|  |  |
| --- | --- |
|  |  |

**CHRONOS**

|  |  |
| --- | --- |
| |  | | --- | |  | |

|  |  |
| --- | --- |
| Machine Safety Analysis - Server | |
| Deliverable No. | D5.1 |
| Date | 2017-08-09 |
| Status: (F: Final, D:Draft) | D |

Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Paragraphs affected | Change information |
| 0.1 | 2016-10-25 | All | New Document |
| 0.2 | 2017-08-09 | All | Here and there |

Authors

|  |  |  |
| --- | --- | --- |
| Name | Company | Chapters |
| Karl-Johan Ode | AZ | All |
| Henrik Eriksson | SP | All |
|  |  |  |
|  |  |  |

Introduction

The CHRONOS test system consists of one or several CHRONOS servers controlling one or several CHRONOS-compatible objects. This could be on the same test area or different test areas at the same time. Malfunctioning hardware and/or software in the CHRONOS server or objects could cause severe injuries and even fatalities. A CHRONOS test system is a kind of machine, and standards related to machine safety becomes applicable. This report goes through applicable safety standards and performs a preliminary safety analysis based on fault trees.

Scope

This document presents a preliminary safety analysis of the CHRONOS architecture with a focus on the server and its interfaces (and communicated messages) to the controlled objects. Standalone, the server does not constitute any risk. However, the controlled objects can represent a serious risk to personal safety.

Table of contents

[Revision history 2](#_Toc490065467)

[Authors 2](#_Toc490065468)

[Introduction 3](#_Toc490065469)

[Scope 4](#_Toc490065470)

[Table of contents 5](#_Toc490065471)

[1. Terms and Abbreviations 6](#_Toc490065472)

[2. Applicable Standards 7](#_Toc490065473)

[3. Server Scope 8](#_Toc490065474)

[4. Hazard Assessment and Risk Analysis 9](#_Toc490065475)

[4.1. Risk Analysis 12](#_Toc490065476)

[4.2. Safety Mechanisms 13](#_Toc490065477)

# Terms and Abbreviations

FTA Fault tree analysis

HAZOP Hazard and operability

IP Internet protocol

TCP Transmission control protocol

UDP User datagram protocol

# Applicable Standards

The following standards are relevant with respect to machine safety and CHRONOS:

* **AFS 2008:3**, Maskiner, Arbetsmiljöverkets föreskrifter om maskiner samt allmänna råd om tillämpningen av föreskrifterna
* **SS-EN ISO 12100:2010**, Safety of machinery – General Principles for Design – Risk assessment and risk reduction
* **SIS-ISO/TR 14121-2:2012**, Safety of machinery – Risk assessment – Part 2: Practical guidance and example of methods
* **SS-EN ISO 13849-1:2016**, Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design
* **IEC 61882:2016**, Hazard and operability studies (HAZOP studies) - Application guide
* **IEC 61025:2006** Fault tree analysis (FTA)
* **SS-EN 61800-5-2**, Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional
* **SS-EN 61784-3**, Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions

# Server Scope

This preliminary safety analysis focuses on the communication interface between the server and the object(s), and especially the messages which are communicated on the two channels: safety (periodic) and control (event). The preliminary safety analysis makes no assumption on the communication media (but it is wireless), but the safety channel uses UDP/IP protocol and the control channel TCP/IP protocol. Default ports are 53240 for UDP and 53241 for TCP, respectively.

|  |
| --- |
|  |
| Figure 1 Typical server-object communication during a simple test |

# Hazard Assessment and Risk Analysis

The preliminary risk analysis will focus on the communication between server and objects. It is assumed that no safety mechanisms are present, and that only one failure is present at the same time. It is assumed that the downlink has the following messages:

* Object Setting Message (OSEM)
  + Contains coordinate system (origin and x axis angle) and correction data source
* Dynamic Object Path Message (DOPM)
  + Contains the trajectory for one object
* Start (STRT)
  + Starts the test now or at a future point in time
* Stop (STOP)
  + Stops the test

and the uplink has the following:

* Monitor (MONR)
  + Contains monitor data (llh, hdg, and vel) for visualization

The server cannot be dangerous by itself, but when controlling a heavy or fast moving object, the server-object combination can be dangerous. It is assumed that persons can be in the vicinity of the object without any preventing barrier in between.

Then the following hazardous events from ISO 12100 become applicable:

* Failure to stop moving parts
* Uncontrolled movements (excluding unintended/unexpected start-up)
* Unintended/unexpected start-up

A failure to stop can occur during a test when the object(s) are following its drive file and the operator actively wants to end the test before the drive file is completed or when the object(s) have reached the end of their drive files.

|  |
| --- |
|  |
| Fig 2. Fault-tree for failure to stop |

As can be seen from the fault tree above, a failure to stop can be caused by:

1. Failure in the stop message (e.g. omission)
2. DOPM failure (e.g. the drive file does not end at zero speed)
3. Object controller failure (software or hardware)

Uncontrolled movements occur while a test its running and the object(s) start(s) to deviate too much from the intended paths in the corresponding drive files.

|  |
| --- |
|  |
| Fig 3. Fault-tree for uncontrolled movements |

Uncontrolled movements can be caused by:

1. OSEM failure (e.g. origin configuration error)
2. DOPM failure (e.g. corrupted drive file)
3. Object controller failure (e.g. positioning error)

Unexpected start occurs when the object(s) are stationary and starts to move (following its drive file or in random direction) without a corresponding start signal.

|  |
| --- |
|  |
| Fig 4. Fault-tree for unintended/unexpected start-up |

## Risk Analysis

The risk analysis to determine the required performance level for the three hazardous events above is performed according to Annex A in ISO 13849-1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Event** | **Severity of injury** | **Frequency and/or exposure to hazard** | **Possibility of avoiding hazard or limiting harm** | **Required performance level** |
| Failure to stop | S2 | F1 | P2 | d |
| Uncontrolled movements | S2 | F1 | P2 | d |
| Unintended start-up | S2 | F2 | P2 | e |

## Safety Mechanisms

In order to remove single-points of failure and to introduce redundancy, the following safety mechanisms are introduced.

To prevent all three failures:

* Emergency stop functionality based on heartbeat

To prevent uncontrolled movements and unintended start-up:

* Supervision functionality in the server
  + Needs monitor (MONR) messages from the objects
  + Checks that objects are sufficiently close to their trajectories
  + Check that objects are sufficiently separated
  + Checks that objects do not enter forbidden areas

To prevent unintended start-up:

* Arm function (objects need to be in armed state before they accept to start)

|  |
| --- |
|  |
| Fig 5. Fault-tree for failure to stop |

|  |
| --- |
|  |
| Fig 6. Updated fault-tree for uncontrolled movements |

|  |
| --- |
|  |
| Fig 7. Updated fault-tree for unintended/unexpected start-up |