Implementation of Network Redundancy in Environment of Road Tunnel Control

Anna Cerovská[1] and Juraj Spalek[2]

[1] BETAMONT, s.r.o., J. Jesenského 1054/44, 960 03 Zvolen, Slovakia
cerovska.anna@betamont.sk
[2] Faculty of Electrical Engineering, University of Žilina,
Univerzitná 1, 010 26 Žilina, Slovakia
juraj.spalek@fel.uniza.sk

Abstract. Availability of individual segments of a road tunnel control system is directly dependent on network infrastructure. A safe tunnel requires a 100 % availability of control. One of the alternatives how to approach the fulfillment of this requirement is the implementation of hardware and link redundancy to the network topology of the road tunnel by means of mechanisms that enable to improve the failure tolerance in Ethernet networks.

Keywords: Tunnel backbone, redundancy, network, redundancy protocols.

1 Introduction

For many current intelligent traffic systems a 24-hour service is required at every of 365 days of the year and to provide this is not so "easy" [4]. Since each system or transmission medium has its life cycle and failure rate, it is necessary to explore this factor. One of the alternatives can be using of redundancy. Its function in the system is to react in desired way to the failure. For that reason it can serve for recovery after the failure. The reserve parts of the system are those, the using of which would be obsolete, if other parts of the system work correctly. According to the way of using reserve in a specific time, we can recognize 2 types of reserves [3]:

- Active reserve – all facilities that perform a certain function are determined for current operation (in technical literature designated also as a "static reserve");
- Standby redundancy – a part of used facilities performing the required function is determined for the working, whereas other parts of used facilities do not perform any work as far as it is not necessary (in technical literature designated also as a "dynamic reserve").

However, systems containing active reserve and standby redundancy often occur in professional praxis, the so called hybrid redundant systems.

Another way to differentiate redundancy is according to elements which require backup:

- **Power redundancy** - industrial products should have at least two power inputs to accept power from a primary and a backup source, guaranteeing uninterrupted operation.

J. Mikulski (Ed.): TST 2010, CCIS 104, pp. 75–84, 2010.

- **Media redundancy** - A basic requirement for industrial networks is media redundancy, which involves forming backup paths for network access.
- **Node redundancy** - In many industrial networks, certain devices must always be available and communication must not be interrupted at any time, otherwise great losses are incurred. For this reason, critical devices can be backed up by setting up dual network nodes. Both network nodes should be connected to a dual-homing controller, which is able to select the most suitable homing path. To continue normal network communication even when a network disaster occurs, the dual-homing control must establish connections with certain critical end devices.
- **Network and system redundancy** - Some industrial networks may rely on two physical networks, even two complete systems, as a redundant solution. Once media and node redundancy have been implemented, advanced management of redundant systems must be taken into consideration, including the management of two completely independent networks with two communications ports on each connected devices. Network and system redundancy are more complete solutions, but involve greater cost and complexity [2].

2 Control of Safety Critical Processes

Control system of road tunnels can be designated as control of safety critical processes (i.e. safety relevant systems) which fulfill the control functions with defined safety level. For safety critical process such technological process is considered, at which the failure of prescribed functions can bring up the occurrence of non-intended event, or sequence of events can incur that cause endangering of human lives, significant damage of environment, large material losses, or may cause the loss of provided service [1].

Safe road tunnel requires 100% control availability. Availability of individual segments of the road tunnel control system depends directly on network infrastructure. The uppermost task at its designing is the proposal of appropriate network topology. To achieve the best possible availability of network segments by simple doubling of all active network components and interconnections would be very costly. Therefore it is appropriate to analyze carefully each control level and to evaluate the necessary stage of network redundancy.

3 Network Redundancy Mechanisms

In recent years, redundant Ethernet technology has been rapidly and popularly adopted in the industrial automation field due to its enhanced reliability. There are many existing mechanisms that can enhance fault-tolerance in an Ethernet network. The most common of these are the Mesh networking, STP, RSTP and proprietary ring redundancy [2].

