Crib for 4C4 Design Methods 2019

Version: POK/4

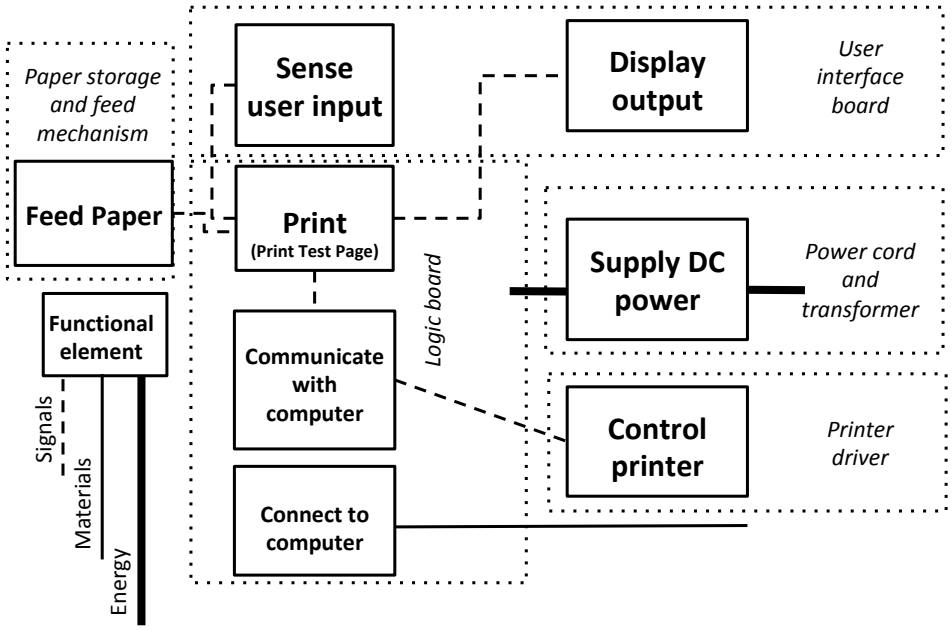
Question 1

a)

There are several possible solutions here, however, the statement must be solution-neutral and at a reasonable level of abstraction. An example statement can be of the form: Devise a means of transferring information from the user's computer to paper.

b) and (c)

An example of a function structure for printer (b) and its modularisation (c) is included in the figure below.



d)

Many approaches are possible, however, it is important to clearly map functions against solution principles and be clear about how the concepts are evaluated against each other. The typical approach is to first map functions against solution principles by constructing a table mapping the critical functions for the purpose of this analysis against potential viable solution principles, for example:

Function/Solution	Solution 1	Solution 2	Solution 3
Feed Paper	Manual	Automatic	Magazine
Communicate with Computer	USB Wire	WiFi	Bluetooth
Print	Simplex	Manual Duplex	Automatic Duplex
Sense User Input	Hard Keys	Resistive Touchscreen	Capacitive Touchscreen
Display Output	LED	LCD	Capacitive Touchscreen

Having identified a number of solution principles it is now possible to identify conceptual designs by selecting combinations of solution principles. These conceptual designs are then scored by identifying a set of criteria and their weightings (1–5), for example the following and others:

Criterion	Weighting
Easy of Installation	3
Reliability of Computer Connectivity	4
Security	4
Easy of Understanding Printer Errors	4

It is now possible to compare conceptual designs against the competitor printer by estimating values and corresponding weighted values for the different designs.

Many functions and criteria are possible to use. It is, however, important, that functions related to the question are distilled into sensible solution principles and criteria and that a very brief narrative justifies the most suitable conceptual design and that such a choice is not solely motivated by appealing to a numerical score.

e)

The technology s-curve refers to a sketch (or model) of adoption as a function of time through three phases: 1) innovation; 2) improvement/growth; and 3) maturity.

The product architecture typically changes in response to these phases and starts out with no dominant architecture in the early innovation phase. As this printer design is facing competition with substantially different features, the product architecture is likely to be immature. For example, the logic board identified in (c) is unlikely to have wireless capability and changing from hard keys and LED indicators to a capacitive touchscreen requires different modules. As the printer design's feature set is more robust a dominant product architecture emerges and at the maturity phase the focus is on process, such as improving reliability, consistency and re-use of components.

Most candidates were able to identify the main function structures and distill a modular architecture. Many candidates struggled to carry out a competitive analysis and reason about the product architecture in relation to the technology s-curve.

