IMPLEMENTATION OF A PERSONNEL SAFETY INTERLOCK SYSTEM BASED ON REPROGRAMMABLE I/O HARDWARE

S. Horn, B. Kuner, R. Lange, I. Müller, J. Rahn, H. Rüdiger, BESSY, Berlin, Germany
G. v. Egan, EuKontroll, Berlin, Germany

Abstract

The Personnel Safety Interlock (PSI) at BESSY controls the access to restricted areas inside the storage ring building and interrupts the machine operation when unallowed access occures. The system has to prevent any damage to human beings due to machine operation and is prescribed by German law. The digital I/O hardware of the BESSY modular I/O system (used to interface the bulk of BESSY devices) includes a freely reprogrammable logic stage. This key feature provides the functionality needed to design interlock systems using solely the standard digital I/O set. In combination with the BESSY embedded controller concept and the CAN field bus this implementation fits perfectly into BESSY's field bus based control system concept and is a full alternative to a PLC based system.

1 INTRODUCTION

The 3rd generation synchrotron light source BESSY II consists of a microtron-fed booster synchrotron and an electron storage ring. Both subsystems have to be independently operable and therefore each machine needs its own independent personnel safety interlock system (PSI). Due to the architecture of the storage ring building the PSIs have to observe thirteen restricted areas. Additionally the booster tunnel and the storage ring tunnel need a temporary access facility to enable secure access to the tunnels without breaking the interlock. The PSI status information has to be available to the operator in the central control room and to the control system. In "unsecure" state the PSI blocks the operation of the microtron, synchrotron and the storage ring. Therefore the PSI is of prime importance for running the BESSY II light source and has to be highly available.

2 DESIGN GOALS

The effort needed to support the BESSY control system is minimized by attaching as many different hardware types as possible using only a few different I/O hardware types. The basic concept of the BESSY I/O system, the combination of a small set of I/O hardware with the CAN field bus, has already been shown [2] [1]. The I/O hardware set includes all needed components to interface almost all BESSY devices to the control system. The convincing experiences with the flexibility and robustness of the BESSY modular I/O system suggested using this I/O system in even more complex applications like the PSI systems. Keeping this in mind the following design goals had to be fulfilled:

- Design Goals
  - two independent PSI systems (synchrotron, storage ring)
  - PSI must be in secure state even if local controller breaks
  - audio message system to inform the BESSY personnel about changes in the state of the PSI systems
  - stand-alone status display in the central control room to show the operator all important information (must be independent of the control system)
  - all status information available for the control system (read-only)
  - CAN field bus for control system connection
  - local embedded controller to support a convenient handling of the PSI
  - use the BESSY modular I/O system infrastructure whereever reasonable

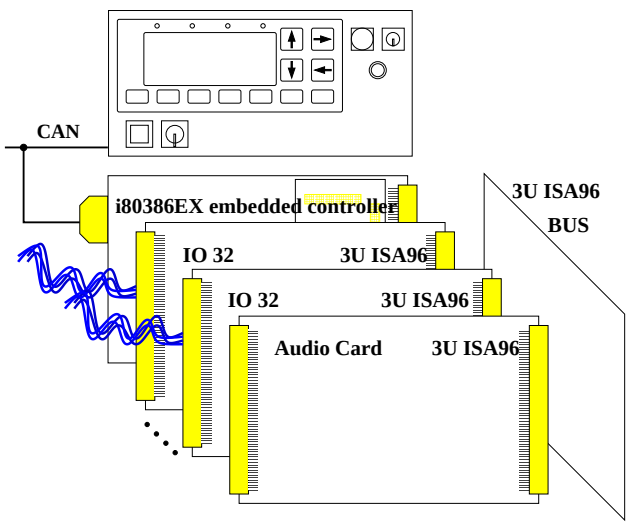

Figure 1: Sketch of PSI Crate

3 IMPLEMENTATION

Design and implementation of the PSI systems has been done in collaboration with the EuKontroll company (Berlin).
A closer look at the BESSY modular I/O system showed

that most of the design goals are reachable using the standard digital I/O cards in combination with the BESSY embedded controller concept [2] and the CAN field bus. Adding an audio card was the only thing needed to implement a small additional messaging facility.
The PSI functionality splits into two major parts, the non safety relevant and the safety relevant part. The non safety relevant functions are implemented in software. The framework for this software is built from the BESSY libraries [3] [1] for the embedded controller including the CAN bus communication. The PSI specific modules are added using the C programming language.

