IMPLEMENTATION OF CONTROL LOGIC FOR MITIGATING SYSTEMS IN DISTRIBUTED CONTROL SYSTEM

S. Narisetty-Gupta, A. Xing, J. Harber
Atomic Energy of Canada Limited
2251 Speakman Drive, Mississauga, ON, Canada, L5K 1B2

Abstract

The ADVANCED CANDU REACTOR® (ACR-1000®) uses a distributed control system (DCS) to perform control and monitoring tasks. This paper briefly describes the control system architecture and presents the conceptual implementation strategy for the control logic for three ACR-1000 systems (heat transport system pumps, second crash cooldown system and reserve water system) in the essential control sub-system (ECSS). The paper also goes on to define the basis for the implementation strategies for each system.

1. Introduction

Computers have been used successfully in CANDU[1] nuclear reactors for the last 40 years to perform protection system actions and monitoring, periodic equipment testing, load following, refueling management etc. They started out as the simple digital computer controllers (DCCs) which were used to perform data acquisition, overall plant control and to provide an operator interface. Now the ADVANCED CANDU REACTOR[2] (ACR-1000), the next generation CANDU reactor, will employ a DCS. The DCS is more reliable, has more computing power and is more flexible than the DCCs. One of the advantages of having a more powerful computer for implementing the control logic for systems is that most of the logic can be computerized which results in less use of hardwired logic hence less number of physical components.

The DCS is divided into two independent subsystems, namely the plant control sub-system (PCSS) and ECSS. The PCSS is further divided into functionally independent partitions and the ECSS is sub-divided into the group 1 ECSS partition and group 2 ECSS partition. A partition is a set of processors and/or hardwired controllers that are dedicated to a particular set of control functions and have some form of independence from components belonging to another partition. The group 1 ECSS partition is comprised of four channelized controllers and associated inputs and outputs (I/O). The group 2 ECSS partition is comprised of two controllers and associated I/O. The ECSS is a Class 2 programmable electronic system. It is used to implement all the essential functions that are not provided by the safety systems, such as those from the safety support and mitigating systems. The PCSS is a Class 3 programmable electronic system. Figure 1 illustrates the basic DCS architecture for the ACR-1000 reactor. More details on the control system architecture can be found in reference [1].

[1] CANDU is a registered trademark of Atomic Energy of Canada Limited (AECL)
[2] ADVANCED CANDU REACTOR (ACR-1000) is a registered trademark of AECL

All instrumentation and control functions are categorized in terms of their safety significance and termed as either category A, B, C or D functions. Class 1 control systems are used to implement category A and lower functions, Class 2 systems for category B and lower functions and Class 3 for category C functions.

This paper will focus on implementing the control logic for systems in the ECSS group 2 controllers. In the ACR-1000 plant, stepback, second crash cooldown, reserve water system, degasser condenser isolation, pressurizer overpressure protection and post accident monitoring are some of the Category B functions that are implemented in the ECSS group 2 partition. This paper will discuss the design decisions that were made while mapping the control logic for the heat transport system (HTS) pumps, second crash cooldown (SCC) system and reserve water system (RWS) to the ECSS group 2 controllers. These three systems are mitigating systems that have been determined (as per [2]) to perform safety functions that warrant the use of a Class 2 control system. The HTS, SCC system and RWS are relatively complex systems that perform Category B functions. Therefore, the options discussed in this paper also apply to other control functions that are implemented in the ECSS group 2 partition.

2. Heat transport system

2.1 HT pump configuration

In the ACR-1000 HTS, four HT pumps circulate coolant through the HTS to remove heat from the fuel. Each HT pump motor is equipped with its jacking oil system. This supplies high pressure oil to the motor thrust bearing during start-up thus reducing friction torque, and providing lubrication in the period before the motor is rotating sufficiently fast for self lubrication.

2.2 HTS pump control

The HT pump control consists of control logic for starting and stopping the HT pumps, the jacking oil pumps and the motor heaters. In addition, it also includes logic for tripping the pumps on low HTS pressure or high upthrust bearing temperature conditional on the reactor power being below a predetermined setpoint. Manual trips of the HT pumps are allowed. HT pump trips by electrical protection are not included as part of the control logic to be implemented in the ECSS. An HT pump is tripped by its electrical protection when electrical faults and/or motor overload conditions are detected. An example of this is a pump trip on high stator winding temperature. An overview diagram of the HT pump control logic is provided in Figure 2. A flow diagram of the HTS along with the HT pumps is shown in Figure 3.

2.3 Implementation concept

The entire HT pump control logic is implemented in the ECSS group 2 controllers. Both controllers run the same logic and the outputs from the two controllers are voted in a manner as shown in Figure 4. Each controller drives two trip digital outputs (DOs) for each HT pump. The two DOs from controller #1 are ORed and ANDed with the ORed result from controller #2. Effectively, this can be viewed as a one-out-of-two twice

voting strategy. This strategy is shown in Figure 4. This strategy reduces the occurrence of spurious trips and increases the reliability of the control system logic.

