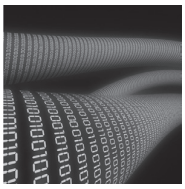

Archives of
Transport System
Telematics

Volume 11

Issue 1

February 2018

Transmission Redundancy in Safety Systems for Railway Transport Using the Example of the Axle Counter

M. BUŁAWA, P. WOŁOSZYK
VOESTALPINE SIGNALING SOPOT, Jana z Kolna 26C, 81-859 Sopot, Poland
EMAIL: Mariusz.Bulawa@voestalpine.com

ABSTRACT

Availability of the modern safety systems for railway transport depends on telecommunication infrastructure for communication of distributed subsystems. In order to limit risks related to transmission interference, various redundancy technologies of transmission networks (media, devices) are used in industrial systems - sometimes including their automatic reconfiguration. This article presents an analysis of the considered methods to provide high transmission availability in the axle counter system, as well as the implemented tailored solution – protocol UniPRP which uses parallel transmission of the doubled data. This solution is an adaptation of those presented in the series of technical standards: IEC 62439 Industrial communication networks - High availability automation networks.

KEYWORDS: high availability, communication, redundancy protocol, axle counting

1. Introduction

Safety related systems in railways are using transmission systems more and more frequently. It is not only to connect different locations but also more and more often to connect parts of the system installed in one location. System in total, just as each subsystem e.g. transmission system, have to fulfil requirements of EN 50129 and EN 50159 standards [1, 2].

In addition, the signalling systems require high availability to ensure continuous traffic operation. As a consequence, high quality components and proper maintenance are requested. In communication subsystems highly reliable network components alleviate the potential for failure of transmission, but also network redundancy is beneficial in order to ensure continuity and avoids disruption of critical communication, as it limits the risk of losing of availability in case of failure.

Redundancy could be implemented [4, 5] as:

1. dynamic (standby, serial), or
2. static (parallel, workby).

Dynamic redundancy does not actively participate in the control. A switchover logic decides whether to insert redundancy and put it to work. This allows to share redundancy and load, implement partial redundancy and reduce the failure rate of redundancy. On the other hand, such switchover takes time.

Static redundancy with costly total duplication provides seamless switchover, continuously exercise redundancy, increase fault detection coverage and provide fail-safe behaviour.

In order to provide high availability networks, several methods were implemented in many industrial applications. The "Highly Available Automation Networks" IEC SC65C WG15 selected many redundancy methods that could be divided into two main categories:

1. "redundancy in the network", e.g. redundant rings, with devices attached to a single bridge only (singly attached devices), while the bridges implement redundancy, and
2. "redundancy in the devices", using devices with two network interfaces attached to redundant networks (doubly attached devices).

The methods above are described in the suite of norms IEC 62439 including:

- Parallel Redundancy Protocol (PRP), implements "redundancy in the devices" method that provides bumpless switchover in case of failure or reintegration.

- High Availability Seamless Redundancy (HSR), similar operation principle to PRP, including zero recovery time, less infrastructure, specialised hardware components,
- Media Redundancy Protocol (MRP) by Siemens/Hirschmann implements "redundancy in the network" with singly attached devices attached to a ring, with moderate increase in availability and disruption delay of 200 ms to 500 ms. This is interesting if the bridges are integrated in the devices, but it also limits topology to a simple ring of up to 50 bridges.
- Cross Network Redundancy Protocol (CRP) by Honeywell/ Fieldbus Foundation implements – like PRP –"redundancy in the devices", offers the same availability as PRP, but has disruption times of 200 ms to 2s. It allows to connect singly attached devices to both network halves, but costs aggregated links in the (mandatory) root bridges.
- Beacon Redundancy Protocol (BRP) by Rockwell/OVDA exhibits characteristics similar to CRP, strives to provide a 20 ms recovery delay by sending a beacon at short intervals.
- Distributed Redundancy Protocol (DRP) by SupCon/China is a ring redundancy protocol which competes with MRP and uses a tight clock synchronization to support time-slotted real-time traffic.
- Redundant Ring Protocol (RRP), another ring redundancy protocol supported by RAPIEnet, LS Industrial Systems Co.