Mesh networking is a network where all the nodes are connected to each other in a complete network. Data travelling on the Mesh network is automatically configured to reach the destination by taking the shortest route. Mesh networking is reliable and

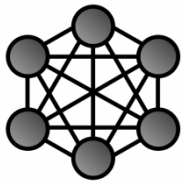


Fig. 1. Full meshed network

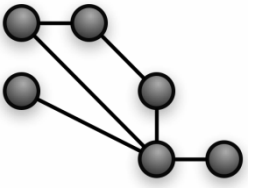


Fig. 2. Partially meshed network

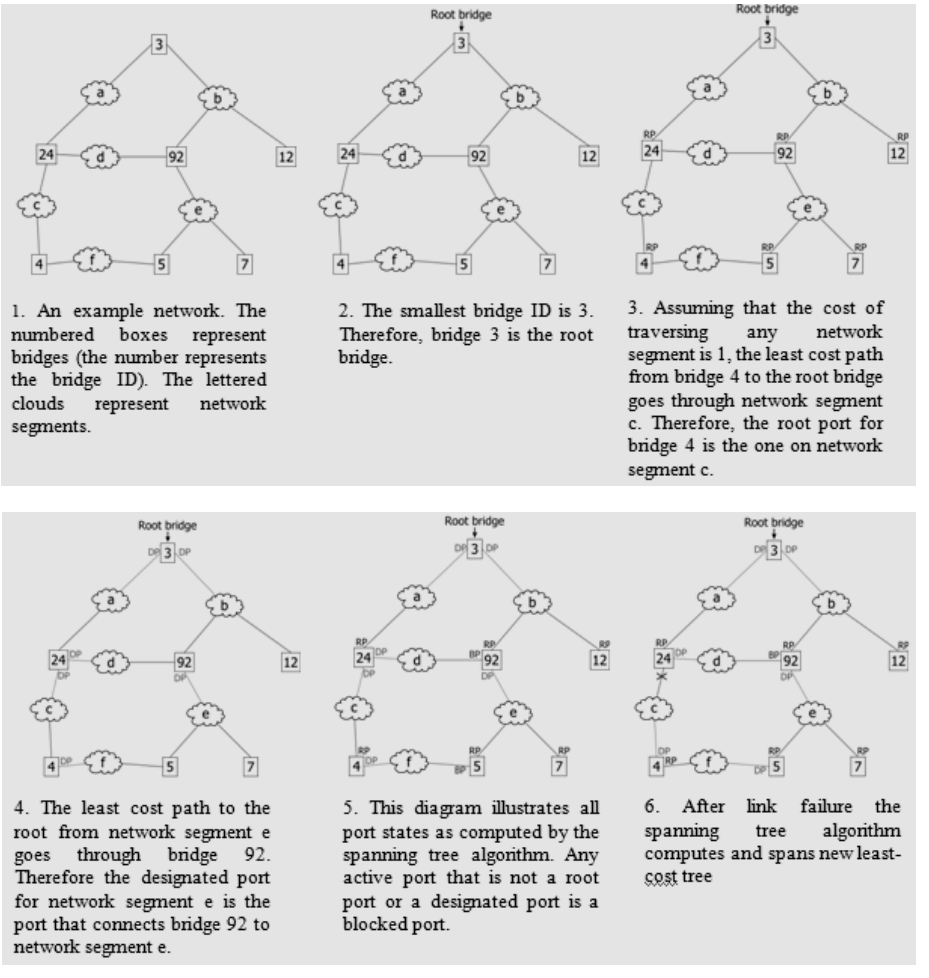
self-repairing. If one node fails, the network finds an alternate route to transfer the data, but there are increased costs from the cables required to connect all the nodes to each other. See Fig. 1 and Fig. 2.