2.4 Rationale for implementation

The HTS pump control logic could have been divided into two parts (HT pump control and HT pump trip) with the former (having less strict requirements) implemented using the PCSS and the latter (with the more strict requirements) implemented using the ECSS. However, this would require communication between the PCSS and ECSS when no network link is present between the two as shown in Figure 1. To add to this, the logic for the two parts is simple and closely coupled. So it was decided to implement both the parts of the logic in the ECSS.

Another option was to implement the control logic for two of the HT pumps in ECSS group 2 controller #1 and for the remaining two pumps in the second controller. However, this would also require communication between the two controllers (when no network link is present) and would require part of the logic to be hardwired (which is being minimized in the ACR-1000 design). Thus it was decided to implement the entire HTS pump control logic in ECSS group 2 controller #1 and duplicate the logic in ECSS group 2 controller #2. As indicated earlier, the outputs from both the controllers are voted in a manner to reduce the occurrence of spurious trips and to increase the reliability of the control system logic. A simple voting strategy would have either ORed or ANDed the single outputs from the individual controllers. However, when the outputs are ORed, the probability of failure on demand decreases at the expense of an increase in the probability of spurious failures. On the other hand, if the outputs are ANDed, the probability of spurious failures decreases but the probability of failure on demand increases. Both the goals are achieved by having redundant digital outputs from each controller (to increase reliability) and then performing an AND operation on the final voted outputs from each controller to decrease the occurrence of spurious trips.

3. Second crash cooldown system

3.1 SCC system description

The SCC system provides an additional line of defence for mitigating both primary and secondary side HTS events. The SCC system is used as a back-up to the first crash cooldown (i.e., emergency coolant injection (ECI)) signal for primary side events and used to automatically depressurize the steam generators (SGs) for both primary and secondary side events.

For primary side events, the SCC system generates the SCC primary side (SCC-P) signal, which actuates many of the same components as the ECI system, to configure the long term cooling system in long-term recovery mode and initiate depressurization of the HTS using the power operated relief valves. For secondary side events, the SCC system generates the SCC secondary side (SCC-S) signal to depressurize the SGs using the power operated relief valves and initiate the components of the RWS to provide back up feedwater to the SGs. It caters for total loss of feedwater (main, start-up, and emergency feedwater) or station blackout events.

3.2 SCS system control logic

The SCC system generates two signals, namely the SCC-P signal and the SCC-S signal. The SCC-P signal is a backup to the ECI signal, which is generated on detection of loss of coolant accidents and the SCC-S signal is generated on detection of total loss of feedwater to initiate backup feedwater supply to the SGs. Provision is made to reduce the HTS low-pressure setpoint during reactor shutdown to prevent spurious generation of the SCC-P signal. Provision is also made to block the SCC-P and SCC-S signals when HTS is cooled below 100 ºC and is depressurized. An overview diagram of the SCC system control logic is provided in Figure 5.

3.3 Implementation concept

Similar to the HTS pump control logic, the entire SCC system logic is implemented in ECSS group 2 controller #1 and duplicated in controller #2. The outputs from the controllers are voted to actuate the end devices.

3.4 Rationale for implementation

Based on the initiating parameters, a single signal is generated to actuate a number of end devices. These end devices are not redundant. So there is no logical split between the devices being actuated hence it was sensible to keep the logic for the entire system in one controller and duplicate it in the other ECSS group 2 controller for reliability.

4. Reserve water system

4.1 Reserve water system description

The RWS is designed to store demineralized water and deliver water by gravity to several user systems such as the HTS, SGs, moderator system, shield cooling system and the containment cooling spray system. It consists of a large tank and isolation valves connecting the tank to the user systems. These isolation valves are opened when supply from the RWS is required.

4.2 RWS control logic

During normal operation, the RWS is poised at all times to respond to an event for which the RWS injection is required. Supply to the reactor inlet headers (of the HTS) is initiated on detection of a loss of coolant accident. Valves connecting the RWS to the reactor inlet headers are opened during a loss of coolant accident and closed when a low level in the reserve water tank is detected to prevent air ingress into the HTS. Supply to the SGs is initiated upon detection of loss of main feedwater, startup feedwater and emergency feedwater to maintain the SGs as a heat sink. Valves connecting the RWS to the SGs are opened on a total loss of feedwater and closed on detection of a low level in the reserve water tank to prevent air ingress into the SGs. They are also closed on a high pressure or high radiation in the reactor building to prevent a containment bypass through the SGs and the main steam lines. Figure 6 provides an overview diagram of the RWS control logic. It shows the logic to open and close RWS valves connecting the reserve water tank to various user systems.

4.3 Implementation concept

The RWS control logic is divided between the two group 2 ECSS controllers. A diagram of the RWS and its components and how the control of these components is divided between the two ECSS group 2 controllers is shown in Figure 7.