Question 2

a)

The hazard function is $h(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1-F(t)}$. After integrating $f(t)$ we have $R(t) = \exp\left(-at - \frac{b}{2}t^2\right)$ and thus $h(t) = a + bt; t \geq 0; a \geq 0; b > 0$. In other words, the hazard function is linear with intercept a and slope b.

b)

For very small b the linear model is a reasonable approximation during the tyre's estimated useful lifespan—the phase where a near constant failure rate is expected. Since only random failure is unlikely to be achievable due to constant wear on the tyre the linear model is reasonable in this specific phase (for appropriate parameter values). The linear hazard function is however unsuitable for describing the failure characteristics in the burn-in and wear-out phases.

c)

Now $f(t) \sim U(a, b)$ and therefore:

$$f(t) = \begin{cases} 0 & \text{if } t < a \\ \frac{1}{b-a} & \text{if } a \leq t \leq b \\ 0 & \text{if } t > b \end{cases}$$

Integrating $f(t)$ results in:

$$F(t) = \begin{cases} 0 & \text{if } t < a \\ \frac{t-a}{b-a} & \text{if } a \leq t \leq b \\ 1 & \text{if } t > b \end{cases}$$

and the hazard function $h(t)$ is then:

$$h(t) = \begin{cases} 0 & \text{if } t < a \\ \frac{1}{b-t} & \text{if } a \leq t \leq b \\ \text{Undefined} & \text{if } t > b \end{cases}$$

d)

The linear hazard function implies a constant increase in the failure rate throughout the tyre's useful life span. Assuming small slope parameter values the linear hazard function is suitable for modelling the useful life-span and indicates a small constantly increasing failure during the tyre's estimated lifespan. The uniform density gives rise to a hazard function that increases without bound towards infinity. It indicates a serious manufacturing error in the tyre as the tyre will exhibit a small increasing failure rate which at a point near, but not at or beyond, the tyre's useful lifespan will catastrophically increase to a near certainty.

e)

This failure is due to a sudden chock and can therefore be assumed to be generated by a process that is both random and memoryless. The hazard function (which is a conditional density) is then constant, $h(t) = \lambda$, where λ is the failure rate, as the hazard function does not depend on the previous condition of the tyre.

By inspection of the definition of the hazard function, the derivative of $R(t)$ is $-f(t)$ and thus $h(t) = -\frac{d}{dt} \ln R(t)$. Integrating from 0 to t, using the boundary condition $R(0) = 1$ (the probability of failure at $t = 0$ is zero), and solving for $R(t)$ yields $R(t) = \exp\left(-\int_0^t h(t)\, du\right) = \exp\left(-\int_0^t \lambda\, du\right) = e^{-\lambda t}$ and the probability of failure in time t is then $1 - R(t)$.

An alternative solution is to directly observe that an exponential failure density function gives rise to a constant hazard function and then derive the reliability function from the relationship $R(t) = 1 - F(t)$, which again yields the probability of failure in time t as $1 - R(t)$.

A small number of candidates failed to derive the linear hazard function. Most candidates were able to reason about the implications of the two different hazard functions. Many candidates failed to derive a correct expression for the last part of the question, usually because they did not realise the hazard rate was constant.

Question 3

a)

The solution-neutral problem statement given the problem context should define the problem, which is monitoring for suspicious activity in the parcel processing plant, in solution-neutral terms. An example of such a statement is: Devise a method for monitoring for suspicious activity in a large parcel processing facility.

b)

Requirements must be testable and traceable. There are many possible solutions. Many sources are possible. It is also possible to include priorities but not necessary as the question asks about key requirements. Examples of requirements include:

1. Chair must be compliant to British safety and suitability of workplace seating. Source: Regulation.
2. Displays must comply with British standards for ergonomics of displays in control centres. Source: Regulation.
3. Machine learning algorithm must have a true positive rate of 95% or higher. Source: Director of Security.
4. Machine learning algorithm must have a false alarm rate of less than 5%. Source: External psychology expert on control centre design.
5. There must be a mechanism for rewinding CCTV surveillance videos up to two weeks. Source: Director of Security.
6. There must be a mechanism for automatically backing up CCTV surveillance videos every 24 hours. Source: Director of IT.
7. There must be a mechanism for verifying that the operator is alert on suspicious activities. Source: Director of Security.
8. There must be facility ensuring full surveillance when an operator is temporarily unavailable. Source: Director of Security.

c)

A cross-verification matrix consists of a row for each requirements and each row has the following columns:

- Requirement ID (matching the requirements specification)
- Requirement (matching the requirements specification)
- Verification method (without precise method)
- Allocation (indicating the subset of components and modules affected)
- Success criteria

A verification method will refer to an inspection, demonstration, test or analysis protocol.

Referring to the requirements in (b) above (VM = Verification Method; A = Allocation; SC = Success Criteria), an example cross-reference verification matrix is provided below. Other solutions are possible as long as they relate to the requirements and provide sensible verification methods, allocations and success criteria.