Spanning Tree Protocol (STP) as defined in the IEEE 802.1D standard is designed to eliminate loops in a network by cutting the network into a loop free tree shape. It helps a network to achieve link redundancy and path optimization. Its functionality rests upon the fact that between two nodes only one route can be active. Several active routes between nodes can cause loops in network and those data duplication. In spite of the fact that STP resolves loops in network at retaining redundancy it also has its bad features. One of them is a long time for network renewal, usually up to 15 seconds as far as the spanning tree is stabilized and this time is too long for industrial applications.

Rapid Spanning Tree Protocol (RSTP) – to overcome the slow convergence of STP, the IEEE released the IEEE 802.1w standard to make improvements based on STP. This shortened the recovery speed to 1 second. However, for some real-time and mission critical industrial applications, such as road tunnel control system, recovery time must be under 100 milliseconds to ensure the reliability of the network. STP and RSTP are open standards that many Ethernet switch manufacturers have implemented in their managed switch products. The faster self-healing time of RSTP is very helpful in an enterprise network where a few seconds of network delay is acceptable. However in an industrial control network, one second of missed communications can cause serious problems.

Look at visual explanation of basic functionality of Spanning Tree Protocol in Fig. 3.

Ring redundancy is common among today's industrial Ethernet networks. It is a more cost-effective solution than a mesh network, and overcomes the recovery time problem of STP and RSTP. There are many different ring redundancy technologies featuring a guaranteed recovery time of a few milliseconds offered by industrial Ethernet solution providers. Ring redundancy ensures non-stop operation of networks



1. An example network. The numbered boxes represent bridges (the number represents the bridge ID). The lettered clouds represent network segments.

2. The smallest bridge ID is 3. Therefore, bridge 3 is the root bridge.

3. Assuming that the cost of traversing any network segment is 1, the least cost path from bridge 4 to the root bridge goes through network segment c. Therefore, the root port for bridge 4 is the one on network segment c.

4. The least cost path to the root from network segment e goes through bridge 92. Therefore the designated port for network segment e is the port that connects bridge 92 to network segment e.

5. This diagram illustrates all port states as computed by the spanning tree algorithm. Any active port that is not a root port or a designated port is a blocked port.

6. After link failure the spanning tree algorithm computes and spans new least-cost tree

Fig. 3. Spanning tree protocol principle of operation

with an extremely fast recovery time. If any segment of the network is disconnected, the network system will recover in a few milliseconds by activating the backup path in a ring. It is, however, necessary to consider the number of connected network nodes in one ring. With higher number of nodes there is also increase of probability that some nodes may fail at the same time which causes unavailability of those nodes that are connected among the failed ones. It is applicable to create smaller network rings. There are several possibilities how you can connect network rings each other (see Fig. 6). Nevertheless, the ring topology has some significant advantages – mainly an acceptable ratio redundancy level / price which moves it into the position of preferred network topology in the area of intelligent control systems [2].

A completely redundant system consists of redundant switches, redundant communication ports, and redundant device pairs. All Ethernet devices and workstations are connected to both independent ring network architectures (see Fig. 4 and Fig. 5).

Depending on the circumstance, there are two possibilities that fit this redundancy application. One of the possibilities uses devices that have two ports, with one of the ports utilized for the primary path, and the other port serving as the secondary path. The other possibility uses devices that have only one port. In this case, the devices must be upgraded to two Ethernet ports, in order to form the primary and secondary paths (Fig. 6).