4.4 Rationale for implementation

An implementation similar to that of the HT pump control logic and SCC system logic could have also been used for the RWS. However, the implementation discussed above makes full use of the independent controllers in group 2 ECSS. The logic is not duplicated in the two controllers. Instead it is divided between the two controllers in a manner such that loss of any of the two controllers does not affect the safety functions performed by the system. This is mainly achieved by having redundant paths for supply of the water from the reserve water tank to the user systems. For example, as seen in Figure 7, the RWS injection paths to reactor inlet headers 1 and 4 are redundant. The valves on one path can be controlled by controller 1 and valves on the redundant path can be controlled by controller 2. Similar reasoning can be applied for valves connecting the reserve water tank to reactor inlet headers 2 and 3. On loss of one controller, RWS supply is available to all reactor inlet headers. There are no redundant paths for RWS supply to the steam generators (SGs). From safety point of view, once the reactor is shut down, it is sufficient to cool one SG per HTS loop. SGs 1 and 2 are part of the same HTS loop and SGs 3 and 4 are part of the other HTS loop. So if the valves on the path to SGs 1 and 4 are controlled by controller 1 and those on the path to SGs 2 and 3 are controlled by controller 2, on loss of a controller, RWS supply is available to provide cooling to both HTS loops.

5. Conclusion

The control logic for the HTS pumps, SCC system and the RWS is specified for implementation in the ECSS group 2 controllers to fully exploit the benefits of the ECSS group 2 architecture and to achieve maximum reliability. Several options are available for implementing the control logic in the two ECSS group 2 controllers. This paper presents two options that were selected for use by the systems implemented in the group 2 ECSS partition. The first option duplicates the logic in both the controllers and votes the outputs in a manner that increases reliability and decreases the number of spurious trips or initiations. The second option splits the logic between the two controllers. Discussion of the first option is done via an example of HTS pump control logic and the SCC system logic and discussion of the second option is done via an example of the RWS control logic.

In the ACR-1000 plant design, two options are available to the control designers for implementing control functions in the ECSS group 2 partition. The designers will select the appropriate option based on the process redundancy of the systems they monitor and control. Process systems with less process redundancy will implement their control functions using the first option. Process systems with higher process redundancy will select the second option.

6. References

[1] Harber, J., et al., “Control System Architecture for a Modern Nuclear Power Plant”, IAEA Technical Meeting, Beijing, China, November 2008.

[2] International Electrotechnical Commission, Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Classification of Instrumentation and Control Functions, IEC 61226, 2005.

[3] International Electrotechnical Commission, Programmable Controllers Part 3: Programming Languages, IEC 61131-3, 2003.

[4] International Electrotechnical Commission, Nuclear Power Plants, Instrumentation and Control for Systems Important to Safety – General Requirements for Systems, IEC 61513, 2001.

[5] Harber, J., et al., “Documenting Control System Functionality for Digital Control Implementations,” IAEA Technical Meeting, Chatou, France, September 2005.

[6] Perras, J., et al., “Verifying Control Logic Specification Using Mathematical Modeling and Dynamic Simulations,” 2008 CNS Symposium on Simulation Methods in Nuclear Engineering, Ottawa, Canada, November 2008.