In order to address specific application requirements the recommendation below were given:

1. general automation systems – the standard recommends to use RSTP (base: IEEE standards, RSTP) – no need for a new standard < 500 ms.
2. benign real-time systems that are cost-sensitive, grace time < 200 ms – the standard shall define an adequate bridge redundancy scheme and redundant devices attachment (base: RSTP and further developments – solution: MRP, DRP, RRP).
1. critical real-time systems that require higher coverage, grace time: 0 ms – the standard shall define parallel network solutions and redundant device attachment (base: ARINC AFDX and similar – solution PRP, HSR).
2. legacy solutions based on Fieldbus Foundation CRP.

Accordingly in the applications with requested zero recovery time there are two standards recommended: PRP and HSR, operating principles of which can be customised if necessary.

PRP redundancy protocol implements redundancy in the devices, through doubly attached nodes operating according to PRP (DANPs).

A DANP is attached to two independent LANs of similar topology, named LAN_A and LAN_B, which operate in parallel. A source DANP sends the same frame over both LANs and a destination DANP receives it from both LANs within a certain time, consumes the first frame and discards the duplicate.

General architecture of the network used by PRP is presented on Fig. 1.

The two LANs are identical in protocol at the MAC-LLC level, but they can differ in performance and topology. Transmission delays may also be different, especially if one of the networks reconfigures itself, e.g. using RSTP, to overcome an internal failure.

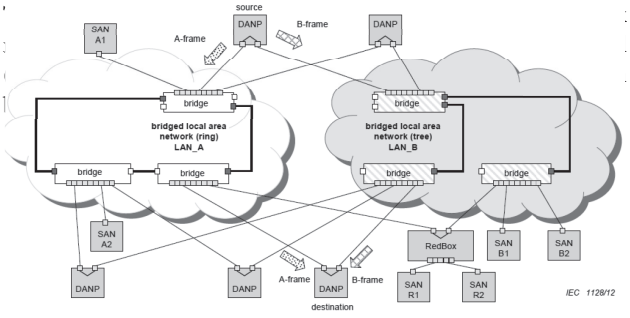

Fig. 1. PRP example of general redundant network [3]

The two networks have no connection between them and can be assumed as fail-independent. Redundancy can be defeated by e.g. common power supply, so additional redundancy also for power supply is needed to prevent a single point of failure. PRP can be implemented entirely in software, i.e. integrated in the network driver.

High-availability Seamless Redundancy (HSR) retains the PRP property of zero recovery time and is applicable to any topology, in particular rings and rings of rings.

With respect to PRP, HSR allows to roughly halve the network infrastructure. With respect to rings based on IEEE 802.1D (RSTP), IEC 62439-2 (MRP) or IEC 62439-6 (DRP), the available network bandwidth for network traffic is roughly halved. Nodes within the ring are restricted to be HSR-capable switching end nodes. General-purpose nodes (SANs) cannot be attached directly to the ring, but need attachment through a RedBox (redundancy box).

As in PRP, a node has two ports operated in parallel; it is a DANH (Doubly Attached Node with HSR protocol). A simple HSR network consists of doubly attached switching nodes, each having two ring ports, interconnected by full-duplex links, as shown in the example of Fig. 2 (multicast) for a ring topology.

