Assurance-Case Driven Framework to Support Cyber-Physical Systems

Wuwei Shen

Department of Computer Science Western Michigan University

- Safety critical applications have been almost everywhere

- Failure of safety critical systems have some serious consequences. Software becomes a main reason for failure of these systems.

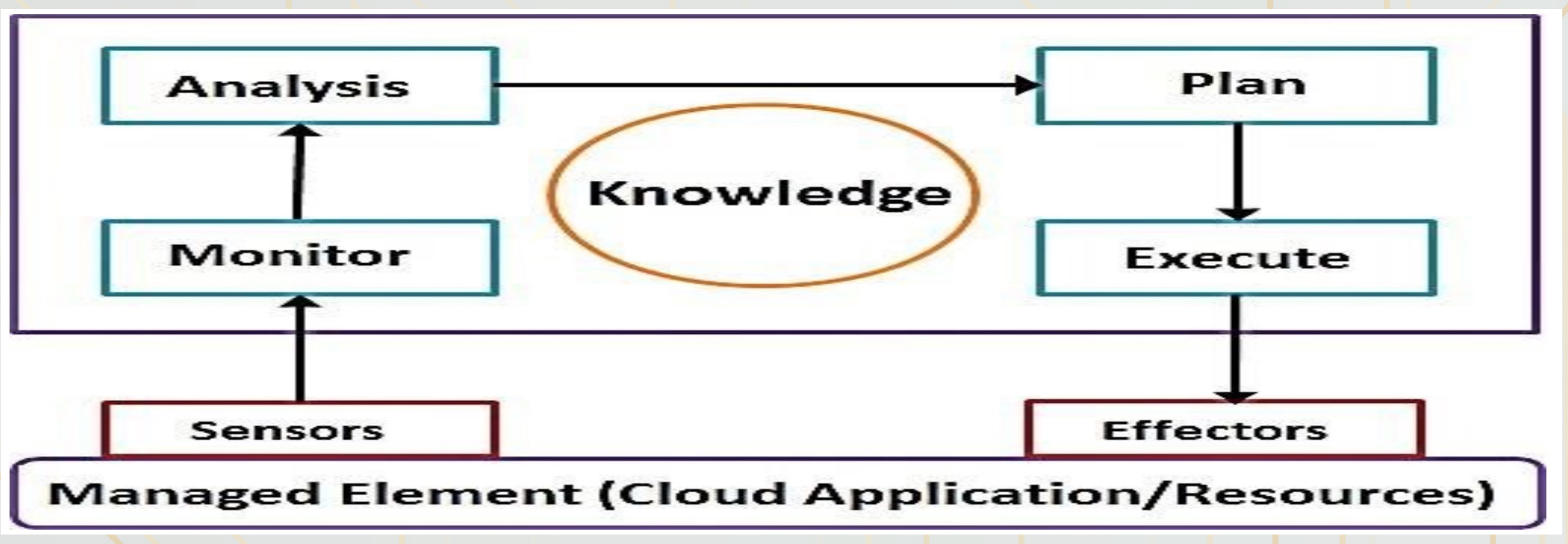
More than a quarter (25.7%) of all medical device recalls in Q4 2017 were due to software issues, making it the top cause for the seventh consecutive quarter

