INCREASED TUNNEL AVAILABILITY THROUGH MODEL BASED DECISION SUPPORT

D.C. Oerlemans, E.W. Worm,
Covalent Infra Technology Solutions, Amersfoort, The Netherlands
diderick.oerlemans@covalent.nl

ABSTRACT
Tunnel safety depends on several systems operating as designed at the required moment. Tunnel Technical Installations (TTI) may function as expected in new tunnels but their functionality will decrease with aging. Maintenance processes help keep the tunnel in good condition, but it is hard to determine the actual safety level. For example, it is difficult to determine if a TTI defect can wait a few days for repair or should be repaired immediately with the tunnel closed. This is where model-based decision support comes in. This article describes the Tunnel Safety Indicator, a model in use in the tunnels of the Dutch cargo train link between Rotterdam seaport and the German border which is now being built into all the other Dutch railway tunnels. Application of this model in road tunnels has just started with a first pilot project.

The top level of the model consists of the four Lines of Defense, i.e. prevention, mitigation, evacuation and rescue. These Lines of Defense must be available at a certain minimum level in order to consider a tunnel safe and available for traffic. Within the tunnel complex, these Lines are maintained by Safety Functions (2nd level). In the Dutch situation there are approximately 45 Safety Functions for a two-tube tunnel. These Safety Functions are fulfilled by the tunnel’s technical systems (3rd level) and ultimately by the technical components (4th level) in a tunnel (Figure 1). This model enables the definition of business rules regarding the deterioration of installations and the ultimate effect of deterioration on the more abstractly defined level of tunnel safety. Using the output from the technical installations (SCADA) combined with the results of regular inspections, the Tunnel Safety Indicator provides an accurate and objective indicator of the tunnel safety required by or agreed upon with the authorities.

Keywords: tunnel safety, decision support system, lines of defense, functional safety/availability

1. INTRODUCTION
During the last few decades, road and railway tunnel disasters have led to an increased interest in tunnel safety. This interest not only focuses on the design and building stages of new tunnels but also on the exploitation of existing ones. Many existing tunnels have the following characteristics:

- increased complexity and a large number of installations and software
- an increased focus on availability (the traffic must not stop)
- deterioration over time that can be quite different per tunnel technical installation
- lack of an objective method to determine when and what systems need maintenance, renovation or replacement
- difficulty in determining whether and how long a safety measure can be compensated by other safety measures
- an operating system with technical troubles from time to time
- lack of an objective method to determine when an operating system has become so weak that safe exploitation is no longer justifiable.

The tunnel operator continuously has to make choices between availability, necessary maintenance and temporary compensatory or mitigating measures. As a consequence, a special tool has been developed for the five cargo railway tunnels in the Rotterdam-German border link (the so-called Betuweroute) in the Netherlands, in order to help the operator in this permanent weighing and balancing between availability and safety; this tool is called the Tunnel Safety Indicator. The tool was tested, tuned and evaluated for a year and has been in official use since 2009. Experiences with the Tunnel Safety Indicator have been so positive that it will be built into all Dutch railway tunnels. In addition, a pilot project is underway to apply the Tunnel Safety Indicator in road tunnels.

7th International Conference ‘Tunnel Safety and Ventilation’ 2014, Graz
2. ANALYSIS

In general, tunnel safety is assessed by looking at the availability of safety functions (measures or provisions for safety) within the four Lines of Defense (LODs), i.e. prevention, mitigation, evacuation and rescue [1]. These LODs must be at a certain minimum level for a tunnel to be considered safe and available for traffic, and they are maintained by the Safety Functions within the tunnel complex. Safety Functions are fulfilled by the tunnel technical systems and ultimately by the technical components in a tunnel. A ventilator (component), for example, is part of the ventilation (system) that takes care of clean and fresh air (function) needed in three different lines of defense, namely safe passage (prevention), safe escape (evacuation) and safe help (rescue).