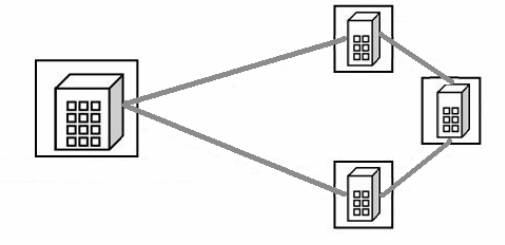


Fig. 4. Ring type network

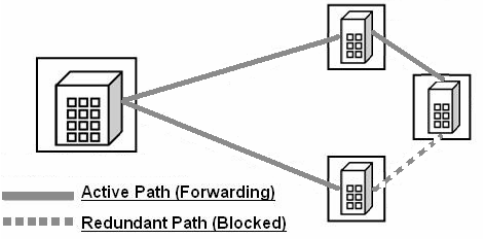


Fig. 5. Ring type network with one segment blocked

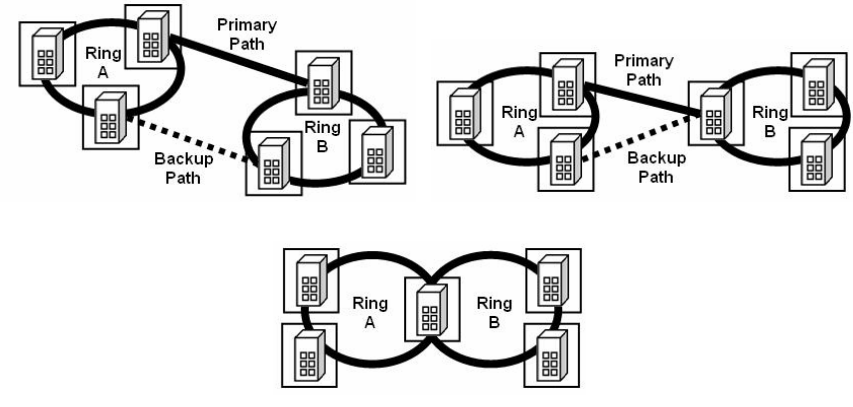


Fig. 6. Ring – to – ring applications

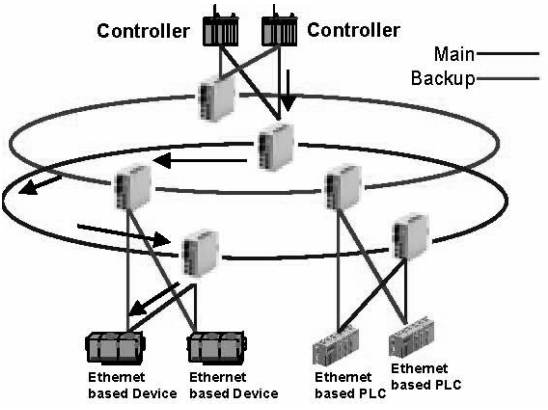


Fig. 7. General flow control in two independent ring network architectures

Complete system redundancy can form an extremely reliable network that minimizes data loss and has fast recovery time (Fig. 7). There must be a dual homing controller that is able to distinguish which Ethernet device is active the primary path or secondary path. The diagnostics can ensure that active devices are fully functional and ready to take over at any time (see Fig. 8 and Fig. 9) [2].

4 Transmission Mediums

The used transmission medium also plays important role in process of road tunnel control. Nowadays the using of fiber optics is preferred since the fiber optics has in comparison with traditional metallic leading couple of benefits, first of all a large bandwidth that gives a possibility to transfer a larger data amount. Signal passing via fiber optics is also significantly less inclined to the disturbances; fibers are much thinner and lighter than classical wires. Cupper line has its limits both in bandwidth and length of line which is at the present time not sufficient.

Optic fibres are basically divided into single mode and multimode ones. The single mode fibre is characterized by its thin core. It is less sensitive to attenuation than multimode fibre, has higher performance and spreads only to one direction with high concentration of photons that allows transmission of information on longer distances (max. distance 3 km) in high speeds. The multi mode fibre is thicker than the single mode one which causes that the light beam can spread in more paths that provides a larger bandwidth, however, at the lower transmission speeds. As a source of light beams there are used the LED-s. It is suitable for realization of interconnections on shorter distances (within 2 km).

The tunnel construction is characterized with its short distances between the connecting points and therefore it uses at the realization of backbone network often exactly the multi mode fibre optic cable which is more acceptable also from economical point of view. It is the price for the cable itself and necessary signal converters (converting the electric signal to the light one and vice versa) that plays the decisive role. The single mode fibre optic cable is often primary used on open motorway sections where the density of the technological components connected to fibre optic line is lower.