- Software assurance becomes an important issue when certifying a CPS

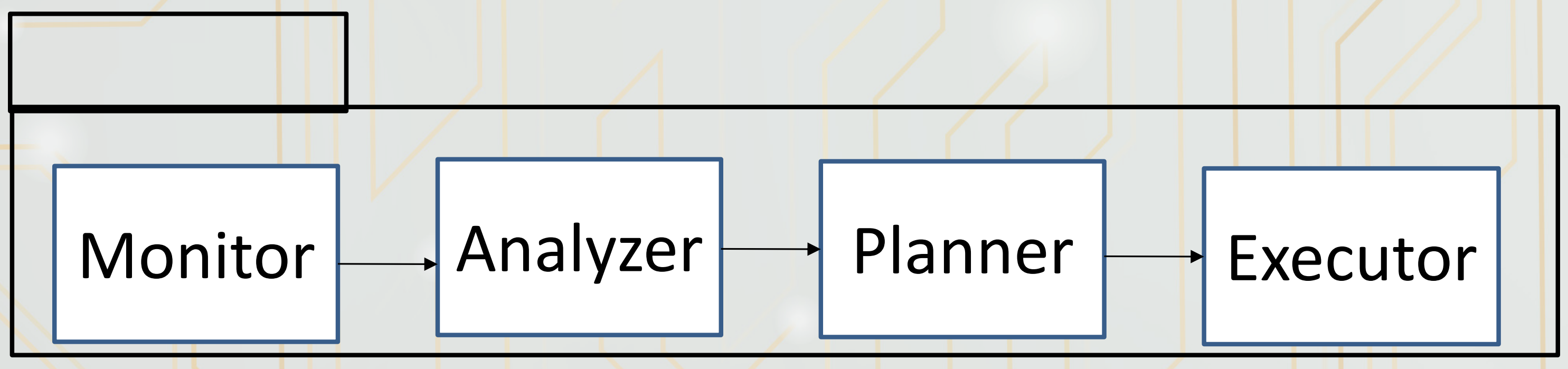
- Most current system certifications are done manually.

- Assurance case has become a main mechanism among different stakeholders to ensure that a CPS can be relied upon.