In the Tunnel Safety Indicator, installation components have been combined into systems offering functional safety in order to maintain the LODs necessary for a safe tunnel. This model makes it possible to define business rules regarding the deterioration of installations and the ultimate effect of this technical deterioration on the more abstractly defined level of tunnel safety that is required by or agreed upon with the authorities. Using the output from the technical installation components through the Supervisory Control and Data Acquisition (SCADA) system in combination with the results of regular inspections, this model provides an accurate and objective indicator of tunnel safety.

This model and the related systems have been developed with three aims in mind:

1. To arrive at an accepted indicator of the agreed safety level of a tunnel by which internal and external parties can be informed transparently and objectively.
2. To gain insight into the condition of a Line of Defense, by providing detailed information about the status of components throughout the systems and functions to the final status of the LOD; this information should be both objective and traceable.
3. To prioritize maintenance based on the expected and actual deterioration of tunnel safety.

3. THE MODEL

![Figure 1: Model to determine safe tunnel availability](image1)

![Figure 2: Model layers and their interrelationships](image2)

The first objective was to create a layered model that would make a link between an abstract definition of safety and concrete technical data. Using the TSI-SRT [1] Lines of Defense (prevention, mitigation, evacuation and rescue) as a starting point for the abstract definition of safety, the Safety Functions have been defined such that they support the Lines of Defense. It appears that these Safety Functions largely comprise the same functions for different road and railway tunnel projects. These Safety Functions serve as functional requirements, which is why they were used to compile a definition of
Logical Systems fulfilling these requirements. Lastly, these Systems were broken down into Components, which are the smallest technical units that produce status data. This approach has led to a four-layer model: Lines of Defense – Safety Functions – Logical Systems – Components. The model resembles a graph fanning out from the LODs to the Components. Between every layer there are business rules, which define how the status of a particular level influences the status of the level above it. This chain of reasoning propagates from the concrete Component layer up to the more abstract Lines of Defense and ultimately to the Tube.

3.1. Component layer behavior and business rules

The component layer contains the definition of all physical components in the Tunnel Technical Installation. The following business rules apply:

- A Component is always either Available (A) or Not Available (NA).
- The SCADA system indicates the status of Components.
- A Component always belongs to only one System, and each System contains one or more Components (one-to-many relationship).
- Each Component is given a weight, thus indicating its relative importance to the System to which it belongs.
- A Component may have a specific position (ordering) in a tunnel tube.
- The status of a Component is either reported by the SCADA system or manually determined as the result of an inspection.

**Example:**
In a sprinkler system, a section valve and main valve for two adjacent sections are examples of components belonging to the same system. The main valve has twice the weight of the section valve, as its importance to the system is similar to two adjacent section valves. Section valves are numbered sequentially in the tube, which indicates their ordered position.

3.2. System layer behavior and business rules

The system layer models the physical systems as closely as possible. Systems are collections of components. The availability of these components determines the total system availability. The following business rules apply:

- A System consists of one or more Components
- A System has a maximum availability, which is determined by adding up the weights of all the Components it contains:
  \[ S_{\text{max}} = \sum C \]  
  (1)
- A System has an actual availability value, which is determined by adding up the weights of all the components with the status Available:
  \[ S_{\text{actual}} = \sum C_{\text{Avail}} \]  
  (2)
- Special rules for degradation may apply, in which case the system degrades further than the sum of the Non-Available components. An extra value R is subtracted from the system availability if such rules apply, acting as a penalty.
- Actual availability is never less than 0.
- A system can contribute to multiple Functions. The weight for each Function will be set such that it indicates the contribution of the specific system to that function.

**Example (simplified):**
A sprinkler system consists of 100 section valves with a weight of 1, so \( S_{\text{max}} = 100 \).

