A Top-Down, Safety-Driven Approach to Architecture Development for Complex Systems

STAMP Workshop Lightning Talk

Justin Poh

6th June 2022

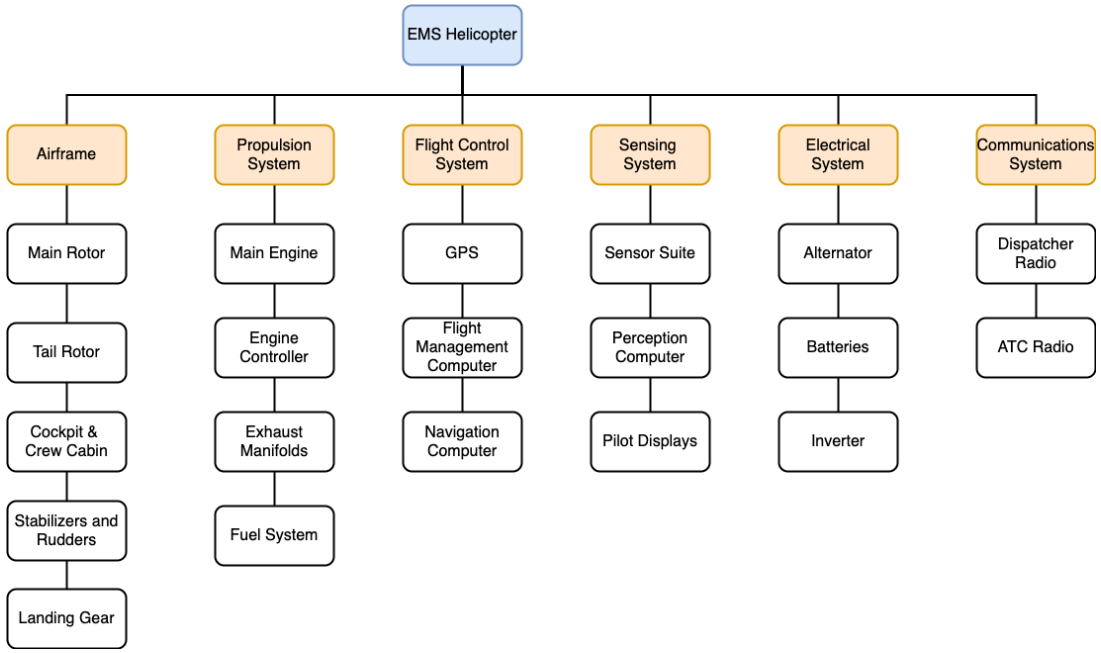
Massachusetts Institute of Technology

Engineering Systems Laboratory

What is a System Architecture?

System Architecture: An abstract description of the entities of a system and the relationships between those entities [1]

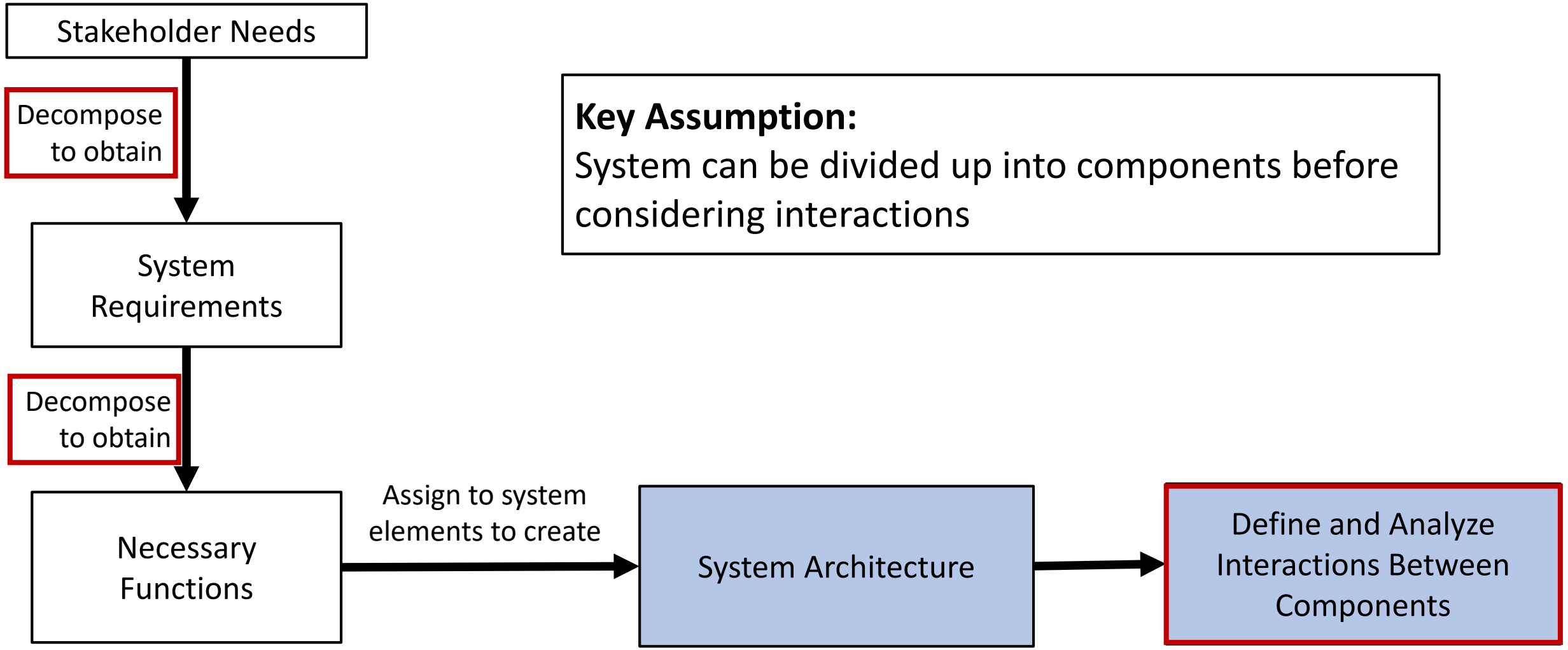
An Emergency Medical Services (EMS) Helicopter [2]



