Checkpoint 4 Notes

At this stage your group has the architecture design of your system. Now your group will pick one of the architectural drivers (a high priority quality attribute scenario). Conduct a lightweight analysis of your architecture for that scenario using tactics-based questionnaire showing clearly:

* The tactic supported or not supported in your architecture
* For the tactics that are supported, describe the specific design decisions made to support the tactic and enumerate where these decisions are, or will be, manifested (located) in the architecture
* The risk of implementing the tactic using a (H = High, M = Medium, L = Low) scale
* The rationale for the design decisions made (including a decision to not use this tactic) and its implications

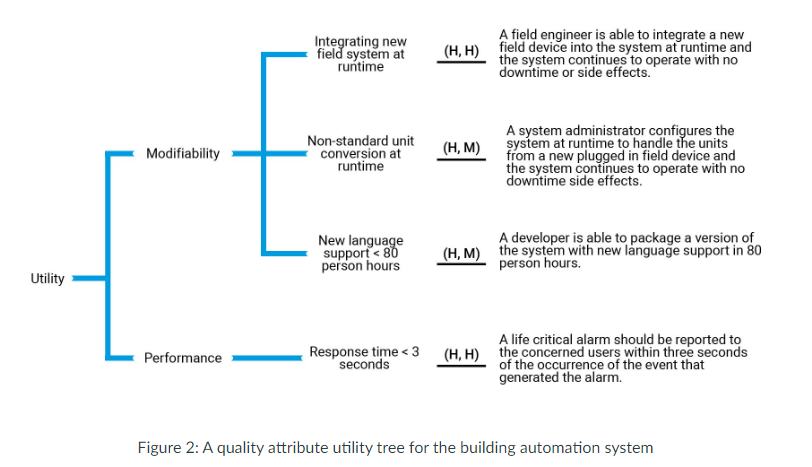
Submit Group Project Checkpoint #4.

|  |  |
| --- | --- |
| **Criteria** | **Ratings** |
| Tactics supported or not supported  For the chosen high priority quality attribute scenario, which tactics are supported or not supported in your architecture. | **2 pts**  **Full Marks**  Analysis of tactics supported or not supported IS clear. |
| Design Decisions  For the tactics that are supported, describe the specific design decisions made to support the tactic and enumerate where these decisions are, or will be, manifested (located) in the architecture. | **4 pts**  **Full Marks**  Where design decisions are manifested in the architecture IS clear. |
| Risk The risk of implementing tactics using a (H = High, M = Medium, L = Low) scale.  For the chosen high priority quality attribute scenario, which tactics are supported or not supported in your architecture. | **2 pts**  **Full Marks**  Risk of implementing tactics IS clear. |
| Rationale  The rationale for the design decisions made (including a decision to not use this tactic) and its implications | **2 pts**  **Full Marks**  Rationale for the design decisions made IS clear. |

Steve notes: we are only doing this for one High Priority Quality Attribute Scenario, please suggest the High Priority Quality Attribute Scenario you think might be the best for us to use to the group.

Brian: Following the ATAM Module on Canvas:

**Phase 1 of ATAM:**  ATAM proceeds in multiple Phases. The intent of Phase 1 of ATAM is to first have a project decision maker (such as a project manager or the system’s customer) provide a system overview from the business perspective. This helps the evaluation team identify the *business drivers or goals*. Next, the lead architect describes the architecture of the system. This helps the evaluation team identify the *architectural approaches* used in designing the system. With the help of the project decision makers, the evaluation team uses the business drivers to articulate the most important *quality attributes* in detail using *scenarios* that are specific, testable and prioritized. This information is captured in a form known as a quality attribute utility tree.



* *Risks*: potentially problematic architectural decisions; related risks can be grouped together into *risk themes*
* *Non-risks*: good architectural decisions
* *Sensitivity points*: places in the architecture that significantly affect whether a particular quality attribute response is achieved
* *Tradeoffs*: properties of a system that affect more than one quality attribute

**Phase 2 of ATAM:** In Phase 2 of ATAM, the evaluation team meets with the project stakeholders to elicit their points of view and verify the results of Phase 1. The team generates a prioritized list of scenarios from the stakeholder community to see how it agrees with the utility tree. The architect is again asked to explain how *architecture decisions* used in the design of the system supports the highest ranked quality attribute scenarios from the stakeholders.

