HRA Exercise – Case Study: The SPAR-H Method

System description♦:

Dissolver off-gas system.

The scenario concerns three tanks (see Figure 1), which are fed by steam to keep the chemical reaction at boiling point. Two fans extract the by-product gas from the reaction, and maintain the tanks under a slight vacuum. Only one of the fans is required to extract the gas and to maintain this partial vacuum, but both fans are nonetheless kept running. The scenario therefore concerns the failure of both these fans. When this happens, within 8-13 minutes, the tanks will reach atmospheric pressure and the off-gas will enter a potentially manned area. This is a highly undesirable event.

Interface description:

The operator in a local equipment room has one console, and 4-6 visual display units (monitor screens) (VDUs) and is connected to a central control room, where 1-2 supervisors are always present. Important operating parameters and control functions are displayed continuously on dedicated VDUs. Other less important functions will need to be accessed by means of a numerical code obtainable from a manual. Equipment status will be accessed in the same way (e.g. 'Feed Pump A running').

Alarms and trip functions are indicated on a dedicated VDU via a flashing line of print accompanied by an audible alarm. An 'Accept' button will be operated to silence the audible alarm until the next event, but the line of print is retained, and is steadily illuminated. It is possible to obtain print-outs of alarm sequences. The alarm/trip hierarchy uses different colors for three different priority levels of alarm. When a VDU alarm occurs, the operator targets 'Fetch alarm' at the bottom-right-hand side of the screen and presses 'Enter'; this takes the operator directly to the VDU mimic 'page' giving details of the alarm and of the relevant area. The operator may also, in multi-alarm situations dedicate one VDU screen to the function of an alarm VDU.

Training

The local operator (usually more than one per area) is well-trained for the activities at his post, with emphasis on the correct operating procedures for the specific tasks carried out at local control and equipment stations.

♦ This exercise is based on the materials for a case study (of Absolute Probability Judgment) described in Kirwan, B., A Guide to Practical Human Reliability Assessment, Taylor and Francis, London, 1994, pp. 436-452.

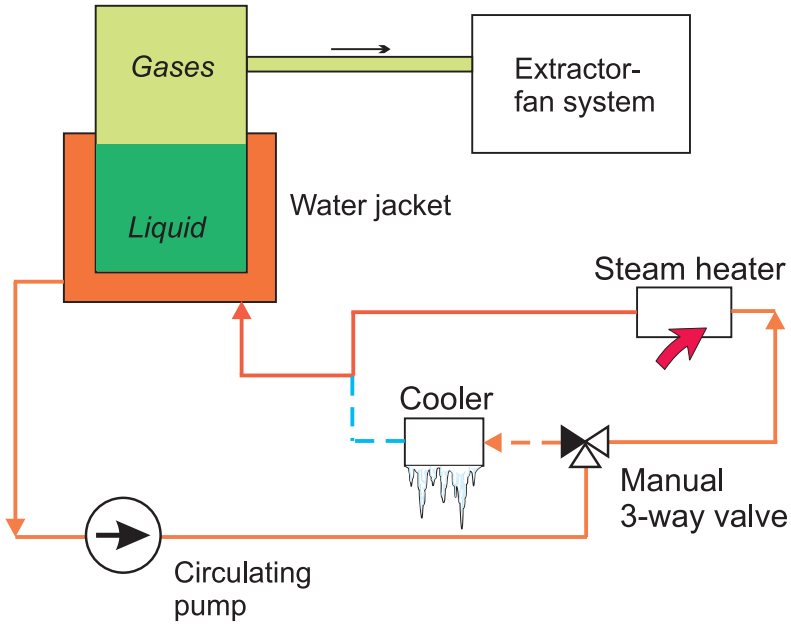

Figure 1. Tank system diagram

Scenario

In events involving the failure of both fans, the operator will receive an audible and flashing alarm. When he targets 'Fetch alarm', he will then be taken to another page showing the message that the two fans have stopped. A fan failure causes a trip of the following functions also, which will each trigger alarms on the VDU:

- **Inlet pipe**
- **Sparge air to tank**
- **Steam to heater**

However, these are not unambiguous indicators of a fan failure, since a spurious alarm set off in relation to the fans could spuriously trip this function (i.e. while the fans are actually still running).