1. VM: Inspection; A: Chair; SC: Compliance with relevant standard.
2. VM: Inspection; A: Displays; SC: Compliance with relevant standard.
3. VM: Test; A: Machine learning algorithm; SC: True positive rate higher than 95% on representative test data.
4. VM: Test; A: Machine learning algorithm; SC: False alarm less than 5% on representative test data.
5. VM: Demonstration; A: Storage/System; SC: Rewinding capability up to two weeks.
6. VM: Demonstration; A: Storage/System; SC: Existence of working back-ups every 24 hours.
7. VM: Test; A: System/Operator; SC: Ability of typical operator to detect suspicious activity for representative test data.
8. VM: Inspection; A: System/Operator; Existence of capacity for either routing surveillance task to alternative operator or ability of system to automatically log unsurveilled data for later review.

d)

The questions for five error-producing conditions. Examples of such factors include:

1. Lack of training.
2. Fatigue.
3. Inattention due to cognitive overload.
4. Inattention due to over-reliance of machine learning system to identify suspicious activities.
5. Inattention due to outside distractions.

e)

While verification of the cross-reference matrix ensures the system meets requirements, it does not necessarily mean the system is effective in practice.

A successful validation strategy provides a conclusive answer that the problem outlined in the solution-neutral problem statement is met in an actual deployment. A validation strategy for this system is then likely to run over several weeks and include repeated random artificial injection of suspicious activities and complete data collection of the operator conditions. This allows the stakeholder to conclude whether the system has addressed the problem statement or not and understand if any of the error-producing conditions pose an unacceptable high risk of operator error. In addition, verification requirements which may succeed in verification but fail in deployment due to their deployment complexity, such as back-ups, can be validated as part of this process as well.

Most candidates were able to derive reasonable requirements, however, many forgot to ensure the requirements were traceable. Most candidates failed to correctly set up a verification cross-reference matrix. A majority of the candidates could reason sensibly about validation given the problem context.

Question 4

a)

Risk management involves a trigger/background that is articulated into a purpose. System mapping then encompasses mapping the system by defining the requirements and describing the system. Risk assessment involves identifying hazards in the system, which are assessed as risks. This leads to a set of proposed actions.

b)

Mapping this system first involves setting the boundary. This is typically best achieved by describing a system more extensive than the one introduced in the question and explicitly defining the boundary within that system description.

Structural diagrams such as a task diagram, organisational diagram and a communication diagram can be used to map the system at sufficient level to set the boundary. Complete and accurate diagrams are not possible to do for this question and not expected in model answers. However, the system should be mapped in terms of organisation (operator team, operator, user), task (detect fall, relay signal, queue request, identify available operator, assess situation, contact emergency services/mobile staff), and information (fall detection signal, possibly including probability of fall, information about the user in conjunction with fall detection signal) and information flow (from the sensor to the microcontroller/software code to the network module to the organisation monitoring alarm signals to a queue of operators to an individual operator and finally to emergency services/mobile staff.

The overall function is then Mitigate Consequence of Fall (or similar formulation), with significant sub-functions Detect Fall, Send Fall Signal, Process Fall Signal and Investigate Fall.

The system boundary can then be defined as within an extended system consisting of the telecommunication network, road network and emergency services and the boundary is set within this system.

Multiple answers are possible but they should map the system by making reference to organisation, communication and tasks and set the boundary within an extended system motivated from the significant sub-functions arising out of the overall function of the system.

c)

There are multiple possible answers, however, it is important the techniques are clearly motivated within the problem context provided in the question. Three examples include:

- SWIFT, which can be used to explore different scenarios, their consequences and impacts and which is carried out by a series of what-if questions and links them to their hazards and risks, relevant controls, a risk ranking and notes about possible actions.
- FMEA, which is used to study the effect of human error on systems and can also be used to study the failure modes on the wearable device. Relevant task steps are linked to failure modes, their causes, their likelihood or severity, recovery steps and any actions.
- A risk matrix can be used rank the consequences and likelihoods of undesired events and can be used in conjunction with FMEA to rank and prioritise risk. The matrix has the dimensions likelihood and impact.

d)

The fault tree can be drawn in a number of ways. The top-level event is Untreated Fall or similar designation and the second-level events may be comprised of Fall Undetected and Failed Intervention. Fall Undetected can be further broken down into Failure to Sense Fall and Failure to

Send Fall Signal. These events can be further broken down into their causes, such as poor machine learning algorithm, poor choices of sensors, poor training data, sensor failure, microcontroller failure, battery failure, connectivity failure, router failure, and failure in the telecommunications infrastructure. Further causes are the user accidentally turning the device off or accidentally turning off the router. Failed Intervention can arise due to multiple causes which form a hierarchy: operator team error, request queuing error (for instance, accidentally dropping requests), operator error, wrong address, confusion with another user, or unavailability of resources to intervene, such as unavailability of mobile support team and/or emergency services.

This was a popular question and it was answered well by most candidates. Many candidates struggled with system mapping, often failing to identify the system boundary or omitting important considerations. On the other hand, the vast majority of candidates were able to suggest and apply correct risk management methods for the problem.