An Approach for Detecting Critical Adaptations in Automated Adaptive Software Systems

Shuji Morisaki[1], Norimitsu Kasai[2]

1: Department of Computing and Software Systems, Graduate School of Informatics, Nagoya University, Japan
2: Quality Assurance Department, Communication Systems Center, Mitsubishi Electric co., ltd, Japan

Background

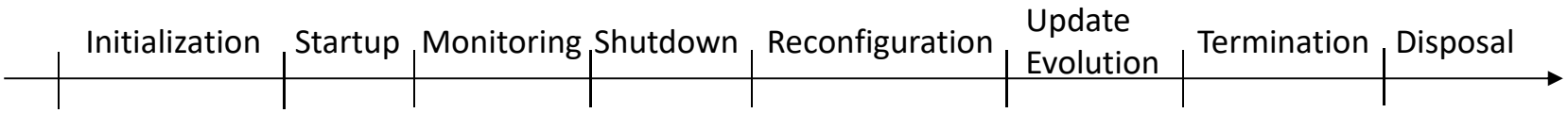
- As a number of devices and systems are connected, demand for automated self-adaptive system is increasing.
- Some self adaptations have potential to be safety- or mission-critical.
- Design time quality assurance activities for such system will focus on critical self adaptations.
  - Accountability is required for high criticality self adaptations.
  - Self adaptations that do not have impacts on the criticalities can be assured by run time quality assurance in near future.

Goal and approach

- Goal
  - to identify potential critical adaptations and to assess that their criticalities are acceptable for assets to be protected.
- Approach
  1. identifying candidates of critical adaptations throughout the software system's life cycle.
  2. decomposing the adaptations into adaptation stages.
  3. estimating the criticality of each stage of them in terms of automation and reliability levels.
  4. assessing that the criticalities are acceptable for assets to be protected.

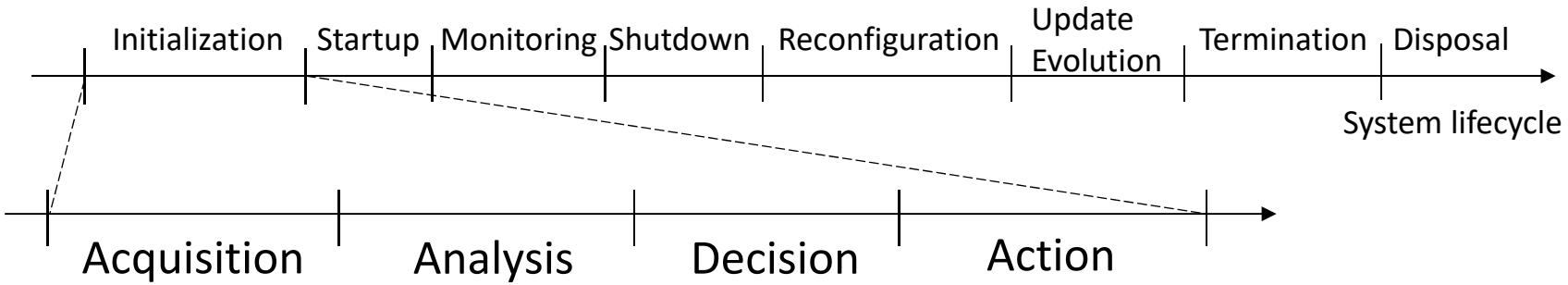
Step 1: Identifying critical adaptation events

- Critical adaptation events trigger critical automated self adaptation features of the adaptive software system.
- This step identifies potential critical adaptation events throughout the life cycle of the adaptive system.
  - Life cycle is a guide to ensure completeness.
  - The axis can be replaced with another that is easy to ensure completeness.



Step 2: Decomposing critical events into stages

- This step decomposes the extracted critical adaptation events into four stages.
  - Acquisition: The input data are acquired.
  - Analysis: The acquired data is interpreted.
  - Decision: A decision is made depending on the analysis stage.
  - Action: A suitable action is carried out to implement the decision.



The stages are defined in Parasuraman model.

R. Parasuraman, T. B. Sheridan, and C. D. Wickens, A Model for Types and Levels of Human Interaction with Automation, IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 30, no. 3, pp. 286–297 (2000)

Step 3: Criticality estimation

- Criticality is estimated by automation and reliability levels for each stage of the critical adaptation events.

Automation levels

Lv.	Definition
5	Fully automated. No external intervention.
4	System requires no assistance. External systems and humans may intervene.
3	System may request assistance, if necessary.
2	Humans or external systems conduct one or more predefined processes.
1	Fully manual

Reliability levels

Lv.	Accuracy	Uncertainty
4	high	low
3	high	high
2	low	low
1	low	high

Step 4: Assessment

- Identifying assets to be protected
  - Human life, property, or privacy
- Assessing potential threats to the assets according to the estimated criticalities.
  - If the estimated criticalities are not acceptable, implementation of automatic self adaptation will be re-considered.

Example analysis

- The same train runs through two or more transport operators such as international train.
- An on-board train speed limit system consists of
  - speed measurement device
  - secondary breaking system
  - radio signal receiver and transport operator table
    - receives station ID from station platform.
    - maximum permitted speed obtained by a table.

Station ID	Transport operator	Maximum permitted speed
100	X	120km/h
101	X	120km/h
…	…	…
132	Y	100km/h
…	…	…

Result of the analysis: identified events

- Identified critical adaptation events are
  - monitoring
    occurring regularly while the train is in service
  - reconfiguration
    occurring when transport operators changed
- Other adaptation events are
  - initialization
  - system startup
  - service startup

Result of the analysis: Decomposed stages

	Acquisition	Analysis	Decision	Action
Monitoring	The system obtains the train's current speed from the speed measurement device.	The system compares the current speed with the maximum speed permitted by the current operator.	If the maximum permitted speed has been exceeded, the system always takes action to reduce the train speed.	If the maximum permitted speed has been exceeded, the system uses the secondary braking system to reduce the train's speed.
Reconfiguration	The system receives a radio signal indicating the station ID on arrival at each of the major stations.	The system identifies the station ID from the received radio signal.	The system looks up the operator for the identified station ID and then finds that operator's maximum permitted speed in table.	If necessary, the system changes the maximum permitted speed according to the found maximum permitted speed.

Result of the analysis: Criticality assessment

- The results of the assessment indicated that the automation reliability level of the acquisition stage of the reconfiguration event are not acceptable for passengers.
  - Radio signal are sent in noisy environment.
- As an alternative solution for the analysis, the system asks the driver to ensure that the station ID from the radio signal is correct.

	Acquisition		Analysis		Decision		Action	
	AL	RL	AL	RL	AL	RL	AL	RL
Monitoring	5	4	5	4	5	4	5	4
Reconfiguration	5	2	4	4	4	4	4	4

AL: automation level; RL: automation reliability level

Conclusion

- An approach for identifying and assessing critical automatic adaptations was proposed.
  - The approach decomposes critical adaptation events into acquisition, analysis, decision, and action stages.
  - The critical adaptation events are assessed by automation levels and reliability levels.
- As a simple example, a train speed limit system was analyzed by the approach.