SYSTEMS & SOFTWARE SAFETY

COMP8180

TAKE HOME EXAMINATION (THE)

2014

THE questions have been generously provided by the High Integrity Systems Group from the University of York, UK.

Instructions:

Attempt **ALL** questions.

The completed THE must be submitted in electronic form no later than **18:00 on June 13, 2014.**

See end of THE for details on submission.

Please note:

This THE represents **100%** of the COMP8180 course assessment.

Drawings and diagrams do not have to be created using computerised tools. Such items can be done by hand provided that they are neat, readable, and labelled appropriately with your name and the question number. Such items can be scanned and attached to an electronic THE submission at the appropriate place if so desired.

This THE is intended for ***INDIVIDUAL*** effort. As for any assessment material, plagiarism rules apply.

Question 1 [35 marks]

HomeSpa Ltd. produces a range of luxury small saunas and steam showers for domestic use. A steam shower is a large shower enclosure, fitted with a steam generator unit and a moulded seat, within which the user can enjoy a “steam bathing” experience like the steam rooms often found in spas and hotel sports centres. A dispensing unit allows controlled amounts of fragrant oils such as eucalyptus to be added to the steam if required.

A partial projection of a typical HomeSpa steam shower installation is shown in Figure 1, and a schematic of the plumbing and wiring installation is shown in Figure 2.

