Higher National Unit specification

General information for centres

Unit title: Principles of Safe Engineering Systems

Unit code: F1BY 35

Unit purpose: This Unit has been designed to provide candidates with knowledge and understanding of how to apply reliability techniques to simple engineering systems. Candidates will also learn about basic fault management techniques used in engineering systems and key hardware, software, human and organisational issues involved in the design of safe engineering systems. Candidates will also investigate the stages involved in the principles of designing safe engineering systems. This Unit is suitable for those candidates who wish to develop knowledge and understanding of the design of safe engineering systems. Such candidates may be currently employed or seeking employment in an electrical, mechanical or engineering systems environment.

On completion of the Unit the candidate should be able to:

1 Apply reliability techniques to engineering systems.
2 Analyse techniques for managing faults in engineering systems.
3 Explain issues involved in ensuring safety is built into engineering systems.
4 Analyse the stages in building safety into the design of an engineering system.

Credit points and level: 1 HN credit at SCQF level 8: (8 SCQF credit points at SCQF level 8*)

**SCQF credit points are used to allocate credit to qualifications in the Scottish Credit and Qualifications Framework (SCQF). Each qualification in the Framework is allocated a number of SCQF credit points at an SCQF level. There are 12 SCQF levels, ranging from Access 1 to Doctorates.*

Recommended prior knowledge and skills: Entry to the Unit is at the discretion of the centre; however candidates should have a general knowledge and understanding of engineering systems. This knowledge and understanding may be evidenced by possession of the following HN Unit: DV9R 34 *Principles of Engineering Systems*.

Core Skills: There are opportunities to develop the following Core Skill component in this Unit, although there is no automatic certification of Core Skills or Core Skills components:

Reading Communication	SCQF level 6
Writing Communication	SCQF level 6
Using Number	SCQF level 5
Using Information Technology	SCQF level 5
Critical Thinking	SCQF level 6
Planning and Organisation	SCQF level 6
Review and Evaluation	SCQF level 6

General information for centres (cont)

Context for delivery: If this Unit is delivered as part of a Group Award, it is recommended that it should be taught and assessed within the subject area of the Group Award to which it contributes. This Unit has been developed for the HND Engineering Systems award.

Assessment: The assessment strategy for this Unit is as follows:

The assessment for Outcome 1 should comprise of a short assessment paper lasting 20 minutes and a software based exercise in which candidates are required to predict the overall reliability of an engineering system, or systems, under different conditions. The assessment may be taken at a single assessment event lasting 1 hour and 15 minutes. Both assessments should be conducted under controlled, supervised conditions.

The assessment for Outcomes 2 and 3 should be combined in the form of an assessment paper, which should be taken at a single assessment event lasting 1 hour and 15 minutes. The assessment paper should be conducted under controlled, supervised conditions.

The assessment for Outcome 4 should be an assignment in which a candidate investigates the stages involved in building safety into the design of an engineering system and produces a report on the investigation.

Higher National Unit specification: statement of standards

Unit title: Principles of Safe Engineering Systems

Unit code: F1BY 35

The sections of the Unit stating the Outcomes, Knowledge and/or Skills, and Evidence Requirements are mandatory.

Where evidence for Outcomes is assessed on a sample basis, the whole of the content listed in the Knowledge and/or Skills section must be taught and available for assessment. Candidates should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1

Apply reliability techniques to engineering systems

Knowledge and/or Skills

- Reliability
- Failure
- MTBF (Mean Time Between Failure)
- Failure rate
- Bath Tub Curve
- Reliability Block Diagrams
- Engineering Systems Reliability Predictions

Evidence Requirements

Evidence for the Knowledge and/or Skills items in Outcome 1 should be provided on a sample basis. The evidence may be provided in response to specific questions. Each candidate will need to demonstrate that she/he can answer correctly questions based on a sample of the items shown under the Knowledge and/or Skills items in the Outcome. In any assessment of Outcome 1 the items Reliability Block Diagrams and Engineering Systems Reliability Predictions must always be assessed using the following assessment criteria:

- use Reliability Block Diagrams to predict engineering systems reliability
- predict overall engineering system, or systems, reliability under different conditions

The remaining five Knowledge and/or Skills items must be assessed on the basis of a sample of any **three out of five** using the following assessment criteria:

- define the term Reliability
- define the term Failure
- define the term MTBF (Mean Time Between Failure)
- define the term Failure Rate
- sketch a typical bath tub curve and explain what the three regions of the curve represent

The assessment for Outcome 1 should comprise of the following:

- a short assessment paper
- a software based exercise

The short assessment paper should be a sample of three of the five Knowledge and/or Skills items listed above. The assessment paper should last 20 minutes and be conducted under controlled, supervised conditions. Assessment should be conducted under closed-book conditions and as such candidates should not be allowed to bring any textbooks, handouts or notes to the assessment.

The software exercise should cover the last two Knowledge and/or Skills items. Candidates are required to predict the overall reliability of an engineering system, or systems, under different conditions. The assessment should be taken at a single assessment event lasting 1 hour and 15 minutes. Assessment should be conducted under controlled, supervised conditions.

Assessment Guidelines

The assessment paper should be composed of restricted response questions.

For the software exercise centres may use commercially based software which determines reliabilities in engineering systems, or a Spreadsheet programme designed to do a similar task, to predict the overall reliability of an engineering system, or systems. Centres may require candidates to perform some reliability calculations as part of the software based assessment.

Outcome 2

Analyse techniques for managing faults in engineering systems

Knowledge and/or Skills

- Faults
- Fault Management Techniques
- Fault tolerant system involving redundancy
- Role of different approaches to fault management

Outcome 3

Explain issues involved in ensuring safety is built into engineering systems

Knowledge and/or Skills

- Hardware
- Software
- Human
- Organisational

Higher National Unit specification: statement of standards (cont)

Unit title: Principles of Safe Engineering Systems

Evidence Requirements

Evidence for the Knowledge and/or Skills items in Outcomes 2 and 3 will be provided on a sample basis. The evidence may be provided in response to specific questions. Each candidate will need to demonstrate that she/he can answer correctly questions based on a sample of the items shown under the Knowledge and/or Skills items in both Outcomes. In any assessment of the Outcomes **three out of four** Knowledge and/or Skills items should be sampled from Outcome 2 and **two out of four** Knowledge and/or Skills items should be sampled from Outcome 3.

Where sampling takes place, a candidate's response can be judged to be satisfactory where evidence provided is sufficient to meet the requirements for each item by showing the candidate is able to:

Outcome 2

- define the term fault and compare two of the following forms of fault:
  - random hardware component faults
  - systematic faults in design
  - errors in design specification

- compare three of the following fault management techniques:
  - fault avoidance
  - fault removal
  - fault detection
  - fault tolerance

- explain one form of fault tolerant system involving some form of redundancy

- compare the role of two of the following in designing a safe engineering system:
  - System Architecture
  - Reliability Engineering
  - Quality Management

Outcome 3

- explain two hardware issues that may affect the way in which safety is built into the design of an engineering system
- explain one software issue that may affect the way in which safety is built into the design of an engineering system
- explain one human issue that may affect the way in which safety is built into the design of an engineering system
- explain the role that organisational structure and culture can play in ensuring safety is built into the design of an engineering system

The assessment for Outcomes 2 and 3 should be combined to form one assessment paper. This assessment paper should be taken at a single assessment event, lasting 1 hour and 15 minutes and carried out under controlled, supervised conditions. Assessment should be conducted under closed-book conditions and as such candidates should not be allowed to bring any textbooks, handouts or notes to the assessment.

Higher National Unit specification: statement of standards (cont)

Unit title: Principles of Safe Engineering Systems

Assessment Guidelines

The assessment paper should be composed of an appropriate balance of short answer, restricted response and structured questions.