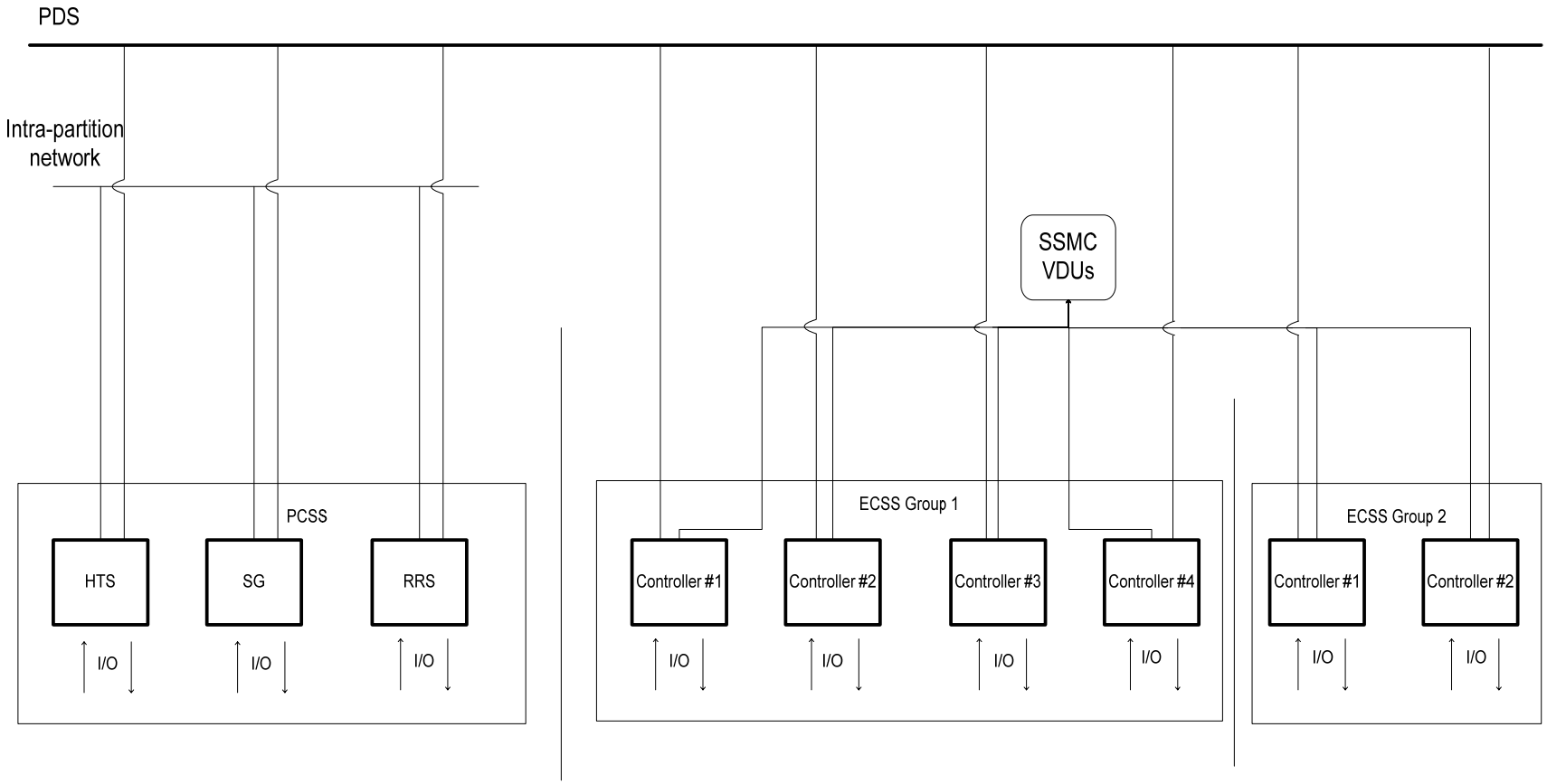

Figure 1: Overview of ACR-1000 DCS architecture

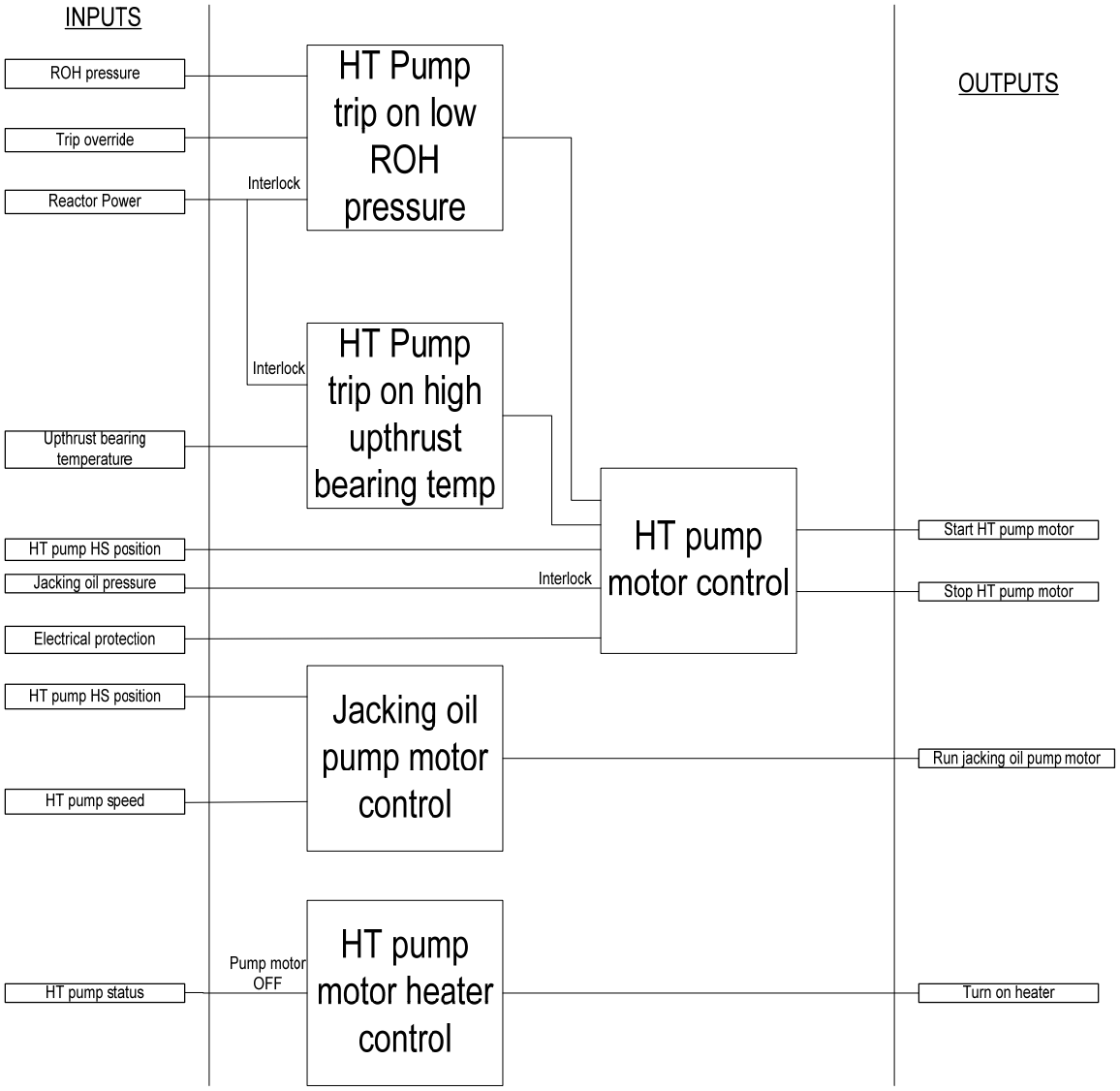