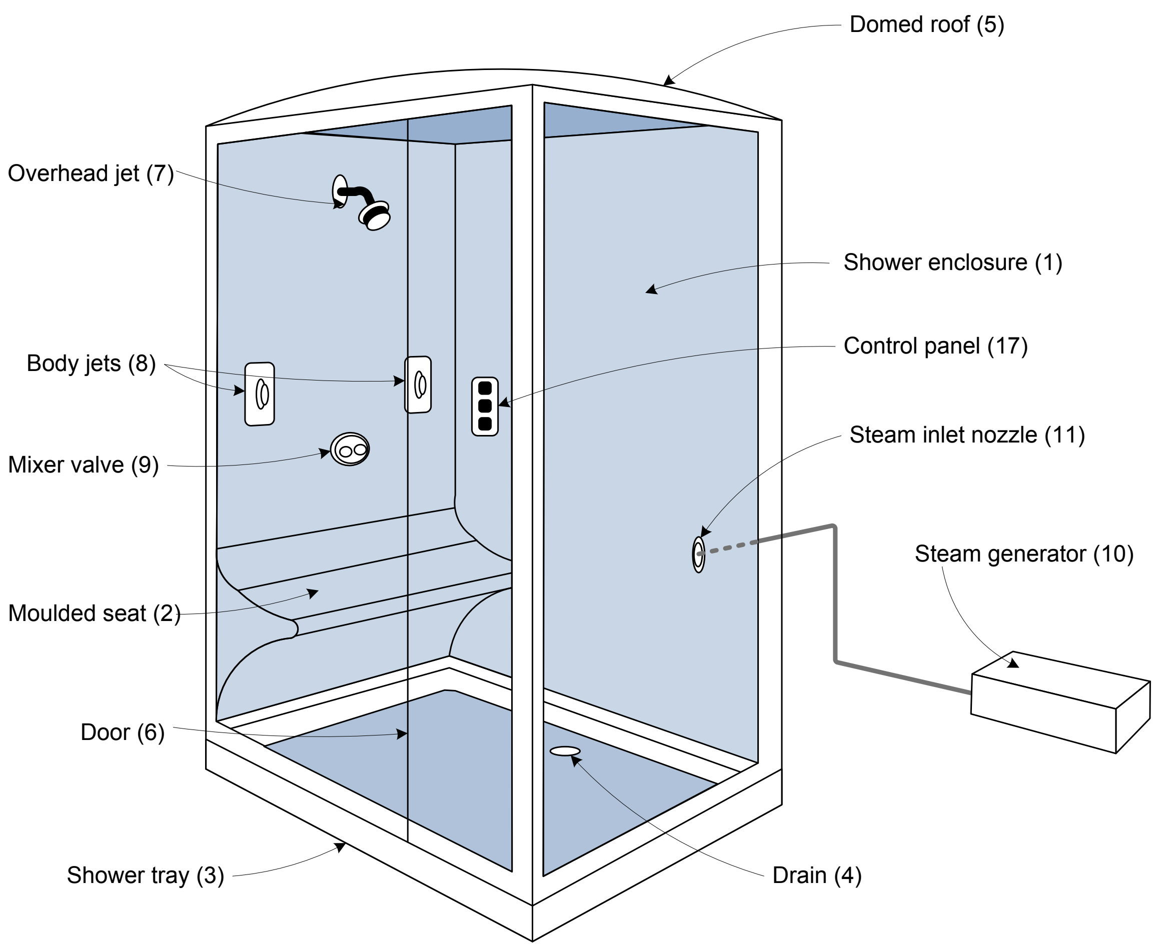

Figure 1: Steam shower

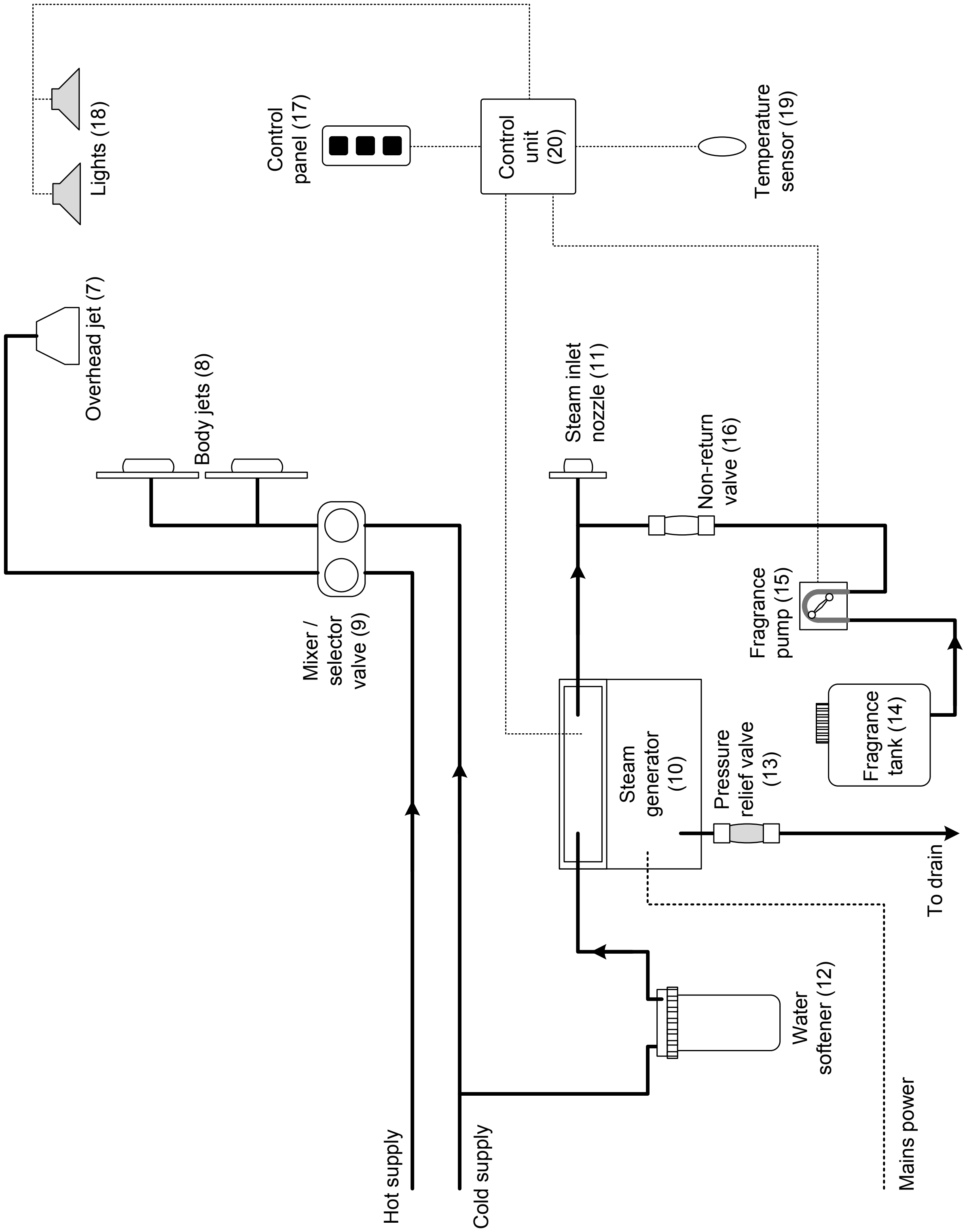

Figure 2: Steam shower plumbing and wiring schematic

The shower enclosure (1) is a single-piece moulding in heavy-gauge acrylic sheeting, so that there are no joints that can leak or act as traps for dirt or mould. The acrylic is bonded with a thick layer of fibreglass, moulded around a frame that supports and strengthens the enclosure, especially providing support for the moulded seat (2). The enclosure stands on the shower tray (3), which is simply a larger version of a conventional shower tray, with normal plumbing to a drain (4). The enclosure is completed by a domed acrylic roof (5) and hinged safety-glass door (6).

Within the enclosure are the conventional shower fittings; these consist of an overhead jet (7) and body jets (8) controlled by a thermostatic mixer/selector valve (9). The plumbing connections between the mixer valve and the shower jets are made on the outside of the shower enclosure. Hot and cold water are supplied to the thermostatic mixer/selector valve from the domestic hot and cold water supplies in exactly the same way as for a conventional shower.

Steam is produced by the steam generator (10), mounted outside the shower enclosure, and enters the enclosure through the steam inlet nozzle (11). Cold water is supplied to the steam generator through the water softener (12), and the steam generator has a safety pressure-release valve (13) that is connected directly to the drain. Oil from the fragrance tank (14) is dispensed into the steam just before it enters the shower enclosure by the fragrance pump (15) via a non-return valve (16).

The user selects steam generator and fragrance pump functions using the low-voltage control panel (17) inside the shower enclosure, which also controls the low-voltage lighting (18) inside the shower enclosure. The temperature sensor (19) monitors the temperature within the enclosure. All of the steam, fragrance and lighting functions are switched through the main control unit (20), located outside the enclosure. This control unit is relatively simple, containing only minimal discrete logic and relay switching.

(i) **[6 marks]**
Use the hazard checklist provided in the file named "*Q1-Hazard-Checklist-2014.pdf*" to identify potential hazards from the HomeSpa steam shower system.

(ii) **[8 marks]**
Repeat your hazard identification, this time using Energy Trace and Barrier Analysis. Full checklists of energy types, barrier and energy conversion problems are provided in the file named "*Q1-ETBA-Checklist-2014.pdf*".

(iii) **[5 marks]**
Compare and comment on your results from parts (i) and (ii), considering (at least) the effectiveness of the techniques, their ease (or otherwise) of application and effort required.

