COMPLEXITY - SECURITY - RESPONSIBILITY IN THE TUNNEL OPERATION

Urs Grässlin
Lombardi AG, Consulting Engineers, CH-6648 Minusio

ABSTRACT

About 30 years ago, several single tube road tunnels with double traffic direction were build and set into operation in the alpine region (Arlberg-, Fréjus-, Gotthard-tunnel). The continuous renewal of the operation and security installations during normal tunnel operation is an exceptional challenge for the owners, the operators and at the system integrators. The first two decades were marked by a constant increasing traffic volume and a relatively simple and long-live control and instrumentation technology. In the last 10 years, with the fast development and trends in computer technology, the request of centralized control and supervision of entire route sections by single operators, set new challenges in the control and communication system and in the responsibility for the operating companies.

Keyword: Process control system, Security, Responsibility

1. INTRODUCTION

On July the 12th 1980 the Fréjus road tunnel was opened, followed by the Gotthard road tunnel on September the 5th 1980, being at that time the longest single tube tunnel with double way traffic of the world. 15 years before, in 1965, the Montblanc tunnel and in 1978 the Arlberg tunnel were opened.

2010 it is the 30th anniversary of the Fréjus and Gotthard tunnels, which on the one hand guaranteed a winter connection through the Alps between France and Italy and between the south (Ticino) and north of Switzerland, and on the other hand produced a crucial impulse for the development of the European transit traffic on the roads. This anniversary allows us to look back at the development in the operation and security equipment over the last 30 years and to compare it with today's standards. What should be done or should have been done differently?

Furthermore the tunnels have now reached an age where one must seriously think about its future development and utilization. The starting points can only be the current situation, the experiences achieved as well as the analysis of the expectances and future developments.

2. SERVICES AND EQUIPMENTS

We can subdivide the last 30 years into different periods, in which we can determine in principle various interrelationships between technology, industry, politics and different increases of the traffic volumes.

2.1 The first 20 years

Manufacturing the tunnel plant with all its operation and safety equipments (BSA) was a big challenge for the industry at that time, since such a large and extensive tunnel was never built before. In fact, due to a lack of experience, in the first three to five years of operation, special efforts were required to optimize the facilities and eliminate "youth" problems, as well to substitute operating elements which did not work as expected.

During these years, most of the experiences concerning electrical, information technology and functional aspects were gained. The operators in the control rooms knew and controlled the tunnel with their own experience, which they mainly acquired by their self's. At that time,

everybody knew exactly what were the scope and effect in the tunnel when pushing a button on the control desk. In contrast, all case scenarios, for example fire or traffic jam, from the beginning were released fully-automatically. In a second stage, the operators could override the automatic reactions with manually interventions if necessary.
During the first 20 years of operation, there are no relevant developments and changes regarding the equipment as well as the operation rules of the tunnel. The operational and security equipments were maintained and replaced when required. Special attention was paid to the energy-optimized operation of the ventilation system. The traffic volume during these 20 years increased by a factor of 2.4, reaching 6’824’702 vehicles pro year, and the heavy traffic by a factor of 4.3, which corresponds to an increase of the heavy traffic from 11% to 20%.

The rapid development in the information technology during the nineties allowed to replace the old mainframe computer from 1980 by separate ventilation computer as well as a new mainframe and a first SCADA system, above the existing process control system with communication master and remote installations. The push buttons control and the underlying relay-control were replaced by a graphical user interface: the mouse found its way into the control room.
During this first migration stage, the challenges of building and activating a new SCADA system which has to temporarily operate with the existing control system, without any limitations for traffic flow and tunnel security were encountered for the first time. Thanks to the process control system master and remote installations, the relay-control as well as the electrical jumper boards within the tunnel, the communication interfaces between two IT generations could be accomplished. The works were completed in 1995.

For the new mainframe- and ventilation computer system, machines of the Digital Company with a 64 bit VMS OS system were selected and installed. This technically based selection was absorbed by the booming PC-industry. The PC-tendency company Compaq bought Digital and decided to cease their production. Already during the setup of the new systems, it was clear that they had to be replaced in a short time again.

2.2 Windows in advance

The ongoing booming development of the informatics industry, especially in the domain of the communication technology and the graphical user interface, such as Windows, misled to the euphoria that everything is manageable with Windows and Ethernet.
Complex hierarchically structured look & feel architectures, server farms, redundancies, interface management, integration concept for old and new equipments of different BSA systems were developed. It seems possible to be informed everywhere about everything right down to the last detail and to control and manage as desired from every workplace. The rapid development of processor performance, as well as data storage with cost reduction tendency, has accelerated the transition towards Windows based PC solutions.

