The Hemodialysis Machine Case Study

Atif Mashkoor

Software Competence Center Hagenberg GmbH
Hagenberg, Austria
atif.mashkoor@scch.at

1 Introduction

This documents presents a description of a case study concerning the control of a hemodialysis (HD) machine. It provides an overview of the requirements and the design of an HD machine including a sketch of the machine's functionality, related safety conditions, and a top-level system architectural description. This case study is supposed to stimulate research and pedagogical activities related to the use of formal methods in a medical application domain with challenging requirements concerning safety and hardware/software interaction.

Kidney diseases are becoming endemic in recent times. There are several contributing factors such as changed life style as well as increase in hypertension and diabetes. Kidneys are the organs that are responsible for cleaning human blood by removing excess fluid, minerals and wastes. They also aid regulating blood pressure, electrolyte balance, and red blood cell production. When kidneys fail, toxic waste products are accumulated in the human body, causing a rise in blood pressure and a decline in the production of red blood cells. When kidneys fail completely, an artificial system is required that can substitute their functionality.

Hemodialysis (HD) is a treatment for kidney failure that uses a machine to send the patient's blood through a filter, called a dialyzer, for extracorporeal removal of waste products. The blood is transported to and from the patient's body through a surgically created vein during this process. The blood then travels through a tube that takes it to the dialyzer. Inside the dialyzer, the blood flows through thin fibers that filter out wastes and extra fluid. The machine returns the filtered blood to the body through a different tube. A vascular access lets large amounts of blood flow continuously during HD treatments to filter as much blood as possible per treatment. A specific amount of blood (approx. a pint) is conducted through the machine every minute.

This document is structured as follows: Section 2 presents a high-level architectural description of the HD machine describing its main components. Section 3 gives an overview of different types of dialysis therapies and how a therapy is conducted. Finally, Section 4 lists several general and software safety requirements related to the correct operation of the HD machine.

Acronyms. Table 1 contains a list of acronyms used in this document.

AP	Arterial Pressure
BEP	Blood-side Entry Pressure
BP	Blood Pump
DF	Dialyzing Fluid
EBC	Extracorporeal Blood Circuit
HD	Hemodialysis
SAD	Safety Air Detector
TMP	Trans Membrane Pressure
UF	Ultra Filtration
UFP	Ultra Filtration Pump
UI	User Interface
VP	Venous Pressure
VRD	Venous Red Detector

Table 1. The list of acronyms

2 System architecture

As shown in Figure 1, the HD machine under consideration is composed of the following components:

Extracorporeal Blood Circuit (EBC). The EBC consists of the machine's peristaltic pumps, which are used to transport the blood to and from the dialyzer. Blood is pumped through a disposable system that is mainly composed of tubing, connectors, and (aterial/venous) drip chambers connected to the dialyzer. Peristaltic pumps withdraw blood from the patients vascular access into the dialyzer. A syringe pump pumps heparin into the bloodlines in a quantity and time set by the user to avoid the coagulation of the blood in the disposable circuit and the dialyzer filter. The Safety Air Detector (SAD) component is a combined air and red detector. It detects air bubbles and blood in the EBC while transporting blood back to the patient's body. The functionality of the EBC is depicted in Figure 2.

Dialyzer. The capillary dialyzer houses semipermeable hollow fibers encased in a plastic canister. The dialyzer is used to correct the concentration of water-soluble substances in the patients blood before delivering it back to the patient. The blood is separated from the Dialyzing Fluid (DF) by a semi-permeable membrane that permits bidirectional diffusive transport and Ultrafiltration (UF). The process also allows diffusion of substances from the DF into the blood.

Balance chamber. The balance chamber is a closed system that consists of two chambers, each with a flexible membrane, allowing it to fill the chambers from one side while an identical volume is emptied to the other side. Therefore the outlet fluid volume is equal to the input fluid volume. Each membrane has a magnetic sensor which reads the membrane position and controls the opening and the closing of each sub-compartment. The control

