TENTAMEN TDDD07 Realtidssystem

DATUM: 29 March 2016
TID: 14-18
PLATS: TER2
ANSVARIG JOURLÄRARE: Examinator Simin Nadjm-Tehrani (Tel: 013-282411, 0702 282412), Mikael Asplund (Tel: 0707 481462).

Material: English-Swedish-English dictionary
Calculator

No of assignments: 5

Total no. of points: 40

Preliminary grade limits for grades: 3, 4 and 5

3:	20 - 26 p
4:	27 - 33 p
5:	34 - 40 p

INSTRUCTIONS:

Please write your anonymous ID on each sheet of paper that you hand in. Pages should only contain answer to **one question per page** (answers to sub-questions can be on the same page). You are asked to only write on one side of each paper. Please **sort** all the sheets that you hand in, in the order of question numbers.

Make sure that **all** answers are **motivated** and supported by **clear** explanations. Figures or charts can be used to provide a clearer explanation but should be accompanied by a **textual description**. Points will not be given to answers for which the reasoning cannot be followed or that cannot be read due to bad handwriting. Wrong answers/reasoning which is embedded in partially correct ones will lead to deduction of points. You may answer the questions in English (the course language) or Swedish.

Hints: Read the question carefully to find the focus of the question. Make sure your answer is to the point and relevant for the question asked. Take the opportunity of asking questions about unclear issues during the exam session. Otherwise, whenever in doubt about the question, write down your interpretation and assumptions, and answer the question based on the interpretation. Try to dispose of your time on each question in proportion of the assignment points.

Results are reported no later than April 14^{th}.

Good luck!

Simin Nadjm-Tehrani

Q1: Scheduling

a) The following task set is to be analyzed for its real-time properties in a new generation of the Mars Rover: (1) the *trajectory following task* for finding the way to a well-defined physical coordinate, (2) *the sensor & measurement task* that configures and reads various sensor's values, (3) a *disk storage task* that is responsible for periodically writing the buffered measured values on a log on persistent memory, (4) a *communication task* for contacting the ground station and sending cached data. The following table summarises the task set's periods and worst-case execution times (WCET) in milliseconds.

Task	Period	WCET
Trajectory follower	1600	100
Sensor & measurement	400	50
Disk storage	1200	500
Ground communication	400	50

1) Assume that the tasks can be scheduled as independent tasks. Assume further that the task set should be scheduled using a cyclic executive for which the overhead can be considered as negligible. Construct such a cyclic schedule and provide the minor and major cycles for the schedule. Comment on the presence of jitter in your solution.

   (3 points)

2) In order to make the utilization more effective there is a plan to change to rate monotonic scheduling (RMS) and a communication medium that may be shared between the disk storage task and the ground communication task. To deal with the conflicts over the communication medium the immediate ceiling protocol is to be combined with RMS. Find the maximum blocking time of the communication task assuming that the disk storage task's access to the bus can be bound to 150ms each time it gets access to the bus. Motivate your answer!

   (2 points)

b) Prove that the immediate ceiling protocol combined with a fixed priority scheduling algorithm (e.g. RMS) avoids starvation. Note: you are not required to prove absence of deadlocks.

   (5 points)

Q2: Dependability and predictability

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

   (2 points)

b) Take a stand on the following propositions (true or false), and motivate your answer:
   1) A reliable program cannot lead to failures as it will not contain faults that make it incompatible with its specification.
   2) Testing a system in its operational environment is a method for fault prevention.
   3) "Redundancy in time" makes real-time systems fault-tolerant in presence of transient faults.

   (3 points)

c) What attribute of dependability was violated in the following scenario? Motivate your answer!
"In October 2011, researcher Barnaby Jack demonstrated a remote, wireless attack on an implantable insulin pump from the firm Medtronic. The attack could have enabled a remote assailant to command the pump to release a fatal dose of insulin to a diabetic."
(2 points)

d) Many real-time applications are built on top of small proprietary kernels that are adaptations of well-known time sharing operating systems, e.g. through adding preemptive priority-based scheduling. Describe three other adaptations needed in a real-time kernel that makes the kernel operations predictable in a real-time setting.
(3 points)

e) Identify the causal chain in following phenomenon in terms of faults, errors and failures.

"Loss of the fuel unit during the mission of the space shuttle Discovery due to of adverse environment conditions during take-off that led to loss of some binding mechanical linkage shortly after take-off."
(3 points)

Q3: Design

a) What does formal verification bring to the analysis of dependability and timeliness in a system that simulation and test does not? Contrast the named techniques against each other.
(2 points)

b) Define the notion of platform in a real-time system, and describe one phase of system development that cannot be platform-independent.
(2 points)

c) Using clear arguments identify how the design process for the system involved in the following scenario could have averted the failure. Motivate your answer!

