Quality in Civil Engineering for Tunnel Safety

Authors: Marie Fialova, Petr Svoboda, marie.fialova@fsv.cvut.cz, psvoboda@spel.cz

***Abstract* — Safety in tunnels are greatly enhanced by correct design and implementation of control system. The basic pre-requisites for a safe and reliable control system are briefly discussed. The basis of design of network topology, redundancy of PLC, redundancy of networks, interlinking with technology, centralized and decentralized control, and HMI interface is outlined.**

***Index Terms* — civil engineering, construction quality, tunnel control system, PLC, SCADA, industrial communications, tunnel safety, Human Machine Interface, SIL2, MTBF, Electronic Systems Reliability**

INTRODUCTION

Quality of constructions in civil engineering is closely dependent on a quality of underlying project, on following of normative and technological procedures during construction, and most importantly on quality of construction works itself. Our tunnels will be safe only if the project and construction quality is adequate. Nowadays, we are able to quite reliably measure the quality of construction works with the significant help of laboratory tests and advance mathematics. Therefore, we can securely state whether the tunnel is safe from the point of civil engineering or not. One of the major factors, which is almost always missing in these considerations, is the tunnel instrumentation, which has a key importance in safety aside of factors discussed.

In tunnels, numerous accidents with fatal consequences are often caused by insufficient or even missing tunnel instrumentation, or an incorrect design or implementation of safety instruments.

A tunnel control system (TCS) is a key element assuring the correct function of the most of the installed technology in the tunnel. Correct design and implementation of a tunnel control system is a primary key in tunnel safety. Overall reliability of the TCS is determined by the overall concept of control system. More or less, by a following parts: network topology and its redundancy, redundancy of central PLC, redundancy of interconnection with controlled technology, connection to superior systems, human machine interface. Last but not least, overall reliability is then derived from the quality of control algorithms and software equipment.

During the selection of TCS, the Mean Time Between Failures (MTBF) for all main components should be provided by the manufacturer of the control system, preferably in the form of statistical measurements from real applications. Then, the calculation of the MTBF of the overall system should be quite straightforward. For control of complex technologies and traffic complexes is necessary to choose control system capable of high data output on industrial communication network, with possibility to write complex algorithms in a certified and easy transferable language (for example structured text according to IEC 61131-3) and with the overall capacity to interconnect high number of PLCs. All those parameters are a key factor for a fast reaction of the TCS on an ongoing event such as accident or fire.

INDUSTRIAL NETWORK

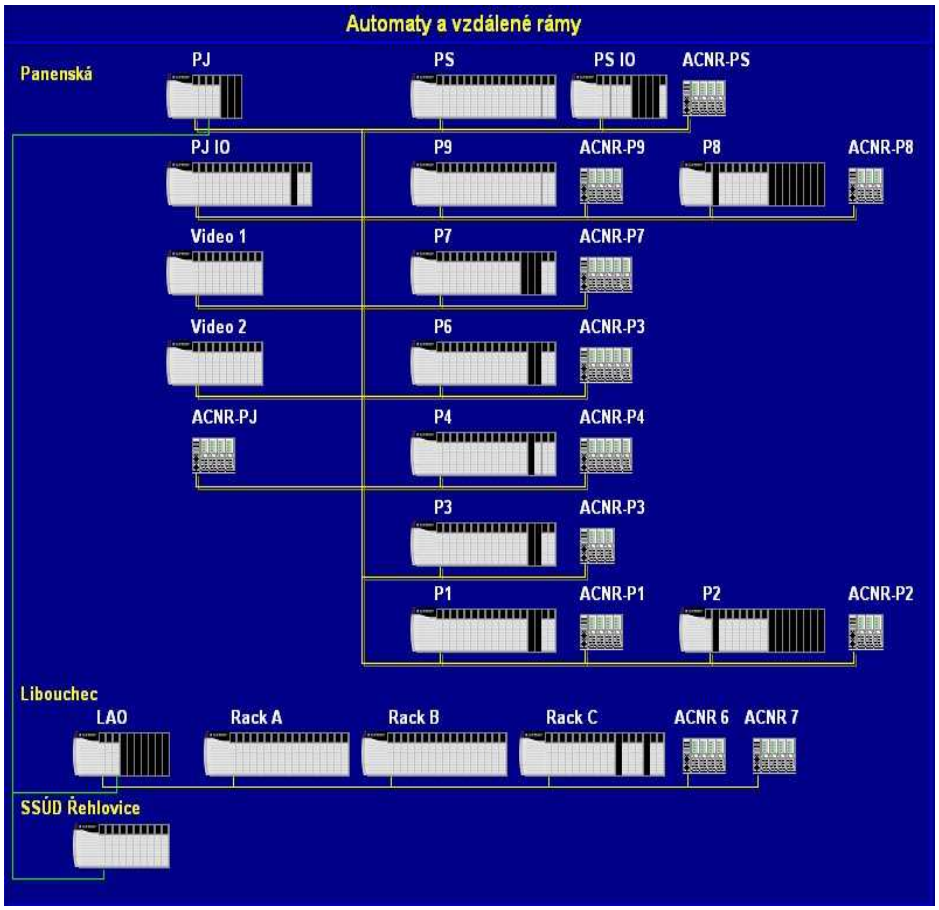
The primary function of the industrial network is the interconnection of all parts of the tunnel control system. The speed and reliability of the TCS can be only as good as the underlying network itself. Considering the amount and importance of the data transferred, the network have to be constructed with the adequate bandwidth, be reasonably fast, and have defined maximal time delay. Nevertheless, the network must be secured against non allowed access.