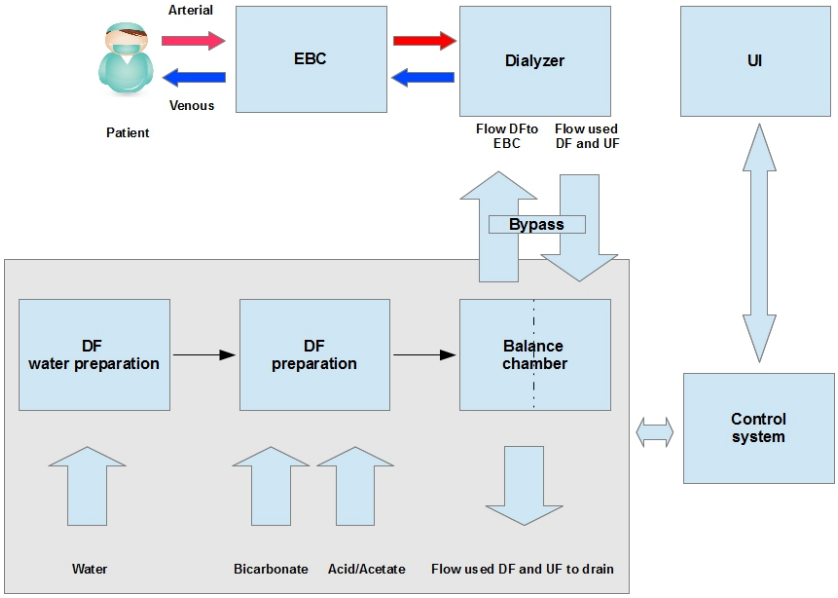

Fig. 1. Architecture of HD machine

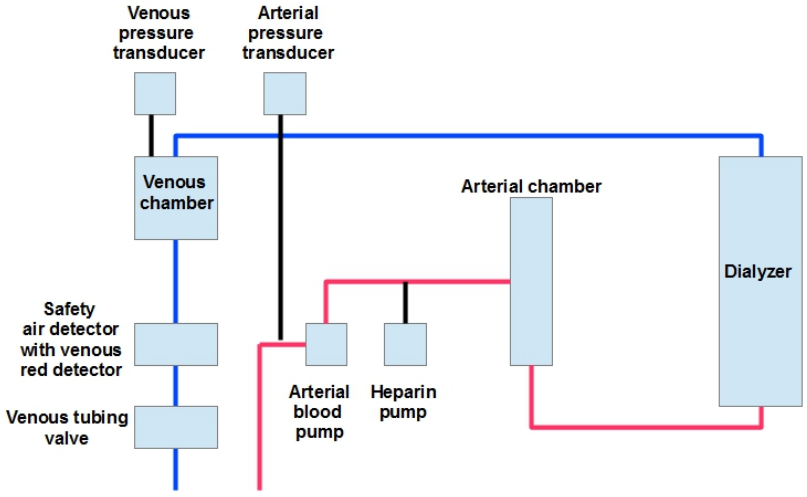

Fig. 2. Schematic view of EBC

of the DF volume is also carried out by the balance chamber. The difference between the used DF and the fresh DF is the UF volume, which is removed from the blood side of the dialyzer. The removal of the UF volume is carried out by the Ultra Filtration Pump (UFP).

DF preparation. In bicarbonate dialysis, which is the most common procedure, concentrate preparation consists of mixing the heated and degassed water with bicarbonate concentrate and acid concentrate. The accuracy of the DF concentration is controlled by the conductivity sensors. If the concentration is incorrect, the dialyzer will be bypassed.

DF water preparation. Purified water coming from the reverse osmosis system has to be degassed and tempered to a predetermined temperature, which is set by the user (usually 37°C), before the concentrate is prepared. A degassing chamber and a heater are integral to the system.

Bypass. Bypass mode occurs when the DF conductivity or temperature goes beyond permissible limits. This is used for safety reasons. This feature allows that the dialyzer is separated from the DF flow without interrupting the DF preparation until temperature and conductivity are back within the acceptable limits. The DF path is then directed to the waste without passing the dialyzer.

User Interface (UI). The UI is a display panel that provides communication between the HD machine and the user. On the display, it is possible to visualize all the dialysis parameters and the relevant information about the procedure and the alarm conditions. By touching the icons on the screen, the user can input all the parameters for the treatment such as the dialysis time, the UF volume and the heparin pump flow.

Control system. The control system is divided into two parts: The top-level control system connects the interface with the user and transmits data to and from other modules. The low-level control system controls and monitors the HD machine and its functions and also communicates with the top-level control system. Both systems operate independent of each other.