- To reduce the burden of developers and certifiers, we propose a new framework that employs the assurance case as a driving force during the design and runtime

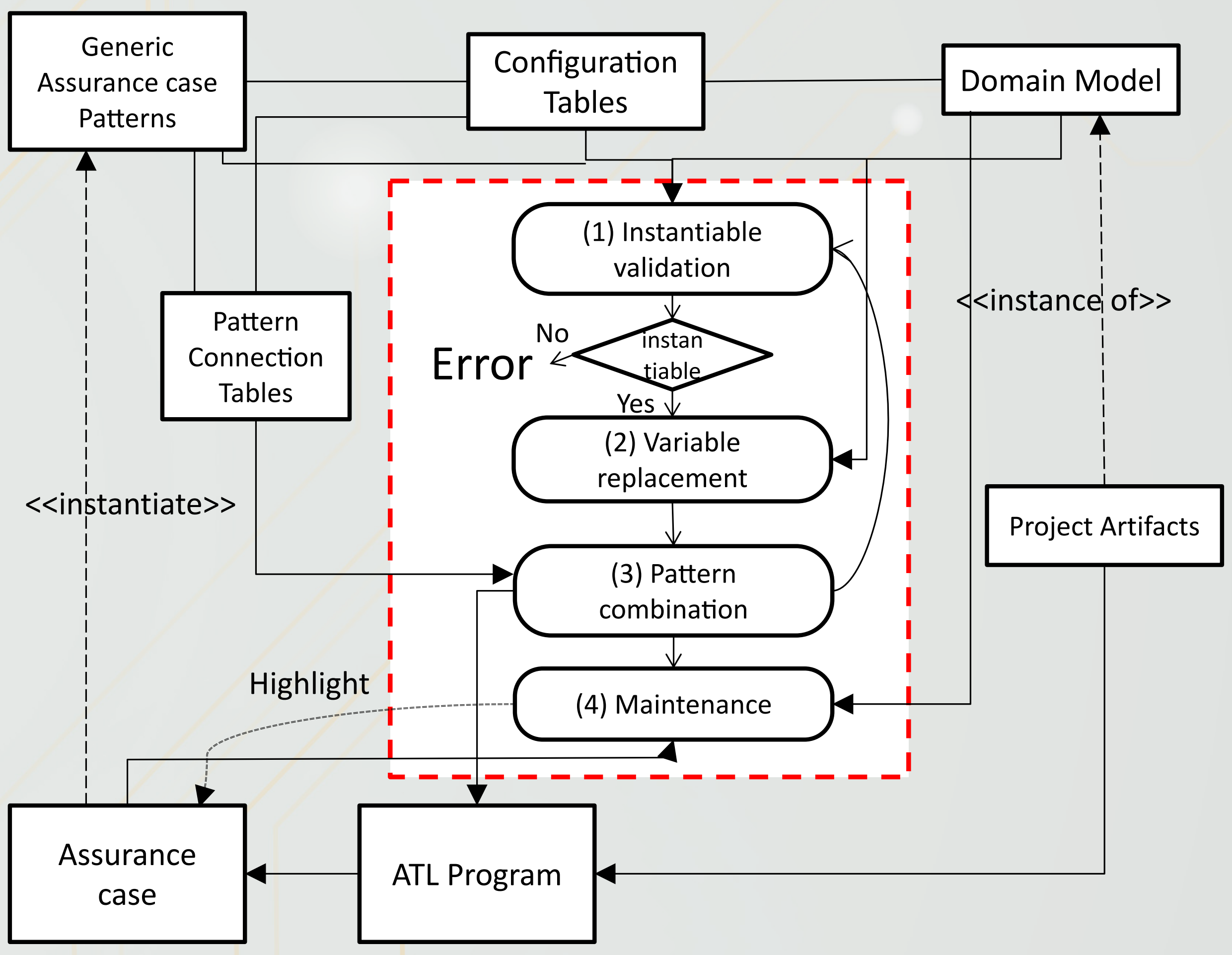
- The MAPE-K process widely used in a CPS



