Surname: . . . . **First Name:** . . . . **Student ID:** . . . .

TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI

VUW **VICTORIA** UNIVERSITY OF WELLINGTON

TESTS – 2021

TRIMESTER 1

SWEN 326

SAFETY-CRITICAL SYSTEMS

Time Allowed: TWO HOURS

CLOSED BOOK

Permitted materials: No calculators permitted.
Non-electronic Foreign language to English dictionaries are allowed.

Instructions: Answer all questions

Question	Topic	Marks
1.	Risk, Hazards and Failure	30
2.	Testing	30
3.	Static Analysis	30
4.	Design Validation	30
	Total	120

1. Risk, Hazards and Failure **(30 marks)**

(a) Consider the following description of a system for controlling a *model railway*:

> "Model trains and sets of points (track switches) are operated by a *software controller*. Track sections contain *sensors* which report the number of trains within that section. Trains travel in a pattern specified by the controller, at the maximum *speed* for the current section of track and proceeding to the next track section determined by the *direction* of travel and the *points configuration*. Under no circumstances should the entire model railway system stop operating."

i. **(2 marks)** Using the terminology of IEC 61508, identify the *Equipment Under Control* for the model railway system.

ii. **(2 marks)** Using the terminology of IEC 61508, identify the part of the system on which the *Functional Safety* of the whole system relies.

iii. **(2 marks)** Identify a *hazard* present in the model railway system.

iv. **(4 marks)** A *risk* can be described by a circumstance involving a hazard with an undesired outcome. Using this pattern, briefly describe a risk involving the above hazard.

v. **(2 marks)** Briefly, discuss the ways that the hazards in a system can be *identified* when performing a hazard and risk analysis.

vi. **(4 marks)** Under IEC 61508 there can never be *zero risk*. Briefly, discuss what this means with respect to the model railway system.

(b) Safety-critical systems often require results be computed in real-time to mitigate the risk of undesired undesired consequences:

i. **(2 marks)** Briefly describe the constraints of *Firm* and *Soft* real-time systems.

ii. **(2 marks)** Worst-Case Execution Time (WCET) is important for *Hard* real-time systems. Briefly identify *two* factors which might be needed to compute a WCET.

iii. **(2 marks)** A safety-critical Real-Time Operating System will have characteristics necessary to meet safety requirements. Briefly identify two such characteristics.

(c) Memory management is important in safety-critical systems:

i. **(2 marks)** Many microcontroller architectures provide a relatively limited data memory space. Briefly describe a risk posed by the *Stack* used for temporary data storage.

ii. **(2 marks)** In systems where memory is managed by an operating system, memory fragmentation is a hazard. Briefly describe the risk posed by memory fragmentation.

iii. **(4 marks)** JSR302 states "One of the design goals of the Safety Critical Java (SCJ) specification has been to enable the development of SCJ applications that are not vulnerable to reliability failures due to memory fragmentation." Briefly, discuss the context of this SCJ design goal.

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

2. Testing **(30 marks)**

Consider the following Java class which compiles without error:

```
public int[] append(int[] lhs, int[] rhs) {
   if(lhs.length == 0) { return rhs; }
   else if(rhs.length == 0) { return lhs; }
   else {
      int[] rs = new int[lhs.length + rhs.length];
      // Copy left half
      for(int i=0;i!=lhs.length;++i) {
         rs[i] = lhs[i];
      }
      // Copy right half
      for(int i=0;i!=rhs.length;++i) {
         rs[i + lhs.length] = rhs[i];
      }
      // Done
      return rs;
   }
}
```

(a) **(10 marks)** Draw the *control-flow graph* for the `append()` method.

(Question 2 continued on next page)

(Question 2 continued)

(b) **(2 marks)** Briefly, discuss why the following should not be considered a valid test.

```
@Test public void test_0() {
   int[] l1 = append(null,null);
   assertTrue(l1 == null);
}
```

(c) **(6 marks)** Write three JUnit tests which achieve 100% *branch coverage* of `append()`.

```
@Test public void test_1() {




}
```

```
@Test public void test_2() {




}
```

```
@Test public void test_3() {




}
```

(Question 2 continued on next page)

(Question 2 continued)

(d) **(3 marks)** Briefly, discuss whether 100% *Modified Condition/Decision Coverage* (MC/DC) is achievable for the `append()` method.

(e) *Unrealisable paths* are a significant challenge for computing code coverage.

i. **(2 marks)** Briefly, state what an unrealisable path is.

ii. **(2 marks)** Identify an unrealisable path in the `append()` method.