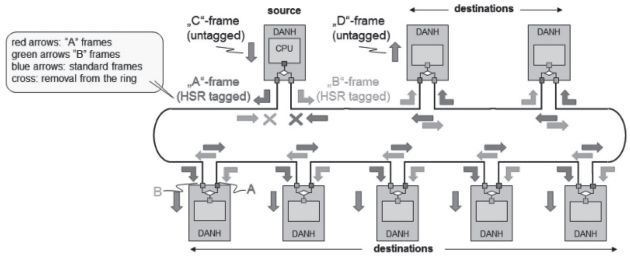

Fig. 2. HSH example of ring topology redundant network [3]

A source DANH sends a frame passed from its upper layers ("C" frame), inserts an HSR tag to identify frame duplicates and sends a frame over each port ("A"-frame and "B"-frame). A destination DANH receives, in the fault-free state, two identical frames from each port within a certain interval, removes the HSR tag of the first frame before passing it to its upper layers ("D"-frame) and discards any duplicates.

The nodes of HSH require hardware support (FPGA or ASIC) to forward or discard frames within microseconds. This cost is partly compensated because Ethernet switches are not required.

2. Communication redundancy in UniAC2 axle counting system

The UniAC2 axle counting system is intended to monitor the track vacancy and sections on railway lines, shunting and marshalling yards with low, medium and high traffic, railway sidings, tram depots and loops, and lightweight railway lines.

The UniAC2 system is a new generation, modular solution designed to address high availability requirements of the modern signalling subsystems. The system consists of unified AXM modules exchanging the information over the embedded Ethernet network, with tailored layer 2 protocols.

The following transmission subsystems can be distinguished:

1. Subsystem 1: A non-safety related transmission between two AXM modules or between an AXM module and an external system. The transmission system is defined as Black Channel network and is implemented in a black box unit. Non-safety protocol encapsulates safety protocols and is used as medium converter. All safety issues are covered by the safety protocol (Subsystem 2).
2. Subsystem 2: A safety-related transmission between AXM modules or between an AXM module and an external system. Transmission is encapsulated by Subsystem 1.
3. Subsystem 3: A safety-related, on-board transmission between Safety Channels on one board implemented through the copper tracks on PCB.

One of the main challenges for the implemented solution is to provide high availability transmission system for communication between all AXM modules over Ethernet network. The individual logic peer-to peer connections ensure the quasi-continuous exchange of states between unrestrictedly defined AXM modules.

High availability is related to characteristic of the UniAC2 system, which provide the requested level of operational performance over a long period.

The main principles for that kind of system are:

1. Failure of a component shall not lead to a failure of the whole system. A single point of failure shall be eliminated by adding redundancy.
2. The crossover (decision point) in system becomes a single point of failure, so it shall be reliable.
3. The reliable failure detection even, if it does not limit availability of system. Maintenance process shall take into account that kind of events.

To provide redundancy, more components are used in the system. It leads to more complex system and can negatively impact availability because of more potential failure points. In the UniAC2 system, the following principles were defined:

- redundancy implementation as simple as possible,
- static redundancy solution,
- zero downtime system design.

To fulfil the abovementioned principles and requirements, the following solutions were implemented:

1. Reconnect in transmission system or toggling between main and second network (warm redundancy) can be a cause of system failure. Because of that "redundancy in the network" was replaced by "redundancy in the devices". As result a simplified parallel redundant technique was chosen (Fig. 3), as it does not need crossover point and algorithms of dynamic redundancy.
2. Standard, popular telecommunication devices should be used in design of telecommunication part of the system. In addition complexity of the embedded software should not be high. Proprietary protocol UniPRP, close to PRP, but with the simplified operation principles, was designed and implemented in order to proper system operation with both networks providing different performance e.g. bandwidth, lags, reliability.
3. To support a high system availability the hardware layer of transmission system ensures no single point of failure solution. The standard Ethernet switches are installed on the backplane integrating AXM module creating an embedded, doubled communication network with high reliability, doubled power supply.

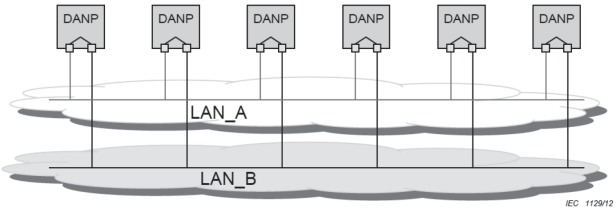

Fig. 3. UniPRP network – similar to PRP example of redundant network as two LANs (bus topology)[3]

As a final result, the tailored solution was developed around bus topology with two separate networks MAG_NET1 and MAG_NET2 connecting local and distant AXM modules (Fig. 4), using proprietary UniPRP protocol.

