

## FAIL SAFE CONTROLLER FOR POINT MACHINES

Ventsislav Trifonov, Vasil Vatakov

[vtrifonov@vtu.bg](mailto:vtrifonov@vtu.bg), [vvatakov@vtu.bg](mailto:vvatakov@vtu.bg)

*Todor Kableshkov University of Transport,  
Sofia, Geo Milev Str. 158,  
BULGARIA*

**Abstract:** *The control of railway switches is carried out with switch devices. The main control schemes are safe and are in the computer centralizations. Only power cables are installed next to the devices, through which commands for reversing the switches are given. The power cables are tied to the control scheme of the switch device. In this way, a very large amount of copper cable is consumed. This also affects the increase in construction costs in terms of the pipe network.*

*The article discusses a new approach in which the logic for controlling the devices is in a controller, which is installed in the device itself. The device control commands are sent from the station centralization via an optical cable to the controller. The controller decodes the command in a safe way and ensures the device's reversal. Then the controller forms a telegram for the new state of the device and sends it back to the interlocking system. Communication between the interlocking system and the controller is carried out using a secure and safe Ethernet protocol. The controller allows it to be used for various types of devices in terms of the principle of electrical control. It is possible to include additional sensors to control the position of the tongues. This allows you to optimize the number of copper cables in the station and to connect the switches into a common communication network. The article discusses the architecture of the control controller, the structure of the communication protocol and the principles of safe behavior after failure.*

**Key words:** *fail-safe controller, signaling, railway safety, safety processor system.*

### 1. INTRODUCTION

The station interlocking system provides centralized control of point machines at a station (in most market solutions). Point Machines are controlled by object controllers. Each point machine is controlled by its own object controller. The object controller is connected to the turnout by means of a different number of wires. The number of wires is determined by the wiring diagram for controlling the motor and how to receive feedback from the contact system. During the turning of the arrow from the + position to the "-" position, the motor current and the turning time are also monitored. In this way, a scheme for individual control of the arrows is implemented. Thus, it is necessary to install individual cables next to each arrow. The schematic wiring diagram, in existing circuits, is shown in the following figure.

In this case, there is a large consumption of copper cables, which are used for direct control of the arrows. The article discusses a new model of control of a turnout apparatus with a built-in safe object controller, to the apparatus of the turnout apparatus. The principle schematic diagram for the implementation of connection of wires is present of Fig. 1.

In [1] a model for decentralized station centralization is presented, with the controller being deployed as a separate component of the turnout apparatus. In [2], an architecture for control of the security of railway applications is proposed, which covers the area from the dispatch center to the computer centralization, without reaching the final field elements. Safety Requirements for Railway Structure are present in [3] as pattern model for functional safety requirements. Paper [4] presents a proprietary protocol for fail safe communication used in signaling systems.

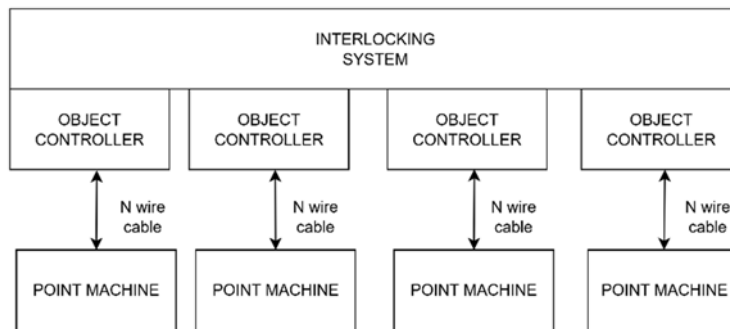


Fig. 1. Direct Cable Connection

Current paper present new kind of solution where object controller should be a part of point machine.

