Software Architecture and Enterprise Risk Management

Lauren Cooper

Cybersecurity Engineer

CERT Division

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-1189

Agenda

- About the SEI
- Software Architecture
  - Overview
  - Architectural Tradeoff Analysis Method
- Enterprise Risk Management
- The Big Picture

About the Software Engineering Institute (SEI)

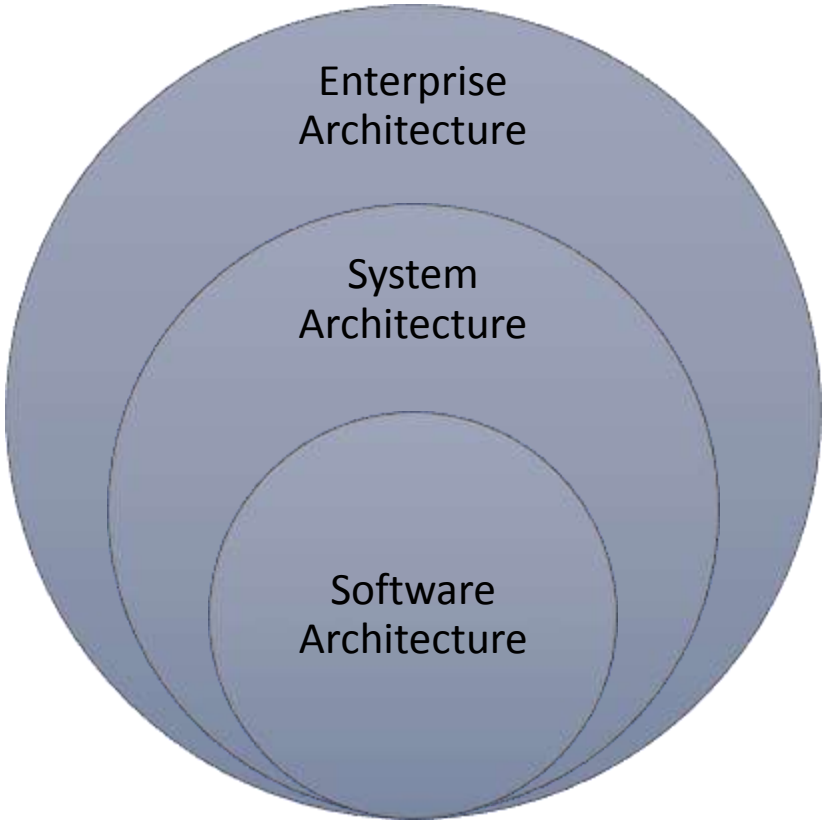
DoD FFRDC operated by
Carnegie Mellon University

The SEI's mission is to support the nation's defense by advancing the science, technologies, and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

https://www.sei.cmu.edu/

Software Architecture

Ways to Consider Architecture



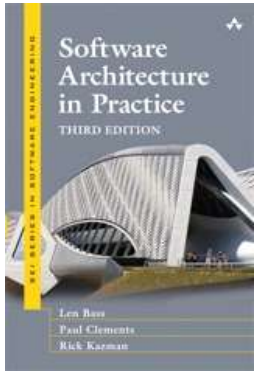
What is Software Architecture?

Software Engineering Institute Definition:

"The software architecture of a system is the set of structures needed to reason about the system, which comprise software elements, relations among them, and properties of both."[1]

Key Points:

- Every software system has an architecture
- A software architecture is not inherently good or bad



[1] Bass, L.; Clements; P. & Kazman, R. *Software Architecture in Practice, Third Edition.* Boston, MA: Addison-Wesley, 2013.