Figure 2: Overview diagram of HT pump control and trip logic

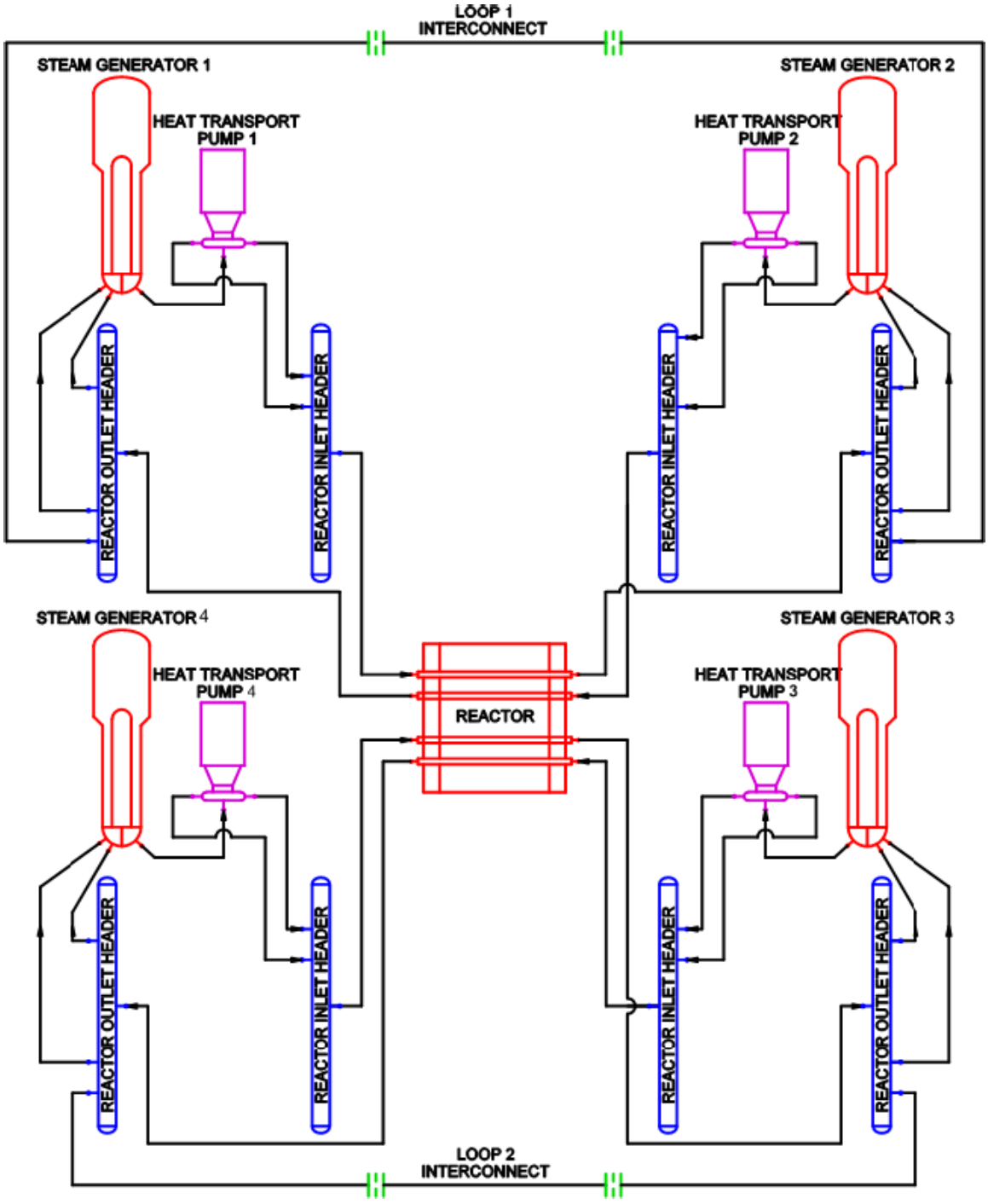