(f) An important test critereon is *simple path coverage*.

i. **(2 marks)** Briefly, state what simple path coverage is.

ii. **(3 marks)** Briefly, discuss whether 100% *simple path coverage* is achievable for the `append()` method.

Student ID: . . . .

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

3. Static Analysis **(30 marks)**

(a) Computing the *Worst-Case Execution Time (WCET)* for a given instruction sequence is important for real-time embedded systems.

For this question, you may assume it takes exactly *one cycle* to execute a single instruction.

```
0x0000:  rjmp 5
0x0001:  cp r24, r22
0x0002:  cpc r25, r23
0x0003:  brge 1
0x0004:  movw r16, r12
0x0005:  ret
0x0006:  push r28
0x0007:  push r29
0x0008:  movw r24, r8
0x0009:  rcall -9
0x000A:  mov r22, r28
0x000B:  pop r29
0x000C:  pop r28
```

i. **(2 marks)** Determine the WCET for the above instruction sequence (in cycles).

ii. **(5 marks)** Briefly, outline how a *control flow analysis* can be used for computing WCET. You should use the instruction sequence shown above to illustrate.

iii. **(5 marks)** Static analyses are often said to be *conservative*. Briefly, discuss what this means in the context of WCET.

iv. **(4 marks)** Briefly, discuss why *loops* present a significant challenge when computing WCET using control-flow analysis.

v. **(4 marks)** Briefly, discuss why *indirect jumps* present another challenge when computing WCET using control-flow analysis.

(b) An alternative way of computing the WCET for an instruction sequence is to use *explicit-state model checking*.

i. **(4 marks)** Briefly, outline how explicit-state model checking *differs* from using a control-flow analysis.

ii. **(6 marks)** Briefly, discuss the *pros* and *cons* of using explicit-state model checking for calculating WCET.

SPARE PAGE FOR EXTRA ANSWERS

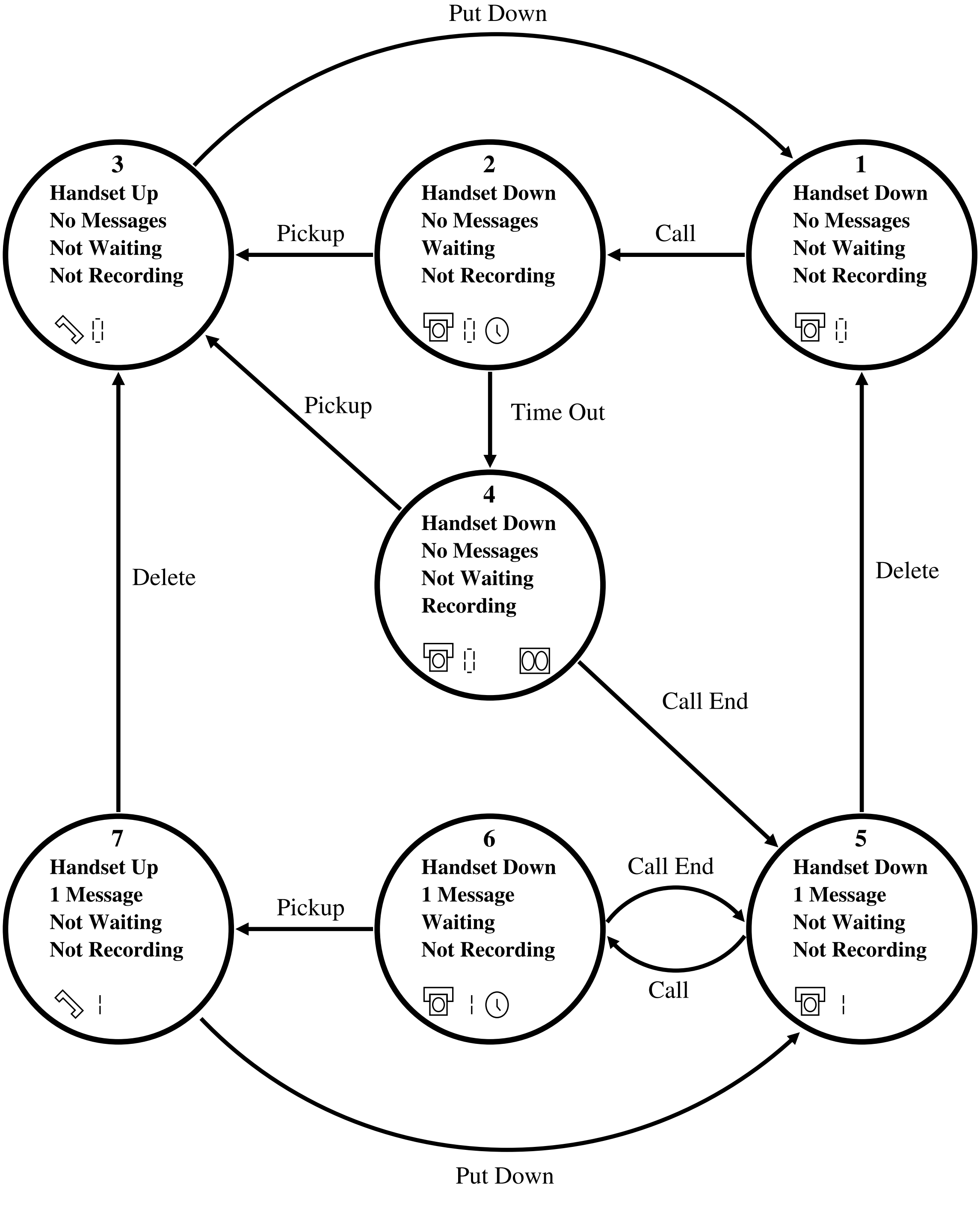
Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

