Использование марковского анализа для оценки отказобезопасности программно-аппаратных комплексов

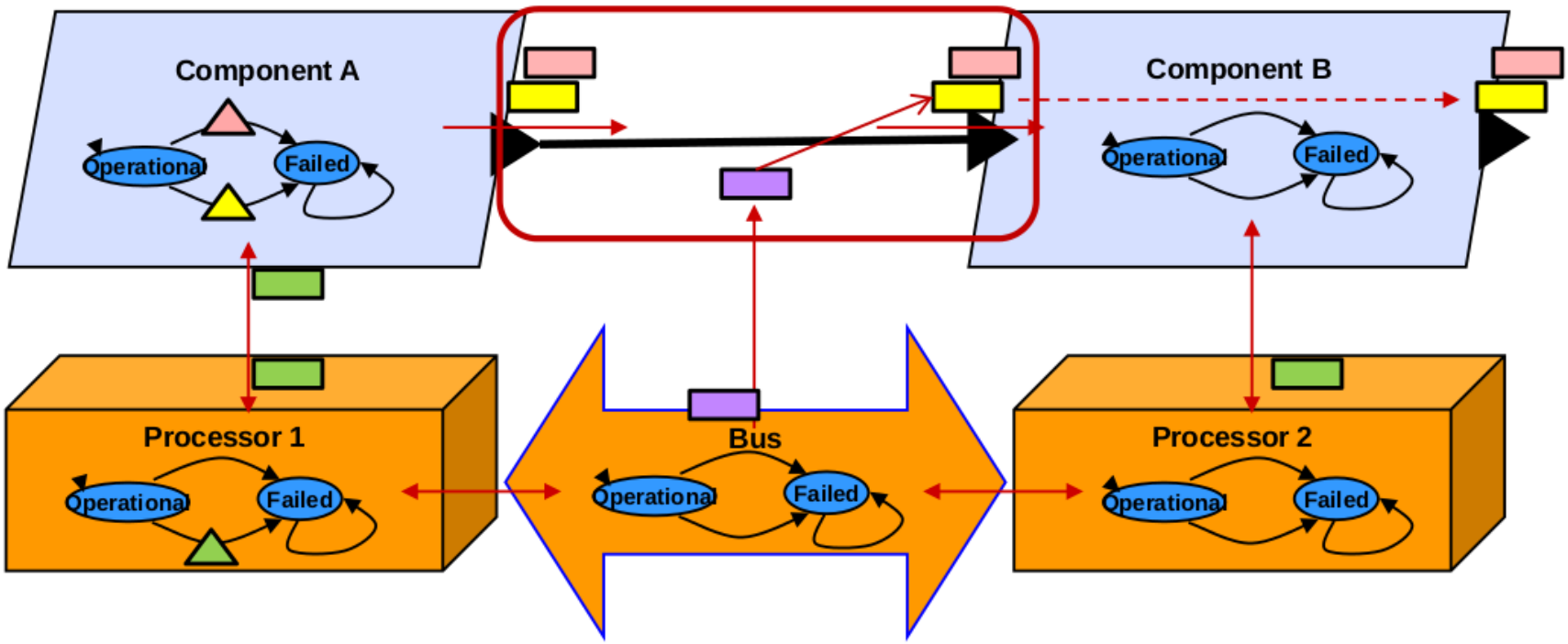
А. В. Хорошилов
С. В. Зеленов
А. А. Карнов

Кафедра системного программирования

18.04.2018

AADL и Error Model Annex

- Architecture Analysis & Design Language (AADL) – архитектура системы
- Error Model Annex – поведение системы



SAE ARP4761

Процессы SAE ARP4761:

- Оценка функциональной опасности (Functional Hazard Assessment)
- Предварительная оценка безопасности системы (Preliminary System Safety Assessment)
- Оценка безопасности системы (System Safety Assessment)

Методы оценки безопасности системы:

- Анализ дерева неисправности (Fault Tree Analysis)
- Анализ логической схемы (Dependency Diagram Analysis)
- Марковский анализ (Markov Analysis)

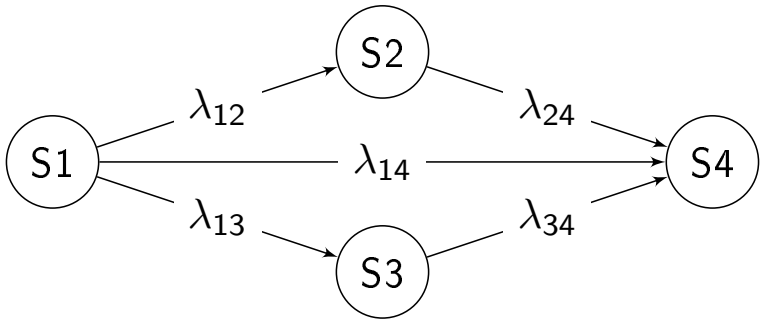
Задача

MASIW – инструментарий с открытым исходным кодом для работы с AADL-моделями, разрабатываемый ИСП РАН совместно с ФГУП ГосНИИАС для проектирования систем интегрированной модульной авионики.

Цель: разработка и внедрение инструмента марковского анализа моделей программно-аппаратных комплексов в рамках проекта MASIW.