Outcome 4

Analyse the stages in building safety into the design of an engineering system

Knowledge and/or Skills

- Safety critical and non-safety critical systems
- Customer specification
- Project planning
- Risk assessment
- Design standards
- Top level design (Architectural Design)
- System partitioning for safety
- Detailed design stage
- Evaluation of the design

Evidence Requirements

All Knowledge and/or Skills items in Outcome 4 should be assessed.

The evidence should be presented in response to an assignment in which the candidate is set the task of undertaking an analytical investigation into the way in which safety is built into the design of an engineering system. The system chosen may be one that the candidate has selected herself/himself or one selected by the centre.

A candidate's response can be judged to be satisfactory where the evidence provided is sufficient to meet the requirements for each item by the candidate showing that he/she has:

- defined the difference between a safety critical and non-safety critical engineering system
- identified customer design requirements and related these to what is technically possible
- outlined a project plan
- undertaken a risk assessment on the design
- identified any standards, codes of practice or guidelines applicable to the design
- identified safety issues associated with the engineering system at the top level design stage
- identified any system partitioning to achieve improvements in the overall safety of the engineering system
- analyse any safety issues with the engineering system at the detailed design stage
- analyse any issues associated with the evaluation of the engineering system design

Evidence for this Outcome should be gathered by the candidate preparing a report which covers the Knowledge and/or Skills items for this Outcome.

The report should be between 1,200–1,500 words long plus diagrams and appendices. Candidates should have access to course notes, relevant textbooks, suppliers catalogues and hardware and software documentation whilst doing the assignment.

Candidates should complete the assessment for Outcome 4 in their own time. Centres should make every reasonable effort to ensure that the written report is the candidate's own work. Where copying or plagiarism is suspected candidates may be interviewed to check their knowledge and understanding of the subject matter. A checklist should be used to record oral evidence of the candidate's knowledge and understanding.

Assessment Guidelines

While the exact structure of candidates reports is left to centres to decide the following is a suggested structure:

- Introduction
- Background
- Conclusions
- Recommendations
- Suggestions for Further Work

As part of the assessment process centres may wish candidates to undertake a preliminary and final review of their assignment.

It is recommended that candidates are not provided with the assessment for Outcome 4 until they have completed their studies on Outcomes 1, 2 and 3. It is anticipated that the investigation and report writing for Outcome 4 should take approximately 10 hours to complete. This will be completed within the candidate's own time.

Administrative Information

Unit code: F1BY 35

Unit title: Principles of Safe Engineering Systems

Superclass category: VF

Original date of publication: May 2007

Version: 01

History of changes:

Version	Description of change	Date

Source: SQA

SQA acknowledges the valuable contribution that Scotland's colleges have made to the development of Higher National qualifications.

Additional copies of this Unit specification can be purchased from the Scottish Qualifications Authority. Please contact the Customer Contact Centre for further details, telephone 0845 279 1000.

Higher National Unit specification: support notes

Unit title: Principles of Safe Engineering Systems

This part of the Unit specification is offered as guidance. The support notes are not mandatory.

While the exact time allocated to this Unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this Unit

This Unit has been written in generic terms so that it can be applied to a wide range of engineering systems. It is recommended that at least some of the engineering systems considered should contain a software element so that all Knowledge and/or Skills items in the Unit can be delivered. The software element may be embedded within the system's hardware or may be a discrete element such as a PLC, microcontroller or pc.

Designing engineering systems, especially where safety is a critical aspect of the design, can be a large and complex subject. In this Unit it will only be possible to give candidates an introduction to this very important subject. However, even at an introductory level it will be important to emphasise that safety in the design of engineering systems does not simply happen, it has to be built into every stage of the engineering system's design process from the initial conception of the design to the final evaluated product. It will be important to get candidates to think safety at all times. They should be encouraged not only to question safety at each stage of the design process but to question everything involved in the design including the reliability and consistency of any hardware and software tools used to evaluate the design.

