Automatic Failure Mode and Effect Analysis (FMEA) for Little-JIL Processes

Danhua Wang, Bin Chen, George S. Avrunin, and Lori A. Clarke
University of Massachusetts, Amherst

Presented by Bin Chen
Outline

- Introduction of FMEA
- Motivation
- Automatic FMEA for Little-JIL processes
- Future Work
Introduction to FMEA

- Systematic
- Safety analysis technique
- Identify
  - Where and how a component might fail – failure mode
  - How each failure mode might cause failures in other components
Motivation

- Intend to apply FMEA to analyze processes
- Traditionally, FMEA is performed manually
  - Time-Consuming
  - Error-Prone
- Hypothesis: FMEA can be automated if the process is precisely defined
  - We use the Little-JIL process definition language
Automatic FMEA for Little-JIL Process

- Identify the failure mode (s)
- Identify the effect (s) for each failure mode
- Identify the cause (s) for each critical failure mode
Running Example
Automatic FMEA for Little-JIL Process

- Identify the failure mode (s)
- Identify the effect (s) for each failure mode
- Identify the cause (s) for each critical failure mode
Identify the Failure Mode(s)

- Failure mode: artifact-related
  - A large number of interesting failure modes are artifact-related or can be easily turned into artifact-related failure modes
  - In many processes, hazards are caused by the delay of certain steps. To capture such failure modes, we can associate an artifact representing the execution time to each step. Then the delays can be handled just like the other artifact-related failure modes.
Identify the Failure Mode (s)

- Predefine two types of failure mode for Step s:
  - Type1: Artifact p from Step S is wrong
    (P is an Out parameter of Step S)
  - Type2: Artifact p to Step S is wrong
    (P is an In parameter of Step S)
Identify the Failure Mode(s)

- Failure modes:
  - Artifact “Patient Name” to “Obtain patient’s blood type” is wrong
  - Artifact “Blood Type” from “Obtain patient’s blood type” is wrong
  - ...

Automatic FMEA for Little-JIL Process

- Identify the failure mode (s)
- Identify the effect (s) for each failure mode
- Identify the cause (s) for each critical failure mode
Artifact Flow Graph (AFG)

- AFG is used to decide whether an artifact is data dependent on another
- Artifact Flow Graph (AFG): <Node, Edge>
  - Node: artifact
  - Edge: data dependence between two artifacts
    - E.g. There is a parameter binding from \( p_1 \) to \( p_2 \)
    - E.g. \( p_1 \) is an IN parameter of \( S \), \( p_2 \) is an OUT parameter of \( S \)
      \( \rightarrow \) \( p_2 \) is potentially data dependent on \( p_1 \)
Artifact Flow Graph (AFG)
- Annotation: PN-Patient Name, BT-Blood Type, BU-Blood Unit, PBL-Patient Bed Location. Root-Perform in-patient blood transfusion, S₁-Obtain patient’s blood type, S₁₁-Contact for patient’s blood type, S₁₂-Test patient’s blood type, S₂-Pick up blood from blood bank, S₃-Administer blood transfusion, S₃₁-Find patient location in computer, S₃₂-Blood Transfusion
Artifact Flow Graph (AFG)
Artifact Flow Graph (AFG)

- Annotation: PN-Patient Name, BT-Blood Type, BU-Blood Unit, PBL-Patient Bed Location. Root-Perform in-patient blood transfusion, S₁-Obtain patient’s blood type, S₁₁-Contact for patient’s blood type, S₁₂-Test patient’s blood type, S₂-Pick up blood from blood bank, S₃-Administer blood transfusion, S₃₁-Find patient location in computer, S₃₂-Blood Transfusion
Identify Effect (s) for Each Failure Mode

- Given a failure mode “Artifact p to Step S is wrong” or “Artifact p from Step S is wrong”, can determine all artifacts that p can flow to by traversing the AFG of the process.
- Faults of these artifacts are defined as effects of the failure mode.
Identify Effect(s) for Each Failure Mode
Identify Effect (s) for Each Failure Mode

Failure Mode:
Artifact “Blood Type” from “Obtain patient’s blood type” is wrong
Automatic FMEA for Little-JIL Process

- Identify the failure mode(s)
- Identify the effect(s) for each failure mode
- Identify the cause(s) for each critical failure mode
Identify Cause (s) for Critical Failure Mode

- Critical failure modes can be used as the TOP-events of fault trees
  - Fault tree provides a graphical depiction of all possible parallel and sequential combinations of events that could cause that top event to occur
- Used our fault tree derivation tool to generate the fault tree for each critical failure mode
Identify Cause(s) for Critical Failure Mode
Future Work

- Resource related failure modes
- Agent related failure modes
Thank you!