



---

# An Integrated Approach for Software Safety Analysis

---

FAYOKEMI OJO

TANGEE BEVERLY

# Introduction

---

Software safety analysis is not based on an integrated model to be both functional and safety. In result, it does not give an analysis of all possible failures. The objective of this research is to integrate safety analysis methods with functional requirements to reduce failures in performing the two independently. We are suppose to use the Fault Tree Analysis(FTA), which is used as a way to analyze causes of hazards, and create the UML statechart diagram. The UML statechart diagram is the standard for representing the functional specifications of a software system.

# Research Goals

---


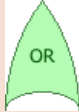
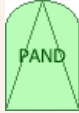


- Gather knowledge on State chart and Fault Tree.
- Find a case study
- Create a Fault Tree
- Create a State chart diagram

# Fault Tree Analysis (FTA)

---

- FTA is used for reliability and safety security.
- The purpose for FTA is to determine possible combinations of causes which can lead to certain undesirable event(s).
- Task of a FTA
  - The generation of a graphic/logical tree structure to understand the connections
  - Identify any possible failure causes and their combinations
  - Calculation of the probability of the undesirable event.

# Fault Tree Block Types

	AND	All input events TRUE
	OR	At least one input event TRUE
	PRIORITY AND	The output event occurs if all input events occur in a specific sequence
	NOT	The output event occurs if the input event does not occur.
	INHIBIT	The output event occurs if all input events occur and an additional conditional event occurs

# State chart Diagram

---

- Statechart diagrams are also known as a statechart and state machine.
- Illustration of the states in the Unified Modeling Language(UML).
- It show how objects interact to meet some system requirements
- A statechart composed of states, events and transitions.
- Statechart diagrams used for forward and reverse engineering of a system.
- Statechart diagram describes the flow of control from one state to another state.

# Statechart keywords

---

- Initial State
  - It represents the source of all objects.
- States
  - Is a condition of an object in which it performs some activity or waits for an event.
- Events
  - Trigger a state transition.
- Transitions
  - The movement from one state to another state.
- Final state
  - It is the end of an object's existence

# Purpose of a Statechart

---

- To model the dynamic nature of a system.
  - They define different states of an object during its lifetime and these states are changed by events
- To model the life time of a reactive system.
  - Reactive systems are defined as a system that responds to external or internal events.
- To describe different states of an object during its life time.
  - From creation to termination
- Define a state machine to model the states of an object.



# Design of a Statechart Diagram

---

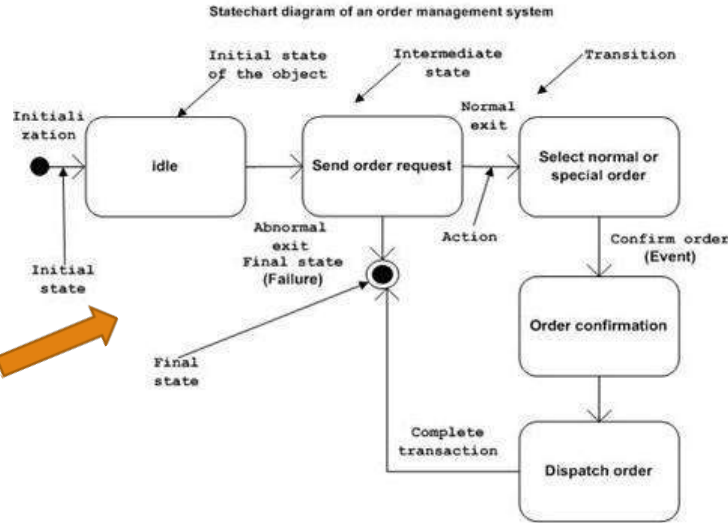
- Before drawing a Statechart diagram we need to do the following points
  - Identify the objects to be analyzed
  - Identify the states
  - Identify the events



# Continued

First state is an idle from where the process start.

Abnormal exit occur due to a problem in the system.



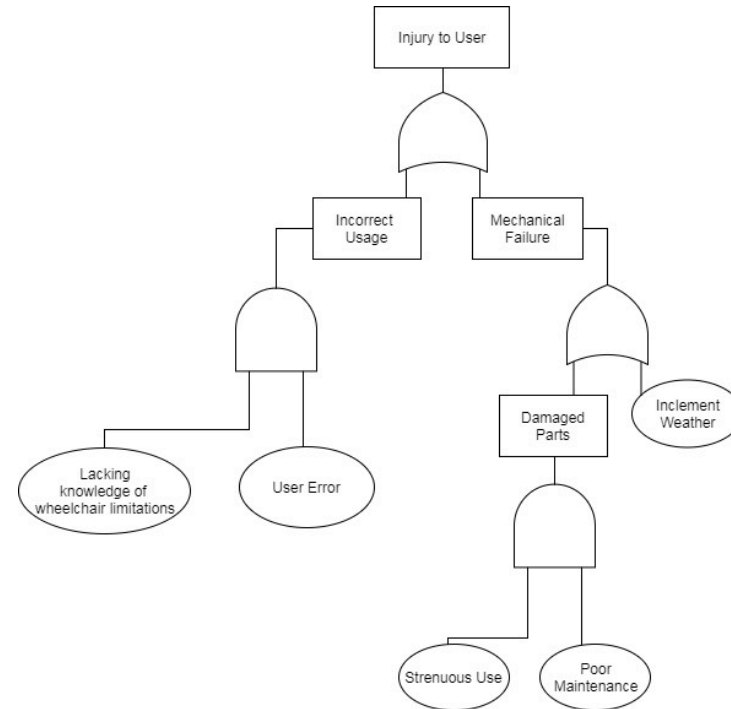
The next states are arrived for events like send request, confirm request, and dispatch order.