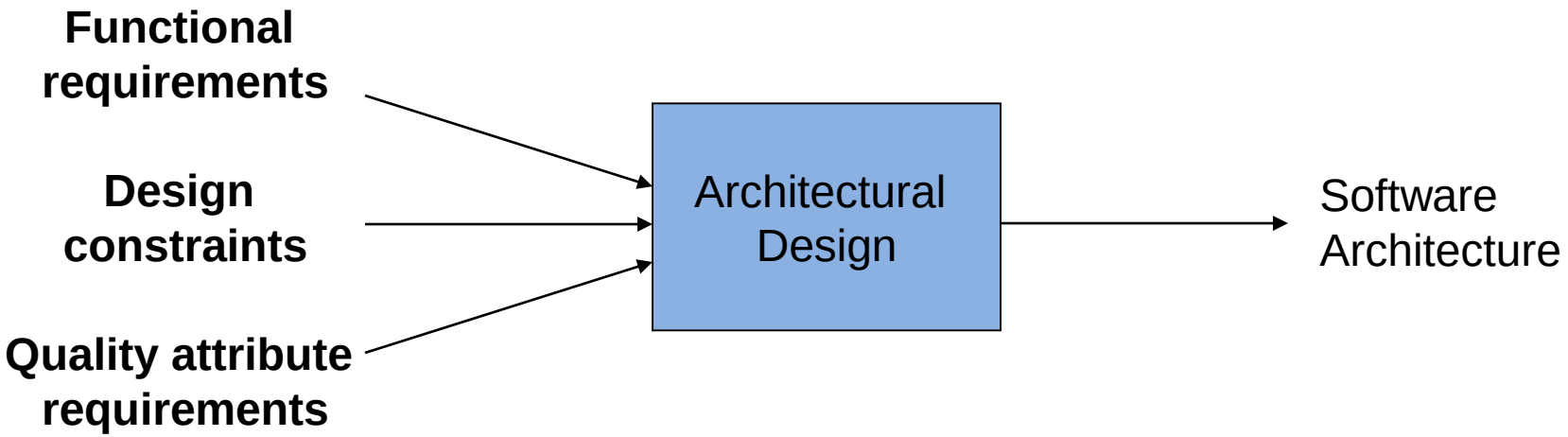
SEI Software Architecture Principles

Software architecture is a bridge between business and mission goals and a software-reliant system.

1.Quality attribute requirements drive software architecture design.

1.Software architecture drives software development through the life cycle.

From Principles to Requirements

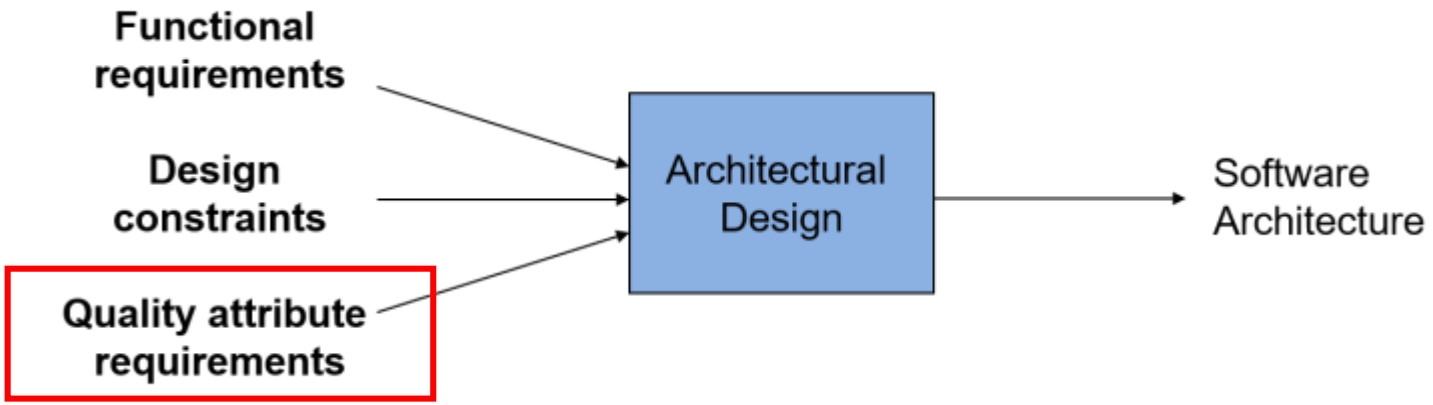


Questions to consider:

- *What determines whether these requirements are met?*
- *Which requirements are the most important when it comes to structuring an architecture?*

Beyond Functional Requirements

If functionality is the only thing that matters, any software architecture will do!