Figure 3: Flow diagram of the HTS

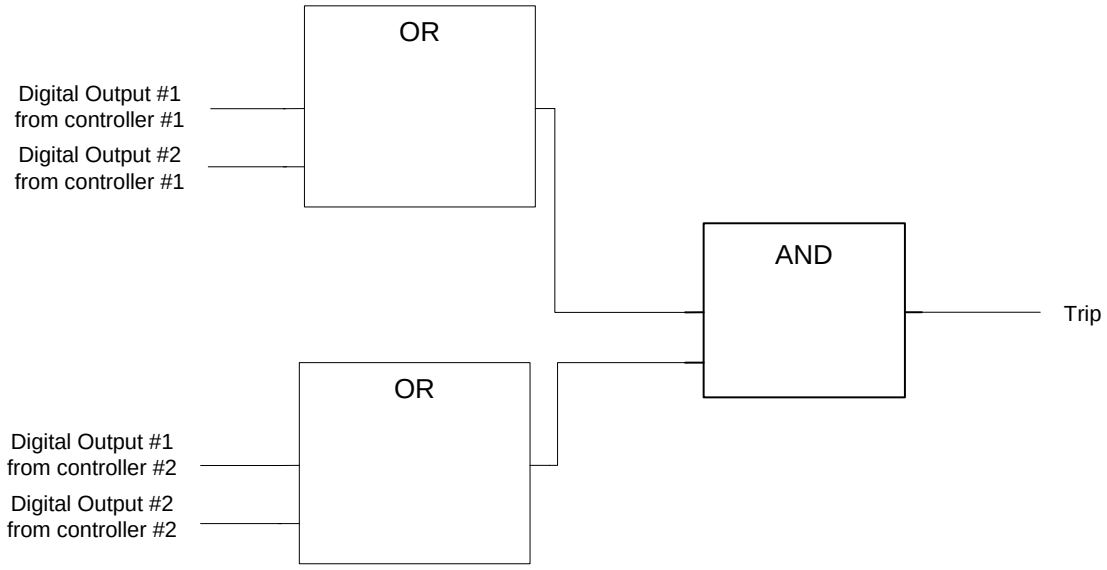

Figure 4: Voting strategy for HT pump 1 trip

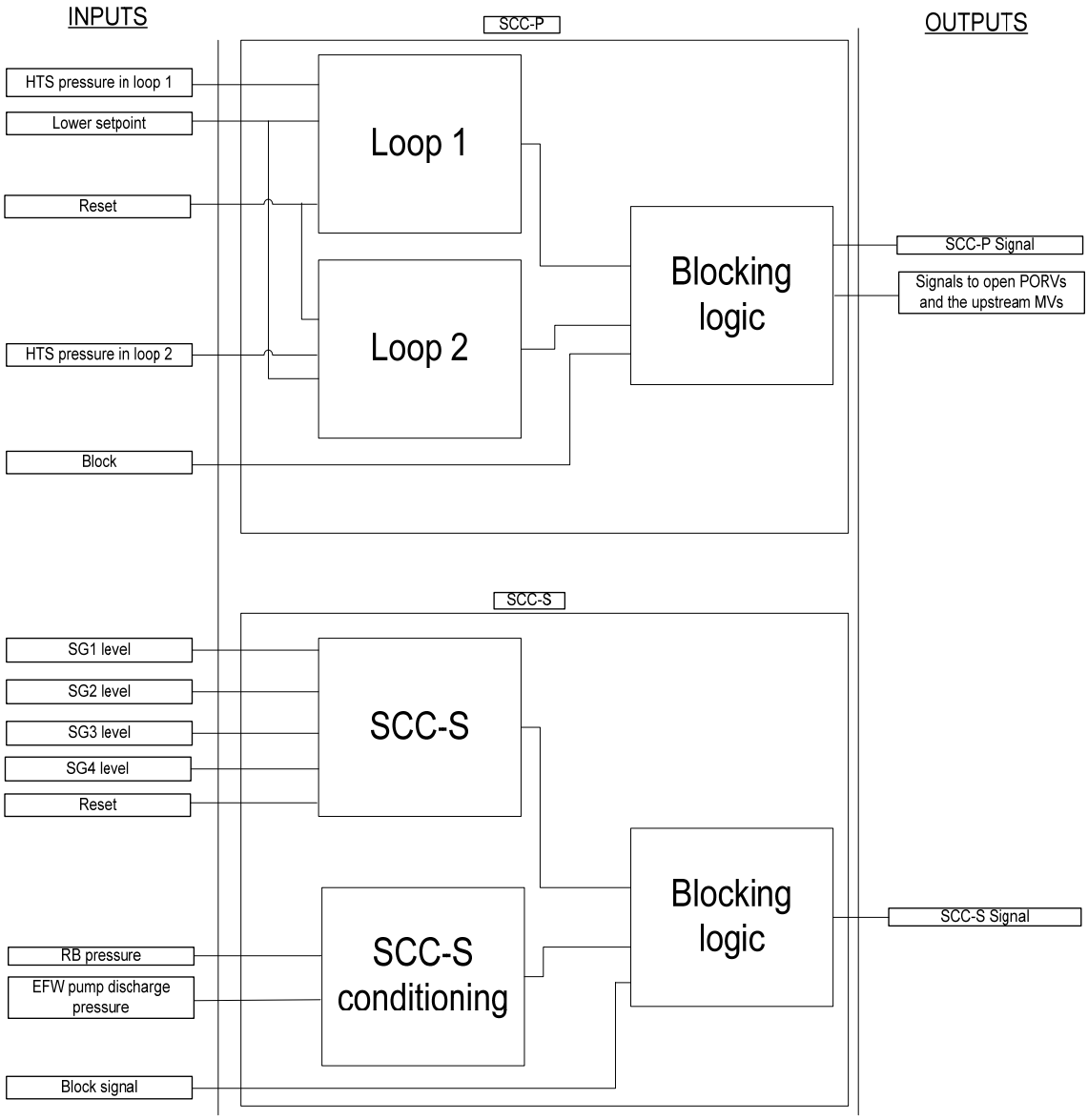