The Unit follows a logical delivery sequence in Outcome terms. In Outcome 1 Reliability and terms associated with it such as Failure, Mean Time Between Failure and Failure Rate should be introduced. The bath tub curve should be drawn to illustrate how hardware components and systems fail in practice. The exponential law of Reliability can be introduced. The concept of reliability block diagrams should be introduced as a means of predicting the overall reliability of an engineering system. Reliability calculations can become increasing difficult as more complex engineering systems are introduced. It is recommended that centres limit calculations to cascade (series), parallel and series parallel reliability block diagrams. However, centres should also get candidates to use commercially based software which determine reliabilities in engineering systems, or a Spreadsheet programme designed to perform a similar task, to predict overall reliability in an engineering system, or systems. Lecturers delivering the Unit may wish to use as an example the contrast between repairable and non-repairable systems, but with the focus principally on repairable systems.

In Outcome 2 candidates should be introduced to the definition of and nature of faults in engineering systems. Faults in systems can be classified as follows:

- random such as hardware component faults
- systematic faults in the design (which can be both hardware and software in nature)
- errors in the specification of the system

Higher National Unit specification: support notes (cont)

Unit title: Principles of Safe Engineering Systems

Fault management in systems can be achieved using the following techniques:

- fault avoidance — preventing faults from entering the system at the design stage
- fault removal — attempts to remove faults before the system enters service
- fault detection — detect faults during the operation of the system so that faults can be minimised
- fault tolerant systems — allow a system to continue to work in the presence of a fault in the system

Candidates should be encouraged to examine the way in which fault tolerant systems operate. Such systems use some form of redundancy arrangement. Such arrangements make use of one of the following: majority voting, averaging or median and select.

Finally in Outcome 2 candidates should briefly examine the way in which System Architecture, Reliability Engineering and Quality Assurance contribute to fault management techniques.

In Outcome 3 candidates should be allowed to explore the way in which hardware, software, human and organisational issues can affect the way in which safety is built into an engineering system at the design stage. There are many such issues that can affect the design process so it is important that lecturers are selective in their choice of issues. Some possible issues are given below:

Hardware

- mechanical parts and systems — design or selection of parts to withstand stresses and strains under all operating conditions, choice of couplings and drives to satisfy safe operating requirements
- electrical — selection of correct motor(s) for given application in the system, methods of electrical protection used in systems
- electronics — design or selection of interfaces to meet specifications under all operating conditions, selection of microprocessor, PLC, microcontroller or pc for given systems application
- instrumentation — selection of transducers to make appropriate variable measurements in engineering systems
- control — selection of suitable controller(s) to ensure reliable and safe operation of the engineering system

Software

- choice of programming language for the system
- nature and extent of documentation to support the engineering system in operation

Human

- safeguards against human error
- potential for automation to eliminate operator errors
- processes for minimising system designer’s errors

Organisational

- organisational structure to ensure safety is built into the design process
- organisation culture and its impact on safety in the design process
- safety issues involved with multi-team and multi-organisational engineering systems developments

Outcome 4 provides candidates with an opportunity to integrate the knowledge and understanding they have gained in the first three Outcomes by reporting on an engineering system design of their choice or one provided by the centre. The way in which safety is built into all stages of the design should feature prominently in the report produced by the candidate to satisfy the Evidence Requirements in Outcome 4.

Guidance on the delivery and assessment of this Unit

This Unit may be delivered by a combination of lecturing, group work, investigation (including the use of the Internet) and case studies. The Internet contains a rich and varied range of materials relating to engineering systems design including the following subjects: Design for Safety, Quality Assurance, Reliability Engineering, Systems Engineering and System Engineering Processes. The use of case studies can be a particularly powerful tool in illustrating how safety can be built in at all stages of the engineering systems design process. Examples of possible case studies include the following:

- Airbags in a car
- Car braking system
- Circuit breaker
- Fire sprinkler
- Heart-lung machine
- Nuclear reactor control system
- Railway signalling and control systems

Industrial visits may prove useful in allowing candidates to explore in a real engineering environment both the stages in the engineering systems design process and how safety is built into each stage of the process.