# Case Study: Stair Climbing Wheelchair

---

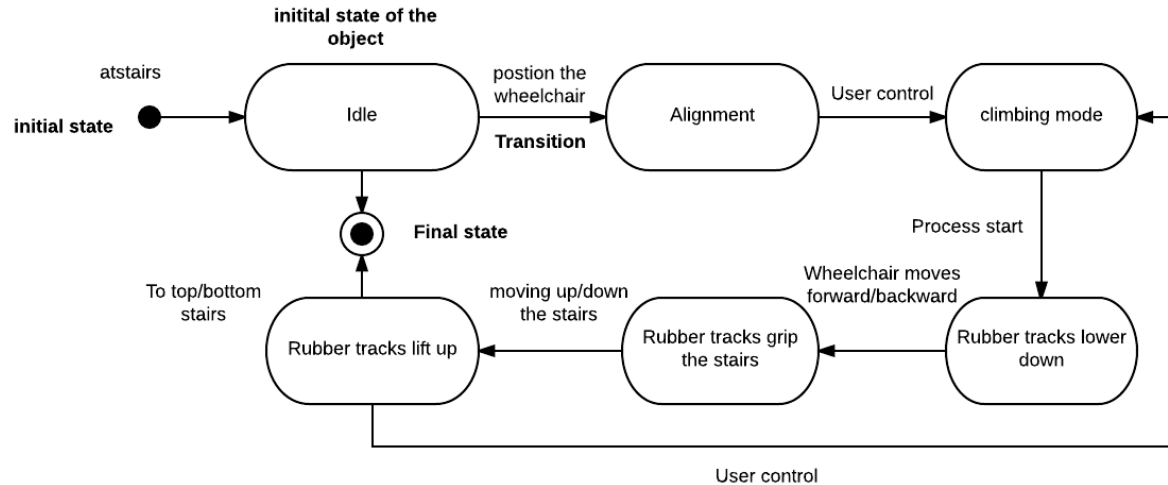


# Fault Tree Model



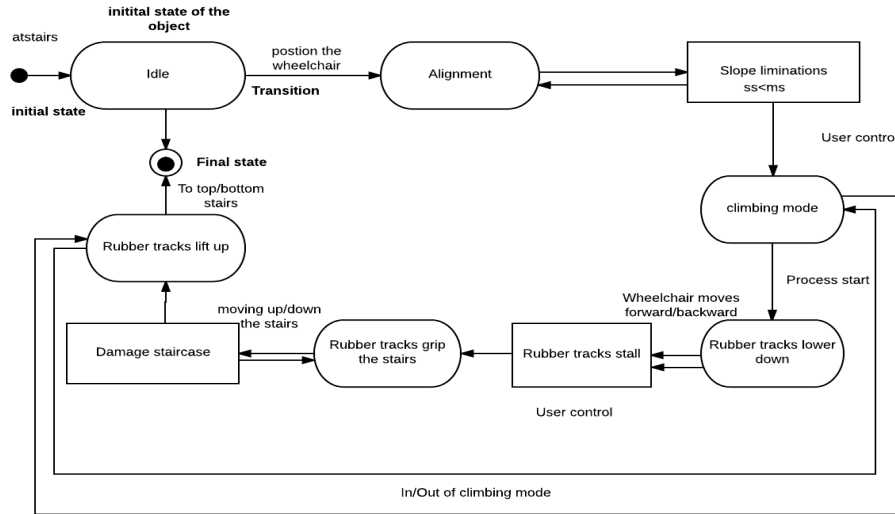
# UML State Machine

Stair climbing wheelchair state chart diagram (UML)



# Final Statechart

Stair climbing wheelchair state chart diagram (UML)



# Challenges

---

- Communication
- Time Constraints
- Gathering Information

# Future Research

---

- Find better ways to integrate functional requirements and safety faults
- Apply this method to larger, more complex systems



# Conclusion

---

We found ways to integrate some of the events in the fault tree diagram into the state machine.



# Acknowledgement

---

We would like to give thanks to Dr. Eric Wong for providing this opportunity to conduct research and NSF for funding the research project.

# References

---

*Ariss, Omar El, Dianxiang Xu, and W. Eric Wong. "Integrating Safety Analysis With Functional Modeling." IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans 41.4 (2011): 610-24. Web.*

*Ciobotaru, Matei. "The Fault Tree Tutorial." N.p., n.d. Web. 18 July 2017.*

*"Design Patterns and Refactoring." SourceMaking. N.p., n.d. Web. 19 July 2017.*

*Flaus, Jean-Marie. "Fault Tree Analysis." Risk Analysis (2013): 229-51. Web.*

*Guidelines: Statechart Diagram. N.p., n.d. Web. 19 July 2017.*

*M, Mohtashim. "UML - Statechart Diagrams." Www.tutorialspoint.com. N.p., n.d. Web. 18 July 2017.*

*Rouse, Margaret. "What is state diagram (state machine diagram or statechart diagram)? - Definition from WhatIs.com." SearchMicroservices. N.p., n.d. Web. 18 July 2017.*

*"State Machine Diagram Tutorial." Lucidchart. N.p., 05 June 2017. Web. 18 July 2017.*

Questions?

A solid orange horizontal bar at the bottom of the slide.