(iv) **[16 marks]**
Carry out a HAZOP study of the steam shower system. Ensure that your study clearly identifies:

- Which flow(s) are being considered
- Potential deviations from correct behaviour
- Effects of these deviations, and which effects are potentially hazardous
- Possible causes of these deviations

- Existing features of the design of the system which will eliminate, control or mitigate the potential hazards
- Any recommendations you may have for further (safety-related) improvements to the system design.

IMPORTANT: This analysis clearly has the potential to become very large. In presenting your answer, it is acceptable to select the most interesting results from your analysis. However, you must clearly state that you have chosen to do this, and summarise what you have omitted.

HINT: You may wish to consider that electrical current flows.

Question 2 *[25 marks]*

An emergency disease response centre stores large quantities of vaccine, which must be kept refrigerated. Vaccine that is not properly stored at appropriate temperatures will degrade and may even become harmful if administered to people. If the temperature of stored vaccine cannot be maintained, it must therefore be destroyed. The refrigeration facility is shown schematically in Figure 3.

The insulated vaccine store [1] has a refrigeration system that works on the same principle as a domestic refrigerator. It consists of a compressor [2], heat-exchange coils outside the insulated store [3], an expansion valve [4], and heat exchange coils inside the insulated store [5]. The heat exchange circuit is filled with a refrigerant gas. The compressor is powered by an electric motor [6].

As the compressor runs, it compresses the refrigerant gas, which heats up as it is pressurized. The heat exchange coils outside the store become hot, and dissipate heat to the surrounding atmosphere. As the compressed gas flows through the expansion valve, it expands and cools, because the action of the compressor reduces the pressure within the heat exchange coils inside the store. These coils become cold, absorbing heat from inside the store and cooling it. The refrigerant gas flows back to the compressor, completing the cycle.

The operation of the refrigeration system is controlled by a thermostat [7], which switches the electric motor on when the temperature inside the store rises above a set point, and switches it off again when it has been sufficiently lowered.

The refrigeration system has sufficient capacity to maintain the temperature of the entire store in all anticipated environmental and operating conditions.

The refrigeration system is normally powered from the site mains electrical supply [8]. If the mains supply fails, the voltage monitor [9] will start the diesel engine [10] which powers the backup generator [11]. Once the generator has stabilized, the switch [12] will switch over automatically so that the backup supply powers the refrigeration systems. Starting the diesel engine requires that the battery [13] is well charged, and that the starter motor [14] is working. The engine uses diesel from a fuel tank [15].

It is considered acceptable to have a single voltage monitor and automatic switch, as the failure of the mains power will be noticed by staff (there are staff on site 24 hours a day), and the switch [12] can be operated manually if automatic switch-over does not occur.

There will be no power for a few seconds whilst the backup supply starts and stabilizes, but this is not a problem. The store is well insulated and it will take an appreciable period of time (several hours) for the internal temperature to become dangerously high provided that the door is not opened. There is therefore an indicator [16] which shows that the refrigeration system is running; procedures prohibit staff from opening the door unless the refrigeration system is working.

Switching back to mains power once electrical supplies are restored is again automatic, but can also be achieved manually if required.