3 Therapy

During a therapy, an HD machine pumps blood through a vascular access from the patient into the dialyzer. Inside the dialyzer, metabolic waste products are separated from the blood. The dialyzer operates as a filter that is divided into two parts by a semipermeable membrane. On one side, the patient's blood is flowing and on the other side, the DF.

The DF, a chemical substance that is used in HD to draw fluids and toxins out of the bloodstream and to supply electrolytes and other chemicals to the bloodstream, is prepared by the HD machine for the therapy. It consists of prepared water that contains certain quantities of electrolyte and bicarbonate, depending on the individual patient's requirements. The concentrations of electrolyte and bicarbonate in the DF are adjusted in such a way that certain substances can be removed from the blood through convection, diffusion and

osmosis, while other substances are added at the same time. This is achieved mainly by diffusive clearance through the semipermeable membrane of the dialyzer. The DF transports the metabolic waste products from the dialyzer into the discharge line. The cleaned blood is then recycled back to the patient.

During therapy, the HD machine performs extracorporeal monitoring of blood circulation, pumps blood and DF in separate circulation systems through the dialyzer and monitors the composition and volume balance of the DF. The heparin pump, which is also part of the HD machine, is used to add anticoagulants to the blood so as to prevent the formation of blood clots.

In addition to cleaning metabolic waste from the blood, the HD machine removes water from the blood which would be excreted through the kidney in healthy humans.

3.1 Types of therapy

Double-needle therapy. If arterial and venous vascular access are different, the therapy method is called double-needle therapy. The double-needle procedure is the standard technique in HD. Blood is extracted from the patient through the arterial vascular access. The blood pump continuously pumps the blood through the arterial tube system to the dialyzer. There, the exchange of metabolic waste products between the blood and the DF proceeds through the semipermeable membrane of the dialyzer. After that, the blood is taken back through the venous tube system, the bubble trap and a second vascular access to the vein.

Single-needle therapy. If arterial and venous vascular access are identical, the therapy method will be called single-needle therapy. The single-needle therapy is applied when patients experience problems with the predominantly used double-needle dialysis. In the single-needle procedure, only one needle is applied to the patient. The arterial and venous ends of the tube system are connected via a Y-connector. This procedure allows reducing the number of punctures by half compared to double-needle dialysis, thus preserving the patient's shunt. The single-needle clamp procedure allows ending a running double-needle dialysis in case of problems (e.g., at the shunt). The single-needle therapy is out of scope of this case study.

3.2 Phases of therapy

A therapy session follows the following sequence of phases: 1) preparation, 2) initiation, and 3) ending.

Therapy preparation

1. **Automated self test**
   First the HD machine automatically checks all control functions relevant to the safety of the machine. If the test is successfully completed, signal lamps on the monitor change to green.

2. **Connecting the concentrate**
   On successful completion of the test, the requested concentrates, e.g., acetate/acid, are connected to the HD machine.
3. **Setting the rinsing parameters**
   The rinsing parameters are entered in the machine. The parameters must be within the defined ranges as shown in Table 2.

Text	Range	Description
Filling BP rate	50 - 600 mL/min	The rate with which the blood side is filled or rinsed
Filling BP volume	0 - 6000 mL	The BP stops after it has rinsed the blood side using the set volume
Rinsing BP rate	50 - 300 mL/min	BP rate for rinsing program
DF flow	50 - 300 mL/min	DF flow rate for rinsing program
Rinsing time	0 - 59 mins	Duration of adjusted rinsing program
UF rate for rinsing	0 - 3000 mL/h	When rinsing with a physiological saline solution
UF volume for rinsing	0 - 2950 mL	When rinsing with a physiological saline solution
Blood flow for connecting patient	50 - 600 mL/min	

Table 2. Rinsing parameters

4. **Inserting, rinsing and testing the tubing system**
   (a) Standard arterial/venous (A/V) tubing is inserted. Both arterial and venous tubes must be properly connected. All other components of the machine as depicted in Figure 2 should be in place.
   (b) Saline bag levels in the blood line chambers for preparation are set.
   (c) Bloodlines are inserted.
   (d) Rinsing and testing the tubing system.
      – The BP speed is increased to 150 mL/min to complete priming. Priming is the process by which a pump is filled with fluid and made able to operate.
      – Once the saline solution has filled the venous line past the drip chamber, the drip chamber and the vent line are completely filled.
      – When the BP stops, the arterial and venous patient ends are connected for recirculation and the BP is restarted. The membrane inside the pods should be moving slightly when the BP is running. The faster the BP speed is, the more movement should be detectable.
5. **Preparing the heparin pump**
   (a) The heparin syringe is inserted.
   (b) The heparin line is vented.