3.1 Hardware Architecture

The PSI systems are implemented as 3U crates with an ISA96 BUS as shown in figure 1. These crates typically consist of an i80386EX embedded controller with CAN field bus, a set of digital I/O cards and an audio card. The control room status terminal is realized using an industrial CAN bus terminal. Additionally the PSI is connected to the control system via the CAN bus.

3.2 Used I/O Hardware

The block diagram in figure 2 shows the functionality of the BESSY digital I/O cards. The most important part for the PSI implementation is the Programmable Logic Array (PLA) unit, a freely programmable logic chip with register facilites. These features of the PLA allow implementing state machines as hardware logic.

3.3 Overall Architecture

Figure 3 shows the implementation principle of the BESSY PSI system. The left column contains the functionality implemented as software on the embedded controller. The functionality of the middle column is implemented by programming the PLAs on the I/O cards.

The main task of the software is to support the area scan procedure. This procedure ensures that no person remains in a restricted area after that area has been scanned by the operator.
The software controls the complex but non safety relevant functions of the PSI system. The software state machines (SSM) enforcing the area scan procedures are implemented as software modules on the embedded controller. Additionally the software controls the output of audio messages (using the local audio card) as well as the control room status display and the transfer of status information to the control system (using the CAN field bus).

Programmed into the I/O cards' PLA chips are the less complex but safety relevant hardware state machines (HSM) that build the area interlocks and the global summation logic (the logic for a sample area is shown in figure 4). The I/O lines of the digital cards are used to control the PSI equipment (door switches, buttons etc.) and to provide

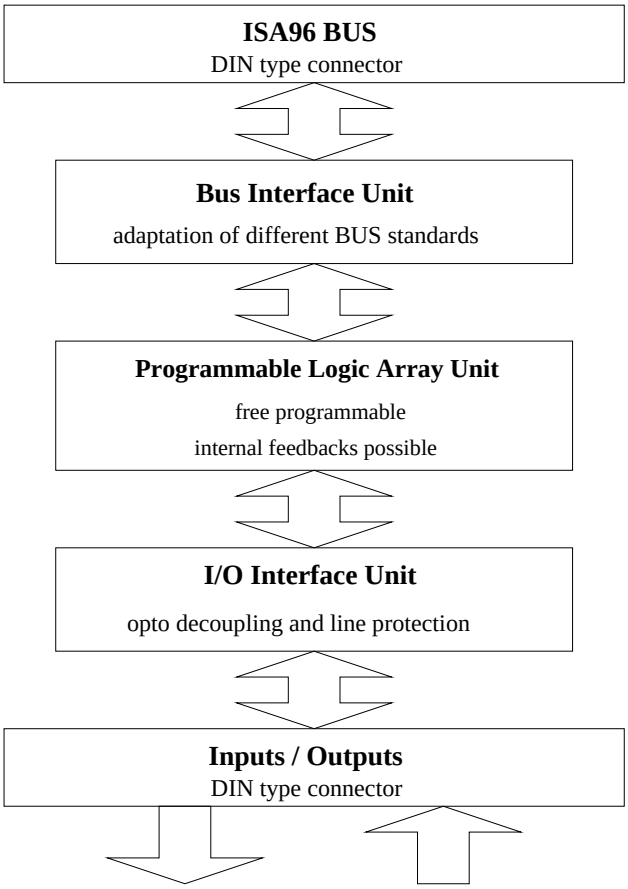

Figure 2: Block Diagram of a Digital I/O Card

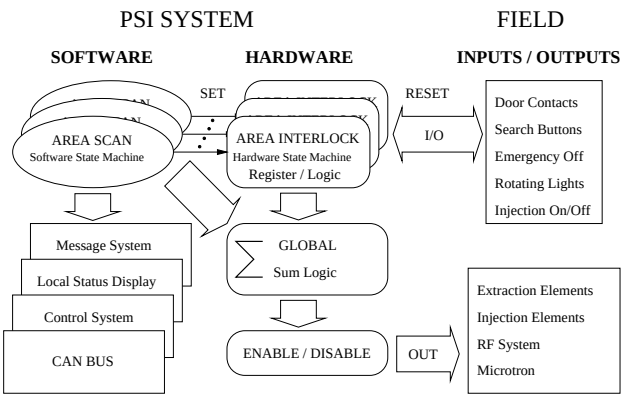

Figure 3: PSI System Block Diagram

the interlock signals for the external hardware (extraction, injection, rf, microtron etc.).

