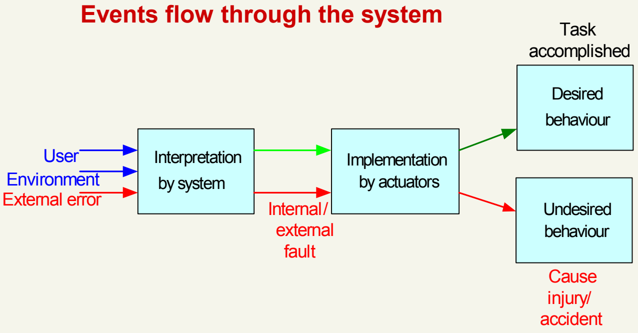
Institute of Automation

Formal Methods in Rehabilitation Robot Amarob

Events flow through the system



Safe operation of the system

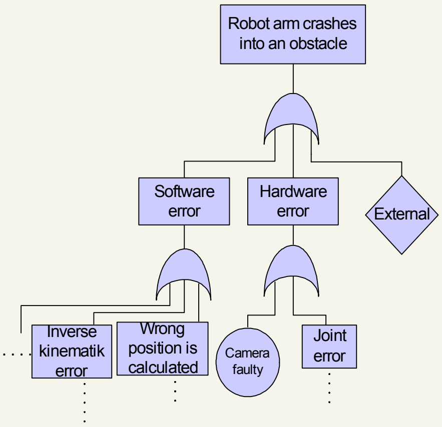
Follow the trajectory from user request for a task to desired behaviour and finally accomplishing the task

How to achieve safe operation of the system

-Find all possiple hazard/fault that may happen during system operation
-Write the requirment/specification of the system for a safe operation in formal language
-Find formal model of the system including fault model
-Force the system to meet specification

Why formal?

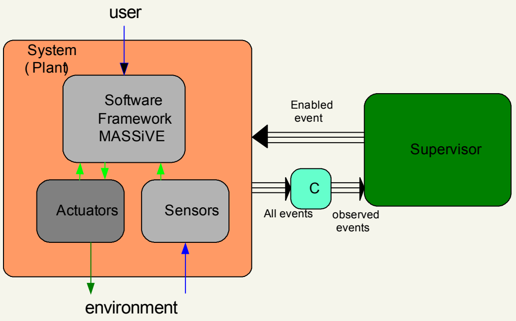
Natural language
-is ambiguous
-hard to process automatically



FTA for failure: Robot arm crashes in to an obstacle

Supervisor

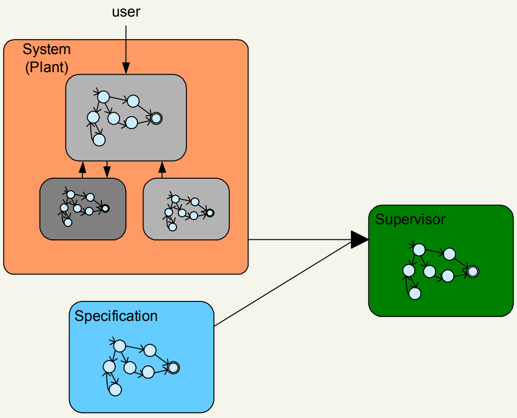
_ Undesired sequences of events may lead to a catastrophic system state
_ Force plant (system) to avoid undesired sequences of events.
_ The availability of the system must be guaranteed by supervisor. E.g. when robot is pouring a drink, standstill cannot be a safe state



system and safety module's architecture

Supervisor Realisation

-Build formal model (e.g. automaton) of all sub modules in the system
-Combine submodules together to make the system
-Build formal model (e.g. automaton) of specification
-Build the supervisor that forces the system to meet specification



Build the supervisor

Formal methods in discrete event systems application in service robotic

Aim

_ Safe operation of system
_ Availability, reliability and dependability will be guaranteed
_ No injury or harm for the user
_ Certification and Appoval by TÜV

Research

_ Methods of hazard analysis
_ (HAZOP, FTA,…)
_ Event discrete system
_ Formal methods
_ Petri net analysis
_ Automaton and language theory
_ Model-based system verification

Contact Person:
M.Sc. Leila Fotoohi
Otto-Hahn-Allee
Gebäude NW1
D-28359 Bremen
Tel: +49 421 218-3490/-7523
Fax: +49 421 218-4596
fotoohi@iat.uni-bremen.de
www.iat.uni-bremen.de

Universität Bremen