Physical medium: considering the maximum reliability and harsh environment in tunnels, the only reasonable medium for industrial network is a fiber optics. From the economical point of view, only one primary fiber optic network for all tunnel appliances can be constructed. However, the following conditions should be met:

- TCS communicates over fiber optics is separate from other technologies
- each node of TCS is using the redundant connection - two independent fiber optic cables should be used

Network Topology: Network topology is determined by the specific needs of each project. There are, however, two basic possibilities which are commonly used: star topology and ring topology - both in redundant version.[1]

[1]As a reference project, we can show the tunnel Panenská (2200m length, two tubes), where the network topology is a redundant star. In combination with the smart energy distribution plan, it is possible to achieve zero voltage level in any part of the tunnel without the loss of communication. This is a crucial for a safety of passengers during a fire hazard.



Tunnels Panenská and Libouchec: *technological network ControlNet interconnecting PLC for the technology control, simplified schema taken from HMI*

.Centralized vs. Decentralized Control

Decentralized control system is a conceptually young alternative. It is becoming widely used for large-scale projects in the field of artificial intelligence (see multi-agent systems). Furthermore, this concept can be applied to TCS implementation for tunnel control. In decentralized control, the controlled technology is segmented into a logical segments, which are then independently controlled by PLCs. Any of the PLC can know the basic state of the rest of PLCs, and therefore adequately interact with controlled technology

based on the current state of the tunnel. This type of system can dynamically adapt to failures of one or more of the PLCs and or to large topology changes.

Opposite in a concept, for the centralized control there is a one dedicated PLC which directly or through other PLCs control all of the processes. This is a classical concept of TCS. Great advantage of this settings is an considerably easier software implementation and clearly defined connections. On the other side, the failure of the central PLC results in a collapse of technology. Also, the bandwidth on a network is less optimal.

An ultimate solution should take the best of the both worlds. Thus, use a centralized PLC to communicate with PLCs which autonomously control technological parts. These PLCs accept commands from the central PLC which acts as a coordinator. In a case of failure of central PLC, the rest of the PLC continue to operate independently putting the tunnel into a safe state based on the last status it got from central PLC.

.PLC REDUNDANCY

For a central PLC it is desirable to achieve a functional state in any condition. For so, the redundancy of central PLC is advisable. Solution is to use two PLC interconnected by an optical link. The PLC which has actual control over technology is called primary PLC, a redundant partner s secondary PLC. Primary PLC should communicate with the secondary PLC all the time to ensure on-line transition of control in case of failure of primary PLC.

MTBF of PLC is very high, therefore the failure of primary PLC is mostly due to the power failure, communication failures, due to mechanical damage, or SW error. All of these aspects must be taken in account during a design of PLC redundancy to assure failure-prove concept.

.LINKAGE OF TCS AND TECHNOLOGIES

It is necessary to assure a trouble free operation of a tunnel even in a case of a minor breakup of link between TCS and controlled technology. Therefore, for the key technologies which directly involve safety of passengers, the redundant link of TCS and these technologies must exist.

Major part of linkage of PLC and technology is by a binary inputs and outputs. Usual concept is to use relays, where signals are transferred by voltage

level, or by a pulse. The controlled technologies are usually power distribution, lighting, regulation of ventilation, and others.

For the systems of measurement and regulation in tunnel (MAR), the classical analog inputs and outputs are a good solution of linkage. The usage of current loop is advisable to limit possible noise induction.

