Selected solutions for TDDD07 Real-time Systems

Massimiliano Raciti
Jordi Cucurull
Simin Nadjm-Tehrani

Real-Time Systems Laboratory
Department of Computer and Information Science
Linköping University, Sweden

November 2019

SOLUTIONS

Q3.1:

Shorthand answers are provided. The student is expected to develop it in full sentences.

- The transmission of a world cup football game in all countries stopped for 35 minutes due to a software misconfiguration that crashed the central live streaming server in the head quarters of the media company which is in charge of relaying the game.
  Software misconfiguration -> Server crash -> Transmission stopped

- Broadband services were experienced as being slow several hours after the electricity outage was created due to lightning.
  Electricity outage -> Service overloaded after reboot -> Slow service

- In Java 1.6.0_21, the company field was changed from 'Sun Microsystems, Inc' to 'Oracle.' Some applications depend on that field to identify the virtual machine. For example, all Eclipse versions since 3.3 including the recent Helios release (2010) have been reported to crash with an OutOfMemoryError due to this change.
  Field changed -> OutOfMemory error -> Software crash

Q3.2:

(a) We have the following parameters

Message	period (ms)	Jitter	Priority
m1	20	1	3 (highest)
m2	10	2	2
m3	5	0	1 (lowest)

The time taken to transmit one bit τ_{bit} is less than 1 ms.

The maximum blocking time for respective messages is $B_1 = B_2 = 1ms$ and $B_3 = 0ms$. Frames sent by n_3 have the lowest priority, reason why their blocking factor is defined to zero. The transmission time is $C_i = 1ms$.

Response time R_2: We calculate first the length of the busy period for message 2:

$$t_2^0 = C_2 = 1ms$$

$$t_2^1 = B_2 + \left\lceil \frac{t_2^0 + J_1}{T_1} \right\rceil C_1 + \left\lceil \frac{t_2^0 + J_2}{T_2} \right\rceil C_2 = 1 + \left\lceil \frac{1+1}{20} \right\rceil 1 + \left\lceil \frac{1+2}{10} \right\rceil 1 = 3ms$$

$$t_2^2 = B_2 + \left\lceil \frac{t_2^1 + J_1}{T_1} \right\rceil C_1 + \left\lceil \frac{t_2^1 + J_2}{T_2} \right\rceil C_2 = 1 + \left\lceil \frac{3+1}{20} \right\rceil 1 + \left\lceil \frac{3+2}{10} \right\rceil 1 = 3ms$$

$$t_2^2 = t_2^1 = t_2 = 3ms$$

Then the number of instances Q_2 that become ready:

$$Q_2 = \left\lceil \frac{t_2 + J_2}{T_2} \right\rceil = \left\lceil \frac{3+2}{10} \right\rceil = 1$$

The response time must be calculated for each of the Q_2 instances:

$$w_2^0(0) = B_2 + 0C_2 = 1ms$$

$$w_2^1(0) = B_2 + 0C_2 + \left\lceil \frac{w_2^0 + J_1 + \tau_{bit}}{T_1} \right\rceil C_1 = 1 + 0 + \left\lceil \frac{1+1+\tau_{bit}}{20} \right\rceil 1 = 2ms$$

$$w_2^2(0) = B_2 + 0C_2 + \left\lceil \frac{w_2^1 + J_1 + \tau_{bit}}{T_1} \right\rceil C_1 = 1 + 0 + \left\lceil \frac{2+1+\tau_{bit}}{20} \right\rceil 1 = 2ms$$

$$w_2^2 = w_2^1 = w_2 = 2ms$$

$$R_2(0) = J_2 + w_2(0) - 0T_2 + C_2 = 2 + 2 + 0 + 1 = 5ms$$

$$R_2 = \max_{q=0..Q_2-1}(R_i(q)) = R_2(0) = 5ms$$

a) Where is the MEDL (message descriptor list) of a TTA bus stored and what is its role?

The Message Descriptor List (MEDL) of a TTA bus is stored in each TTP controller and contains information about the time slots that each node has to send their messages.

Q3.3:

a) Give an example technique that helps to discover early design faults in embedded real-time systems.

Design faults in embedded real-time systems can be discovered using simulation techniques or formal verification.

b) What is meant by platform independence, and why is it a good property in modelling languages for real-time systems?

Platform independence applied to systems design means that one system can be designed using abstract languages with independence of the underlying platform architecture.

It is a good property because the design is reusable for many platforms just applying some specific transformations.

Q3.4:

a) Take a stand on the following propositions (true or false), and motivate your answer:
   1) Application program timing faults can never be detected by the run-time environment.

      False, for example the operating system can detect tasks that miss a deadline.

   2) Simulation of the design of a program can be used to study run-time fault tolerance properties.

True, because some of the faults can be tested in the simulation.

3) Voting systems (e.g. triple modular redundancy) cannot be used to tolerate the same software design fault appearing in every replica.

True, because in this case usually error manifestation will be the same in each replica.

b) Describe four drawbacks with checking real-time systems for correctness and timeliness only on the platform for which they are intended, as opposed to being tested in a platform-independent design phase first.

Read the article J. Huang and J. Voeten, "Platform-independent Design for Embedded Real-time Systems", 2003.

Q3.5:

a) Consider a collision avoidance component in a flight control system. Decide which of the following properties is a functional property and which is an extra-functional property (also sometime called a non-functional property):
   1) When another aircraft is within X meters of own aircraft on the same altitude, the marking on both pilot display screens should change colour within Y milliseconds.

      Functional property. It deals with a function that is part of the operational goal of the air traffic control.