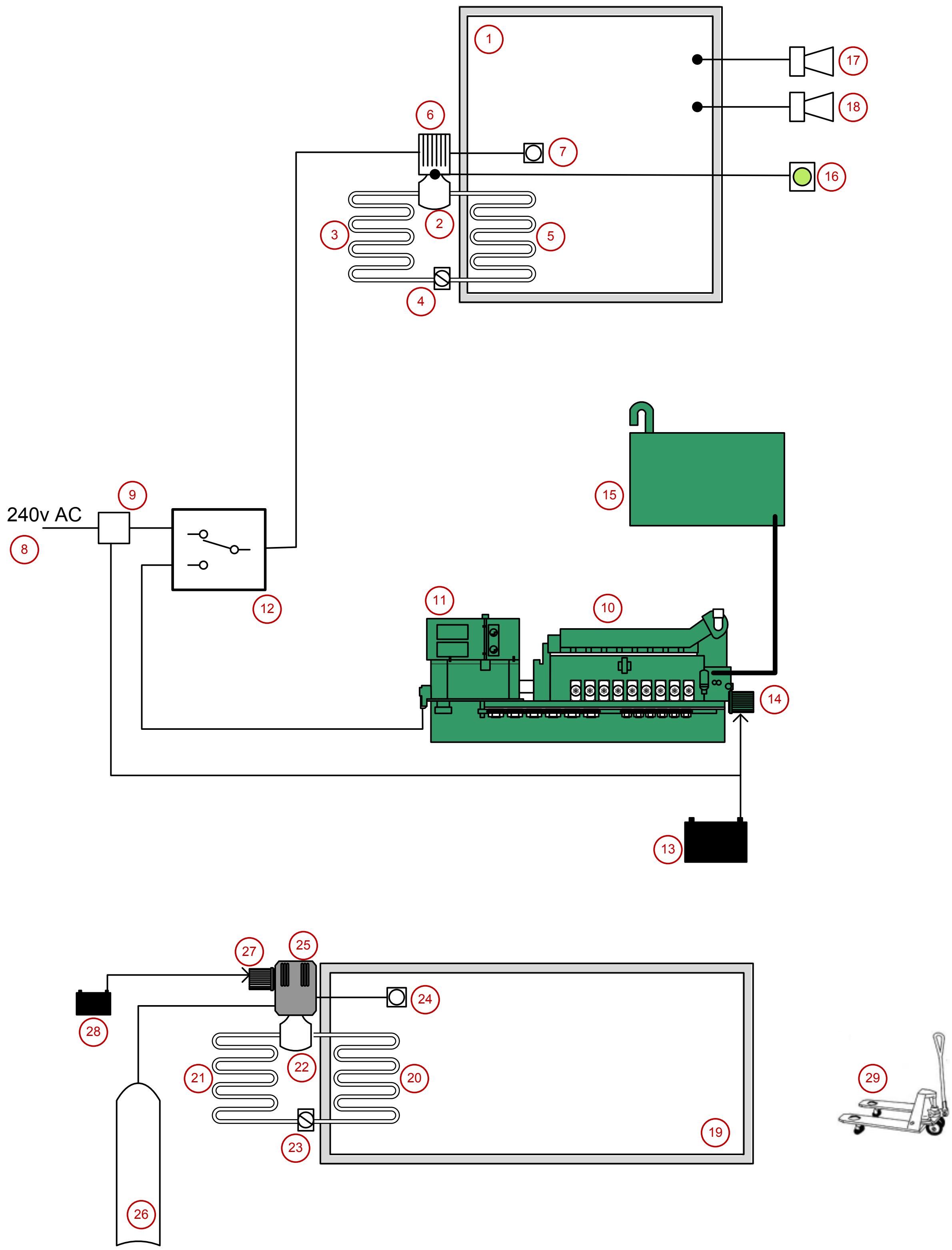

Figure 3 – Vaccine refrigeration facility schematic

The store is fitted with two independent high-temperature alarms [17, 18], which are set to sound at a temperature that is above the normal storage temperature but below the temperature at which the vaccine would be harmed.

In case the main refrigerated store fails, the site has a refrigerated shipping container [19] available as a completely independent storage facility. This is essentially a standard insulated shipping container equipped with a refrigeration system, which works on exactly the same principles as the refrigeration system on the main store, having internal [20] and external [21] heat exchange coils, a compressor [22], an expansion valve [23] and a control thermostat [24]. The compressor on this system is powered by a small engine [25], which runs on gas from a storage cylinder [26]. The engine is started manually, using the starter motor [27] and battery [28].

Once started, the refrigeration system will take some time to bring the shipping container down to the proper vaccine storage temperature, although this can be achieved before the temperature in the main store rises too high, provided procedures regarding non-opening of the store door are observed. Once a decision is taken to move the vaccine to the shipping container for continued cold storage, this must be done quickly. To achieve this, entire racks of shelves are moved using a special trolley [29].

i) [20 marks]

Construct a fault tree for the event "Disease response centre unable to provide refrigerated vaccine storage" down to the level of detail provided in the description of the system and diagram above.

There is no need to try to represent the effects of time in your fault tree; (e.g. it will be acceptable to use standard AND gates rather than priority-AND gates even where there is a definite order of failure).

State any assumptions you make in completing your fault tree.

- There is no requirement to use software tools to produce the fault tree required by this question. The marking scheme is such that those students who have access to tools will have no advantage over those who do not.
- Use standard fault-tree symbols. A neat hand-drawn tree using the standard symbols is preferable to a non-standard notation. ("Tagged" events, such as are produced by the Fault Tree Plus tool, are acceptable.)

ii) [5 marks]

Identify which events in your tree represent potential dormant failures.

Question 3 [25 marks]

Coyote Technology Ltd is a well-established firm specialising in industrial weighing and measuring equipment. One of their key products is a range of overload warning and protection devices for cranes.

The original “Coyote CheckWeight”, designed in the 1960s, was an electro-mechanical overload warning device, fitted to mobile cranes with a lift capacity of no more than 10 tons. The crane operator set a “lift duty”, which identified basic parameters of how the crane was being operated (e.g. length of the jib). The “CheckWeight” system combined the lift duty with measurements of the angle of elevation of the jib and the pressure in the hydraulic system to activate warning lights and a bell when the safe load capacity of the crane was approached and/or exceeded.

The system “calculated” when the safe load limit was being exceeded by using a set of cams, working against a pair of micro-switches (one for “approaching limit” and one for “limit exceeded”). The initial position of the cams was established when the lift duty was set, and subsequent changes in the elevation of the jib or the hydraulic pressure caused the cams to rotate. This system was simple and robust, but had the disadvantage that the cam profiles were unique to each application; to fit the device to a new model of crane, it was necessary to design and manufacture new cams. There was no active protection function; safety relied on the operator taking heed of the warnings, and returning the crane to a safe condition. However, the device was reliable and competitively priced, and the company gained a significant market share.

Over the next three decades, the requirements for crane safety became increasingly stringent, and the company responded by adding additional functionality. A simple system was devised to measure jib extension automatically, instead of requiring the operator to set it manually, and protection was also incorporated against under- and over-winding the cable (i.e. so that either the hook block would be pulled all the way up and impact the jib, or all the cable on the drum would be wound out). However, these functions added significant complexity to the initially simple design, and users began to report reliability issues, and problems with poor sensitivity of calibration.

A key requirement of modern crane safety standards is that active protection (load limiting) devices are required, rather than merely overload warning. This implies a need to integrate the safe load calculations with the crane control functions to prevent the operator continuing with actions that would result in unsafe conditions (e.g. increasing the working radius by further lowering or extending the jib after the load limit has been reached).

Coyote Technologies concluded that the requirements of these new standards could not be satisfied by further development of electro-mechanical designs. This conclusion, combined with the need to improve reliability and calibration accuracy, led to the decision to develop a completely new range of computer-based overload warning and protection devices.

The Coyote CheckWeight 2000 was designed as a flexible, extensible system, which could be rapidly customised and calibrated to suit a very wide range of mobile cranes. The heart of the new system is a control and interface panel fitted in the cab of the crane (Figure 4).