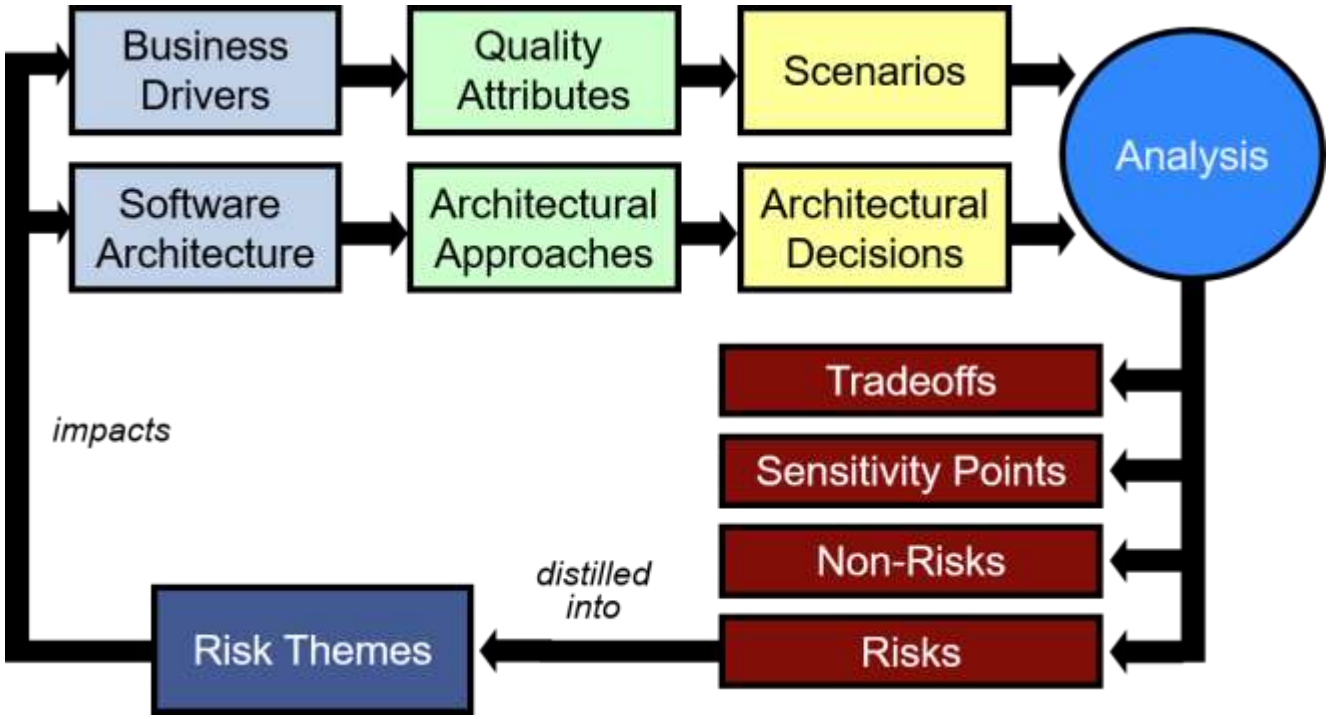


- Performance – Availability – Interoperability – Modifiability – Security – etc.
- No complete list of “universal” quality attributes
- Measurable and derived from business and mission goals for the system

Software Architecture Review

Architecture Tradeoff Analysis Method (ATAM)