- Software Design for the MAPE-K

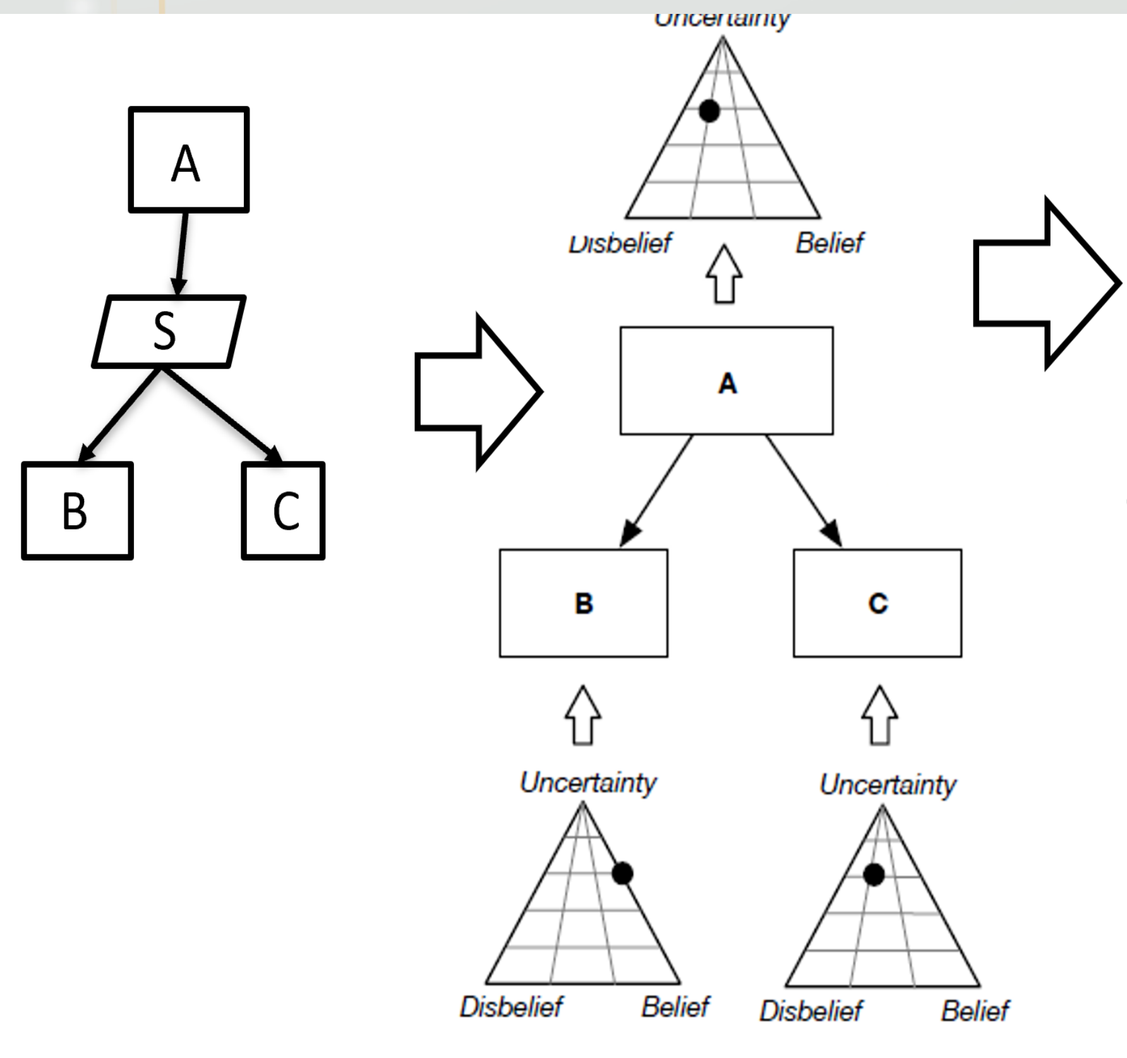


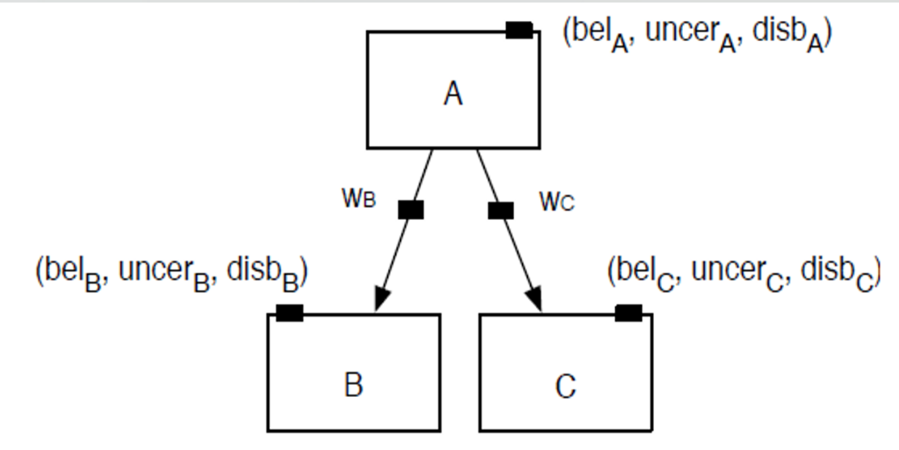
- Assurance Case Driven Framework
  - Design time



  - Design Time Certification: D-S Theory
    - D-S theory is a general framework for reasoning with uncertainty.
    - For each claim A, the frame of discernment is denoted as Ω_A={A ̅, A}
    - The mass function $m^\Omega(P) \in [0,1]$ denotes the degree of belief committed to the hypothesis that the truth lies in P where P is a power set of Ω, i.e. P $\in 2^\Omega$

$$\begin{cases} bel_A = m(A) & \textit{represents the belief in A} \\ disb_A = m(\overline{A}) & \textit{represents the disbelief of A} \\ uncer_A = 1 - bel_A - disb_A & \textit{represents the uncertainty} \end{cases}$$





