1.11.3 The Mine Pump Controller

The example of this section has been taken from [40] which in turn took the example from [41]. The following implementation is however simpler than the one given in [40]. The task of the mine pump controller is as follows: Water percolating into a mine is collected in a sump to be pumped out of the mine (see Figure 1.45). The water level sensors D and E detect when water is above a high and a low level, respectively. A pump controller automatically switches the pump on when the water reaches the high water level and off when it goes below the low water level. To avoid the risk of explosion, the pump must not operate when the methane level is above a critical level. Moreover, if due to a failure of the pump, the water cannot be pumped out, then the mine must be evacuated within one hour.

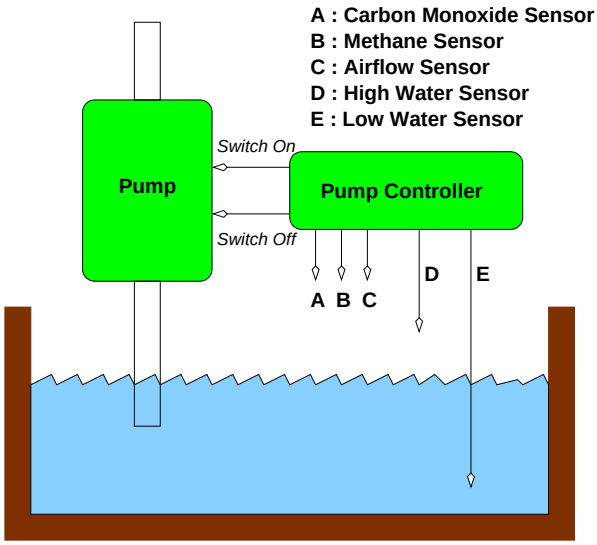

Fig. 1.45. Mine Pump Controller

The overall structure of the mine pump is given in Figure 1.45. The mine has other sensors A, B, and C to monitor the carbon monoxide, methane and airflow levels. An alarm must be raised and the operator informed within one second if any of these levels becoming critical so that the mine can be evacuated within one hour. The sensors D and E signal if the water level is above the low and high water level, respectively.

Human operators can also manually control the operation of the pump, but with limited rights. There are two manual modes of the mine pump with different rights: An *operator* can switch the pump on or off

if the water is below low and high water levels. A special operator, the *supervisor*, can switch the pump on or off without this restriction. In all cases, however, the methane level must be below its critical level if the pump is operated.

Module *PumpController* is used to switch the pump on or off. There are two locations *PumpOn* and *PumpOff* that correspond with the pump's operation mode. Whenever the mode of the pump is changed, then the signals *SwitchOnPump* and *SwitchOffPump* are emitted to control the pump's motors. The inputs *StartPump* and *StopPump* of the pump controller are generated manually by either the operator or the supervisor, or automatically by the environmental monitoring modules *MethaneMonitor* and *WaterMonitor*.

Module *OP* is used to transfer the supervisors and operators commands to the *StartPump* and *StopPump* signals of the pump controller. Note that the supervisor's actions have a higher priority than the operator's ones, and that the *StartPump* signal is only emitted when the methane level is uncritical.

There are three further modules to observe the environment: the *COAirFlowMonitor* observes the carbon monoxide level and the airflow, module *MethaneMonitor* observes the methane level, and module *WaterMonitor* finally observes the water level. The implementation of *COAirFlowMonitor* is simple: At any point of time, *AlertOP* is emitted if either the carbone monoxide level or the airflow becomes critical. Module *MethaneMonitor* has two locations that correspond with a critical and uncritical methane level. The locations are changed whenever the methane level sensor's signal moves from High to Low or vice versa. Note that if the methane level becomes critical, then the pump is switched off to avoid risk of explosion. If the water level is high and the methane level is also high, then the pump can not be switched on, so that the mine must be evacuated.

The entire system is then given as the synchronous parallel composition of the mentioned modules. The mine pump controller is a safety critical system that must satisfy the following specifications:

$$
\begin{aligned}
S_1 &: \mathsf{G}[\mathit{MethaneCritical} \rightarrow \mathit{PumpOff}] \\
S_2 &: \mathsf{G}[\mathit{SwitchOnPump} \wedge \mathit{MethaneCritical} \rightarrow \mathit{MethaneLVLow}] \\
S_3 &: \mathsf{G}[\mathit{WaterLVHigh} \wedge \neg \mathit{MethaneCritical} \rightarrow \mathit{StartPump}] \\
S_3' &: \mathsf{G}\left[\begin{array}{l} \mathit{WaterLVHigh} \wedge \neg \mathit{MethaneCritical} \\ \wedge \neg \mathit{SVStopPump} \wedge \mathit{PumpOff} \\ \wedge (\mathit{MethaneUnCritical} \rightarrow \neg \mathit{MethaneLVHigh}) \\ \rightarrow \mathit{SwitchOnPump} \end{array}\right] \\
S_4 &: \mathsf{G}[\mathit{WaterLVHigh} \wedge \mathit{MethaneCritical} \rightarrow \mathit{Alarm}] \\
S_5 &: \mathsf{GX}[\mathit{COCritical} \vee \mathit{AirflowCritical} \rightarrow \mathit{Alarm}] \\
S_6 &: \mathsf{G}\left[\begin{array}{l} \mathit{MethaneUnCritical} \wedge \mathit{MethaneLVHigh} \wedge \mathit{PumpOn} \\ \rightarrow \mathit{SwitchOffPump} \end{array}\right]
\end{aligned}
$$

```
module PumpController :
input StopPump, StartPump;
output SwitchOffPump, SwitchOnPump;
labels PumpOff, PumpOn;
  loop
    while ¬StartPump ∨ StopPump do
      PumpOff : pause
    end;
    emit SwitchOnPump;
    while ¬StopPump do
      PumpOn : pause
    end;
    emit SwitchOffPump
  end loop
end module

module Operator :
input SVStartPump, SVStopPump,
      OPStartPump, OPStopPump,
      MethaneCritical, WaterLVMid, AlertOP;
output StartPump, StopPump, Alarm;
labels ℓ1;
  loop
    ℓ1 : pause;
    if SVStartPump then
      if ¬MethaneCritical then
        emit StartPump
      end
    else if SVStopPump then
      emit StopPump
    else if OPStartPump then
      if WaterLVMid ∧ ¬MethaneCritical then
        emit StartPump
      end
    else if OPStopPump then
      if WaterLVMid then
        emit StopPump
      end
    end;
    if AlertOP then
      emit Alarm
    end
  end loop
end module
```

Fig. 1.46. Modules for the OP and the Pump Controller

```
module COAirFlowMonitor :
input COCritical, AirflowCritical;
output AlertOP;
labels ℓ2;
  loop
    ℓ2 : pause;
    if COCritical ∨ AirflowCritical then
      emit AlertOP
    end if
  end loop
end module

module MethaneMonitor :
input MethaneLVHigh, MethaneLVLow, WaterLVHigh;
output AlertOP, StartPump, StopPump;
labels MethaneUnCritical, MethaneCritical;
  loop
    MethaneUnCritical : await MethaneLVHigh;
    emit AlertOP;
    emit StopPump;
    MethaneCritical : await MethaneLVLow;
    if WaterLVHigh then emit StartPump end if
  end loop
end module

module WaterMonitor :
input LW, HW, MethaneCritical;
output StopPump, StartPump, AlertOP,
       WaterLVMid, WaterLVLow, WaterLVHigh;
labels ℓ3;
    loop
      ℓ3 : pause;
      if ¬LW then
        emit WaterLVLow;
        emit StopPump
      else if ¬HW
        emit WaterLVMid;
      else
        emit WaterLVHigh;
        if ¬MethaneCritical then
          emit StartPump
        else
          emit AlertOP
         end
      end if
    end loop
end module
```

Fig. 1.47. Modules for Environment Monitoring

```
module MinePump :
input COCritical,
      MethaneLVLow, MethaneLVHigh,
      AirFlowCritical, LW, HW,
      SVStopPump, SVStartPump,
      OPStopPump, OPStartPump;
output Alarm, SwitchOffPump, SwitchOnPump;
locals StartPump, StopPump,
      WaterLVLow, WaterLVMid, WaterLVHigh,
      AlertOP;
labels PumpOff, PumpOn,
      ℓ1, ℓ2, ℓ3,
      MethaneUnCritical,MethaneCritical;
      run PumpController
   ||
      run Operator
   ||
      run COAirFlowMonitor
   ||
      run MethaneMonitor
   ||
      run WaterMonitor
end module
```

Fig. 1.48. Entire System for the Mine Pump Control

The specifications have the following meaning: S_1 is the most important one and states that the pump must be off when the methane level is critical. S_2 means that the pump should only be switched on if the methane level is uncritical or gets currently uncritical. S_3 assures the automatic invocation of the pump whenver the water level becomes high and the methane level is not critical. S_3 is stated for the *StartPump* signal which is a local signal that is translated by the module *PumpController* to the signal *SwitchOnPump*. However, not any *StartPump* yields to a *SwitchOnPump*:

If, however, the water level is high and the methan level is critical, then an alarm must be given (S_4). An alarm must also be given if the carbone monoxide level or the airflow becomes critical (S_5). In fact, these are the only cases when an alarm is given, but this matter is not so important.