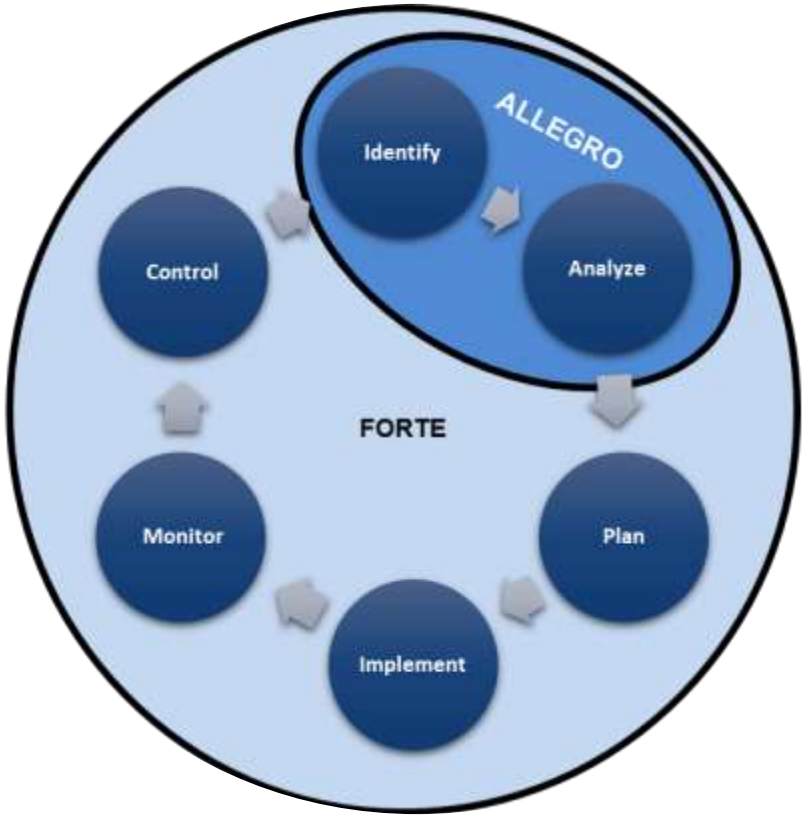
The ATAM is an architecture evaluation method that focuses on multiple quality attributes.