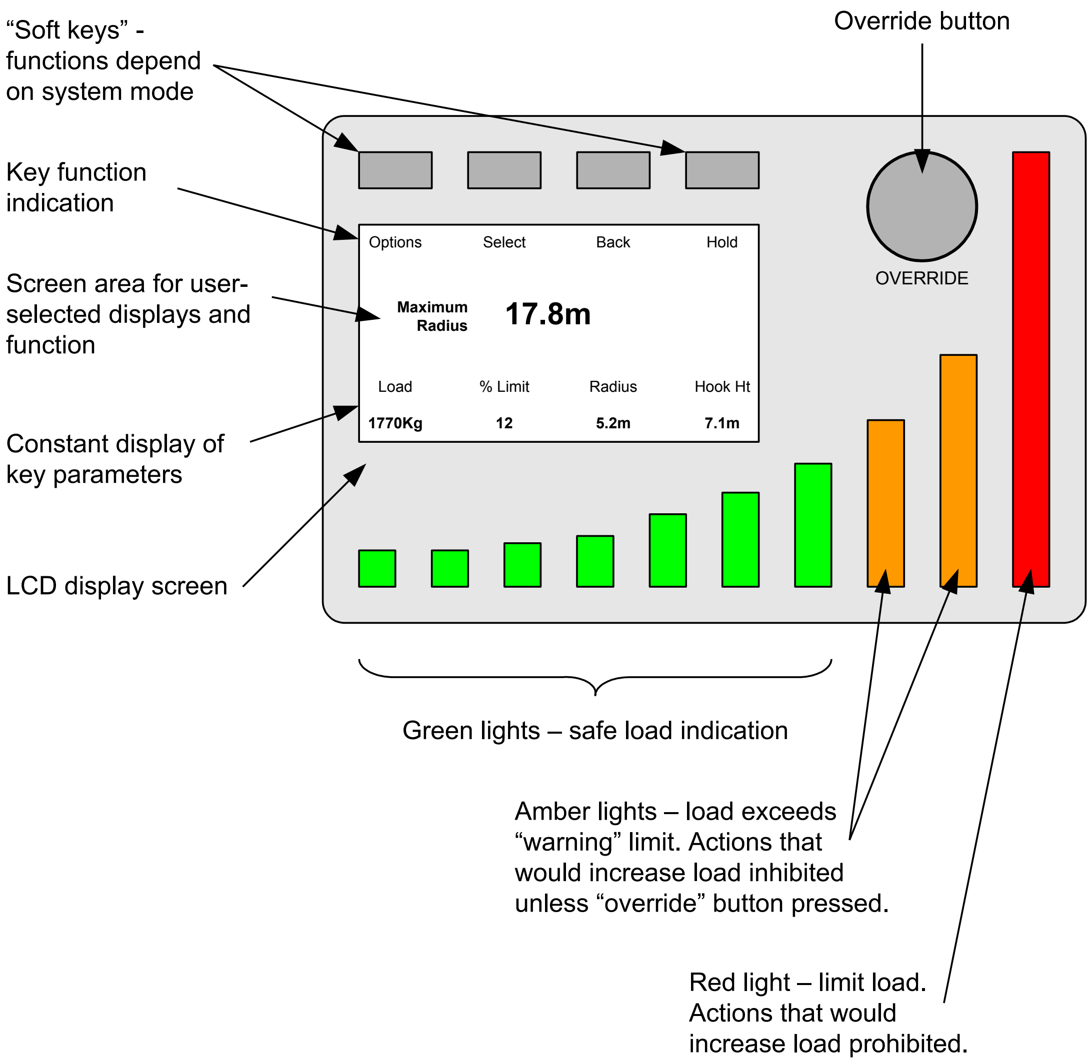

Figure 4 – Coyote CheckWeight 2000 Control / Interface Panel

In every application, the system will always be fitted with sensors for key parameters:

- Jib length
- Jib elevation angle (this is combined with jib length to calculate the effective working radius)
- Pressure in the hydraulic ram which elevates the jib
- Cable over-wind or under-wind.

Extra data may be needed for correct load calculation in some cases:

- Load weighing via a load cell in the hook block
- Outrigger deployment (i.e. whether the crane is being operated just on its wheels, or with the hydraulically operated outrigger feet lowered)
- Outrigger length (the effective base area of some cranes can be increased by extending the outrigger feet sideways on steel beams)
- Whether a fly jib is in use, and its effective length
- Whether the load is being lifted single- or double-cable.

Key parameters are illustrated in Figure 5.