Architecture of an EMS Helicopter

[1] Crawley et. al., 2004
[2] Image from: https://www.mercyflight.org/history-of-ems/

Current Approach to Architecture Development



Key Assumption:
System can be divided up into components before considering interactions

Challenges in Using the Current Approach for Architecture Development

1. **Future Complex Systems are becoming more complex and interconnected**
   - Example: More software and sensors being introduced to modern EMS helicopters to enable them to fly in inclement weather
   - Using decomposition, it becomes more difficult to identify or avoid introducing flaws in the system architecture

A Modern Helicopter [3]

2. **The desirable system behaviors or properties are increasingly the result of component interactions**
   - Example: To achieve safe flight, need to make sure that the pilots and automated flight systems can work together effectively
   - If interactions are only considered later, desirable system behaviors or properties may not be fully realized

Pilots Interacting With Automated Flight Systems [4]

[3] Image from: https://www.businesswire.com/news/home/20141204005656/en/CHC-Helicopter-Announces-Multimillion-Pound-Building-Project-in-Aberdeen-World-Class-Terminal-and-Hangar-Complex-Will-Benefit-Offshore-Workers-Others
[4] Image from: https://www.airbus.com/en/newsroom/news/2021-07-the-global-helicopter-fleet-with-helionix-avionics-logs-500000-flight-hours

The Research Problem

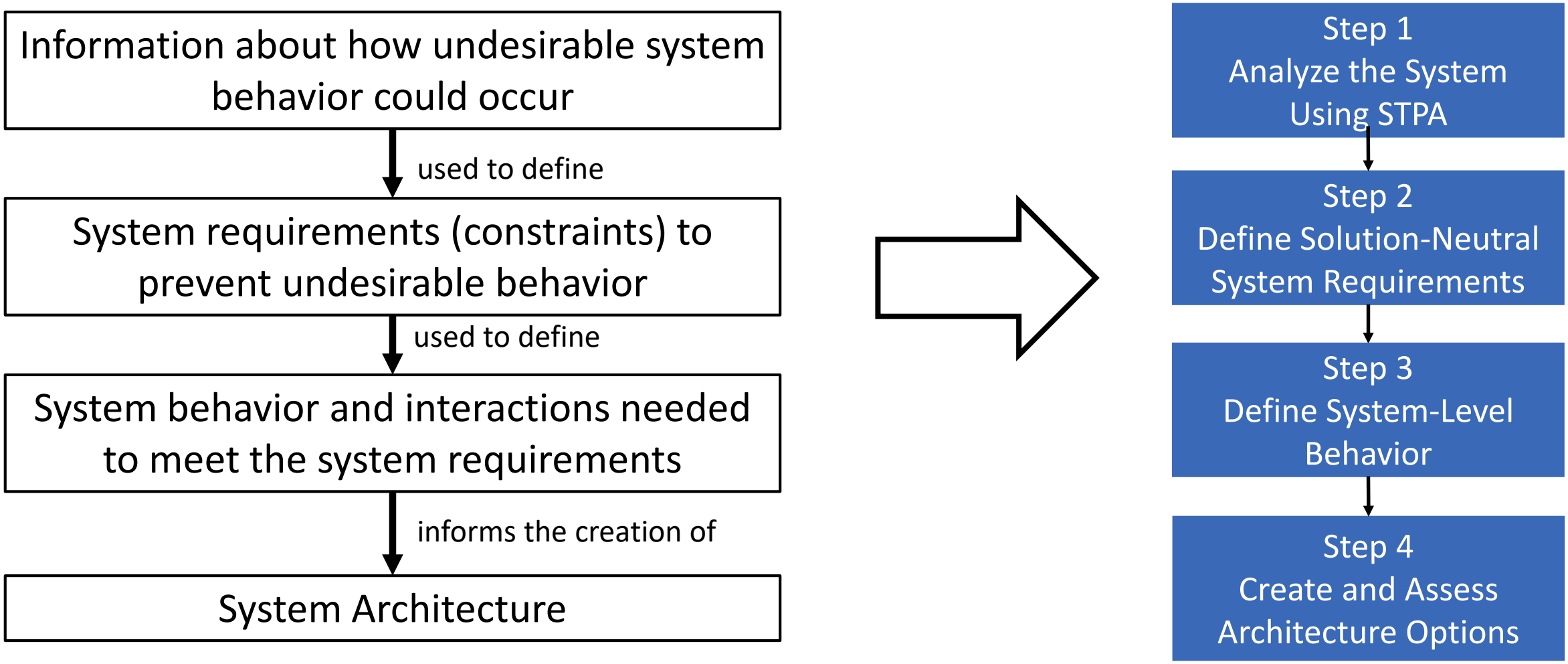
Need a new approach to architecture development that overcomes these challenges and considers systems holistically