Enterprise Risk Management

Enterprise Risk Management

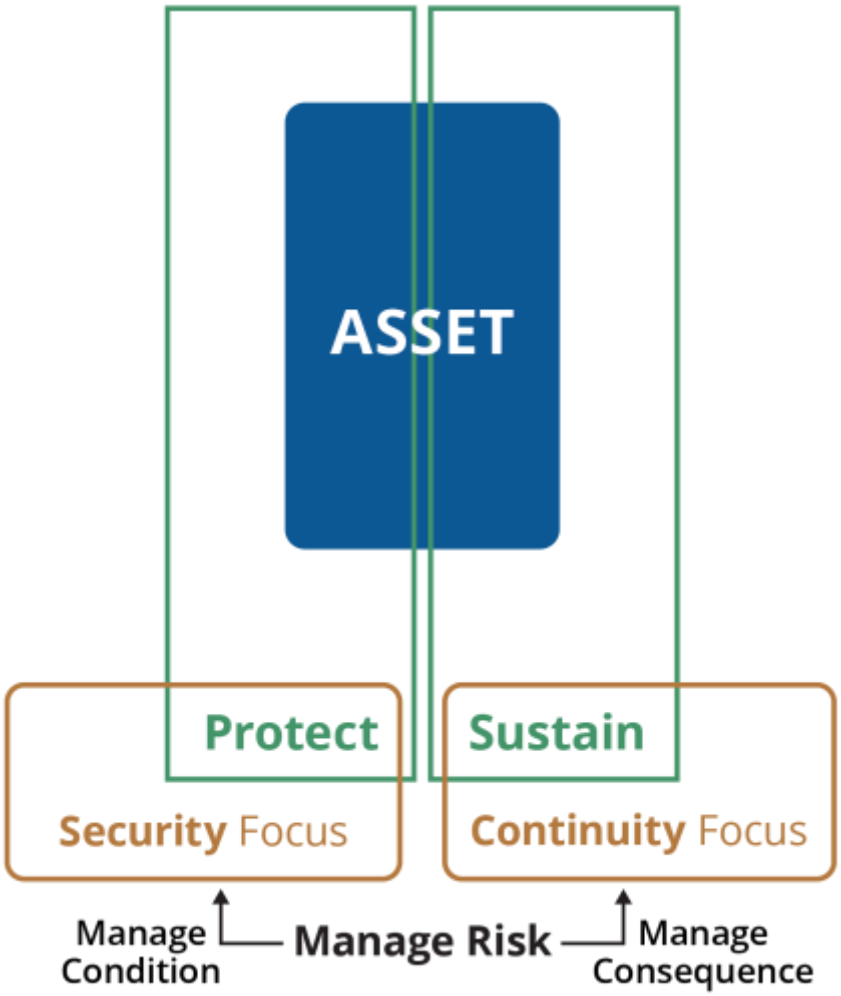
OCTAVE Framework



Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) framework

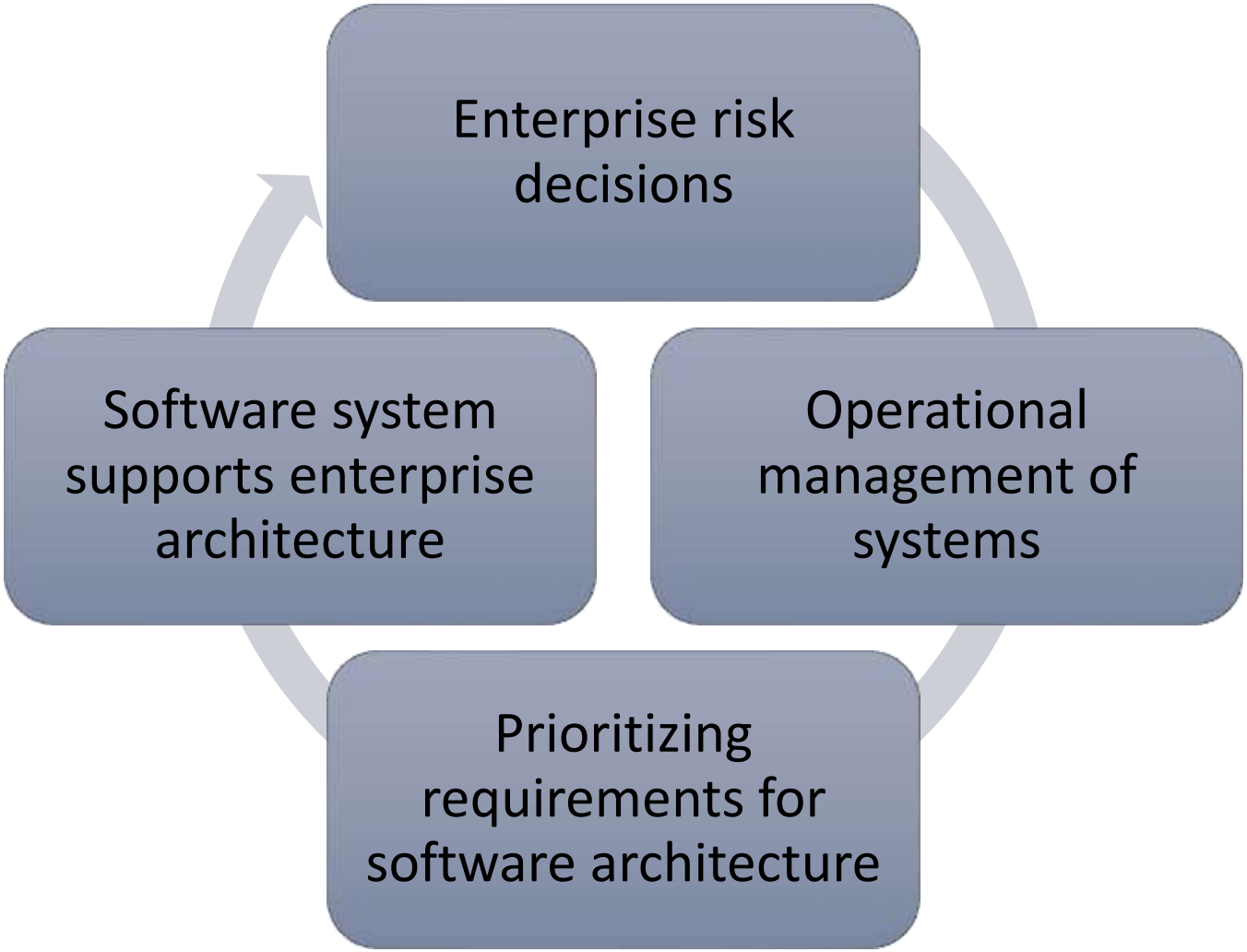
- ALLEGRO
  - Risk identification & analysis
- FORTE
  - Risk management lifecycle

Goal: Operational Resilience



- Depends on the value of the asset to the architecture and the cost of deploying and maintaining the strategy
- Iterative approach through the risk lifecycle will help prioritize risks
- An aggregation of unmanaged operational risk—a cascading risk

The Big Picture



Questions?