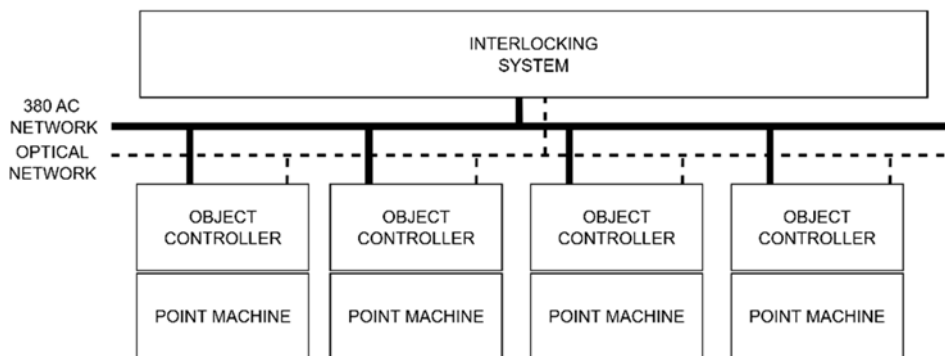


Fig. 2. One cable connection

The proposed solution provides:

- Using one power cable for one station throat;
- Use of a single 4-fiber fiber optic cable to provide redundant communication between object controllers and station interlocking system

It is also possible to implement a two-time (reserved) power supply from two sources to each turnout switch.

The effect of saving copper cables by number of arrows is shown in the following table:

Table 1 Copper Cable Statistic

| Point Machine Number | Direct Cable Connection | New Solution Cable Numbers |
|----------------------|-------------------------|----------------------------|
| 1                    | 1                       | 1                          |
| 5                    | 5                       | 1                          |
| 10                   | 10                      | 1                          |

## 2. SOLUTION ARCHITECTURE

The principal controller architecture is present on Fig. 3

The point controller consists of:

- Two communication modules (Ethernet based)
- Fail Safe Command Decoder
- Fail Safe State Encoder
- Fail Safe Power Switch (380)
- Fail Safe Position Controller for Switch Contact System
- Switch Contact System
- Switch Motor (AC or DC)

