A CONFIGURABLE INTERLOCK SYSTEM FOR RF STATIONS AT XFEL

M. Penno, W. Köhler, H. Leich, B. Petrosyan, G. Trowitzsch, R. Wenndorff, DESY, Zeuthen Site, Germany
S. Choroba[2], T. Grevsmühl[2], DESY, Hamburg Site, Germany

Abstract

The interlock system has to prevent any damage from the cost expensive components of a RF station. The system monitors various system components, collects and processes status information in realtime and reports actual status to the control system. The system is based on self diagnostic and repair strategies to obtain maximum reliability and maximum time of operation. It incorporates a controller and slave modules that perform the I/O operation. The interlock logic is implemented in hardware and operates independent from the software running on the controller. The software accomplishes the hardware selftest after system startup. Further applications provide communication interfaces over Ethernet used by administration and the control system. A runtime software integrity selftest strategy has been implemented for high reliability. It covers detection of stack overflows, thread deadlocks, memory corruption and is able to recover the system without interrupting interlock operation. The interlock system performs well its task at FLASH (DESY, Hamburg Site) and at PITZ (DESY, Zeuthen Site).

INTRODUCTION

The XFEL is a linear accelerator for electrons that get accelerated by superconducting cavities located in the accelerator tunnel under the ground. The RF-power required by these cavities is generated at 27 RF-stations. Each RF-station generates RF-pulses with max. 1.7ms duration and a repetition rate up to 10Hz. Each station feeds 32 cavities at four accelerator modules. A RF-station consists of a 10 MW klystron, a pulse transformer, a special pulse cable of up to 1.7km, a pulsed high voltage power supply (Modulator), a low level RF system, auxiliary power supplies and an interlock system.

The main task of this interlock system is the protection of the cost expensive components of the RF-station and to guarantee reliable and safe operation. In addition it provides slow control functions for the subsystems. Since the interlock system will be installed in the accelerator tunnel (no access during beam operation) the interlock system has to provide monitoring functions, which ease the localization of failures remotely. In addition all monitored signals are communicated to the accelerator's main control system, where correlations between accelerator and RF station operation can be determined. Because of the modular concept, service personnel are able to exchange malfunctioning interlock modules without replacing the complete system during scheduled maintenance time.

INTERLOCK REQUIREMENTS

The Interlock-System has to deal with these types of errors:

Table 1: Interlock Error Types

Hardware Failures	non-reversible malfunctions like broken cables, damaged contacts, dead sensors, etc.
Soft Errors	e.g. sparks in the klystron or the wave guide system, temperature above a threshold, missing or low water flow, etc.

Thus, dealing with real hardware error sources, at the same time the Interlock-System must be as robust and reliable as it operates in a noisy environment with transient noise produced by the RF-Station itself (caused by the pulsed power operation). Errors should be treated with two types of thresholds and channel masking:

- Absolute max./min. thresholds: any violation of these thresholds will force the shutdown of one or more subsystems of the RF station.
- Programmable (soft) thresholds: a violation of these conditions will generate an alarm message to the Control System. Soft thresholds are only available for analog input channels.

To collect the error information from the components of the RF-Station, the Interlock-System has to handle different input signal types, detect error conditions and react appropriately by generating several output signals that can block the operation of the RF-Station.

Table 2: Input types of the Interlock System

Analog Inputs	Voltage (0-10V), Current (4-20mA), PT100 Sensors Using Min/Max thresholds, violation will produce an error signal
Digital Inputs	Relays Contact, Logical Voltage Signal (0-24V) Open contact or "Low level" results into an error signal
Light Input	Fast input over LWL cable "No light" results into an error signal

Most of the input signals have a masking function implemented, which allows the exclusion of the channel from interlock functions. But for some critical inputs, the

masking function is disabled. All mask configurations are protected by a password-secured access mechanism. Mask operations must cause an entry into the log file. Another important requirement is the continuously reliably and safe operation of the interlock system, independent of any software failure.

INTERLOCK HARDWARE

The interlock electronic is housed in a 19" 4U crate with a dedicated backplane optimized to the application. The interlock system consists of one controller and up to 20 Slave I/O-modules. Signal cables from the RF station are connected via distribution panels to the interlock system to have easy access to all signal cables and make it possible to quickly exchange modules.

A 3U CompactPCI-like board format with two 5-row connectors is used. All modules communicate over the backplane that provides separate bus systems for interlock status information and module access under software control.

Figure 1: Interlock Controller and Slave Modules

INTERLOCK CONTROLLER BOARD

The interlock controller board (Figure 1, left bottom side) manages the interlock system and processes all interlock signals. An ALTERA FPGA, a Cyclone II EP2C35F484 device is used on the controller to implement the following functions:

- logical interlock function for components of the RF station is based on signals preprocessed within the different I/O slave modules
- interlock signal mask function
- NIOS-II processor to configure and manage the interlock system
- interface to the DOOCS control system via Ethernet
- configuration of the I/O slave modules in the crate
- slow control functions
- system check after power up

It is important to mention that the interlock functionality inside the FPGA is strictly separated from the software running on the NIOS-II CPU. The interlock will always work independently from the state of the CPU and any software error.