6. **Setting treatment parameters**
   (a) The DF parameters are set. They are described along with their ranges in Table 3.

Text	Range	Description
Conductivity	12.5 - 16.0 mS/cm	The rate with which the blood side is filled or rinsed
Bicarbonate/Acetate		Selection of the concentrate
Bicarbonate conductivity	2 - 4 mS/cm	
DF temperature	33 - 40°C	
Rinsing time	0 - 59 mins	
DF flow	300 - 800 mL/min	

Table 3. DF parameters

   (b) The UF parameters are set. They are described along with their ranges in Table 4.

Text	Range
UF volume	100 - 20000 mL
Therapy time	10 mins - 10 hrs
Min UF rate	0 - 500 mL/h
Max UF rate	0 - 4000 mL/h

Table 4. UF parameters

   (c) The pressure limits are set. They are described along with their ranges in Table 5.

   Limits window for arterial entry pressure control. The arterial entry pressure AP (pressure between a patient and a BP) is monitored by an automatically set limits window. A maximum lower arterial limit is set in the machine (max. -400 mmHg). The automatically set lower limit cannot fall below this value. The size of the arterial limits window is defined through the respective distance (delta) between the actual value and the lower and upper limits. The total of the two distances to the actual value gives the width of the arterial limits window. When the actual AP is changed slowly, the limits window is continuously adapted to the actual value, but only within the absolute limits set in the machine.

   Limits window for trans-membrane pressure control. The trans-membrane pressure (TMP) of the dialyzer is controlled by an automatically set limits window. The size of the limits window is entered as a percentage of

Text	Range	Description
Limit delta Min/Max AP	10 - 100 mmHg	Limits window for arterial entry pressure AP. Distance to min and max AP
Actual TMP/max TMP	300 - 700 mmHg	
Limits TMP	ON/OFF	Monitoring the TMP at the dialyzer
Low/High	2 - 99 %	Limits window for TMP in % of actual value
Extended TMP limit range	ON/OFF	
DF flow	300 - 800 mL/m	

Table 5. Pressure parameters

the actual value. The limits window is therefore independent of the dialyzer in use. When the limits window is switched off, the control of the dialyzer-dependant maximum TMP is still active. Activating the bypass icon or changing the blood flow causes the limits window to be re-centered.

(d) The heparin parameters are set as described along with their ranges in Table 6.

Text	Range	Description
Heparin stop time	0:00 - 10:00 hrs:mins	The heparin pump is switched off by the set time prior to the end of the therapy
Heparin bolus volume	0.1 - 10.0 mL	Bolus volume for a bolus administration during dialysis
Heparin profile/rate	0.1 10.0 mL/h	Continuous heparin rate over the entire duration of heparin administration
Treatment without heparin	deactivated/activated	Switching on/off the heparin monitoring function
Syringe type	10/20/30 mL	A list of permissible syringe types

Table 6. Heparin parameters

7. **Rinsing the dialyzer**
When the DF is prepared, the machine asks to connect the dialyzer. The (arterial drip) chamber in front of the dialyzer entry (BEP) is filled nearly half full and the venous drip chamber up to approx. 1 cm from the upper edge. Once the dialyzer has been filled, the BP stops running. It is ensured that the blood tubing system and the dialyzer are filled and rinsed with physiological saline solution. It is also ensured that the level in the venous chamber is correct.

Therapy initiation After completion of the preparation work, the icon for connecting the patient on the UI is enabled. The signal lamps on the monitor change to yellow.

1. **Connecting the patient and starting therapy**
   - The patient is connected arterially.
   - The BP is started by pressing the START/STOP button on the UI.
   - The blood flow is set.
   - The blood tubing system is filled with blood. The BP stops automatically when blood is detected on the VRD in the SAD.
   - The patient is connected venously.
   - The blood pump is started and the prescribed blood flow is set.
   - The machine is taken out of bypass mode. The HD machine switches to main flow and bicarbonate running. The signal lamps on the UI switch to green.
2. **During therapy**
   (a) Monitoring the blood-side pressure limits