Figure 5: Overview diagram of the SCC system control logic

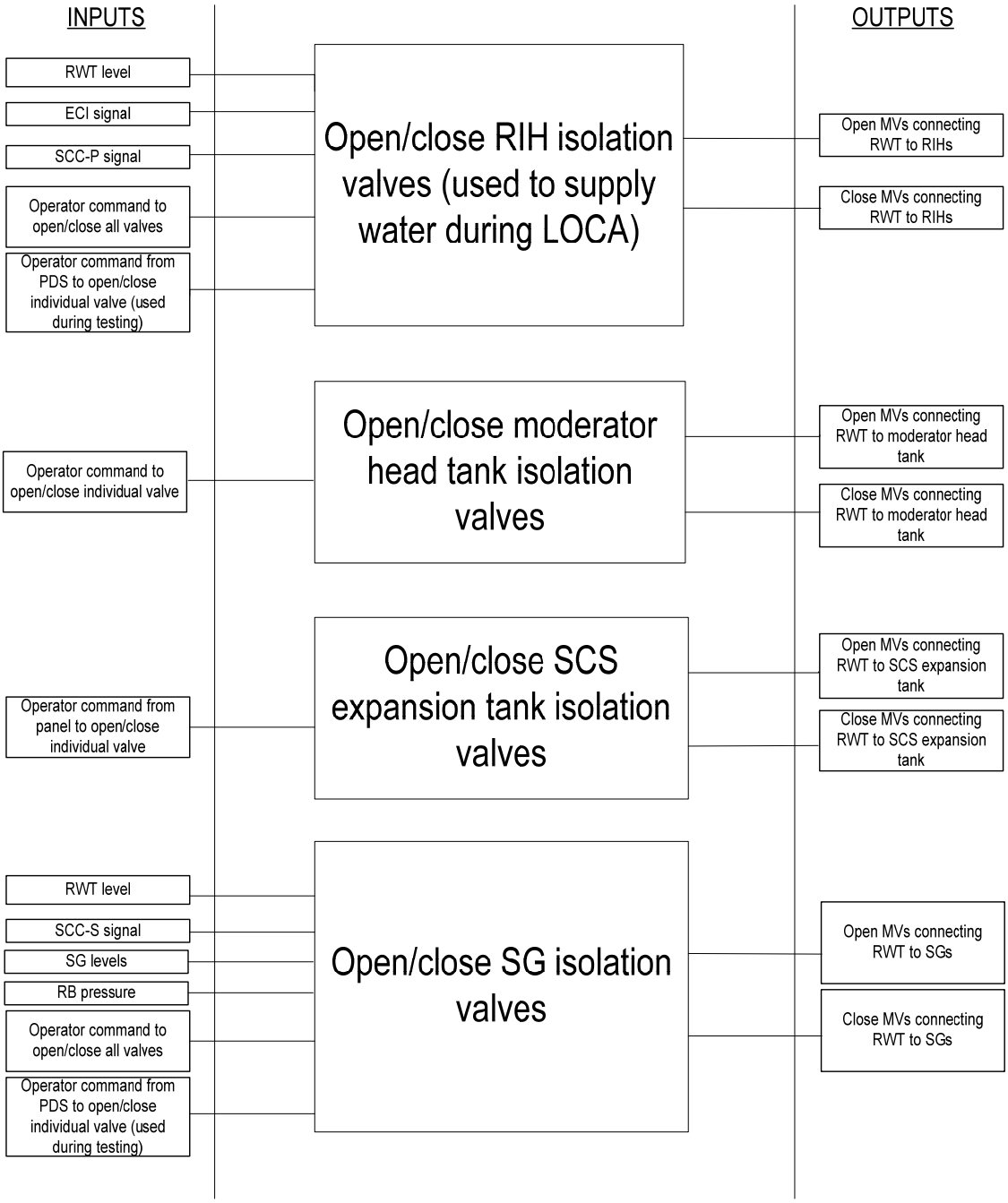