Computer-based software tools may be used to illustrate how the performance of an engineering system can be evaluated at the design stage. However, any limitations of these software tools should also be drawn to candidates' attention.

Opportunities for developing Core Skills

Candidates will have opportunities to develop reading communication skills while reading materials on the design of engineering systems from paper based and electronic sources. Lecturers may choose to ask candidates questions on the materials they have read to check understanding. Candidates may develop their written communication skills through the preparation of the assignment report for Outcome 4.

Candidates may develop their Using Number Core Skill while performing reliability calculations on engineering systems. Information Technology Core Skills may be developed when using commercially based software, or a Spreadsheet, to predict the overall reliability of an engineering system or systems.

Critical thinking skills should be developed throughout the Unit when, for example, considering the way in which safety is built into the design of engineering systems. For example, candidates may wish to reflect on the various factors that may affect safety in an engineering system. They may also wish to think about the benefits of modularisation in achieving safer engineering systems. Planning and organisation and review and evaluation skills may be enhanced while candidates undertake the investigation of the design of an engineering system in Outcome 4.

Details on the approaches to assessment are given under Evidence Requirements and Assessment guidelines after Outcomes 1, 3 and 4 in the Higher National Unit specification: statement of standards section. It is recommended that these sections be read carefully before proceeding with assessment of candidates.

Open learning

This Unit could be delivered by distance learning, which may incorporate some degree of on-line delivery and/or support. However, with regards to assessment, planning would be required by the centre concerned to ensure the sufficiency and authenticity of candidate evidence.

Arrangements would be required to be put in place to ensure that the combined assessment paper for Outcomes 2 and 3 is conducted under controlled, supervised conditions.

Candidates with disabilities and/or additional support needs

The additional support needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments, or considering alternative Outcomes for Units. Further advice can be found in the SQA document *Guidance on Assessment Arrangements for Candidates with Disabilities and/or Additional Support Needs* **(www.sqa.org.uk)**.

General information for candidates

Unit title: Principles of Safe Engineering Systems

The design of engineering systems, especially safety critical engineering systems, is a very important process. For example, it is essential that an airbag in a car operates when it is meant too and a rail level crossing works correctly at all times. In this Unit you will be introduced to some aspects of the principles of safe engineering systems.

In Outcome 1 you will learn how Reliability techniques can be applied in the design of engineering systems while in Outcome 2 you will study fault management methods used in engineering systems. In Outcome 3 you will explore some of the hardware, software, human and organisational issues involved in building safety into engineering systems. Finally, in Outcome 4 you will investigate the stages involved in building safety into an engineering system.

The Unit is likely to be delivered by a combination of lecturing, group work, case studies and investigation work. Case studies on building safety into engineering systems design can be a particularly powerful tool in illustrating many aspects of the design process.

Formal assessment in the Unit will comprise of a short assessment paper and software based assignment for Outcome 1, a combined assessment paper for Outcomes 2 and 3 and an assignment covering the work in Outcome 4. The short assessment paper and software based assignment for Outcome 1, and the assessment paper covering Outcomes 2 and 3 will be taken at assessment events lasting 20 minutes, 1 hour and 15 minutes and 1 hour and 15 minutes respectively. All three assessments will be conducted under controlled, supervised conditions. The assignment for Outcome 4 will involve an investigation of the design of an engineering system you have selected or a system chosen by the centre where you are enrolled to take the Unit. The way in which safety has been built into the design of the system must feature prominently in the investigation. Assessment evidence for Outcome 4 will be generated in the form of a report based on the investigation. It is likely that the investigation plus report will take you approximately 10 hours to complete and this will be completed in your own time.