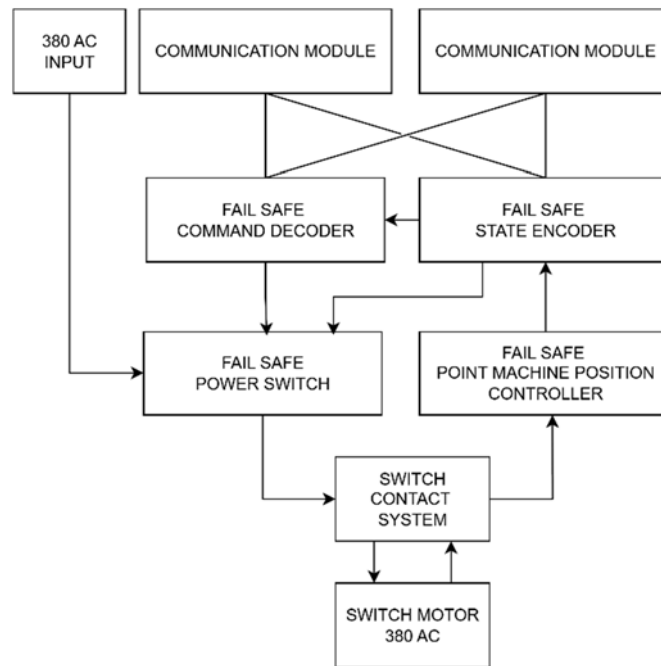


Fig. 3. Controller Principal Architecture

### 3. COMMUNICATION PROTOCOL STRUCTURE

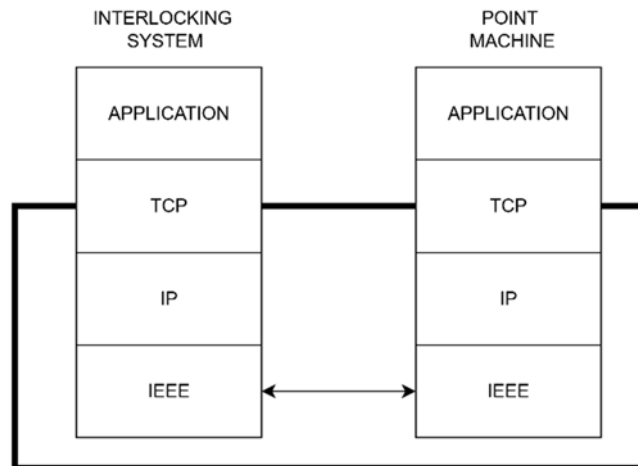


Fig. 4. TCP IP model

The proposed communication protocol is Ethernet based and consists of the following fields:

- Source address of sender;
- Destination address of receiver;
- IP address and TCP port address of interlocking system;
- IP address and TCP port of Dispatching System;
- VPN parameters;
- Type of packet (command or status information);
- State of point machine;
- Point machine parameters (optional);
- Current value of AC current (during movement of rails) ;
- Point Machine Position “ + ” ;
- Point Machine Position “ - ” ;

The proposed communication structure provides the following two main functionalities present on Fig. 5 and Fig. 6

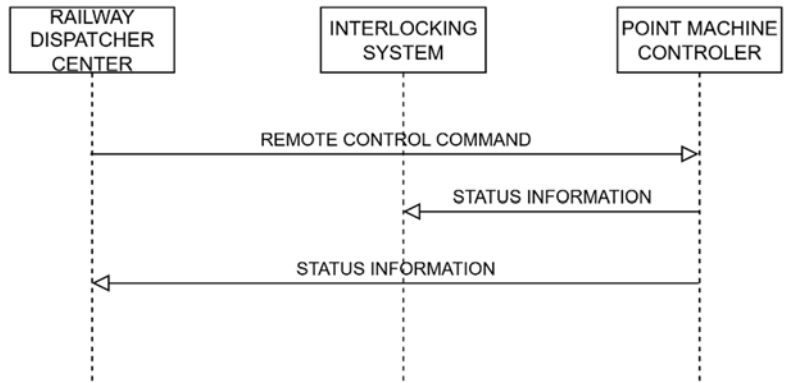


Fig. 5. Remote command from Dispatch Center

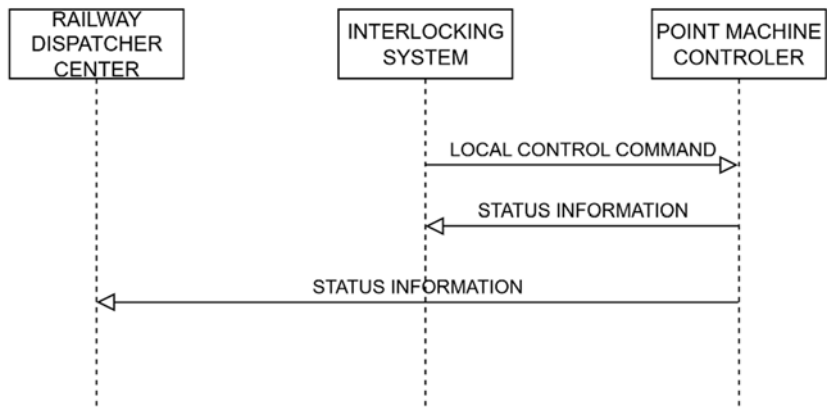


Fig. 6. Local Command from Station Interlocking System

To protect communication channel between interlocking (dispatch) system with point machine controller should be used a VPN solution. Each part of communication partners should use public and private keys. VPN part of communication channel is present on Fig. 7. VPN implementation.