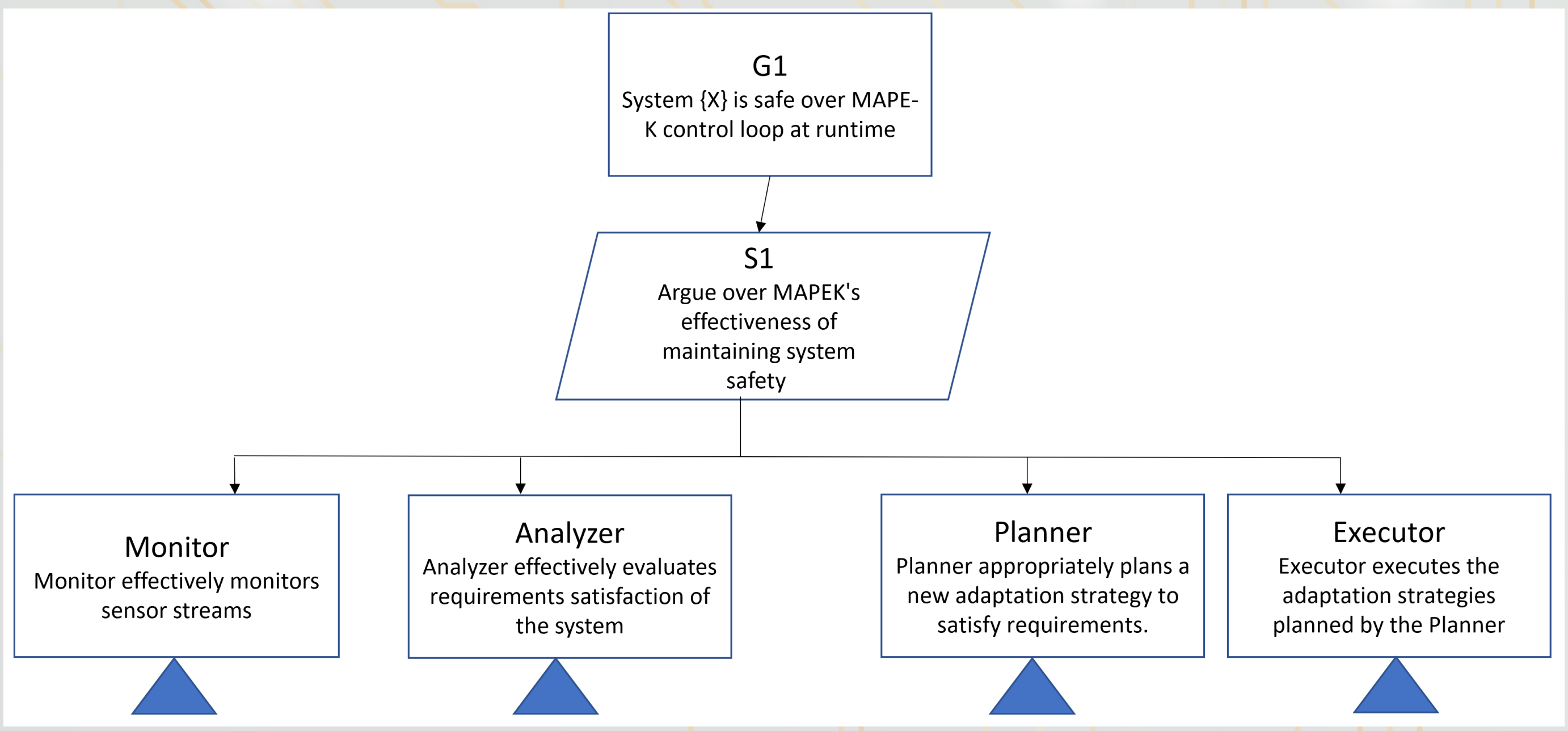
To study appropriateness of B and C in regard of A, we have

