

Application Note DK9322-0809-0004 EtherCAT Master Redundancy

Keywords
redundancy basis
control redundancy
EtherCAT master
warm standby
redundancy
EtherCAT

EtherCAT Master Redundancy - Warm Standby

Control redundancy can enhance productivity and availability in critical processes. Depending on the requirements for the system behaviour in the event of a control system failure, a suitable architecture must be chosen for the redundant system in order to ensure that the required switching time is guaranteed. This application note explains the basic redundancy requirements and introduces a „warm standby“ concept for redundant EtherCAT masters.

Basic Principles

A system/process is usually managed by a control system. The control system operates the I/O stations of the subordinate field level by reading sensor data, actuating output modules and controlling axes and motors. The control system communicates the process data to the higher-level control systems, databases and servers or similar in order to store the data or use them to visualise the process.

Without redundancy, an unexpected failure of the control system not only leads to a loss of existing system infrastructures, but also to indeterminate states and uncontrollable processes.

- The production material contained in the system is at risk or irreversibly damaged.
- In an integrated system, a failure of a system component leads to a shutdown of the whole process.
- The system itself is at risk through incomplete production processes; examples: solidifying of a melt in a glass furnace or uncontrolled operation of a gas turbine.

A redundant control system enhances the system availability, since the backup system can be used in the event of a failure of the primary control system. In the simplest case, it is a 1 of 2 system. 1 of N redundancy is also conceivable. The following criteria are relevant for the specification of the switching behaviour from primary control to backup control:

1. How does the switchover to backup control take place? (Automatic or manual)

Application Note DK9322-0809-0004

EtherCAT Master Redundancy

2. Is redundant wiring available, or can the wiring be reconnected during switchover?
3. What switching time is available?
 - a. **Cold Standby:** The backup system can be booted during the switchover. The switching time can be several minutes, e.g. a control system in a remote water monitoring station
 - b. **Warm Standby:** The backup control runs in passive mode during regular operation. During switchover initialisation of the process data causes an „initialisation jolt“ in the system. Switching takes place in the single-digit seconds range. This may be suitable for moving theatre stage sets, for example..
 - c. **Hot Standby:** The backup control runs in passive mode during regular operation and accesses the current process data in the event of a failure of the primary control system. The switching time may only be a few milliseconds, e.g. in a control system for a large energy storage flywheel.
4. Is reinitialisation of the field level through the backup control acceptable, or is seamless continuation of the control process required?
5. Is a full restart of the backup control acceptable or is seamless continuation desirable after the current process data have been transferred from the primary control?

In addition to control redundancy, cable redundancy may be required. It ensures that an interruption of the connection to the field level or between individual devices does not lead to failure of these devices. Common systems for cable redundancy are dual cabling or ring closure.

Framework data

The following framework data characterise the concept for realising 1 of 2 control redundancy presented in this document:

1. Control System
 - Two identically equipped Beckhoff IPC systems operate an EtherCAT field level.
 - The controllers are installed separately from each other in a protected zone.
 - The controllers are equivalent, there is no prioritisation. If the current active control system fails, the passive control system tries to take over the field level.
 - The identical TwinCAT PLC project under TwinCAT version 2.11 runs on both systems.
2. Communication
 - If possible, the two control systems exchange process data with each other. This exchange is configured by the user. TCP-based 100 Mbit EtherCAT master-master communication and TwinCAT ADS are used as exchange channel.
 - The two IPCs are connected with the EtherCAT field via suitable Ethernet switches.
 - The cable redundancy is single-error tolerant. Due to the cable redundancy, two Ethernet ports are occupied on both IPCs.
3. Switching over
 - The switchover and takeover through the backup computer takes place automatically once an invalid state has been detected.

Application Note DK9322-0809-0004

EtherCAT Master Redundancy

- A switching time of < 1 second is achieved.
4. I/O field
- The handover of the field level is jerky, since at least the watchdog in the output modules necessitates a reset of the EtherCAT devices (INIT --> OP).
 - Only EtherCAT slaves without distributed clock functionality are used.
 - No safety modules are used.

Implementation

1. Regular operation

During normal operation, control master 1 (M1) operates the field level. The cable redundancy path is closed. If this path is interrupted at one point, continuous transfer of EtherCAT datagrams on both sides ensures continuous communication to all slaves. Controls M1 and M2 exchange information to ensure sound operation of the two controllers. In addition, controller M1 sends the current process data to controller M2 based on user configuration, e.g. through application of a publisher/subscriber procedure based on real-time Ethernet or EtherCAT master-master communication. As long as controller M1 operates error-free, it communicates the process data of the field level. The EtherCAT master is in OP state. Meanwhile controller M2 keeps its master in INIT state in order to prevent it sending data actively. Both TwinCAT PLCs are in RUN state.

2. Initiating events

The switchover is triggered by one of the following events:

- A. Through initiation by the software (demo)
- B. The active controller loses the connection to real-time Ethernet.
- C. Both EtherCAT connections of the active controller are disconnected.

3. Switching to backup control

The switchover from the control system to the backup system takes place according to the following sequence:

- The EtherCAT master of the active controller M1 switches to INIT state, thereby indicating that it is inactive.
- When the passive controller M2 no longer receives signs of life from M1 or detects its reported inactivity, the EtherCAT master for controller M2 is set to OP state and M2 becomes active.
 - A prerequisite for the switchover is that both masters are not affected by the same fault.
- Depending on the chosen time limits for fault detection and the size of EtherCAT network, the handover takes place in < 1 second.

Application Note DK9322-0809-0004

EtherCAT Master Redundancy

Notes

The control redundancy concept with EtherCAT master-master communication, which can, in principle, be extended to 1 of N control redundancy, is subject to restrictions:

The switches used must not impair the real-time characteristics of the network. Distributed clock functionality is not available with this redundancy concept. The EtherCAT connections between controller and switch must not be at risk of interruption, otherwise further measures are required.

Please be aware of this when configuring the control redundancy. If application of the technologies that are subject to restrictions is unavoidable, alternative topologies for realising a redundant control system are available on request.

EtherCAT www.beckhoff.com/EtherCAT

PLC and Motion Control on the PC www.beckhoff.com/TwinCAT

This publication contains statements about the suitability of our products for certain areas of application. These statements are based on typical features of our products. The examples shown in this publication are for demonstration purposes only. The information provided herein should not be regarded as specific operation characteristics. It is incumbent on the customer to check and decide whether a product is suitable for use in a particular application. We do not give any warranty that the source code which is made available with this publication is complete or accurate. This publication may be changed at any time without prior notice. No liability is assumed for errors and/or omissions. Our products are described in detail in our data sheets and documentations. Product-specific warnings and cautions must be observed. For the latest version of our data sheets and documentations please visit our website (www.beckhoff.com).

© Beckhoff Automation GmbH, August 2009

The reproduction, distribution and utilisation of this document as well as the communication of its contents to others without express authorisation is prohibited. Offenders will be held liable for the payment of damages. All rights reserved in the event of the grant of a patent, utility model or design.