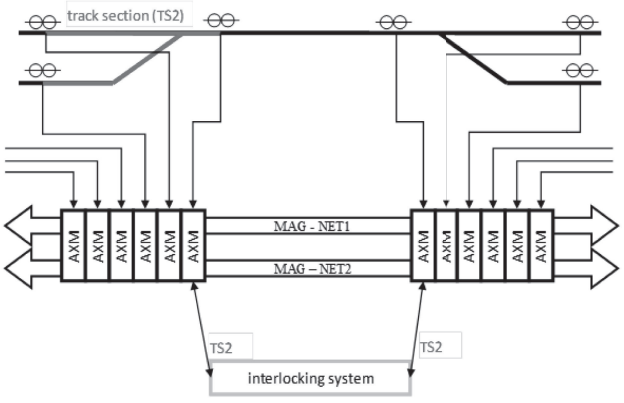

Fig. 4. Redundancy of transmission system [own study]

Each AXM module has two ports and is attached to Network 1 (MAG_NET1) and Network 2 (MAG_NET2). Information transferred between AXM modules is sent via both networks in parallel. In case of damage of one network, the second network is

enough to deliver messages on time. Redundancy on this level is executed in Black Channel unit. Safety Channel sends one message (MESSAGE), that I doubled on Black Channel level and it is send via MAG_NET1 (MESSAGE1i) and MAG_NET2 (MESSAGE2i). Black Channel on relevant AXM module (receiver) receives MESSAGE1i and MESSAGE2i. The first MessageXi (X=1,2) is transferred to Safety Channel; second message is discarded as a duplicate.

2.1. Solution characteristics

Additional layer in the UniAC2 protocol provides seamless failover against failure of any network component. Link Redundancy Entity layer (LRE) is responsible for duplicate and discarding frames. Layer LRE is transparent for higher layers of protocol. It allows higher layer network protocols to operate without modification.

The internal structure of frame is compatible with specified in IEEE 802.3 structure. To simplify the detection of duplicates, the frames are identified by redundancy trailer. It contains a sequence number that is incremented for each frame sent according to the protocol. MAC addresses are used as source and destination identifiers. This trailer is ignored by nodes and network equipment that are unaware of the specific protocol and considered as padding. Payload containing specific data is presented in a table below (Table 1).

Table 1. UniPRP - structure of frame [own study]

No	Field	Description
1	Safety and non-safety related data	Data specified for UnIAC2 system
2	Redundancy trailer:	Set of data related to parallel redundancy protocol.
2a	64-bits sequence number	Sequence number
2b	4-bits NET identifier	NET1 = 0xA; NET2 = 0xB
2c	12-bits frame size	Cover data in field 1 and trailer in field 2
2d	16-bits protocol suffix	Protocol type identifier
3	Network management	Set of data related to network monitoring and management e.g. timestamp

The sequence number size is enough to cover about 100 million years of system work. It simplifies the algorithm and allows to distinguish many border scenarios with two different behaviours of MAG_NET 1 and MAG_NET2.

2.2. Sender

The main task of the sender is to send two identical (or rather similar because of different MAG_NET identifier field) frames to the receiver. The sender maintains table of logical connections with receivers. For each of them, it increments specific sequence number. This ensures a proper failure detection coverage, which is one of the main purposes of high availability systems. The sender cannot modify payload of the frame, so LRE layer has no impact on safety-related data. Redundancy trailer is added as an additional part of the frame information. Thanks to that, connections with and without redundancy protocol can exist in the same network.