4. Design Validation **(30 marks)**

Consider the following description of a simple *answering machine*:

> "The answering machine can store up to one phone message, and has a handset for answering calls manually. When an incoming call rings, a timer is started. If the user picks up the handset before the timer elapses, then he/she may answer the call. Otherwise, the machine begins to record the message. At this point, the user may still pick up the handset and answer the call. "

A *state machine diagram* for the answering machine has been provided:



(a) For each of the following statements, indicate whether you think it is a true or false statement based on the state machine diagram.

i. **(2 marks)** If the handset is down and an incoming call occurs, the machine immediately begins recording.

ii. **(2 marks)** If the machine is recording a message, the user can always pick up the phone and answer it.

iii. **(2 marks)** If an incoming call occurs and the handset is up, the machine will record a message.

iv. **(2 marks)** The user may delete a message whilst answering a call.

v. **(2 marks)** If the machine has already stored a message, then it will not record another until the first is deleted.

(b) Provide a suitable *execution trace* for the following scenarios. For each state, you need only list its number. Your execution trace may start from any state you chose.

i. **(2 marks)**

"When the phone rang, Jane answered it immediately. It was a wrong number, so she put the handset down."

ii. **(2 marks)**

"John deleted the message. Then, the phone rang, but he could not answer it. So, a new message was recorded."

(c) Consider the following *incomplete* Whiley model of the answer machine:

```
type State is {
   bool handsetUp,
   bool waiting,
   bool recording,
   int messages
}
where messages >= 0
// Cannot be waiting and recording
where !(waiting && recording)

function call(State s1) -> (State s2)
// handset cannot be up
requires !s1.handsetUp
// cannot be already waiting
requires !s1.waiting
// cannot be recording
requires !s1.recording:
   s1.waiting = true
   return s1

function callEnd(State s1) -> (State s2)
// must be either recording or waiting
requires s1.recording || s1.waiting:
   if s1.recording:
      s1.messages = s1.messages + 1
   s1.recording = false
   s1.waiting = false
   return s1

function pickup(State s1) -> (State s2)
// handset must be down
requires !s1.handsetUp
// must be waiting
requires s1.waiting:
   s1.handsetUp = true
   s1.waiting = false
   return s1
```

i. **(2 marks)** Give a valid instance of `State` which corresponds to state four from the diagram on page 14.

ii. **(2 marks)** Give a valid instance of `State` which does not correspond to *any* state from the diagram on page 14.

iii. **(4 marks)** Complete the following function to model the “Delete” transition from the diagram on page 14.

```
function delete(State s1) -> (State s2)
```

iv. **(2 marks)** The function `callEnd()` allows more transitions than described in the state machine diagram on page 14. Briefly, explain why.

v. **(2 marks)** What key functionality is provided by the Whiley model but not the state machine diagram on page 14?

(d) **(4 marks)** Briefly, discuss the *pros* and *cons* of using formal languages (such as Whiley) compared with hand-drawn diagrams (such as that on page 14)

* * * * * * * * * * * * * * *

Student ID: . . . .

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.

Student ID: ....

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.
Specify the question number for work that you do want marked.