For the verification, we may first translate the entire system into an equivalent equation system. The resulting equation system is given in Figure 1.49.

Data Flow:

- $\mathit{WaterLVLow} = \ell_3 \wedge \neg \mathit{LW}$
- $\mathit{WaterLVMid} = \ell_3 \wedge \mathit{LW} \wedge \neg \mathit{HW}$
- $\mathit{WaterLVHigh} = \ell_3 \wedge \mathit{LW} \wedge \mathit{HW}$
- $\mathit{StartPump} = \begin{pmatrix} \ell_1 \wedge \mathit{SVStartPump} \wedge \neg \mathit{MethaneCritical} \vee \\ \ell_1 \wedge \neg \mathit{SVStartPump} \wedge \neg \mathit{SVStopPump} \\ \quad \wedge \mathit{OPStartPump} \\ \quad \wedge \mathit{WaterLVMid} \wedge \neg \mathit{MethaneCritical} \vee \\ \mathit{MethaneCritical} \wedge \mathit{MethaneLVLow} \\ \quad \wedge \mathit{WaterLVHigh} \vee \\ \ell_3 \wedge \mathit{LW} \wedge \mathit{HW} \wedge \neg \mathit{MethaneCritical} \end{pmatrix}$
- $\mathit{StopPump} = \begin{pmatrix} \ell_1 \wedge \neg \mathit{SVStartPump} \wedge \mathit{SVStopPump} \vee \\ \ell_1 \wedge \neg \mathit{SVStartPump} \wedge \neg \mathit{SVStopPump} \\ \quad \wedge \neg \mathit{OPStartPump} \wedge \mathit{OPStopPump} \\ \quad \wedge \mathit{WaterLVMid} \vee \\ \mathit{MethaneUnCritical} \wedge \mathit{MethaneLVHigh} \vee \\ \ell_3 \wedge \neg \mathit{LW} \end{pmatrix}$
- $\mathit{AlertOP} = \begin{pmatrix} \ell_2 \wedge (\mathit{COCritical} \vee \mathit{AirFlowCritical}) \vee \\ \mathit{MethaneUnCritical} \wedge \mathit{MethaneLVHigh} \vee \\ \ell_2 \wedge \mathit{LW} \wedge \mathit{HW} \wedge \mathit{MethaneCritical} \end{pmatrix}$
- $\mathit{SwitchOffPump} = \mathit{PumpOn} \wedge \mathit{StopPump}$
- $\mathit{SwitchOnPump} = \begin{pmatrix} \mathit{start} \wedge \mathit{StartPump} \wedge \neg \mathit{StopPump} \vee \\ \mathit{PumpOff} \wedge \mathit{StartPump} \wedge \neg \mathit{StopPump} \end{pmatrix}$

Control Flow:

- $\mathsf{X}\mathit{PumpOff} = \begin{pmatrix} (\neg \mathit{StartPump} \vee \mathit{StopPump}) \wedge \mathit{start} \vee \\ (\neg \mathit{StartPump} \vee \mathit{StopPump}) \wedge \mathit{PumpOff} \vee \\ \mathit{PumpOn} \wedge \mathit{StopPump} \end{pmatrix}$
- $\mathsf{X}\mathit{PumpOn} = \begin{pmatrix} \neg \mathit{StopPump} \wedge \mathit{start} \wedge \mathit{StartPump} \vee \\ \mathit{PumpOff} \wedge \mathit{StartPump} \wedge \neg \mathit{StopPump} \vee \\ \mathit{PumpOn} \wedge \neg \mathit{StopPump} \end{pmatrix}$
- $\mathsf{X}\ell_1 = \mathit{start} \vee \ell_1$
- $\mathsf{X}\ell_2 = \mathit{start} \vee \ell_2$
- $\mathsf{X}\ell_3 = \mathit{start} \vee \ell_3$
- $\mathsf{X}\mathit{MethaneUnCritical} = \begin{pmatrix} \mathit{start} \vee \\ \mathit{MethaneCritical} \wedge \mathit{MethaneLVLow} \vee \\ \mathit{MethaneUnCritical} \wedge \neg \mathit{MethaneLVHigh} \end{pmatrix}$
- $\mathsf{X}\mathit{MethaneCritical} = \begin{pmatrix} \mathit{MethaneUnCritical} \wedge \mathit{MethaneLVHigh} \vee \\ \mathit{MethaneCritical} \wedge \neg \mathit{MethaneLVLow} \end{pmatrix}$

Fig. 1.49. Equation System for the Mine Pump Controller