> The online newspaper The Province reported on 10th March 2013: "About 70 per cent of Shaw Communication's email customers were affected when the company was troubleshooting an unrelated email delay problem and an attempted solution caused incoming emails to be deleted. Shaw has about 1.9 million Internet subscribers across Canada, with the majority in Western Canada. Emails were deleted for a 10-hour period between 7:45 a.m. and 6:15 p.m. Thursday, although customers did not learn about the problem until Friday, and only then by calling customer service or accessing an online forum for Shaw Internet subscribers. Spokesman Chethan Lakshman said the problem was difficult to detect because Shaw was dealing with the email delay problem at the same time. About 98 per cent of email to any account is junk mail, Lakshman said, and the standard approach among email service providers is to filter and delete the spam immediately. The spam is not backed up. The error occurred when the Shaw server deleted all email, not just spam. As such, the emails were not backed up. Shaw promised to email affected customers sometime over the weekend with a list of deleted messages and details such as sender, subject and time sent. The actual content of the emails, however, is unrecoverable".

(2 points)

Q4: Real-Time Communication

a) Ms. Klurig is an engineer at HighTech AB and currently responsible for determining whether an event-driven or a time-driven bus should be adopted by the company in its new development project. Describe two factors that may affect the decision whether to use a CAN bus compared to a TTP bus.

(2 points)

b) Assume now that the company has decided to use a CAN bus to schedule the messages in the development project. The list of messages that would have to be scheduled on the CAN bus is presented below (where "Tx time" stands for worst case transmission time of a message on the bus). Ms. Klurig was asked to prioritise the messages for sending on the CAN bus. How should she answer the question?

Message	Period	Tx time
m_1	10	3
m_2	20	4
m_3	50	5
m_4	40	5

(1 point)

c) Compare the characteristics of the CAN bus and the standard Ethernet in terms of suitability for hard real-time deadlines. Give at least one similarity and one difference between the protocols. (2 points)

Q5: Distributed systems, QoS

a) Consider 4 nodes in a distributed system in which the local clocks are to be synchronised using the Lamport/Melliar-Smith algorithm (i.e upon exchange of local clock values, a value with a difference higher than δ is replaced by own clock and then the reported values are averaged to produce the value that replaces the own clock value). Consider a case where none of the clocks is a two-face clock (i.e. acts Byzantinely). Explain if the synchronisation requirement is met at node A if node A reads its own clock value t, and receives 3 values from nodes B, C, and D where two out of the readings differ from t by exactly δ.

(4 points)

b) Describe the notion of skewness as defined mathematically in the context of adaptive load sharing in data centres (as used in the paper by Xiao et al 2013).

(2 points)

Notation for Processes

C = Worst-case execution time
B = Worst-case blocking time
D = Relative deadline
n = Number of processes
T = Period
R = Worst-case response time
J = Release jitter

Schedulability test for Rate Monotonic:

$$\sum_{i=1}^{n} \left(\frac{C_i}{T_i} \right) \le n(2^{1/n} - 1)$$

Schedulability test Earliest Deadline First:

$$\sum_{i=1}^{n} \left(\frac{C_i}{T_i} \right) \le 1$$

RMS Response time analysis

$$w_i = C_i + B_i + \sum_{\forall P_j \in hp(P_i)} \left\lceil \frac{w_i + J_j}{T_j} \right\rceil C_j$$

$$R_i = w_i + J_i$$

$hp(P_i)$ is the set of processes with a higher priority than process P_i.

Timing Analysis of CSMA/CR

B = blocking time
C = transmission time of entire frame
T = period
τ_{bit} = transmission time of one bit
w = response time for the first bit of a frame to be sent
R = total response time
J = Jitter
t = Longest busy interval
$lp(m)$ = set of messages with lower priority than m.
$hp(m)$ = set of messages with higher priority than m.
$hep(m)$ = set of messages with higher or equal priority than m.
n = number of bytes in message (data field)

$$R_m = \max_{q=0..Q_m-1}(R_m(q))$$

$$R_m(q) = J_m + w_m(q) - q \cdot T_m + C_m$$

$$w_m(q) = B_m + q \cdot C_m + \sum_{\forall j \in hp(m)} \left\lceil \frac{w_m(q) + J_j + \tau_{bit}}{T_j} \right\rceil \cdot C_j$$

(with $w_m{}^0(q) = B_m + C_m q$)

$$Q_m = \left\lceil \frac{t_m + J_m}{T_m} \right\rceil$$

$$t_m = B_m + \sum_{j \in hep(m)} \left\lceil \frac{t_m + J_j}{T_j} \right\rceil \cdot C_j \qquad \text{(with } t_m{}^0 = C_m \text{)}$$

$$C_m = \left(8n + 47 + \left\lfloor \frac{34 + 8n - 1}{4} \right\rfloor \right) \tau_{bit}$$

$$B_m = \max_{j \in lp(m)}(C_j)$$