The operator must therefore check to see (via the VDU mimic information system) whether there is:

- **Low pressure alarm on the fan discharge manifold**
- **Differential-pressure low alarm on three treatment columns in the off-gas system.**

These alarms should be triggered and also appear on the VDU system without the operator having to search for them. **In a correct diagnosis**, the operator will have decided that the fan failure is real and not spurious. At this point, he should enter the procedure or take action based on his or her memory of the procedures. **In the case of an incorrect diagnosis**, he concludes that the fan failure is spurious and fails to act.

System behavior:

Safety is assured if valves are in cooling position and pump is circulating. With the pump ON, there are 8-13 minutes available to switch the loops to cooling. With the pump OFF, there are 40 minutes available.

System failure modes (given no off-gas fans):

1. Valves are not in cooling position
   With pump on, time window (TW) =8 mins
   With pump off, TW=40 mins
2. Valves are in cooling position but pump is off
   TW=40 mins

Strategy of the procedure:
Move valves to cooling position and ensure pump is circulating

Possible incorrect understanding of the system:

1. System is OK if pump is off (no "feed" to system), i.e. failure to consider decay heat.
2. System is OK if valves are in cooling position, i.e. failure to consider need to circulate.

Procedure for Stoppage of Both Off-gas Fans

Entry condition: stoppage (failure) of off-gas fans

1. **Check that pump is ON**
2. **Check operational state of the loops**

State of loop	Loop 1	Loop 2	Loop 3
INPUT			
BLEACH			
TRANSFER			

3. **MOVE circulation (3-way) valves from HEATING to COOLING position in the following order**
   - **Circulation valve for Input Loop**
   - **Circulation valve for Bleach Loop**
   - **Circulation valve for Transfer Loop**
4. **IF pump has tripped, RESTART pump**

Analysis assumptions

No hardware failures and no instrumentation failures.
Pump may or may not trip after fan failure.

Operator actions to quantify

D-FAN FAILED the operator fails to conclude (diagnose) the fan failure as real (the operators incorrectly conclude the fan failure alarm is spurious)

HEOCA failure to move valves to cooling within 8 minutes, given successful diagnosis.

Operator action descriptions.

Applies to all of the following actions.

Training: The response to this scenario is walked-through once a year. The secondary solution is known among operators but is not proceduralized. However, it is not illegal.

D-FAN FAILED the operator fails to conclude (diagnose) the fan failure as real (the operators incorrectly conclude the fan failure alarm is spurious)

Procedural guidance: There does not appear to be a procedure.

Significant preceding actions:

Task complexity: The sequence of the 3 valves to be manipulated depends on the operational state of the three loops. The order should be "Input", "Bleach", and "Transfer". The valves are not in a room adjacent to the (local) control room.

Adequacy of time: Since it takes about 5 minutes to perform the manipulations (HEOCA), there are 3-8 minutes available. A time window of 3 minutes should be assumed.

Training: The response to this scenario is walked-through once a year.
.

HEOCA failure to move valves to cooling within 8 minutes, given successful diagnosis.

Procedural guidance: Step 2 of procedure

Significant preceding actions:

Task complexity: The sequence of the 3 valves to be manipulated depends on the operational state of the three loops. The order should be "Input", "Bleach", and "Transfer". The valves are not in a room adjacent to the (local) control room.

Adequacy of time: Training has shown that an experienced and trained operator requires 5 minutes to accomplish this series of tasks.

Training: The response to this scenario is walked-through once a year.

Event tree sequence descriptions:

1 : Successful diagnosis, pump does not trip, TW=8 mins, Move valves to cooling position < 8 mins - SUCC

2 : same as 1 except Failure to move valves to cooling positions < 8 mins - FAIL

3 : Successful diagnosis, pump trips, TW=40 mins, Move valves to cooling position < 40 mins, Restart pump < 40 mins - SUCC

4 : same as 3 except Failure to restart pump < 40 mins - FAIL

5 : Successful diagnosis, pump trips, TW=40 mins, Failure to move valves to cooling position - FAIL

6: Failure to diagnose, Secondary solution - trip pump, TW=40 mins, Move valves to cooling position < 40 mins, Restart pump - SUCC