I. w_B is disjoint contributing weight of B to A.

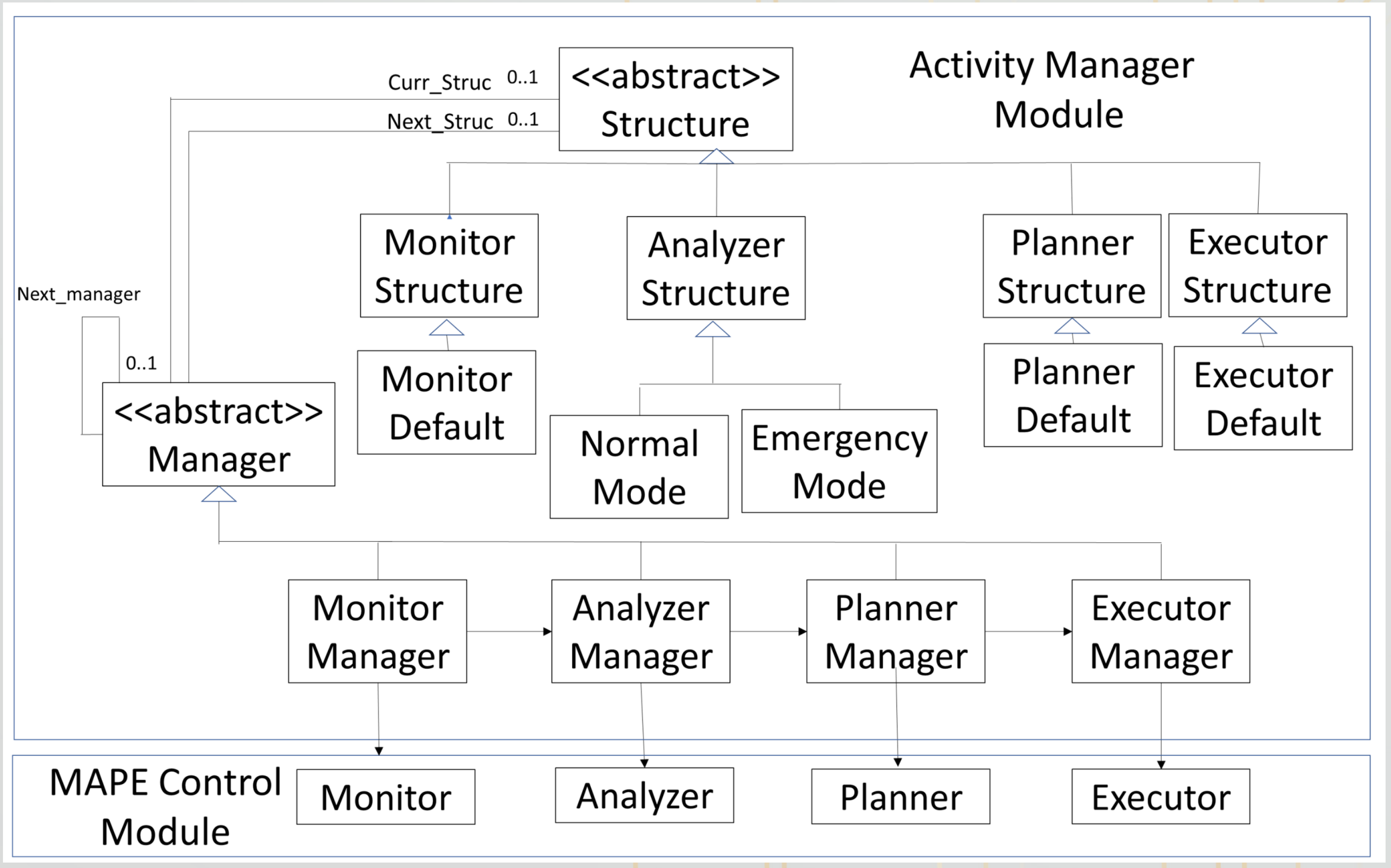
II. w_C is disjoint contributing weight of C to A

III. *v* is called discounting factor

- Assurance Case Driven Framework @Runtime
  - Assurance Case Template


G1
System {X} is safe over MAPE-K control loop at runtime
S1
Argue over MAPEK's effectiveness of maintaining system safety
Monitor
Monitor effectively monitors sensor streams
Analyzer
Analyzer effectively evaluates requirements satisfaction of the system
Planner
Planner appropriately plans a new adaptation strategy to satisfy requirements.
Executor
Executor executes the adaptation strategies planned by the Planner

  - Design of the Framework to Support runtime adaptive feature



HCSS

THE TWENTY-THIRD ANNUAL
HIGH CONFIDENCE
SOFTWARE AND SYSTEMS
CONFERENCE
MAY 8 -10, 2023 | http://cps-hcss.org