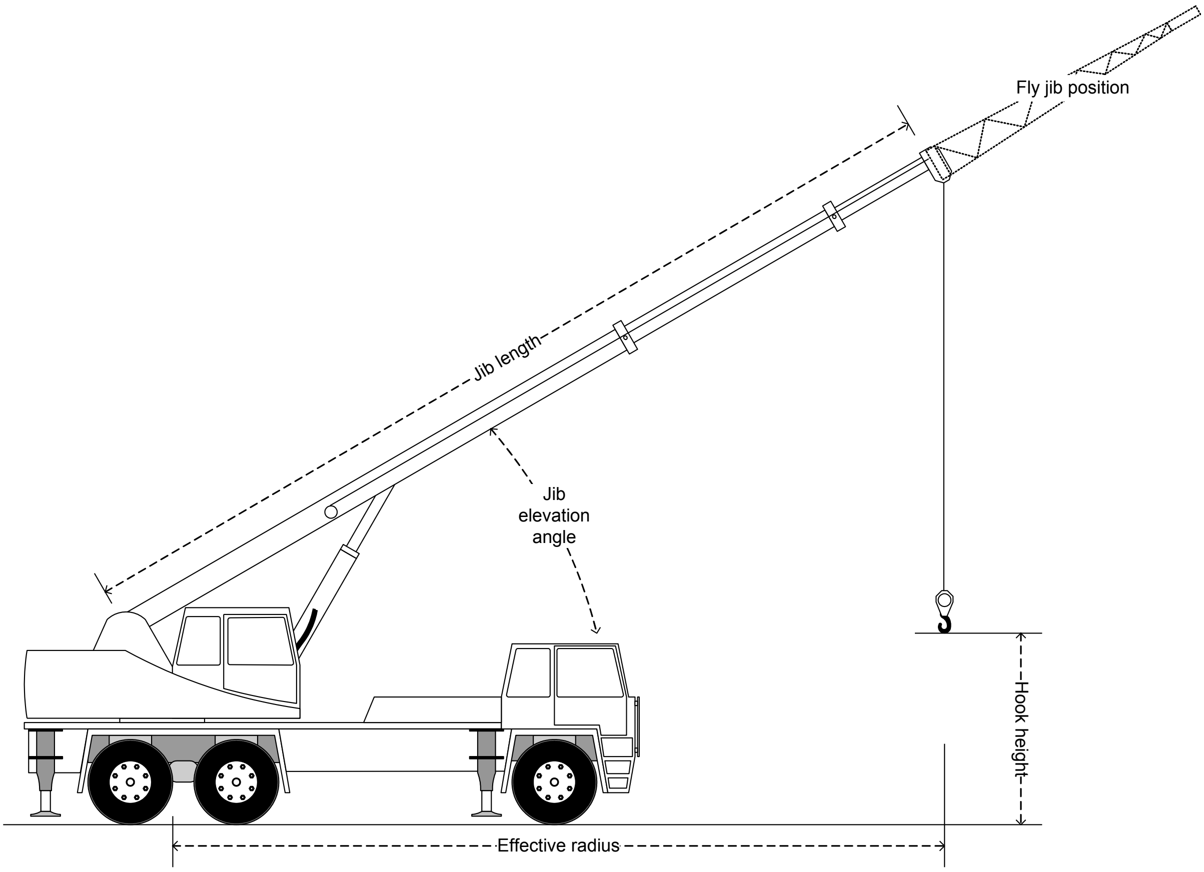

Figure 5 – Typical mobile crane showing key parameters

The CheckWeight 2000 incorporates circuitry for some of the optional inputs, but also allows any of these parameters (except for load weight) to be entered manually by the operator if sensors are not fitted. (If a load weight sensor is not fitted, the load weight is calculated indirectly from other parameters). The system also provides seven additional binary (on/off) inputs and three spare analogue inputs (with analogue-to-digital converters), which can be used as required when configuring the system to suit specific cranes.

The system is designed to provide increased protection over earlier devices by forcing the operator to acknowledge when the limits of safe operation are being approached, and actively preventing limits being exceeded. To achieve this, the

CheckWeight 2000 incorporates a set of relays. These relays function as switches which are normally closed (switch on), but which are opened (switch off) when the load reaches the limit. By connecting these into the crane's operating controls, unsafe actions can be prevented. The relays open at the "warning" load, but the operator is provided with an override button; by holding this button in, he can continue with actions that increase the load on the crane. However, when the "limit" load is reached, the relays will open regardless of whether the override button is being held. This ensures that the limit load can never be reached unexpectedly; the operator must have previously acknowledged a warning state by pressing the override.

The CheckWeight 2000 panel constantly gives a visual indication of how the lift in progress relates to maximum safe working load, using a set of green, amber and red lights. In addition, the LCD display screen constantly shows key parameters such as the current load weight, percentage of safe working load, hook height and current effective working radius. The system provides a number of "convenience" functions for the crane operator, including the ability to perform calculations such as determining the maximum safe radius for a given load.

The CheckWeight 2000 also incorporates a "lift history" function. Key parameters of every lift that the crane makes are stored in flash memory in the control panel, and a serial port is provided so that a computer can be connected to download the data. This allows crane operators to build up a history of the work a crane has done, which can be used to assist in planning maintenance and inspection, or determining when components such as the main lift cable are reaching the end of their safe lives.

The main inputs and outputs of the CheckWeight 2000 are summarised in Tables 1 and 2.

Table 1 – CheckWeight 2000 Primary Inputs

Input	**Data Type**	**Description**
Jib length	16 bit word	Jib length, measured by drum and cable mechanism on side of jib. Mechanism returns an analogue value, converted to digital by input circuitry. Relationship between data value and actual jib length is calibration parameter.
Jib elevation angle 1	16 bit word	Jib elevation angle, measured by gear-driven potentiometer from jib pivot. Analogue value converted to digital by input circuitry. Relationship between data value and actual jib elevation angle is calibration parameter.
Jib elevation angle 2	16 bit word	As jib elevation angle 1 (redundant input)
Ram pressure 1	16 bit word	Pressure in hydraulic ram that elevates jib. Measured by pressure transducer in hydraulic system. Analogue value converted to digital by input circuitry. Relationship between data value and actual hydraulic pressure is calibration parameter.
Ram pressure 2	16 bit word	As ram pressure 1 (redundant input)