You can think of Phase 1 as a *top down analysis* that identifies gaps between what the primary business decision makers want and what the primary technical decision makers will deliver. Phase 2 is a *bottom up analysis* that identifies gaps between the needs of the primary stakeholders of the system and its primary business decision makers, and gaps between these needs and what the primary technical decision makers will deliver.

**Tactics-based questionnaires** (included in chapters 4 – 13 for each of the predominant quality attributes) can be used as part of light-weight analysis. Questions can be raised to determine risks from the use or non-use of tactics related to the design objectives associated with the quality attributes under analysis. If a tactic is used, the specific design decisions made to realize the tactic along with its rationale and any assumptions can be recorded. To use these questionnaires (included in chapters 4 – 13 for each of the predominant quality attributes), simply follow these four steps:

**Step 1.** For each tactics question, fill the “Supported” column with “Y” if the tactic is supported in the architecture and with “N” otherwise.

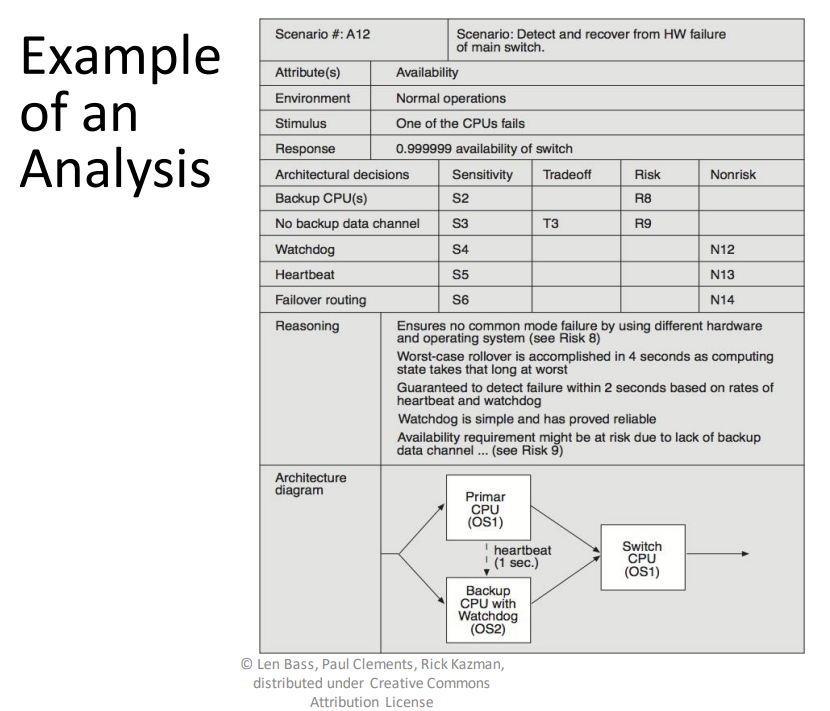
**Step 2.** If the answer in the “Supported” column is “Y,” then in the “Design Decisions and Location” column describe the specific design decisions made to support the tactic and enumerate where these decisions are, or will be, manifested (located) in the architecture.

**Step 3.** In the “Risk” column indicate the risk of implementing the tactic using a (H = High, M = Medium, L = Low) scale.