   Venous return flow pressure. The venous return flow pressure (VP) is monitored by an automatically set limits window. The limits window is set 10 seconds after the last activation of the BP and is identified by markings on the bar showing the venous return flow pressure. The width and thresholds of the limits window are set in the HD machine. The venous lower limit value is automatically adjusted during treatment. This means that the distance between the lower limit and the actual pressure decreases. This compensates for the hematocrit increase generally caused by UF. The adjustment is carried out every 5 minutes and adds up to 2.5 mmHg at a time. The minimum distance of 22.5 mmHg is, however, always maintained. The venous lower pressure limit during HD is checked. An optimal interval is approximately 35 mmHg between the lower pressure limit and the current value. By changing the speed of the BP for a brief period, it is possible to reposition the limits window.

   Arterial entry pressure. The arterial entry pressure is automatically monitored within set limits. The limits window is set 10 seconds after the last activation of the BP. These limits are active in the initiation phase and during final circulation.

   Blood-side entry pressure at the dialyzer. The BEP must be connected during preparation. If the BEP transducer protector is used, the BEP at the dialyzer is controlled by its upper limit. The BEP monitoring function warns or signals a possible blockage of the dialyzer due to a kinked tube or increased clotting within the dialyzer. The BEP measurement allows the user to monitor the formation of a secondary membrane layer in the dialyzer. A possible filter clotting might be avoided. The limits can only be set via the alarm limits screen at the beginning of the therapy.

(b) Treatment at minimum UF rate
Treatment at minimum UF rate can be activated to achieve, for instance, an immediate lowering of the set UF rate in case of falling blood pressure and unstable circulation.

(c) Heparin bolus
There is a risk of blood loss due to blood clotting in case of insufficient anticoagulation. Complete heparin bolus as required.

(d) Arterial bolus (saline)
Using the function "arterial bolus" a defined volume of sodium chloride is infused from a Sodium Chloride (NaCl) bag. The required bolus volume is entered on the UI. The BP stops automatically and a safety message appears on the UI. A bag with physiological saline solution to arterial infusion connector is connected to the machine. The arterial bolus is infused. The values can be monitored in the settings window. Once the set quantity has been infused or the arterial bolus has been terminated by an alarm, a window appears to confirm bolus termination.

(e) Interrupting dialysis (bypass)
The therapy can be interrupted by switching to bypass mode. The signal lamps on the UI switch to yellow. The bypass mode can also be terminated likewise.

(f) Completion of treatment
On completion of the treatment, an acoustic signal can be heard, the message "treatment time completed" is displayed, and the signal lamps on the monitor switch to yellow. The UF rate is set to 50 mL/h. The BP is still running.

Therapy ending.

1. **Reinfusion**
   The physical arterial connection is removed from the patient. The arterial line to the infusion Y on the saline line containing the physiological saline solution is connected. The arterial disconnection on the UI is confirmed. The BP starts the reinfusion. The reinfusion screen appears on the UI. The HD machine monitors the reinfusion volume and reinfuses until the red detector (VRD) detects the physiological saline solution. The BP stops. To continue reinfusion, start the BP by pressing the START/STOP button on the UI. The BP stops automatically after 400 mL have been reinfused or when a reinfusion time of 5 minutes has elapsed. The procedure can be repeated and the HD machine will carry out reinfusion of another 400 mL, or reinfusion for 5 minutes. The venous patient connection is disconnected.
2. **Emptying the dialyzer**
   The dialyzer is emptied by pressing the respective button on the UI.
3. **Emptying the cartridge after dialyzer drain**
   The cartridge is emptied automatically by the machine.
4. **Overview of the therapy carried out**
   An overview of the therapy is shown with the actual values, e.g., the treated blood volume, the UF volume, the heparin volume, and the time lapsed.

4 Safety requirements

4.1 General requirements

S-1 Arterial and venous connectors of the EBC are connected to the patient simultaneously.

S-2 As an intervention, in case of a drop of the patient's blood pressure, an infusion is applied in order to stabilize the cardiovascular circulation. Flow saline at the set volume and the set rate from the saline bag/bottle with closed arterial access through the dialyzer to their venous connection.

S-3 To prevent coagulation of blood, an anti-coagulation pump doses an anti-coagulant into the bloodline between the BP and the dialyzer. Anti-coagulant is flown at the set rate or the set volume from the syringe into the EBC during treatment.