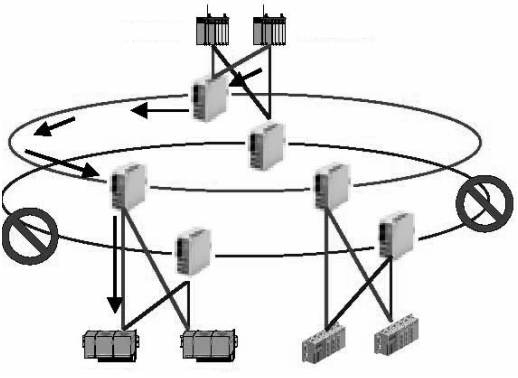


Fig. 8. Network failed

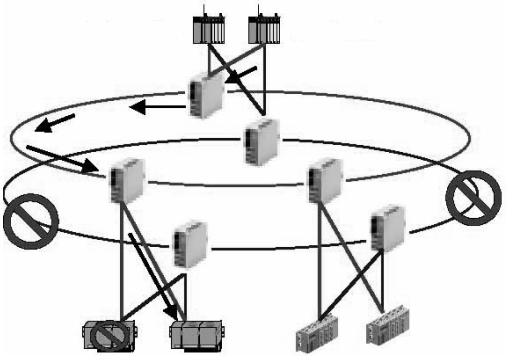


Fig. 9. Network and device failed

5 Constructional Readiness for Redundancy Implementation

Constructional architecture of tunnel constructions plays also important role at the proposal of redundancy for road tunnel backbone network. It affects mainly the problems of placing the redundant elements of network where a physical re-distribution of safety critical elements on various places is preferred. For instance, it is appropriate to lead the alternative communication routes through a separated cable line in order that the availability of communication is secured also in case of damaging the primary cable route. Similarly, it is appropriate to arrange two local operational centres for a road tunnel (control rooms) with placing of central control system of the particular road tunnel in order that the superior level, for example a regional operational centre (which is in charge of control and supervision of all tunnels in region), or a central operational centre (administration and supervision of all road tunnels in Slovakia) has in case of a failure of one of them an alternative access to the control. It is not necessary that both local dispatching centres are equipped with surveillance for operation (CCTV surveillance, operator working station etc.), since the control command comes

from the superior level. It is sufficient just to place the redundant technological elements in ideal way, for instance on both sides of the tunnel tube.

6 Proposal of Redundant Backbone Network for a Selected Tunnel as an Example

Cable lines in this model tunnel (dashed lines lines in Fig. 10) are proposed by both alongside of both tunnel tubes to secure the physical separation of alternative communication paths. Technological and at the same time network nodes are in this case placed in special electrical distribution rooms (or cabinets) in cross interconnections of tunnel tubes (dark boxes in Fig. 10) that serve as escape ways both for persons and vehicles of emergency crews.

The redundancy on this level is provided in the form of doubling of nodes whereas one node serves primary for mediation of control system communication with control segments for a certain section of the first tunnel tube (e.g. the southern tunnel tube) and the second one serves primary for mediation of control system communication with control segments for a certain section of the second tunnel tube (e.g. the northern tunnel tube). They are, however, interconnected, in order to provide a substitution of these nodes if one of them fails. On both sides of the one, or the second tunnel tube are located redundant control rooms of the tunnel where also a connection point to the main fibre optic cable route of the whole motorway section is situated. By doubling the tunnel control room we secure the availability of central control system also if one of these control rooms fails (failure, or fire).

Active network elements[1] are connected into a ring whereas primary communication path is led through internal cable line of one of the tunnel tubes and the network ring is closed by outer cable line of the second tunnel tube. That means it is provided that except of the fact that the alternative communication path is led through another cable line, the cable line is in other tunnel tube as well. In such a way two primary network rings connected in level of control rooms into two redundant active network elements (each ring is terminated in another active network element) are created. It is still possible to increase the network availability by doubling these proposed network rings in that on the level of control room they will be connected into another active network element as it is at primary network rings (cross connection). See Fig. 11.