Figure 6: Overview of the RWS control logic

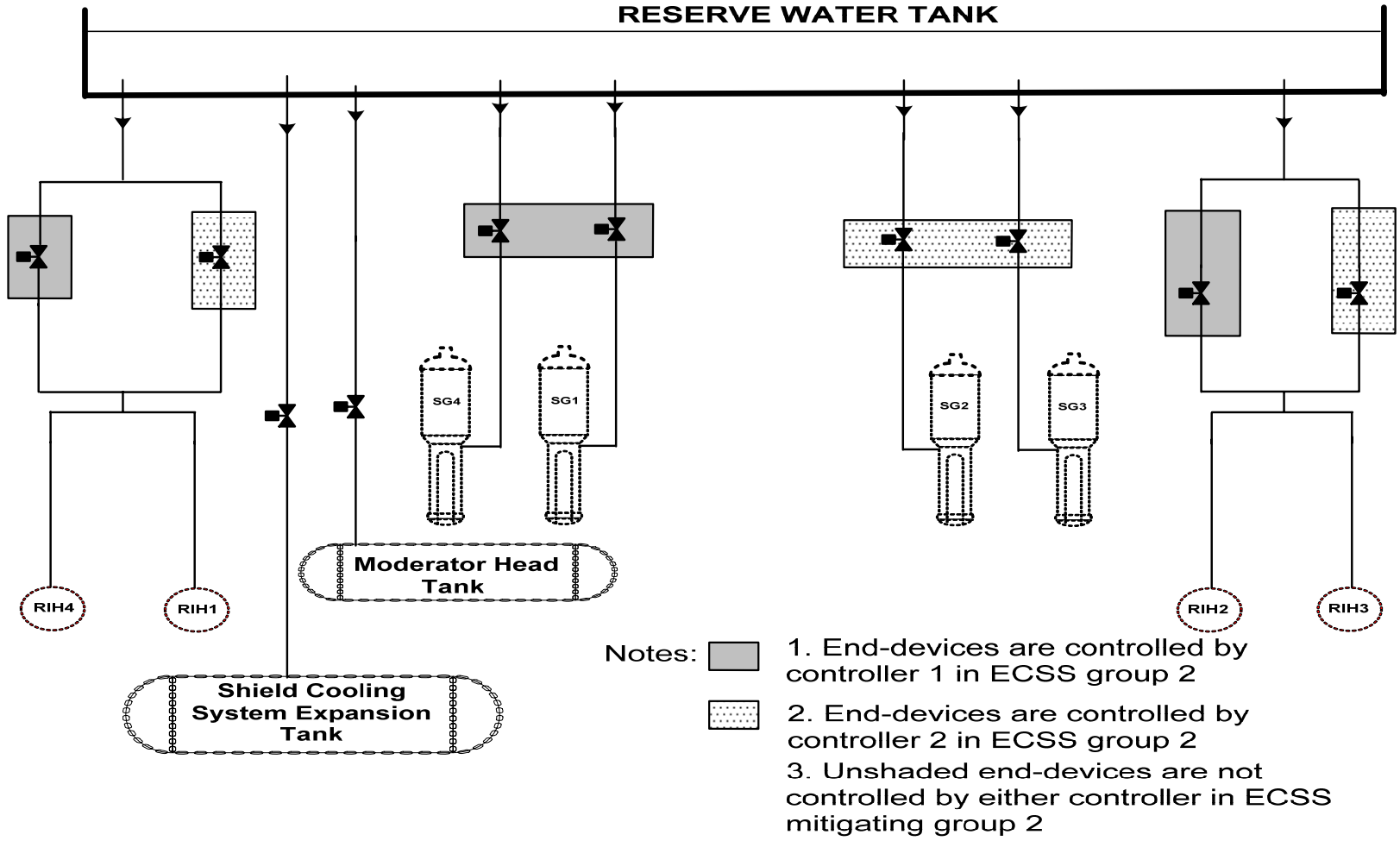

Figure 7: Conceptual flow diagram for the RWS