Марковский анализ

- Марковская цепь



- Задача Коши

$$dP_i(t)dt = -\sum_{k=1}^{n} \lambda(S_i/S_k)P_i(t) + \sum_{k=1}^{n} \lambda(S_k/S_i)P_k(t)$$

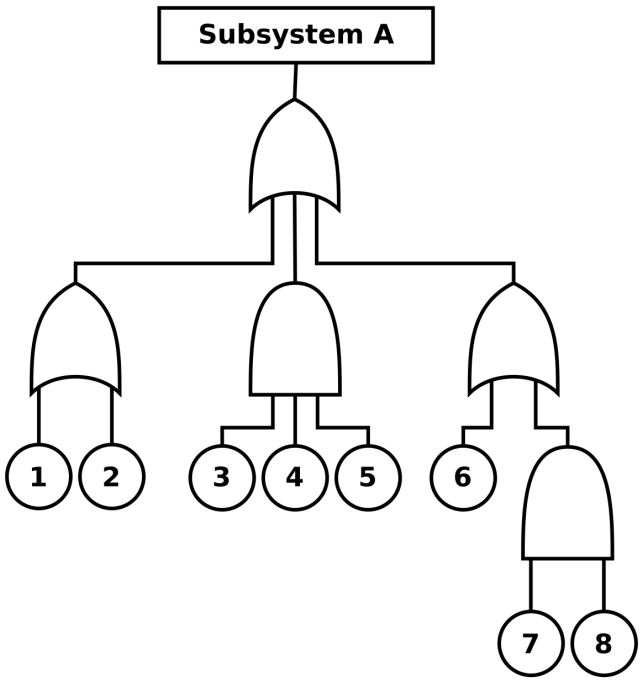
$$P_1(0) = 1, P_i(0) = 0, i = \overline{2, n}$$

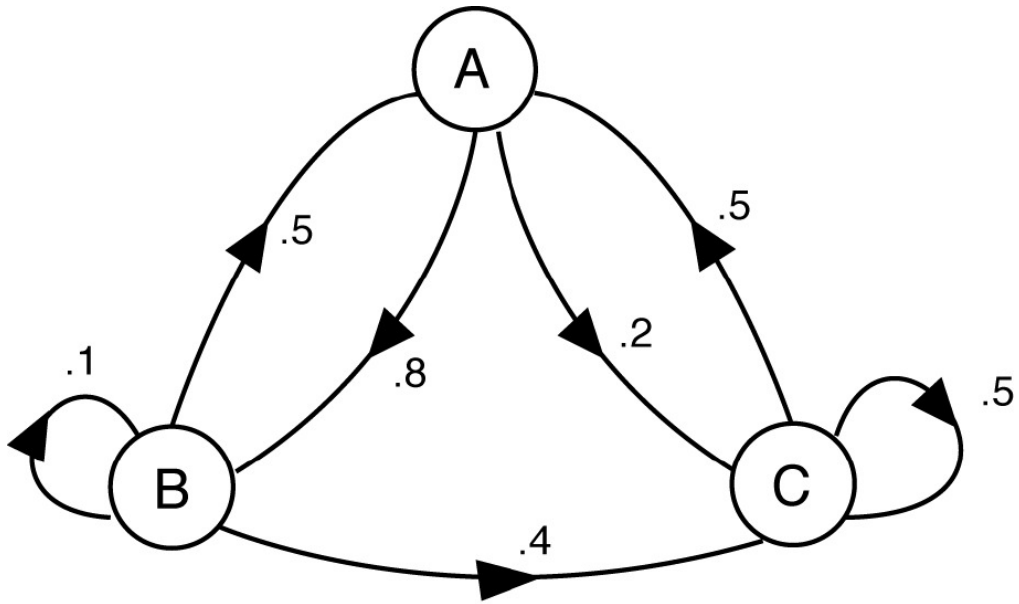
- Результат

$P_i(t)$ – вероятностная функция нахождения системы в состоянии S_i

Особенности марковского анализа

- Размер марковской цепи растет экспоненциально от размера системы
- Необходим алгоритм трансляции
- Марковский анализ работает с состояниями всей системы в целом
- Марковский анализ применим к системам с восстановлением





Другие работы

- Анализ системы с одним компонентом
- OSATE 2

Все известные инструменты имеют существенные ограничения на архитектуру анализируемой системы.

Алгоритм трансляции

Состояние марковской цепи – состояние системы, т.е. комбинация состояний всех её компонентов.
Переход в марковской цепи – переход между состояниями системы, инициируемый набором событий.

Существует слишком много комбинаций состояний компонентов.
Будем рассматривать только **достижимые** и **стабильные** состояния системы в марковской цепи.

Задача Коши

- Уравнение для любого состояния цепи легко построить, перебирая все входящие и исходящие переходы.
- Задача Коши решается численными методами из семейства Рунге-Кутты.

Ускорение работы инструмента

Эвристики:

- Ограничение рассматриваемых наборов событий по их вероятности
- Игнорирование переходов из «финальных» состояний системы в марковской цепи

Все эти модификации могут повлиять на результат анализа, но их применение ускоряет время работы на порядок. На данный момент, «финальные» состояния системы находятся автоматически.

Пример (система из 24 компонентов):

Полный анализ	Опция 1	Опция 2	Опции 1 и 2
60 min	7 min	10 sec	10 sec

Пример работы инструмента

Система	Кол-во компонентов	Размер цепи
Methodology_KBO	46	2526
ATA_XX1 (подсистема)	25	612
AltitudeSensor (компонент)	1	2

Система	Состояние	t = 0	t = 10	t = 24
Methodology_KBO	Operational	1.000000	0.999520	0.998849
	Failed	0.000000	0.000480	0.001151
ATA_XX1 (подсистема)	Operational	1.000000	0.999700	0.999280
	Failed	0.000000	0.000300	0.000720
AltitudeSensor (компонент)	Operational	1.000000	0.999990	0.999976
	Failed	0.000000	0.000010	0.000024

Заключение

- Предложен новый алгоритм трансляции AADL и Error Model Annex модели в маковскую цепь
- Разработан инструмент марковского анализа
- Добавлены улучшения для ускорения работы инструмента

Предложенный инструмент поможет оценить достоинства марковского анализа на практике.