



MODULAR PROGRAMME
ASSESSED COURSE-WORK SPECIFICATION

Module Details:

Module Code: UFMF3D-15-M	Module Title: Programming Embedded Systems	
Module Leader: Nigel Gunton		
Module Tutors: Nigel Gunton		
Assignment CW1	Element Number: Weighting 50%	Total Assignment Time: 20 hrs

Dates:

Date assignment issued to students: wb Oct 18th '11	Date for return of marked work: ??th ??/??
Submission Place: Project Room, 2Q30 open 09.00-18.00	Date of Submission: ??th ??? ??
	Time of Submission: 14.00am

Deliverables:

As listed on the Assignment spec sheet

1. Designing and Developing a Safety Critical System.

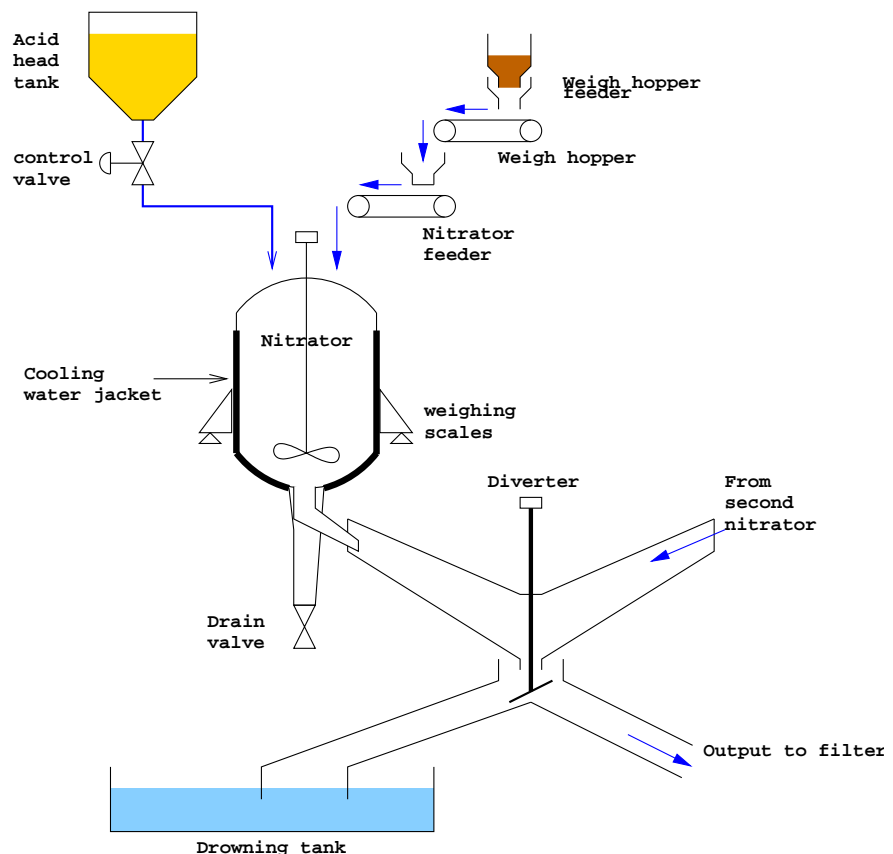
Overview¹

A manufacturing plant produces the explosive chemical pentaerythritol tetranitrate (PETN) by combining nitric acid and pentaerythritol (PE) in a batch process. An accurately weighed quantity of PE has to be added to a measured volume of nitric acid. The chemical reaction is exothermic, therefore the mixing vessel must be cooled while the reaction is taking place. The temperature must not exceed 35°C. An excess of PE will lead to increased temperatures as will impurities in the PE.

After the correct time interval, and assuming the temperature of the PETN has dropped to below a predetermined level, the PETN is released from the mixing vessel into a filtering system for further processing.

There is a risk of toxic fumes, fire and possible explosion if the mixing vessel overheats. In these circumstances the contents of the mixing vessel must be dumped into a drowning tank. The drowning tank must contain a minimum volume of water. Compressed air is then fed into the bottom of the drowning tank to ensure rapid mixing of the contents. The primary hazard of this process is decomposition due to overheating during mixing.

From *Safety Critical Computer Systems*, Storey, N. Figure 15.2



¹ Derived from the example in the HSE Guidelines, Part 2 (HSE, 1987)

2. Requirements:

To design an embedded system for the plant described above. The system should:

- monitor the plant status;
- ensure that the correct volume of acid is fed into the nitrator;
- ensure that the correct weight of PE is added to the nitrator;
- respond appropriately in the event of a nitrator temperature in excess of 35°C
- output the PETN to the filter when the temperature in the nitrator falls below 15°C

In order to do this you will need to identify the inputs and outputs needed for your system, the safety factors and critical conditions of the plant. You will also need to consider the reliability of the control system, the effect of failure of key components and the means by which control could be regained.

You will need to write a report, of up to 4,000 words, covering these factors and any assumptions that you make. Your code must also be included as an appendix to this document. It is assumed that you will develop at least part of your system in the C programming language using a small real-time operating system such as FreeRTOS and that it will be demonstrated on the Altera embedded boards. You should evaluate and document the performance of your implementation using the functionality provided within FreeRTOS.

To help you with starting the design and analysis, it is suggested that you take the following steps.

- 1 Perform a safety assessment of the plant using the HSE guidelines discussed in the lecture:
 - hazard analysis
 - identification of safety related systems
 - allocation of safety integrity requirements
 - design to meet integrity requirements
 - analysis of safety integrity
 - comparison of integrity achieved with that required
- 2 Implement first and second level fault trees for the primary hazard of this plant. The full fault tree analysis for this plant could run to 12 levels.
- 3 Identify all the sensors and actuators required on the plant. Note that they are not all shown on the diagram.
- 4 Identify independent software tasks to implement the control and safety of the plant along with any necessary communication channels between the tasks.
- 5 Allocate priorities and periodicity to the tasks and assess the schedulability using the Rate Monotonic Algorithm. You will need to make assumptions regarding the timing and flow rates of the process.
- 6 Identify any areas where there may be a risk of priority inversion.
- n Implement and verify aspects of your design.

3. Marks Allocation

No detailed marking scheme is provided as there is likely to be a wide variety in the designs. However there will be ongoing discussion and feedback as the work progresses. A general guideline to the standard of work required can be found via the module web page. Remember that the pass mark is 50%, the minimum standard that you should achieve.

4. Resources

Reference material will be made available on the module webpage and via the tutorials.

The document at http://www.cems.uwe.ac.uk/~ngunton/worksheets/sil_proposals.pdf provides an overview of the different safety levels and may be used to judge the required safety level of this plant.

This assignment should be done in line with the IEC 61508 guidelines on software in programmable electronic systems, which is available electronically via the UWE library web-site. The documents can be found via the BSI link. (British Standards Institute).

It may be beneficial to review the documentation on the use of C programmes in the motor industry. The MISRA C documents are also available from the library.

5. Deliverables

- A fully referenced document describing your designs and conclusions from points 1 - 6 under section 2 above.
- An appendix containing your code.