Two block	Binary	Cable under-wind (hook block about to contact jib). Returned by a microswitch actuated by a collar on the cable 100mm above hook block. Negative logic, i.e. binary "0" indicates under-wind TRUE (NB thus fail-safe, as any wiring or electrical fault will appear to indicate under-wind condition).
Cable out	Binary	Cable wound out to maximum extent (attempting further extension will begin to reverse-wind cable on drum). Condition sensed by microswitch activated by follower on threaded rod driven from drum. Negative logic, i.e. binary "0" indicates cable out TRUE (NB thus fail-safe, as any wiring or electrical fault will appear to indicate cable out condition).
Load weight	(Optional) 16 bit word	Measured by load cell in hook block. Analogue value converted to digital by input circuitry. Relationship between data value and actual suspended mass is calibration parameter.
Outrigger 1	(Optional) Binary	Front left outrigger deployed. Sensed by microswitch in outrigger leg mechanism.
Outrigger 2,3,4	(Optional) 3 x Binary	As outrigger 1 for front right, rear left and rear right outriggers respectively.
Fly jib rigged	(Optional) Binary	Fly jib fitted. Sensed by microswitch on fly jib mounting plate.
Analogue 1,2,3	(Spare) 16 bit word	Spare A-D channels for expansion / configuration use.
Binary 1-7	(Spare) 7 x Binary	Spare binary inputs for expansion / configuration use.
Button 1-4	4 x Binary	Soft key inputs from panel.
Override	Binary	Override button input from panel.

Table 2 – CheckWeight 2000 Primary Outputs

Output	Data Type	Description
Alarm	Binary	Activates built-in alarm sounder in panel.
Relay	Binary	Activates all the control function interlock relays. Negative logic, i.e. relays default to contact OPEN state (control functions inhibited); relay output must be held high (binary "1") to enable operation – thus fail-safe.
Segment 1-10	10 x Binary	Drives 7 x green + 2 x amber + 1 x red lights on panel.

Internally, the design of the CheckWeight 2000 is fairly simple. There are four separate circuit boards:

- input circuitry including filtering, protection and analogue-to-digital converters where required; binary (on/off) input circuits also include opto-isolators, so that there is no direct electrical connection between switches which run at the crane battery voltage (12 or 24V) and the inputs to the computer system.
- the user interface circuit board, which carries the warning lights and buttons.
- the main computer board, with the CPU, support chipset (such as system clock and timers), RAM, program EPROM, configuration EPROM and flash memory to store lift history. The LED display is also driven directly from this board.
- the output board, which carries the relays used to inhibit unsafe control operation.

Note that the company's intention is that the core software should never change; customisation for each model of crane to which the system is fitted will be achieved by changing the calibration parameters (mostly look-up tables mapping sensor values to engineering units) in the configuration EPROM.

IMPORTANT – in answering parts i) and ii), you should take "the computer" to mean the main computer board.

i) [5 marks]

Examine the computer system outputs:

- What are the controlled (real world) variables in this system?
- What are the actual outputs from the computer? How do these correspond to the controlled variables?
- Which computer system outputs represent (safety) critical information?
- What are the potentially hazardous failure modes of the outputs?
- In designing the software for this computer system, which output(s) would you prioritise, and why?

ii) [8 marks]

Now consider the computer system inputs:

- What are the monitored (real world) variables in this system?
- What actual inputs are available to the computer? How do these correspond to the monitored variables?
- Which inputs represent (safety) critical information?
- How quickly will the software need to respond to each input?
- What faults are possible on the inputs? Are these faults detectable? How? How should the software respond to detected faults?
- In designing the software for this computer system, which input(s) would you prioritise, and why?

iii) [4 marks]

What do you think are the principal modes of operation of the CheckWeight 2000? Represent these *either* as a mode table, or as a state transition diagram. Whichever you choose to use, make sure that the events that trigger mode transitions are clearly identified.

Which of the modes represent normal operation of the system, and which represent failure detection and management?

iv) [4 marks]

Coyote Technology's software engineers propose to implement the controller software primarily in MISRA C, with small sections of code written in assembly language where they believe this is necessary (for example, to implement interface code for some of the hardware devices). They do not intend to buy in or implement an operating system; all the functions will be implemented as procedure calls from a single main loop. However, they do intend to write a set of functions to implement the hardware interfaces – effectively a minimal hardware abstraction layer – so that the main blocks of functional code could be reused on different hardware without modification.

- What are the positives and negatives of these choices?
- Do you think these are reasonable decisions for this system?

v) [4 marks]

What are the implications of the decision to separate the code from the configuration data? Is this a sensible decision for this system?

Question 4 [15 marks]

NOTE: This question requires reading (but not necessarily answering) Question 3.

The Tokushima Engineering Corporation of Japan has recently launched a new range of mobile cranes. The new models are distinguished by the use of novel materials and modern structural engineering design techniques, which give them exceptionally good lift capacity for a given crane weight. The heavier cranes in the range are also built with removable ballast and counterweights, so that the travelling weight of the crane can be reduced; the ballast and counterweights are carried on separate trucks, and fitted to the crane when it reaches each work site.

Topsborough Plant Services (TPS) has been awarded the UK distribution contract for these new cranes, and has concluded that the Coyote CheckWeight 2000 appears to be an ideal overload warning and protection system to supply with the range. The expansion capability of the CheckWeight 2000 will make it possible, for example, to provide automatic detection of whether the removable counterweights are in place.

However, Mike Dent, TPS's chief engineer, is concerned about the company's liability in supplying this system; the company has almost no software expertise and, as well as buying the CheckWeight 2000 systems from Coyote, will also need them to produce the configuration of the system to suit the Tokushima range.