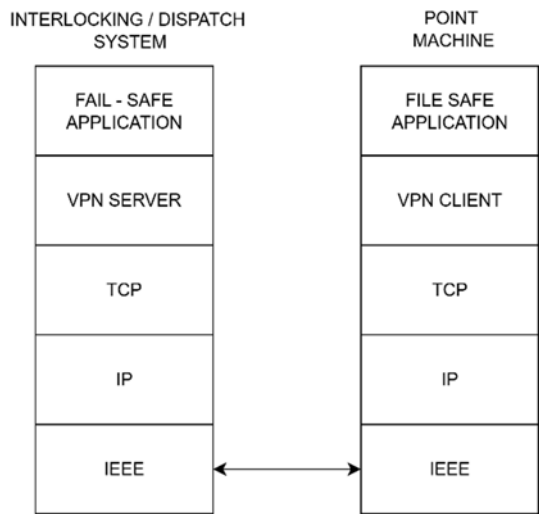


Fig. 7. VPN implementation

#### 4. FUNCTIONAL DESCRIPTION

The command to move the point machine from position "+" to position "-" can be given both from the interlocking system at the station or remotely from the dispatcher system for the related section. The command, which is made by one of the two systems, has a safety level of SIL 4. The command must be sent through an encrypted channel (protected by VPN) to ensure the intrusion resistance of the communication channel. The decoding of the command in the object controller of the arrow is performed by a safe microprocessor device (FAIL SAFE DECODER). The FAIL-SAFE DECODER after decoding send a command via switch contact system to the point machines. "Command" means how to order phases for AC motor or "+" / "-wire for DC motor. During the movement of the point blades, FAIL-SAFE POINT POSITION CONTORLER receives in real time information about process of movement and send this information to the FAIL-SAFE STATE ENCODER. FAIL-SAFE STATE ENCODER is different fail safe microprocessor device. State Encoder prepares information for the switch and send it to interlocking/dispatch system and to the FAIL-SAFE COMMAND DECODER. In case of faults (during the point blades movement) FAIL-SAFE COMMAND DECODER performs a stop operation (command) and movement is blocked (stopped). In case of normal movement FAIL-SAFE STATE ENCODER send to COMMUNICATION MODULE (S) information about point machine final state.

#### CONCLUSION

The paper proposes a model of a safe controller for decentralized control of railway switches. The paper presents a block diagram of the possible architectures for implementation. A functional description of the operation of the controller is proposed. A principled architecture for the implementation of safe communication between the controller and the control systems of a higher hierarchical level is proposed.

#### REFERENCES:

- [1] TAKASHI KUNIFUJI 2017 Safety Technologies in Autonomous Decentralized Railway Control System IEEE 13th International Symposium on Autonomous Decentralized System (ISADS) Safety Technologies in Autonomous Decentralized Railway Control System. Year: 2017, Pages: 137-142 DOI Bookmark: [10.1109/ISADS.2017.15](https://doi.org/10.1109/ISADS.2017.15)
- [2] MICHAEL ECKEL, DON KUZHIYELIL, CHRISTOPH KRAUB, MARIA ZHDANOVA, STEFAN KATZENBEISSER, JASMIN COSIC, MATTHIAS DRODT, JEAN-JACQUES PITROLLE, Implementing a Security Architecture for Safety-Critical Railway Infrastructure, *2021 International Symposium on Secure and Private Execution Environment Design (SEED)* Year: 2021, Pages: 215-226 DOI Bookmark: [10.1109/SEED51797.2021.00033](https://doi.org/10.1109/SEED51797.2021.00033)
- [3] XIAOHONG CHEN, LI HAN, JING LIU, HAIYING SUN. Using Safety Requirement Patterns to Elicit Requirements for Railway Interlocking System 2016 IEEE 24th International Requirements Engineering Conference Workshops (REW) Year: 2016, Pages: 296-303 DOI Bookmark: [10.1109/REW.2016.055](https://doi.org/10.1109/REW.2016.055)
- [4] YITIAN GU, SHOU-PON, MAXEMCHUK F., A fail safe broadcast protocol for collaborative intelligent vehicles. 2015 IEEE 16th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)