   2) For two aircrafts on the same altitude if own aircraft is instructed to rise, the other aircraft has agreed to descend (go down).

      Functional property. It defines what the system should do while delivering the service of aircraft separation.

   3) If the altitude measurement delivered by the altitude-metering system is inaccurate then the collision avoidance system should switch to an alternative source for altitude value.

      Extra-functional property. It defines how the system should adapt to the presence of faults.

b) Name two types of languages that can be used to describe a system at a higher level of abstraction than the platform-dependent programming language. For each language describe one benefit that the language brings to the system development process.

Read article:

J. Huang, J. Voeten, A. Ventevogel and L. van Bokhoven. *Platform-independent Design for Embedded Real-Time Systems* In Proceedings of FDL'03, pp. 318-329, 2003.

Q3.6

a) Explain whether production defects in microchips are an example of faults, errors or failures.

The production defects in a microchip can be a failure and a fault in two different contexts:

- *Failure of the production line of the microchips.*
- *Fault of an incorrectly delivered service that uses these microchips.*

Nevertheless they cannot be an error, because they are not the symptom of a problem.

b) Describe the relation between "degraded mode" and "system failure". You may use an example to explain whether these terms are synonyms or have differences.

System failure implies that the main functionality of a system is lost, e.g. the engine of a car breaks and the car cannot transport anyone.

Instead, degraded mode implies that only a subset of the system functionality is available or that it is available with reduced performance, e.g. a cellular network that because of congestion only allows to send SMSs, but not to establish a call.
Therefore, system failure is the worst scenario, since the service is not provided at all after the failure, while in degraded mode the system still provides part of the services.

Q3.7:

a) Explain the notion of graceful degradation and give one example of it in a real application setting.

Graceful degradation is the capability of a system to offer a reduced service or performance in case of failure of some of its components.

An example can be a communications network that has some of its links down and it still can offer the service, but with a reduced bandwidth available and higher latency, e.g. Internet.

b) Take a stand on the following propositions (true or false), and motivate your answer:
    1) Redundancy in hardware through triple modular redundancy does not increase the response time of an application compared to a non-replicated solution.

***True**, if the time spent for voting over the results is negligible.*

    2) TCP employs redundancy in data when a message is retransmitted to achieve reliable communication.

***False**, TCP includes a checksum to detect errors, but not to correct them.*

    3) TCP employs redundancy in time when a message is retransmitted to achieve reliable communication.

***True**, TCP retransmits segments of data that has been lost or corrupted.*

Q3.8

a) Identify the causal chain of fault-error-failure in the following scenario, including whether the fault was permanent, transient or intermittent.

On 7th October a newspaper in Colorado reported that real-time alerts had ceased for a number of persons being electronically monitored instead of being in jail. BI Inc., a company that provides electronic monitoring for several nationwide agencies, experienced a problem with one of its offender monitoring servers at 7:29 a.m., temporarily disabling the server's notification system and delaying violation notifications to customers. The technical glitch happened when one of BI's servers exceeded its threshold of 2.1 billion records. "The offenders and suspects on the monitoring system did not know their devices were down at the time, the company officials said, and there were no major problems reported as a result of the technical failure."

Fault: *The server is designed for a capacity below of 2.1 billion records*
Error: *Once reached this threshold, the server went down*
Failure: *Real-time alerts are not sent for a number of monitored persons.*

The fault is permanent since it is a design fault.

Q3.9:

a) Identify the causal chain of fault-error-failure in the following scenario.

> The University College London Hospitals Trust (a consortium of hospitals in London) was on 22nd February 2011 forced to halt a number of services, including the cancellation of 50 per cent of its operations, due to a faulty network switch. The faulty switch left computers across the connected London hospitals unable to access various systems such as the trust's patient administration system and its patient records software CareCast.

Fault: *Faulty network switch*
Error: *No access to various systems (patient administration and patient records)*
Failure: *A number of services are halt, including 50 per cent of the operations*

Q4.1:

a) Explain the notion of reliability, and provide a metric (= means of measuring) that can be used for measuring this attribute in a system.

The notion of reliability refers to the ability of a system to offer a continuous service (without failures) under specific stated conditions during a specified period of time.

Metric: Mean Time Between Failures (MTBF)

$$MTBF = \frac{\sum(start\_downtime - start\_uptime)}{Number\_failures}$$

b) Take a stand on the following propositions (true or false), and motivate your answer:

1) A real-time operating system may tolerate program design faults by redundancy in time, i.e. a scheduling algorithm that runs a process again if the first run of the process fails.

False, a design fault will raise again if the process is executed with the same parameters. Design faults are permanent.

2) Simulation of the design of a program can be used to eliminate all requirements faults.

*False, because 1) no method can eliminate **all** the faults in a program, 2) missing requirements cannot be detected, and 3) usually it is not possible to explore all the states of a program by simulation.*

3) Voting systems (e.g. triple modular redundancy) can be used to tolerate transient faults but not permanent faults.

We focus on permanent faults part of the statement.
True, if the fault occurs in software. All the replicas will present the same (design) fault, therefore redundancy would not help.
False, in the case of hardware, as long as the fault is not present in all the replicas.

4) A method for fault forecasting is to build in adaptive load control in the design of the system.

True, switching load from one server to another (as in the case of the Google mail server) would need identification of current/future load and adaptation to it.

c) Describe four functions in a real-time operating system that need to be implemented in a different manner from an ordinary operating system.

Read article in literature:

Baskiyar, S. and Meghanathan, N. *A Survery of Contemporary Real-time Operating Systems* 233-240 2005 29 Informatica