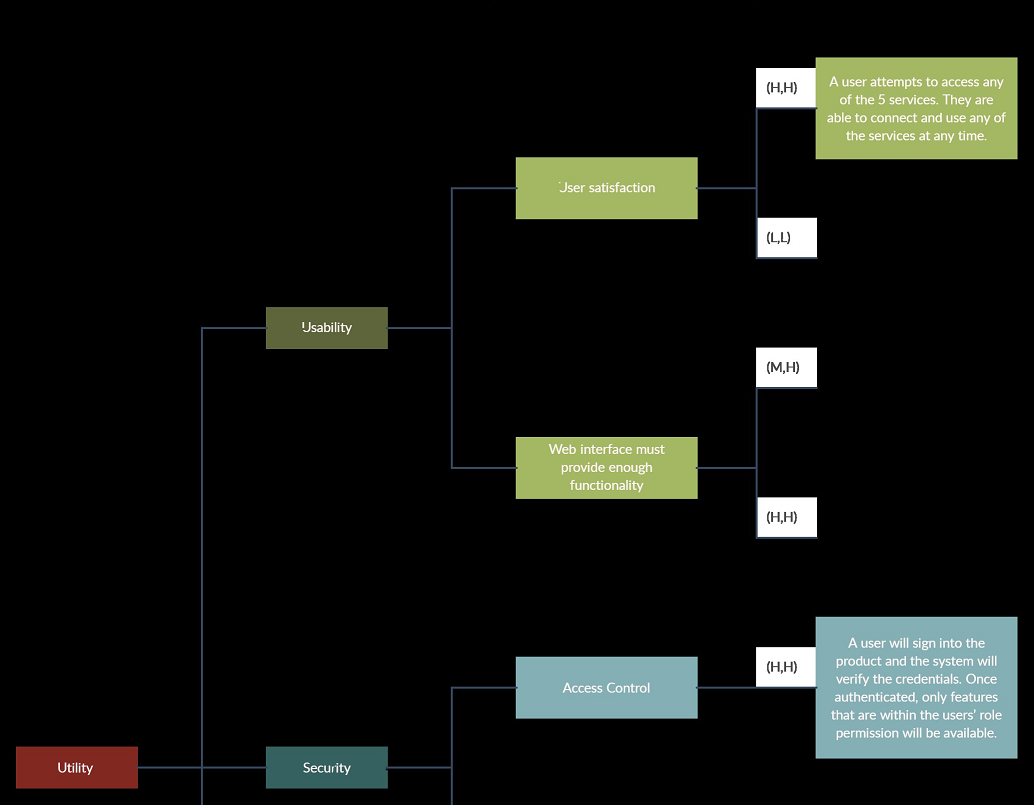
**Step 4:** In the “Rationale” column, describe the rationale for the design decisions made (including a decision to not use this tactic). Briefly explain the implications of this decision.

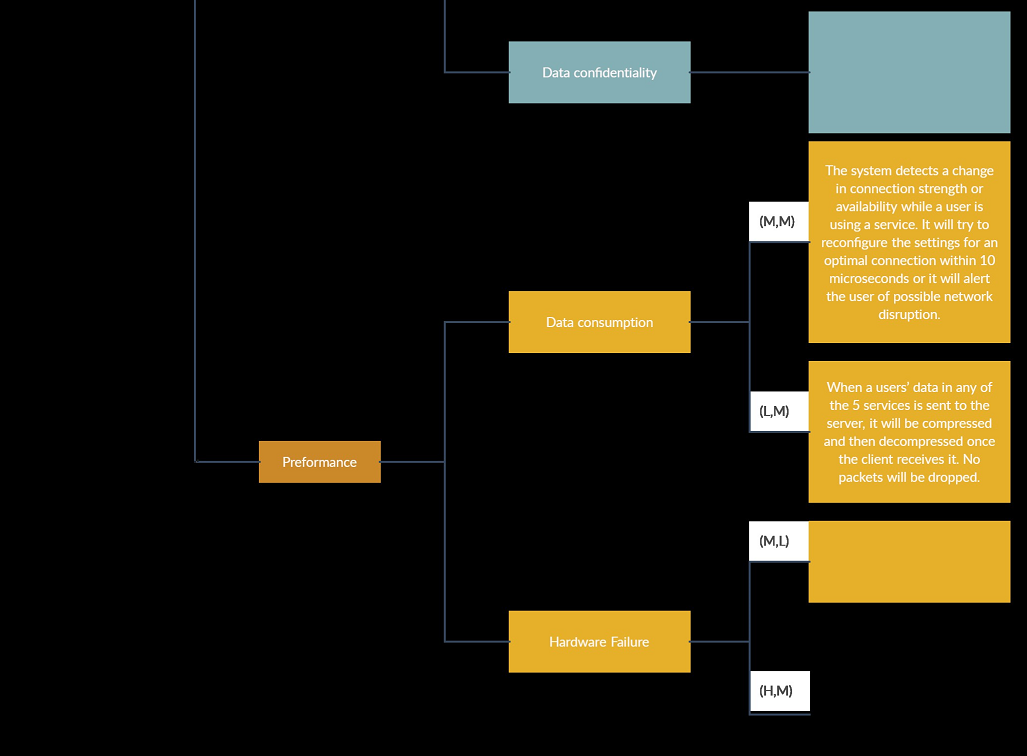
While this questionnaire-based approach might sound simplistic, it can actually be very powerful and insightful. Addressing the set of questions forces the architect to take a step back and consider the bigger picture. This process can also be quite efficient: A typical questionnaire for a single quality attribute takes between 30 and 90 minutes to complete.