S-4 When the patient is connected to the EBC, the saline solution in the EBC is replaced with blood. The saline solution can be discarded to a bag or a bucket connected to the venous connector of the EBC. The saline solution and the blood are exchanged using the BP. The BP is stopped when either the VRD detects blood or the BP has transported a predefined volume.

S-5 The patient cannot be connected to the machine outside the initiation phase, e. g., during the preparation phase.

S-6 The BP cannot be used for infusion outside the initiation phase, e.g., during saline infusion.

S-7 When the blood flow stops because of BP failure during loss of main power, blood clotting could cause blood loss. The blood should be returned to the patient manually.

S-8 There is a risk to the patient due to hemolysis if the blood flow rate setting is too high for the selected fistula needle (AP too low)! The blood flow rate should be adjusted, taking into consideration the AP.

S-9 There is a risk to the patient due to reduced dialysis effectiveness if the actual blood flow rate is lower than the displayed flow rate if the AP is highly negative. The blood flow rate setting should be corrected and treatment time should be extended.

S-10 There is a risk to the patient due to reduced dialysis effectiveness if the blood flow rate is too low. It should be ensured that the blood flow rate is optimal.

S-11 Once "empty dialyzer" has been confirmed, the BP cannot be started anymore.

4.2 Software requirements

Arterial bolus.

R-1 During arterial bolus application, the software shall monitor the infusion of saline into the patient and if the infused volume exceeds 0.4 l, then the software shall stop the blood flow and execute an alarm signal. The blood volume can be detected by measuring the pump rotations with the speed sensor of the BP.

Blood pump.

R-2 During initiation, the software shall monitor the blood flow in the EBC and if no flow is detected for more than 120 seconds, then the software shall stop the BP and execute an alarm signal.

R-3 During initiation, if the machine is not in bypass, then the software shall monitor the blood flow in the EBC and if the actual blood flow is less than 70% of the set blood flow, then the software shall execute an alarm signal.

R-4 During initiation, the software shall monitor the rotation direction of the BP and if the software detects that the BP rotates backwards, then the software shall stop the BP and execute an alarm signal.

Blood-side entry pressure.

R-5 During initiation, if the software detects that the pressure at the VP transducer exceeds the upper pressure limit, then the software shall stop the BP and execute an alarm signal.

R-6 During initiation, if the software detects that the pressure at the VP transducer falls below the lower pressure limit, then the software shall stop the BP and execute an alarm signal.

R-7 During initiation, if the software detects that the pressure at the AP transducer exceeds the upper pressure limit, then the software shall stop the BP and execute an alarm signal.

R-8 During initiation, if the software detects that the pressure at the AP transducer falls below the lower pressure limit, then the software shall stop the BP and execute an alarm signal.

R-9 While connecting the patient, if the software detects that the pressure at the VP transducer exceeds +450mmHg for more than 3 seconds, then the software shall stop the BP and execute an alarm signal.

R-10 While connecting the patient, if the software detects that the pressure at the VP transducer falls below the defined lower pressure limit for more than 3 seconds, then the software shall stop the BP and execute an alarm signal.

R-11 While connecting the patient, if the software detects that the pressure at the AP transducer falls below the lower pressure limit for more than 1 second, then the software shall stop the BP and execute an alarm signal.

R-12 During reinfusion, if the software detects that the pressure at the VP transducer exceeds +350mmHg for more than 3 seconds, then the software shall stop the BP and execute an alarm signal.

R-13 During reinfusion, if the software detects that the pressure at the AP transducer falls below -350mmHg for more than 1 second, then the software shall stop the BP and execute an alarm signal.

Connecting the patient.

R-14 While connecting the patient, the software shall monitor the blood flow in the EBC and if no flow is detected, then the software shall stop the BP and execute an alarm signal. The blood flow can be detected by measuring the pump rotations with the speed sensor of the BP.

R-15 While connecting the patient, the software shall monitor the filling blood volume of the EBC and if the filling blood volume exceeds 400 mL, then the software shall stop the BP and execute an alarm signal. The blood volume can be detected by measuring the pump rotations with the speed sensor of the BP.

R-16 While connecting the patient, the software shall use a timeout of 310 seconds after the first start of the BP. After this timeout, the software shall change to the initiation phase.

R-17 While connecting the patient, the software shall monitor the blood flow direction and if the reverse direction is detected, then the software shall stop the BP and execute an alarm signal. The blood flow direction can be detected by the direction sensor of the BP.