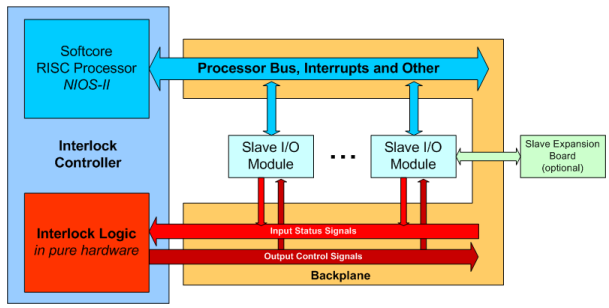

Figure 2: Basic Interlock Architecture

The strict separation is done by using independent bus systems for processing the interlock logic and register access via the processor. A hardware lock mechanism disables write access to sensitive registers (e.g. filter constants, thresholds, etc.) after the interlock system has been configured and starts normal operation.

Every module of the Interlock Systems has its own unique identification and a firmware revision number. The system detects hardware changes and firmware upgrades automatically after restart and will not give clearance until the interlock administrator has acknowledged the hardware changes.

INTERLOCK SOFTWARE

The interlock software is running on a 32Bit NIOS2 soft-core processor. It performs several tasks during boot up, configures the system and establishes the connection to the control system. One primary task is to perform the system hardware test and detect hardware changes and errors. A complete backplane test is performed, address conflicts are tested and module firmware compatibility is checked. On success, the software gives clearance to the interlock system and puts it into normal operation. Then, the software starts the communication services for connection to the control system and starts additional network services for remote administration and diagnostics. For a maximum reliability, it is important that the interlock continues with normal operation, even in a case of a software crash. A hardware watchdog has been implemented, that automatically restarts the software in case of a crash. In addition, a dedicated software process monitors the health status of the software sub systems. It detects stack overflows, memory misallocation, the manipulation of read-only data and it automatically detects inactive hanging processes. In case of a fault the software generates a report and restarts itself automatically. All hardware registers of the interlock system are write-protected during normal operation. Only some special registers can be written by using a dedicated hardware lock/unlock mechanism. All registers will not loose there content during a software reboot, thus the software is always able to recover the actual state of the interlock system and continues operation.

Administration

The Interlock administrative functions are accessible over the http server. Access is limited to authorized persons by checking username, password and IP address. The administrative interface allows the user to view actual signal status, to edit interlock-signal masks, to set thresholds of analog inputs (e.g. temperatures, flow) and it gives access to slow control functions. Several other configuration options are accessible.

The interlock system supports remote firmware updates for the controller and every slave module. An expert tool is used to upload new firmware remotely over network to the interlock system. The flash-process on the interlock system is able to update the firmware of all slave modules simultaneously and this reduces the time of a full-system firmware update. Firmware updates only get into effect after a complete hardware reset and do not affect the running interlock operation.

Communication Interface

The interface that communicates with the control system (DOOCS) operates the multi platform protocol "Network Queue", developed at DESY. The protocol uses UDP Packets and has implemented a hand shaking mechanism that is able to detect packet losses. Thus, the protocol benefits from the flexibility of UDP but also has the ability to detect data losses. Other advantages are automatic conversion of platform dependent data types, storage of type information and guaranteed backward compatibility. The protocol has been designed for peer to peer communication and supports IP address binding.

INTERLOCK SIGNAL MANAGEMENT

The Interlock System is able to handle many hundreds of signals. For example, the interlock used for the electron-gun at PITZ is processing up to 270 different signals.

All interlock signals are specified and collected in a signal list that contains the name, the type, the corresponding slave module and channel, filter constants, and many more information for each signal. Also, the list contains all interlock actions that have to be operated in case of a failure. The signal list is used to automatically generate several other configuration files for the interlock software and the control system. It is also used to generate the pure interlock logic as VHDL code, which is used by the interlock controller.

RESULTS

Two full featured interlock systems are actually in use at DESY in Hamburg at the Klystron Teststand. Two interlock systems are in use at DESY in Zeuthen for PITZ at the RF-Stations and another has been adapted to be used for the electron-gun at PITZ. Two further systems are planned to be used at the Modulator test Facility in Zeuthen.

The Interlock Systems are working very well and fulfil our expectations. The automation of the processing of the signal list eases the adaptation of the technical interlock system to new situations and other environments. We are planning to develop an automated test system for interlock-modules for quick validation and a short setup process.

REFERENCES

[1] TESLA Technical Design Report, DESY TESLA-2001-011, 2001

[2] S. Choroba, T. Grevsmühl, H. Leich, S. Simrock, "The TTF2 / XFEL Klystron Interlock: Requirements and Implementation"

[3] H. Leich, "Architektur eines Interlock-Systems für TTF2/XFEL", Bericht der Frühjahrstagung 2004 der SEI, ISSN 0936-0891, S.12 – 27

[4] TINE (Three-fold Integrated Networking Environment), http://desyntwww.desy.de/tine

[5] Micrimm Technologies Corporation http://www.ucos-ii.com/

[6] Altera Corporation, http://www.altera.com