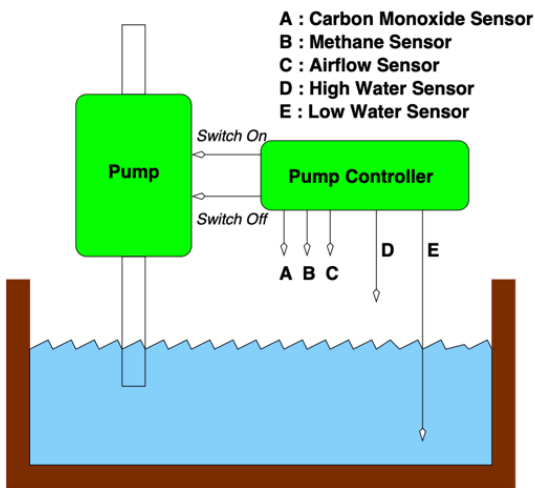


The Mine Pump Problem

This verification benchmark was adapted from [GiKJ97] which in turn used the implementations discussed in [Jose96] where the example was studied using different approaches. The Quartz program considered here as a small verification benchmark describes the controller of a mine pump that must maintain the water level in a mine between minimum and maximum levels as water continuously percolates into the mine. To this end, the controller switches the pump on when the water level reaches the high water level and switches it off when the water level falls below the low water level. The controller consists of the following parallel components:

1. water monitor
2. methane monitor
3. airflow and CO monitor
4. operator interface
5. pump controller



The controller has the sensors A,B,C,D,E (shown in the following figure) which provide boolean valued inputs as listed below. Additionally, there is a human operator with limited rights who can press buttons to manually switch the mine pump on or off, and there is also a human supervisor with unlimited rights who can also press buttons to manually switch the mine pump on or off. Therefore, the controller has the following inputs:

- SensorCriticCO (A) holds iff the carbon monoxide level is critical.
- SensorMethaneHgh (B) holds iff the methane level is too high.
- SensorCriticAir (C) holds iff the air flow is critical.
- SensorWaterHgh (D) and SensorWaterLow (E) hold if the current water level is above the high and low water level, respectively.
- SVStopPump and SVStartPump hold if the supervisor presses buttons to switch the pump off/on.
- OPStopPump and OPStartPump hold if the operator presses buttons to switch the pump off/on.

The main outputs of the controller are the following ones:

- Alarm must be signalled if SensorCriticCO, SensorCriticAir or SensorMethaneHgh & SensorWaterHgh holds since humans must be evacuated in these cases (methane is not toxic, but there is the risk of explosion if the mine pump is on which is required if the water level is above the high level)
- StartPump switches the mine pump on which must not happen if the methane level is high. If the

methane level is not high, then StartPump may hold for three reasons:

1. The water reached the high level, so that the pump must be automatically switched on.
 2. The supervisor pressed the start button.
 3. The operator pressed the start button, the supervisor did not press the stop button, and the water level is between the low and the high water level.
- StopPump switches the mine pump off which may happen for the following reasons:
 1. The water is below the low level, so that the pump must be automatically switched off.
 2. The supervisor pressed the stop, but not the start button.
 3. The operator pressed the stop, but not the start button, the supervisor did not press the start button, and the water level is between the low and the high water level.

Moreover, there are the following local signals used for the communication of the above components:

- PumpOff and PumpOn signal the current status of the mine pump, being either off or on.
- SwitchOffPump and SwitchOnPump are events which hold when the mine pump is switched off/on, i.e., changes from PumpOn to PumpOff or vice versa.
- MethaneCritical and MethaneUnCritical hold if SensorMethaneHgh is true or false, respectively.
- WaterLevLow, WaterLevMid, and WaterLevHgh hold if the water level is below the low water level, between the low and high water levels, or above the high water level, respectively.

As mentioned above, the mine pump controller consists of five components that run in parallel. They are described briefly below.

The Pump Controller

This component signals the status of the mine pump which can be either PumpOff or PumpOn. It switches from PumpOff to PumpOn if StartPump & !StopPump holds and signals the transition by SwitchOnPump. Similarly, it switches from PumpOn to PumpOff if StopPump holds and signals the transition by SwitchOffPump. Initially, PumpOff holds.

Human Operator Interface

This component controls the start/stop buttons used by the human supervisor and operator. It produces signals StartPump and StopPump when the corresponding buttons are pressed. However, the start button has a higher priority, and the human operator cannot override the supervisor's commands or perform actions if the water level is too low or too high.

CO and Airflow Monitors

This component signals Alarm if either SensorCriticCO or SensorCriticAir holds. It does not affect the control of the mine pump further.

The Water Monitor

Sensors D and E in the above figure provide inputs SensorWaterLow and SensorWaterHgh which are true if the current water level is above the low water level and above the high water level, respectively. Hence, SensorWaterHgh implies SensorWaterLow, and the controller determines three additional signals WaterLevLow, WaterLevMid, WaterLevHgh which hold if the water level is below the low water level, between the low and high water levels, or above the high water level, respectively. The water monitor signals StopPump if the water level is below the low water level, and it signals StartPump if the water level is above the high water level and the methane level is not high. Finally, it signals Alarm if the water level is above the high water level and the methane level is high.

The Methane Monitor

This component monitors the methane level. If a rising edge is detected on SensorMethaneHgh, signal StopPump is raised to stop the pump (if it is running) and signal Alarm is raised if WaterLevHgh holds. If there is a falling edge on SensorMethaneHgh, signal StartPump is raised to start the pump if WaterLevHgh holds.

Specifications

The main specifications that must be verified for the controller are as follows:

- Alarm must be signalled whenever SensorCriticCO, SensorCriticAir, or SensorMethaneHgh&WaterLevHgh holds.
- Switching the Pump Off:
 - The pump must be switched off whenever SensorMethaneHgh is true.
 - The pump must be switched off whenever SensorWaterLow is false.
 - The pump must be switched off whenever the supervisor switches it off.
 - The pump must be switched off whenever the operator switches it off provided there is no action of the supervisor and the water level is between the low and high levels.
 - The pump must not be switched off in other cases as those listed above.
- Switching the Pump On:
 - The pump must not be switched on if SensorMethaneHgh is true.
 - The pump must not be switched on if SensorWaterLow is false.
 - The pump must be automatically switched on if the methane level is not high, but the water level is high and the supervisor does not want to stop the pump.
 - The pump must be switched on if the supervisor presses the start button in an uncritical case, i.e., if SensorMethaneHgh is false and SensorWaterLow is true.
 - The pump must be switched on if the operator presses the start button, the supervisor does not press any button in an uncritical case, i.e., if SensorMethaneHgh is false and SensorWaterLow is true.

References

- [Jose96] M. Joseph; "Real-Time Systems: Specification, Verification and Analysis", Prentice Hall, 1996
- [GiKJ97] P. Giridhar, V. Kumar, and M. Joseph: "The Mine Pump Control Program in Esterel - Synchronous Programming"; Computer Science Research Report CS-RR-332, University of Warwick, August 1997