Flow bicarbonate concentrate into mixing chamber.

R-18 During preparation of the DF in the bicarbonate mode, if acid concentrate is provided instead of bicarbonate concentrate, then the software shall detect the mix-up of concentrates and disconnect the dialyzer from the DF and execute an alarm signal.

R-19 During preparation of the DF in bicarbonate mode, if acetate concentrate is provided instead of bicarbonate concentrate, then the software shall detect the mix-up of concentrates and disconnect the dialyzer from the DF and execute an alarm signal.

Heat and degas DF water.

R-20 If the machine is in the preparation phase and performs priming or rinsing or if the machine is in the initiation phase and if the temperature exceeds the maximum temperature of 41°C, then the software shall disconnect the dialyzer from the DF and execute an alarm signal.

R-21 If the machine is in the initiation phase and if the temperature falls below the minimum temperature of 33°C, then the software shall disconnect the dialyzer from the DF and execute an alarm signal.

Heparin.

R-22 If anticoagulant delivery is running, then the software shall monitor the anticoagulant flow direction and if the reverse direction is detected, then the software shall stop the blood flow and the anticoagulant flow, and execute an alarm signal.

Safety air detector.

R-23 If the machine is in the preparation phase and performing rinsing of the EBC or if the machine is connecting the patient or if the machine is in

the initiation phase or if the machine is in the reinfusion process, then the software shall monitor the flow through the SAD sensor and if the flow through the SAD sensor exceeds 1200 mL/min, then the software shall stop the BP and execute an alarm signal.

R-24 If the flow through the SAD sensor is in the range of 0 to 200 mL/min, then the software shall use an air volume of 0.2 mL as limit for air detection by the SAD sensor.

R-25 If the flow through the SAD sensor is in the range of 200 to 400 mL/min, then the software shall use an air volume of 0.3 mL as limit for air detection by the SAD sensor.

R-26 If the flow through the SAD sensor is greater than 400 mL/min, then the software shall use an air volume of 0.5 mL as limit for air detection by the SAD sensor.

R-27 The software shall update the air volume detected by the SAD sensor every 1 mS.

R-28 If the machine is in the preparation phase and performing rinsing of the EBC and if the software detects that the air volume exceeds the air volume limit depending on the actual flow through the venous blood line, then the software shall stop the blood flow and execute an alarm signal.

R-29 During the application of arterial bolus, if the software detects that the air volume exceeds the air volume limit depending on the actual flow through the venous blood line, then the software shall stop the blood flow and execute an alarm signal.

R-30 While connecting the patient, if the software detects that the air volume exceeds the air volume limit depending on the actual flow through the venous blood line, then the software shall stop the blood flow and execute an alarm signal.

R-31 During the initiation phase, if the software detects that the air volume exceeds the air volume limit depending on the actual flow through the venous blood line, then the software shall stop the blood flow and execute an alarm signal.

R-32 During the reinfusion process, if the software detects that the air volume exceeds the air volume limit depending on the actual flow through the venous blood line, then the software shall stop the blood flow and execute an alarm signal.

Ultrafiltration.

R-33 The software shall monitor the net fluid removal rate in the balance chamber and if the net fluid removal rate exceeds a safe upper limit, then the software shall stop flow from and to the dialyzer and execute an alarm signal.

R-34 If the machine is in the initiation phase and net fluid removal is enabled, then the software shall monitor the rotation direction of the UFP and if backward rotation of the UFP is detected, then the software shall put the machine in bypass and execute an alarm signal. The backward delivered volume shall not exceed 400 mL.

R-35 If the machine is in the initiation phase and net fluid removal is enabled, then the software shall monitor the net fluid removal volume and if the net fluid removal volume exceeds (UF set volume + 200 mL), then the software shall put the machine in bypass and execute an alarm signal. When the alarm is acknowledged by the user, then the software shall increase the UF set volume by 200 mL.

R-36 If the machine is in the initiation phase and net fluid removal is enabled and if the bypass valve is opened, then the software shall stop the DF flow to and from the dialyzer and execute an alarm signal.

5 Final Remarks

We have documented the requirements and design of an HD machine to provide an open example of model-based engineering of safety-critical active medical devices. We are now looking for solution models formulated in various rigorous methods and encompassing related high-level safety and efficacy properties whose correctness can be effectively asserted using conventional or unconventional verification and validation methods.