2.3. Receiver

The receiver analyses frame and redundancy trailer. Based on it, it decides if specific frame shall be sent to next layers, or discarded. The most important logic of the receiver is the duplicate discard algorithm. This algorithm has the following steps:

1. IF current sequence in new frame > last received sequence number THEN frame is valid.
2. IF current sequence in new frame < start sequence number THEN frame is discarded, restart of sender is detected. Start sequence number equals last received sequence number minus window size. Windows size is a distance between next proper sequence number and detection of sender restart.

Window size depends on the frequency of frames between nodes and lags on the slower network. This approach assumes that network with poorer parameters shall be good enough to connect all nodes. The lags in network shall not be higher than the window size in the algorithm.

2.4. Supervision

The simplified supervision of the communication network was implemented. The black channel processor in a node collects the information indicating the state of communication from its perspective, e.g. it keeps a node table of all detected partners and registers from the last time a node was seen, as well as the number of received frames which the nodes receive from each other over both interfaces. As safety application generate an intensive traffic by sending cyclic status data, there is no need of dedicated supervision frames for checking continuously all paths.

The embedded monitoring system of UniAC2 ensures that the diagnostic data registered on the AXM level (not only related to communication) is collected on the system level by a specialized diagnostic ADM module.

3. Conclusion

The progress of communication technologies is opening new opportunities for designers of embedded network systems and safety related applications. The new, so-called industrial Ethernet solutions are able to replace the former field bus technologies not only because of their higher bandwidth, but especially because of the ability to create highly available industrial networks. Over the last 20 years many methods of redundancy were developed and successfully implemented in Ethernet networks, combining outstanding reliability with acceptable costs.

In railway signalling systems the industrial Ethernet combined with the concept of "black channel" brings new possibilities, providing increase of configurability and maintainability of systems that should adapt to diversity of railway infrastructure.

The UniAC2 axle counter system is an example of a new generation modular solution designed to address high availability requirements of modern signalling subsystems. One of the challenges during the design phase was to develop a redundancy

concept for embedded communication network integrating the distributed AXM modules.

Having examined the redundancy methods available, no appropriate redundancy protocol was find. In consequence, due to the specific safety related requirements and required simplicity, the tailored solution UniPRP was implemented.

UniPRP allows seamless switchover and no frames are lost. AXM modules fulfil the role of doubly attached nodes (DANP), which was achieved with relatively low costs.

The double network consisting of two independent sets of inexpensive Ethernet switches limit the risk of losing connection.

The current state of Ethernet technology is well able to fulfil the requirements of the most demanding embedded applications. The right assumptions and proper technical choices during the planning phase of a communications network should minimize project risks, especially connected with management of complexity. The existing well-known standards, especially PRP, can be an inspiration for the tailored solutions adapted to the needs of embedded safety related systems. The main challenge seems be located in the area of balance between performance and simplicity.

Bibliography

[1] EN 50129:2003. Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signaling.

[2] EN 50159:2010. Railway applications – Communications, signalling and processing systems – Safety related communication in transmission systems.

[3] EN 62439 series. Industrial communication networks – High availability automation networks Part 1-7.

[4] HIRSCHMANN/BELDEN: WP1003-White paper. Media Redundancy Concepts. High availability in Industrial Ethernet (http://belden.picturepark.com/Website/Download.aspx?DownloadToken=b427cf97-d5bc-4628-b41a-57d3d2eca706&Purpose=AssetManager&mime-type=application/pdf).

[5] KIRRMANN H., DZUNG D.: Selecting a Standard Redundancy Method for Highly Available Industrial Networks, in Proceedings of 2006 WFCS, IEEE International Workshop on Factory Communication Systems, pp. 387-394.

[6] KIRRMANN H.: PRP – Parallel redundancy Protocol. An IEC standard for seamless redundancy method using parallel networks, applicable to hard-real time Industrial Ethernet. (http://lamspeople.epfl.ch/kirrmann/Pubs/IEC_62439-3/IEC_62439-3.4_PRP_Kirrmann.pdf)

[7] UniAC2 axle counting system. Technical documentation.