The dramatic tunnel fire on October, 24th, 2001 in the Gotthard road tunnel, as well as the fires in the Montblanc tunnel and the Tauern tunnel, presented an essential cut. Substantial means were provided in order to ensure safety in tunnels, to avoid such tragedies in the future. Ongoing BSA renewal projects were adjusted, new projects started, priorities changed and generally accelerated. The control- and routing concepts in developing were adopted in a hurry and started to be realized. Windows PCs find their way into the tunnel.

2.3 Renovation of BSA equipments

It follows a 10 years long period of conversion and renovation of the different BSA equipments, especially the replacement of the process control systems, master and remote installations and the relay-controls. During this second stage of migration, the main challenge was once more to build and activate the new equipments and communication structures, without reducing neither the traffic flow nor the operating safety in the tunnel.

This long time of conversion and renovation was conditioned by the required stepwise proceeding in order to be able to renew the equipments gradually and to keep the system stable. Beside, not all expectations and promises related to the new technologies were completely fulfilled. Several concepts were technically not convertible as required. What looked easy, became finally more complex and especially much more expensive and economically hardly reasonable.

The command and control concepts had to be modified, which produced negative effects on the realization of the projects. The realization schedule became longer and consequently more expensive. Through mutual dependence, a project influenced the others. Transition solutions were demanded and realized, which again had consequences on the costs. Certain installations were taken in standalone operation mode, while others could not be fully integrated as desired.

The communication technology didn't also stand still. The KOM-Net realized in the Gotthard tunnel based on ATM-technology was not furthermore developed by the industry, but replaced by the relatively simpler and more advantageous Gigabit technology. The ultimate consequence was to change the backbone communication from ATM to Gigabit technology. Fortunately, no direct effects were accused by the single BSA installations, but nevertheless one had to replace the not yet fully amortized installations which were still working properly.

Another turning point was the re-engine from the intended data point integration with a second security level browser access between the different equipments to a full browser control concept. Only few and, for security reasons, really important data points are transmitted to the overall SCADA system. All different single systems are now managed from their front end calculators.

This had an important impact on all single systems, because they are nevermore independent but they had to be adapted to given management rules and graphic style guides. Consequences are that all the single and different SCADA systems from every equipment had to be adapted whenever possible with new complementary common functions generating extra costs.

These ten years were a big challenge for the operators in the control room, to survey the tunnel with continuous works and changes of the function conditions of the operation and security equipments in the tunnel. Instead of the few planned stations, more video monitors were necessary in order to cover the transition phases, used for the temporary control of the evolving installations.

Another unpredictable effect has influenced this long working and chancing time: the systems became cheaper, but the life cycle, availability and product support dramatically decreased. In extreme cases, the live cycles for some single components are shorter than the installation time. For example, data servers had to be replaced before the project end.

2.4 Once - today

The Gotthard road tunnel always had a layout similar to the modern road tunnels. Changes concerned modifications and installations aimed to increase the security level during the last 10 years. The most significant are:

- Ventilation system Realisation of a redundant exhaust ventilation system in all ventilation sectors.
  Installation of 178 fire dampers for concentrated exhausts extraction.
  Redundant ventilation system for the security tunnel.
- Fire detection The single heat detectors are replaced with a fibre optic linear detector.
  Installation of 178 smoke detectors next to every fire damper.
  Discrimination between a still and a moving smoke source.
- Illumination Two continuous light strips.
  Optical guide installation.
  Self rescue with flash lights.
- Traffic management Drop counter for dosing heavy traffic.

Completely different, after two migrations steps, have now become the SCADA systems of the single equipments and the overall process control system. At tunnel opening, the equipments were uniform and coordinated, today we have a multitude of different operating and communication systems for every single operation and security system under a common overall SCADA process control system.