New approach needs to:

- Consider interactions and undesirable system behavior early in the design process
- Uses that information to design the necessary interactions and system behavior into the system

Overview of Approach

Safety-relevant information can be used to drive architecture development



System Requirements Include Safety Considerations From the Beginning

- STPA is performed at the beginning of the design process
- System requirements are generated based STPA analysis and considers how undesirable system behavior can be prevented

Example Requirements for Safe EMS Flight:

- The system must respond within <threshold time> under <worst-case weather conditions> to change the desired flight path and avoid a collision
- The system must be able to detect all objects and other aircraft in the environment, even when visibility is suboptimal

System Design Defined Based On Need to Enforce Safety Constraints

- Determine the behavior of the system and interactions needed to enforce safety constraints
- Systematically define each element of a control loop (e.g. functions/responsibilities, control actions, feedback) to achieve adequate control

Example Requirement: The system must respond within <threshold time> under <worst-case weather conditions> to change the desired flight path and avoid a collision

- Function: Respond by selecting control inputs based on current and desired flight path, accounting for weather effects
- Control Actions: Roll/Pitch/Yaw inputs to aircraft
- Feedback Needed: Current weather conditions, Current aircraft position and speed, Effects of weather on aircraft handling

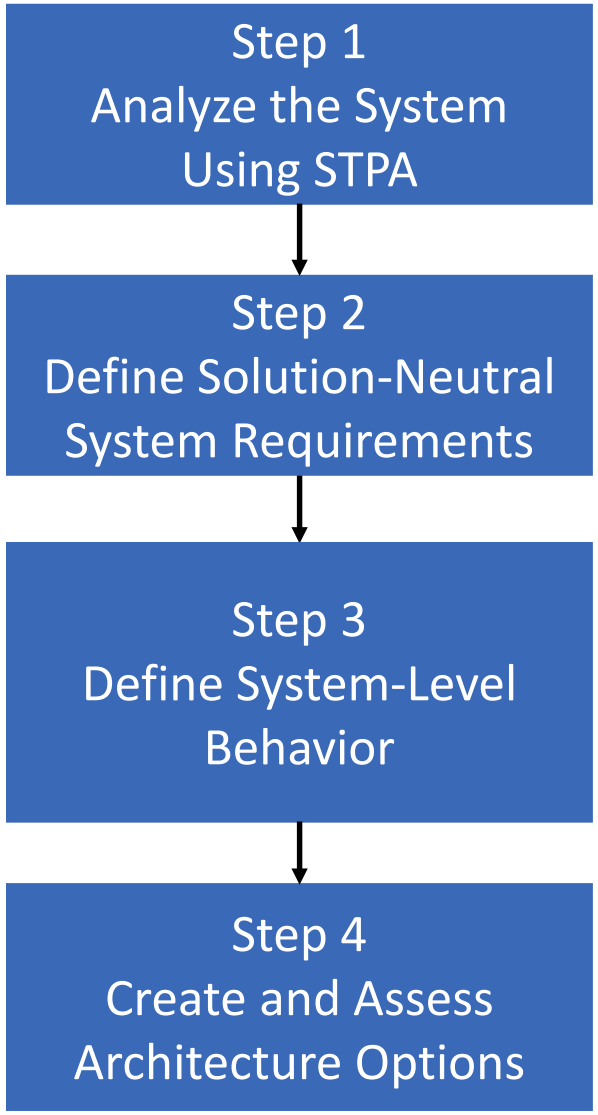
Architecture Creation Informed by System-Level Behavior

System-Level Behavior informs which functions should be assigned to which components and compare different assignment options

Example Considerations for Enabling Safe EMS flight:

- Should the responsibility for selecting control inputs be assigned to the pilot or the automated controller?
- What are the pros/cons of having the pilot or automated controller select control inputs?

Summary



New method is a structured, safety-driven approach to creating and assessing system architectures

- Considers interactions and unsafe behavior early in the design process
- Uses safety-relevant information to drive the identification of system requirements and the creation of a system architecture
- Ensures that safety is designed into the system from the beginning

Questions?

- Feel free to contact me with any questions/comments: **jpoh@mit.edu**

- Thesis available to download from **https://www.justinpoh.com/publications.html**
  - Describes how each step in the method is performed
  - Case study is developed in detail including descriptions of the architecture options and how they were assessed to determine the tradeoffs between them