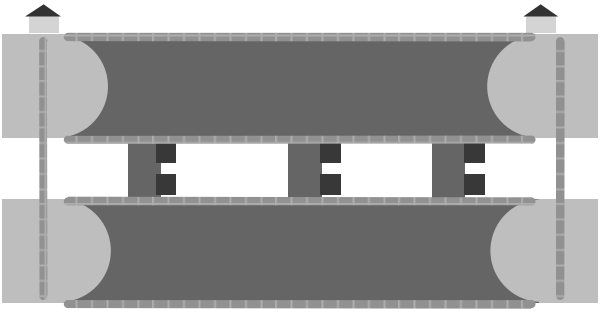


Fig. 10. Cable lines

[1] In this case network switches, eventually routers are assumed

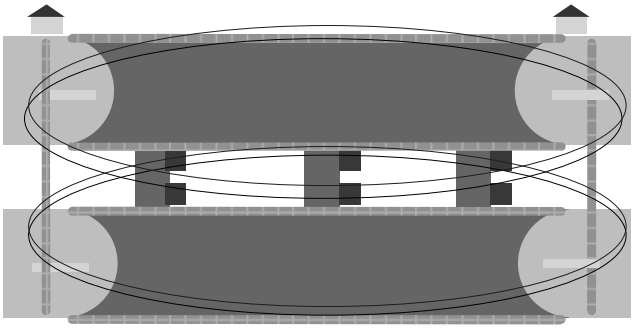


Fig. 11. Network rings

But this is only one variant of backbone network interconnection. As it was mentioned in chapter about ring redundancy, it is more reasonably to create smaller network rings, mainly in case of long road tunnel. There is possibility to divide tunnel tube into more sections connected each other.

The goal of this complex network topology is to achieve the control availability also in the most critical cases, such as fire in control room and the following damage of the placed technology, or fire in one of the tunnel tubes, eventually to create a possibility to accomplish service without the necessity of disconnection the other parts of the control system.

7 Mastering the Failure Consequences

Not even the careful application of proceedings is able to exclude completely the occurrence of failures during system operation. Thus, the system has to provide such features that enable to find out a failure and to guarantee the transition of the system into a safe default state. That means for instance that if one part of the control system (control segments) losses connectivity with central control system, those control segments will locally control the traffic process according to the defined default scenarios. If a failure of the control segment itself occurs, an initial safe level has to be predefined into which the individual controlled technological elements would get in case of detected fault. Re-leaving of this state can occur only after failure removal. Repeated putting the system into operation cannot occur spontaneously, but must be under control.

8 Conclusions

The goal of this paper is to demonstrate to a reader the problem of availability improvement in the safety critical technical systems situated in road tunnels. On the principal level basic techniques and mechanisms for success redundancy implementation in road tunnel backbone network were explained.

Acknowledgements. This work has been supported by the Grant Agency VEGA of the Slovak Republic, grant No. 1/0023/08 "Theoretical apparatus for risk analysis and risk evaluation of transport telematic systems". The paper was prepared under the support of the ERDF - European Regional Development Fund, project No. ITMS-26220120028, "Centre of excellence for systems and services of intelligent transport".

References

1. Zahradník, J., Rástočný, K., Kunhart, M.: Safety of Railway Interlocking Systems, pp. 27–30. University in v Žilina /EDIS – publishing house ŽU, Slovak republic (2004) ISBN 80-8070-296-9
2. CCNA Exploration 4.1, Cisco Networking Academy Course Materials
3. Přibyl, P., Janota, A., Spalek, J.: Analysis and Risk Control in Transport. Technical literature BEN, Praha, pp. 419–432 (2008) ISBN 978-80-7300-214-5
4. Urgela, S.: Applications of the Railway Information Systems (in Slovak). In: Road Conference, pp. 218–223 (2003)