There is a special Rule that says that no two consecutive section valves may have state NA. If this rule is breached, then an additional deduction of \( R = 5 \) applies. In the following numerical example two adjacent section valves have status NA: \( S_{\text{actual}} = \sum C_A - R \Rightarrow 98 - 5 = 93 \). Therefore the system has a current availability of 93 out of 100 (or 93%).
3.3. Function layer behavior and business rules

Safety Functions define abstract behavior of the Tunnel which can be realized by one or more systems, which may or may not be redundant. It is particularly important to make a distinction between Safety Functions, which define the functional behavior of an abstract system such as ‘ventilation’, and system functions, which describe the technical behavior of an installation such as a ventilator. The following business rules apply:

- A Function has either the state Available (A) or Not Available (NA).
- A Function is realized by one or more Systems (many-to-one relationship).
- Within a Function, systems may overlap, for example handrail, lighting and exit signs overlap within the Safety Function ‘offering an escape route’.
- For different combinations of Systems, the thresholds can be set per individual system. By using simple proposition logic (and/or combinations of Systems), the status of the Function can be determined.
- A Function can be assigned to one or more Lines of Defense (one-to-many relation).
- For every Function-LOD assignment, a Safety Class will be set, indicating the contribution (the weight) of the specific function to the specific LOD.

Example:
To realize the Function ‘cooling tunnel downwind’, the sprinkler system must be available at a 95% minimum (see the previous example). The longitudinal ventilation system, which has a maximum availability of 30 based on the added weight of its components (ventilators), has a minimum limit of 80% when running on mains power. If running on emergency power, the minimum limit on availability is adjusted downward to 40%. Maximum availability for mains and emergency power is 1 (assumptions are made for this example):

<table>
<thead>
<tr>
<th>Overlap</th>
<th>System</th>
<th>Symbol for actual value</th>
<th>Smax</th>
<th>Slimit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sprinkler system</td>
<td>Ssp</td>
<td>100</td>
<td>95 (95%)</td>
</tr>
<tr>
<td>1</td>
<td>longitudinal ventilation</td>
<td>Slv</td>
<td>30</td>
<td>24 (80%)</td>
</tr>
<tr>
<td></td>
<td>mains power</td>
<td>Smains</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>longitudinal ventilation</td>
<td>Slv</td>
<td>30</td>
<td>12 (40%)</td>
</tr>
<tr>
<td></td>
<td>emergency power</td>
<td>Semer</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

The availability (True: 1 or False:0) for this Safety Function can be presented in the following formula:

\[
F = S_{sp} \geq 95 \land \left( S_{lv} \geq 24 \land S_{mains} \geq 1 \right) \lor \left( S_{lv} \geq 12 \land S_{emer} \geq 1 \right)
\]  

This means the Function is either Available, value 1, or Not Available, value 0.

3.4. Line of Defense layer behavior and business rules

Lines of Defense are maintained by Safety Functions. When one or more function is lost, the LODs deteriorate until they are breached. This mechanism is modeled by assigning Safety Class thresholds to the different states an LOD can have. The following business rules apply:

- For every Function-LOD assignment, a Safety Class will be set, indicating the contribution (the weight) of the function to the LOD.
- An LOD has the status Not Degraded, Degraded, Severely Degraded or Breached.
- An LOD is maintained by one or more Safety Functions (many-to-one relation).
- The LOD state is determined by calculating the Safety Classes (the total weight) of its underlying Safety Functions with the state Not Available, and evaluating that sum against a predefined threshold (for example: the threshold for Degraded is 1, the threshold for Breached is 6).
Example:
In the table above all combinations of Safety Classes (3) and relevant number of Lost (= unavailable) Safety Functions are shown together with the resulting sum of degradation. The threshold for the status Degraded is set at 1. The next threshold, for the status Severely Degraded, is set at 3 and the final threshold for the status Breached is set at 6. So if two Functions with Safety Class 2 are unavailable, the total sum of degradation is 2x2 = 4. Because 4 > 3 (the threshold), the LOD in question is Severely Degraded. There is no need to show more than 3 unavailable functions, as that will always lead to a minimum sum of degradation of 4.

3.5. Tunnel Tube layer behavior and business rules

On the highest level in the model, safety per tunnel tube is determined based on the state of its four Lines of Defense. A Tube has an operating status, which can be Operation, Maintenance or Emergency. The safety status is assessed only during the state Operation; in the other two cases the safety status is Undetermined.