Combination of binary I/O with some sort of data communication (serial link, industrial Ethernet etc.) is necessary for the systems of fire prevention, electronic security systems, video-detection etc. Data link can transfer significantly more information than is possible by binary I/O. On the other side, the reliability of data link compared to binary I/O is lower due to a necessary SW implementation of communication protocol. For the SW of the data link it should hold true:

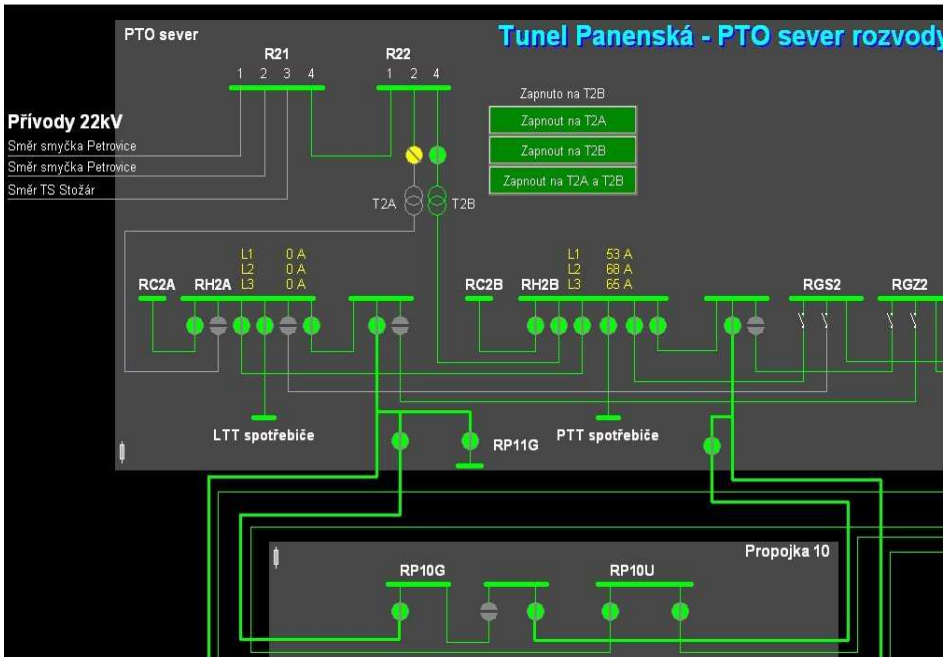
1. every data packet must have control of its data (standardly used is CRC)
2. communication protocol must be industrial, open with fully documented framework.
3. Many protocols are standardized (Modbus, Ethernet/IP etc.)
4. communication failure must be easily detectable (control packets)
5. system must be able to recover from a lost of communication after a failure

For the safety measures, it is improper to control technology by a components with low fidelity such as is a PC with operating system.

.Human Machine Interface (HMI) - SCADA

Visualization is a common tool to achieve a Human Machine Interface (HMI) for a SCADA system - the Tunnel Control System. In tunnel applications, visualization is main element, by which the operator can supervise and control the tunnel technologies. For the sake of simplicity of operation, all tunnel technologies should have unified visualization in one system. The control must be uniform regardless of a controlled technology. This way, we can insure fast and correct operator response in a critical situations. For complex systems the number of informations for the operator must be limited to give a operator overall situation rather then list of problems.

Visualization is a tool to interact between a operator and a TCS, it is not desired to perform any control algorithm by itself. The control algorithms must reside inside PLC, not HMI.



HMI: Tunnel Panenská – example of the HMI window for the energy distribution schema

.Safety in Large Scale Systems

Computing a risk analysis for large scale systems is a challenging task, where the key element – the control system if often overlooked. We must keep in mind, that the level of security of tunnel systems is always primary dependent on the control system used. The reliability of overall solution is then a compromise among control system used, complexity of controlled technology, and financial possibilities. To minimize the risks of injuries or even deaths of passengers, we must design a tunnel control system with the high standard of used components, follow the legislative, and most importantly have a comprehensive concept. Some of the often missed pre-requisites for a safe and reliable control system are discussed by this article.

REFERENCES

1. Directive of European Union 2004/54/ES
2. TP98 -Technologické vybavení tunelů pozemních komunikací
3. Functional safety - EC 61508
4. Zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů a příslušná nařízení vlády ve znění pozdějších předpisů
5. Nařízení vlády ČR č. 17/2003 Sb., kterým se stanoví technické požadavky na elektrická zařízení nízkého napětí (73/23/EHS)
6. Nařízení vlády ČR č. 18/2003 Sb., kterým se stanoví technické požadavky na výrobky z hlediska jejich elektromagnetické kompatibility (89/336/EHS)