Having taken advice from a specialist safety consultant, Mike concludes that Coyote need to supply a software safety case to demonstrate the acceptability of their product. Coyote have never produced a software safety case as such, although they believe they have ample evidence to support their product. They agree to work with Topsborough Safety Services (TSS) – an independent safety consultancy with extensive software experience – to develop a suitable safety case.

TSS review the documentation available from Coyote, and visit their premises to inspect their procedures, with the following results.

1. Before commencing software development, Coyote carried out a full hazard identification and risk analysis at the system level. This was followed by a functional failure analysis of the software functions (excluding the lift history logging).

2. Coyote did not attempt to assign any sort of safety integrity level (SIL) or Development Assurance Level (DAL) to the software functions, nor did they attempt to follow any SIL or DAL conformance processes defined by any particular standard. However, the entire development team is familiar with the application domain, and were well aware of the criticality of the system they were developing. The team was also given a briefing about the need to document design and development decisions so that the company could demonstrate that it had exercised its duty of care in the development of the CheckWeight 2000.

3. The software requirements have been developed using a requirements management tool. They are mostly expressed in English, but the tool has a dictionary facility, which has been used very carefully to define all the important items. The language used is mostly very precise, and strenuous efforts have been made to avoid ambiguity. Where requirements describe mathematical functions, a formal, mathematical notation has been used. Traceability has also been carefully maintained; it is possible to identify the original source of every requirement (most safety requirements are traceable back to the functional failure analysis, for example), as well as the full modification history. A formal Software Requirements Specification (SRS) was produced from the management tool before coding commenced, and subsequent modifications have been issued as updates to the SRS.

4. There is relatively little software design documentation, other than a top level architecture sketch. The software engineers mainly relied on flow charts to represent the logical structure of the code, and worked directly from the mathematical specifications to implement calculations.

5. The code itself appears to have been produced to a high quality. It follows a well-defined modular structure, and every module and function is carefully commented; the comments include traceability back to the SRS.

6. Each code module was subjected to formal peer review (including a walk-through) as it was completed. These reviews have been recorded and minuted, where problems were found, the follow-up actions have also been documented.

7. The code has been subjected to automated MISRA C conformance checking.

8. The SRS was also used to produce separate test specifications for the software modules. These test specifications have been used to develop a suite of test programs, which were designed and coded by a separate small team of engineers.

9. The software was compiled using the GCC compiler, using it initially to compile the code for host testing, and then as a cross-compiler to produce executable code to run on the real hardware.

10. Each module of code was subjected to host testing using the test suite, and then tested on the real hardware using lab equipment to simulate the sensor inputs. All the test parameters and results were logged. 26 errors were found in host testing. 9 of these errors were traced to ambiguities or errors in the SRS, which was corrected and updated. The remainder of the errors were coding faults; all were corrected, and the corrections carefully documented. The lab testing on the real hardware achieved a 100% pass rate.

11. After integration of the separate code modules, the complete CheckWeight 2000 program was subjected to further lab testing, followed by calibration and testing on three different models of real crane. Again, all the test parameters and results were recorded. These tests showed that all the warning and protection functions of the software performed precisely as required. However, it was discovered that the lift history logging functions contained a number of errors, the most serious of which was that each time the unit was switched on, it started recording logging information in the same location in the flash memory, so the history of previous lifts was over-written. The lift history logging functions were therefore subjected to a more rigorous review, and the errors identified were corrected.

12. Configuration data for each new model of crane is initially developed using a standard spread sheet package. Each set of data is plotted as a graph, to ensure that it contains no anomalous data points. Once completed, the data is transferred to a download utility program written by Coyote, which is used to create the EPROM. The system is then tested by using the crane to make a series of lifts using certified test loads under controlled conditions, and checking that the results calculated by the system are within a 1.5% tolerance of the actual loads. All of the calibration test parameters are recorded on a digital data logger.

Imagine you are employed by TSS, and have been asked to work on the Coyote CheckWeight 2000 safety case.

i) **[8 marks]**
Sketch out the structure of a suitable safety argument for this software, making best use of the evidence identified in points 1-12 above. Ideally, this argument structure should be presented in GSN, although there will be no penalty if you are unfamiliar with GSN and choose to use another method (e.g. plain text, or tables) provided that the argument is clear. [Hint: Your argument should consider both the software itself, and the process of producing the calibration data.]

ii) **[7 marks]**
Is there sufficient evidence (as identified in points 1-12 above) available to make a compelling argument? If not, identify what else you believe is needed, and explain why. [IMPORTANT – you should treat this as a real, practical problem, and only ask for evidence which is really necessary to complete your safety case, and that is reasonably practicable to provide. Answers that require every conceivable analysis and trial will attract a low mark!]. Is any of the evidence identified in points 1-12 above of no use in supporting your argument?

COMPLETED THE SUBMISSION

Your completed THE should be emailed to me in electronic format (preferably ‘pdf’) at **Clive.Boughton@anu.edu.au**. The email subject line must contain:

“*<Your Name>* **- COMP8180 - THE Submission**”

where “<Your Name>” needs to be substituted with your first name and surname. For example “**Kevin Rudd – COMP8180 – THE Submission**”.

If you do not have access to tools that enable the creation of ‘pdf’ then ‘Word’ or Open Office format is OK!

Try and limit the effort to **30-40 person hours** and the size of the delivery to less than **30 A4 pages**. Fonts shall be limited to “Helvetica”/”Arial” and “Times (New) Roman” with heading fonts to be no smaller than 12 point and normal body text to be no smaller than 10 point. Margins shall be no narrower than 1.0 cm. Diagrams are permitted but must be readable without the aid of magnification.

The completed THE is to be submitted by 18:00 June 13, 2014.