7: same as 6 except Failure to restart pump - FAIL

8: Failure to diagnose, Secondary solution - trip pump, TW=40 mins, Failure to move valves to cooling position - FAIL

9: Failure to diagnose, Failure to reach secondary solution - FAIL

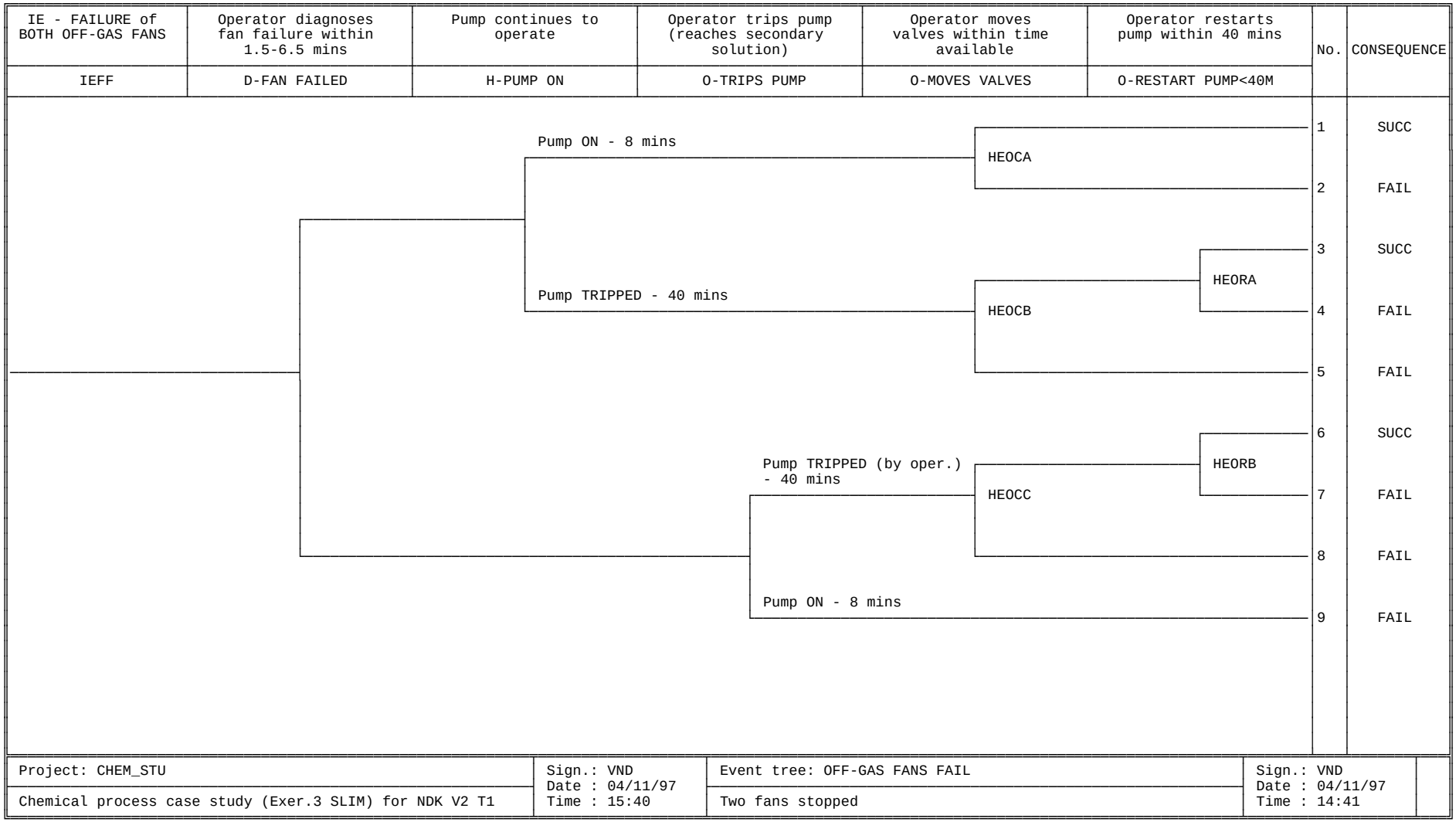

Figure 2. Event Tree For Nuclear Chemical System Study (SLIM Exercise)