If a scan of a certain area is completed correctly, the SSM generates output signals to the corresponding hardware logic that reflect the state of the SSM.
These output signals directly affect the HSM on the I/O cards. Setting the registers of a certain HSM means that the corresponding area is scanned correctly and the interlock of this area is set.
Direct I/O lines (reflecting the state of door contacts, emer-

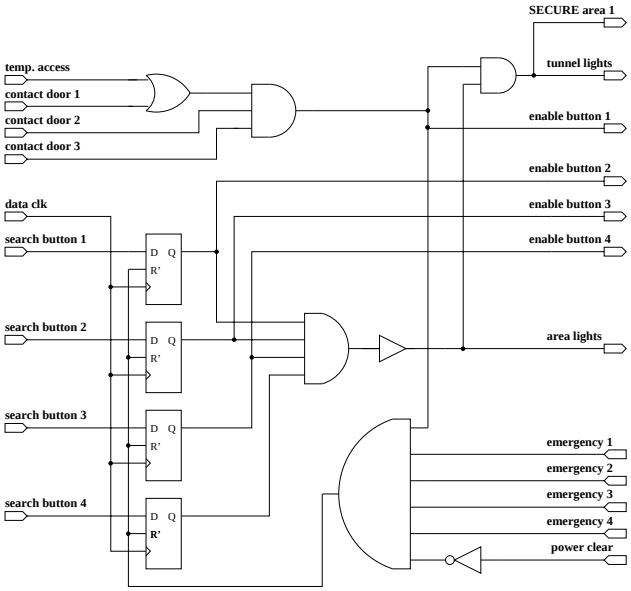

Figure 4: Sample Hardware State Machine (HSM) for One Area

gency buttons etc.) from the field affect the reset logic of the corresponding HSM. These reset inputs are of highest priority: they overwrite any set action from the corresponding SSM. The result is a "break" of the interlock.
If all areas of a PSI system are in safe state, the sum logic generates the interlock output signals which enable the corresponding external hardware.
In case of a malfunctional embedded controller we have to distinguish between two different scenarios:

- PSI is in safe state, external hardware enabled
  - PSI remains in safe state and external hardware remains enabled
  - safety guaranteed by the HSM of I/O cards
  - HSM breaks interlock if unallowed condition occures
  - PSI disables external hardware
- PSI is in reset state, external hardware disabled
  - this is already the safe situation

This means that an embedded controller failure does not affect the safety of the PSI — the PSI stays active and the operation of the machine will be not interrupted. System repair may be delayed until the next maintenance period and there is no unnecessary interruption of the machine run.

4 CONCLUSIONS

This fairly complex, safety relevant application shows that a flexible I/O system is usable and reasonable for applications that are commonly implemented with PLCs. The programmable parts of the I/O hardware provide the features needed for a system that is reliable and secure even in the case of a local controller failure.
Implementation by external companies is easily possible and supported by the software framework. Smooth integration into the existing infrastructure is guaranteed. No additional support lines are introduced, which keeps down the maintenance effort for the whole system.

5 REFERENCES

[1] J. Bergl, B. Kuner, R. Lange, I. Müller, G. Pfeiffer, J. Rahn, H. Rüdiger, "CAN: a Smart I/O System for Accelerator Controls – Chances and Perspectives", ICALEPCS'97, Bejing 1997, China.

[2] J. Bergl, B. Kuner, R. Lange, I. Müller, R. Müller, G. Pfeiffer, J. Rahn, H. Rüdiger, "Embedded Controller, Field Bus and a Modular I/O Concept: Central elements of BESSY II Controls", PAC'97, Vancouver 1997, Canada.

[3] J. Bergl, B. Kuner, R. Lange, I. Müller, R. Müller, G. Pfeiffer, J. Rahn, H. Rüdiger, "Controller Area Network (CAN) – a Field Bus Gives Access to the Bulk of BESSY II Devices", ICALEPCS'95, Chicago 1995, USA.