From the PPT slides:



I made a super-early rough draft of a utility tree. Let me know if you guys would like for me to finish this:





Based on the design from the book:

Tactics-Based Questionnaire for Security:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tactics Group** | **Tactics Question** | **Supported? (Y/N)** | **Risk** | **Design Decisions and Location** | **Rationale and Assumptions** |
| Detecting Attacks | Does the system support the detection of intrusions by, for example, comparing network traffic or service request patterns within a system to a set of signatures or known patterns of malicious behavior stored in a database? | (Y) | (H) |  |  |
| Does the system support the detection of denial-of-service attacks by, for example, comparing the pattern or signature of network traffic coming into a system to historical profiles of known DoS attacks? |  |  |  |  |
| Does the system support the verification of message integrity via techniques such a checksums or hash values? |  |  |  |  |
| Does the system support the detection of message delays by, for example, checking the time that it takes to deliver a message? |  |  |  |  |
| Resisting Attacks | Does the system support the identification of actors through user IDs, access codes, IP addresses, protocols, ports, etc.? | Y | H | This will be achieved by including the Identify Device subcomponent of the Security Component which will contain the code to identify and validate access points. This component is the first piece of the system a device will interact with when it connects. | This is an important step in preventing access from bad actors, as well as assisting in debugging problems for specific hardware/software profiles |
| Does the system support the authentication of actors via, for example, passwords, digital certificates, two-factor authentication, or biometrics? | Y | H | This will be achieved by including subcomponents for an Integrated Authentication Service or an Internal Authentication Service. The device will have to be authenticated with our own user database or a third-party service that a customer can integrate within the system. These subcomponents are found in the Security Component after the device has been identified. | This is included because it how the system will verify that only valid customers can access the system, create traceability within the system by logging actions and attributing them to the user, and is another step to prevent bad actors from gaining access to the system |
| Does the system support the authorization of actors, ensuring that an authenticated actor has the rights to access and modify either data or services? | Y | H | This will be achieved by a subcomponent within the Security component that will get and assign the appropriate permissions for the user based on individual, group, or role. This can is done after the user has been authenticated. | This design decision will keep permissions locked down and prevent all users from having too much access to data or services. This will prevent mistakes by users who don’t need a given permission as well as limit the number of accounts a bad actor can compromise. |
| Does the system support limiting access to computer resources via restricting the number of access points to the resources, or restricting the type of traffic that can go through the access points? | N | L | N/A | This was not included in the system because a single user may be using multiple devices for input/output. They also may be using multiple services at once |
| Does the system support limiting exposure by reducing the amount of data or services that can be accessed through a single access point? | N | L |  |  |
| Does the system support data encryption, for data in transit or data at rest? | Y | H |  |  |
| Does the system design consider the separation of entities via physical separation on different servers attached to different networks, virtual machines, or an “air gap”? | Y | M |  |  |
| Does the system support changing credential settings, forcing the user to change those settings periodically or at critical events? | Y | M |  |  |
| Does the system validate input in a consistent, system-wide way – for example, using a security framework or validation class to preform actions such as filtering, canonicalization, and sanitization of external input? | N | L |  |  |
| Reacting to Attacks | Does the system support revoking access by limiting access to sensitive resources, even for normally legitimate users and uses if an attack is under way? |  |  |  |  |
| Does the system support restricting login in instances such as multiple failed login attempts? |  |  |  |  |
| Does the system support informing actors such as operators, other personnel, or cooperating systems when the system has detected an attack? |  |  |  |  |
| Recovering from Attacks | Does the system support maintaining an audit trail to help trace the actions of, and to identify, an attacker? |  |  |  |  |
| Does the system guarantee the property of nonrepudiation, which guarantees that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message? |  |  |  |  |

Things to do

* Pick tactic groups to do/not to do
* Tactics questions
* Assign people to do respective tactic questions,