1980:

- 2 control rooms
- 2 redundant mainframe VAX PDP 11
- 2 redundant traffic control system (Siemens)
- 1 process control system with communication master and remote installations

2010

- 1 decentralized control room for traffic flow control
- 1 overall SCADA process control system and KOM-Net
- 2 (future) unoccupied control rooms
- 6 operation and security equipments with their own SCADA system , frontend and sector calculators and field equipments
- 6 dedicated networking systems for the different operating and security systems

3. IT DEPENDENCE

The development from self dedicated closed system to open system observing market orientation and contracting politics had considerably influenced the control systems of the operation and security systems and the process control system in the tunnel. If this opening in all directions gives us more secure tunnels must be investigated in detail for confirmation. Doubts are appropriate. The following points can be listed:

- Dependence from the developers of operating systems, e.g. in the last 10 years we had 5 different Windows OS.
- Dependence from the different builders and developers.

- High specialized systems like Windows servers.
- Virus risk in the network systems and necessity to maintain an actualized antivirus protection.
- Central access control, users and priorities management.
- Protections against external IT attacks.
- Continuous increasing in complexity and redundancy since applications in Windows machines and systems often caused crashes and still-stands.
- The complexity of the systems produces a big test effort and difficulties of operation prediction for all possible different configurations.
- The fault diagnosis is aggravated by the system dependencies and redundancies.
- The actual contracting policy produces to have a multitude of different SCADA systems in the single operation and security system.
- The SCADA systems are modified for the specific standard of the overall SCADA process control system. Updates become difficult and create extra costs.
- Updating a system has objective limits. Once a critical point of complexity is reached, rebuilding a system is an easier way.
- Extreme challenge for the owner and operators to acquire and preserve the knowledge over all the operation and security systems, cultivate and improve what is extremely important for new operators.
- The project planning for a new operation and security system must be made in a way to allow more than one migration cycle.
- Process control system with real time and security requirements should be realized generally with PLC technology, with a much longer lifetime cycle.

As example to the points mentioned above, we could choose the complete substitution of a control system of year 2002, composed by 26 PLC, which resulted more economic than a software update of the existing system.

These problems are not single cases linked to the Gotthard road tunnel. The Mont Blanc tunnel company has published the tendering procedure to substitute the overall SCADA system and process control system running from year 2002. At that time, the only stable and improved operating system was Windows NT 4, today no more supported, and IT specialists with this knowledge cannot be found anymore.

Recently a press report was published in Switzerland, describing the necessity to simplify and uniform specific parts of the control system of the recent Lötschberg railway tunnel, which produced a large public discussion. All this underlines how dependent from the IT development and production a tunnel owner is our days .

4. RESPONSIBILITY

The intrinsic security in a road tunnel depends from the reliability of all single system and subsystem that form the overall tunnel machinery. Failure or malfunction of a single component shouldn’t compromise the reaction of the overall system or should remain marginally limited. How to realise this challenge in complex tunnel machinery, composed by different systems build from different IT generations with different functional rules?

Clear definite operation rules and security concepts are not always given. Minimal functional conditions and security dossiers, now demanded by the EU-Norm, have often to be created. For this reason in the contracting prescriptions for the system builders there are no particular security requirements ore responsibilities mentioned.

All tests with all the operational and security systems in a tunnel with serial and parallel reflexes are possible only with a closed tunnel and require complex analysis.

The trend with a fewer number of traffic control centres and to supervise and manage tunnels at distance means to delegate responsibility to the equipments and systems. Where is the limit between automation and manual interventions?

The exact definition of the responsibility for the maintenance, during security tests, instruction and training in real conditions of exercise are essential. Once the overall responsibility is clearly defined, it is possible to define part responsibilities and special responsibility profiles and competences, respectively to delegate. Looking generally to the mentioned problematic of the IT technology, this definition is of absolute priority, to give to all involved people the necessary security in the everyday business.

5. TENDENCIES AND PERSPECTIVE

We can say that with all the achievements done up to now and through the general experience exchange, the different functional states of the road tunnel, the possible expected events and course of events are predictable with a certain accuracy. With this knowledge, operational and security systems are finally designed and programmed.

Today the weak point is nevermore the tunnel as overall system but the control system itself, the communication between components and the manual management. The trend to centralize the tunnel process control system in few traffic control centres underline once more the significance of an efficient and simple architecture in the control systems, that are coherently designed and realised with clear and definite interfaces and localised intelligence and, at least in the ideal case, realised from one single system builder. This creates also a dependency, but gives minor problems compared to having a multitude of different contractors and system builders.

The apparent trend of the tunnel manager requiring process control systems following SIL 2 prescriptions and certified software is not necessarily a good way. The main dependencies still exist, with more costs and grater realization times.

Another possibility in the future could be to adopt the virtualization concepts already in use by complex server infrastructures; this technology could reduce platform and OS dependency.