• A Tube can have the state Green (safe), Yellow (degraded safety) or Red (unsafe).
• The safety of a tube is assessed by means of four Lines of Defense: prevention, mitigation, evacuation and rescue.
• The status Severely Degraded in one LOD causes a status transition to Yellow.
• A tube can only have a Yellow status for a certain amount of time. If this time elapses without any transition back to Green, a status transition to Red will automatically occur.
• If the status of one or more LODs is Severely Degraded or Breached, this causes a transition to Red. If this transition occurs from the Yellow to Red status, the maximum time for Yellow continues to count down in the background.
• If during the status Red, LOD conditions for the status Yellow are met, transition to Yellow takes place. The remaining time for the status Yellow is not reset, but this time continues to count down.

4. TUNNEL SAFETY INDICATOR

The MUST™ suite of applications was used to create the Tunnel Safety Indicator. At present, this Tunnel Safety Indicator (TSI) tool is operational in the five cargo railway tunnels in the Rotterdam-German border link (the Betuweroute), and in the near future it will be implemented in all Dutch railway tunnels and several road tunnels. The tool has been certified by an accredited third party and is tamper-proof.

4.1. System architecture

The model described above can be configured for a specific tunnel using the MUST™ Engineering application. Simulations can be run using different configurations based on actual (logged) or simulated data from the SCADA systems. Simulation can also be used to test and certify (FAT) a new configuration before it goes into production.
Operational data is either retrieved by periodically reading out the SCADA data log, or real time through an OPC UA Alarm & Event server. The Tunnel Safety Indicator is implemented as a web application with regular browsers for clients. There is also an MMI component that acts as an OPC Client. This component can be embedded in existing SCADA MMI.

4.2. System functions

The main functions provided by the TSI system are the Safety Indicator, one traffic light per tube, and the underlying Safety Status overview, a tree-like overview of the model with detailed status information. These main functions are available through a standard web browser or SCADA MMI component.

Figure 4 shows the TSI for a tunnel with 2 tubes. Tube 1 is safe and has been in that state for more than 120 days, whereas Tube 2 has degraded safety. If this status is not resolved in less than 3 days, the tube will be declared unsafe, and this will result in the closing off of the tube.

The TSI makes it possible to drill down and obtain detailed information regarding the safety of the tunnel:
Figure 5 shows a drill down into the model underlying the Tunnel Safety Indicator. The drill down has a tree-like format and shows exactly how failed components affect the safety of the tunnel. Figure 5 visualizes the examples from Chapter 2. Three ventilators are Not Available. As a result, the System ‘Ventilation East’ loses 3/5 of its Availability and drops to 40%, which is below the threshold of 50% set by Function ‘Smoke-free flight path’. This means the Function is lost. Apparently this function has a high Safety Class, because the loss of this single function is enough to breach the LOD Evacuation.

Secondary Tunnel Safety Indicator functions such as prioritized maintenance advice, temporary suppression of false events, entering inspection results and reporting, are supported through the TSI web portal and accessed through a standard web browser.

5. THE BENEFITS

The Tunnel Safety Indicator helps the tunnel operator deal with all the information on the safety status of the tunnel. The enormous load of the rail and road network has led to a situation in which every disturbance causes delays, leading to negative economic consequences. With this tool the operator gains more insight into the continuous balancing between safety, maintenance and availability. The model:

- gives up-to-date information about the tunnel condition and the technical installations
- provides this information in terms of safety and availability
- continuously monitors the safety risks due to diminishing conditions and growing disturbances
- is based on decision rules that have been built in previously, without the pressure of an actual event and in cooperation with all the stakeholders that have power of decision
- continuously monitors the preset standards
- escalates when system warnings are ignored by operators or maintenance parties;
- gives insight into historical data
- provides operating staff with better judgment and less stress when they are confronted with failing components in the tunnel
- increases tunnel availability by avoiding unnecessary closure in case of events. Factual data show a possible 20% increase in tunnel availability.

In sum, the Tunnel Safety Indicator is an excellent tool that provides the tunnel operator with indispensable automatic support in his duties, decisions and responsibilities.
6. REFERENCES
