fails.

To avoid a failure to achieve New Starts funding, I predict that Sound Transit and FTA will order various corrective actions on any safety failings that are revealed in the system in order to achieve safety certification of the design at required train speeds and headways. It concerns me that this approach may be insufficient and misguided if the initial design is sufficiently flawed in its approach to “minimum risk” as described in the hazard guidelines quoted above. Am I missing something in this statement of concern?

I have communicated with you earlier my recommendation for a completely independent review to be conducted on the safety of the Central Link design, focused on the specific hazard of collisions with road vehicles along the alignment, especially in the downtown bus tunnel but also along the street running segment in the Rainier Valley. While I have limited the scope of this communication to collisions with vehicles, my colleagues have reminded me that a similar approach would be justified for the hazards of the Link system to pedestrians.

The draft Certification handbook you sent with its reference to the Hazard Analysis Guidelines serves to reinforce my belief that my recommendation should be ordered by FTA.

In conclusion, I hope you understand that my energy in forcing FTA attention to this issue is matched or even overmatched by the energy of Sound Transit Board members and employees who want to begin construction of this project as designed with as little additional debate and review as possible. I believe that absent USDOT intervention, there is no possibility that the fundamental at grade and mixed-mode design features are subject to modification. After all, FTA has issued a record of decision, despite Seattle citizens raising safety concerns in the Environmental Assessment comment period. I estimate that Sound Transit's safety approach absent further intervention will be to make a potentially inadequate, unsafe light rail system design as safe as possible through the addition of Safety Devices, Warning Devices, and Procedures and Training as described above, rather than through Design for Minimum Risk. I am challenging Sound Transit and FTA to prove to the public that Design for Minimum Risk is not necessary in the case of Seattle Light Rail.

Thank you for your service, and I look forward to what happens next.

Very respectfully,

John S. Niles

John S. Niles
Founder, Public Interest Transportation Forum
Volunteer Technical Director, CETA
(Coalition for Effective Transportation Alternatives)
President, Global Telematics
Research Associate, Mineta Transportation Institute

CC: Ted Uyeno, FTA Region 10
CC: Hamid Qaasim, Sound Transit
CC: Greg Hull, American Public Transportation Association