FBD_FTA:
An Automatic Assistant for Fault Tree Analysis of Function Block Diagrams

Youngju Seo*, Dong-Ah Lee, and Junbeom Yoo
Contents

- Introduction
- Background
- Fault Tree Templates
- FBD_FTA
- Case study
- Conclusion and Future work
- Reference
Introduction
Introduction

- Failures of safety-critical systems
  - Use hazard analysis techniques to assess the hazards.

- Hazard analysis to our target system.
  - It uses Programmable logical controllers (PLC).
  - PLC program uses function block diagram (FBD) for programming language.

- FBD_FTA for FTA about FBD program
  - FBD_FTA uses fault tree analysis (FTA) and temporal fault tree (TFT).
Background
Fault tree analysis (FTA)

- Provides a method for determining causes of the accident.
- Draw fault in a square, basic events in circles.
- Logical gates AND and OR, make relation between events.
- FT can be written as a boolean expression.

Fault : Brake Fails
Relation : OR, AND

Leaf events : Brake Pads Fails, Brake Sensor Fails, Brake Controller Fails, Brake Actuator Fails

Boolean expression

\[ \text{Brake Fails} \rightarrow (\text{Brake pads Fails} \lor (\text{Brake Sensor Fails} \land \text{Brake Controller Fails} \land \text{Brake Actuator Fails})) \]
Background – Temporal fault tree

- Temporal fault tree (TFT)
  - The traditional FT does not handle temporal properties.
  - Temporal fault tree (TFT) uses propositional linear temporal logic (past) (PLTLP) to add temporal properties.
  - The PLTLP uses logical operators and temporal operators.

Example state sequences of some temporal connectives

Temporal gates for fault tree
Background – Temporal fault tree

- PLTL can also be written as a boolean expression and temporal operators.
  - WITHIN \( n : \diamond_{n}^{-} \)
  - FORPAST : \( \square_{n}^{-} \)
  - PREV \( n : O_{n}^{-} \)
  - SOMETIME : \( \diamond^{-} \)
  - ALLPAST : \( \square^{-} \)
  - PREV : \( O^{-} \)

- TFT expression

1. \( \text{rain} \rightarrow (\diamond_{2}^{-} (\text{cold} \land \text{humid})) \)
2. \( \text{lift_arrives} \rightarrow (\diamond^{-} (\text{req_from_floor} \lor \text{req_from_passenger})) \)
Background – Function block diagram

- Function block diagram (FBD)
  - One of programming languages of PLCs.
  - PLCs are used to control of machinery on factory, and nuclear power plant.
  - FBD can describe the function between input variables and output variables.
  - IEC 61131-3 standard defines figures and functions of FBD
  - PLCopen defines the xml formats to save programs written in languages of IEC 61131-3

![Function block diagram](image-url)
**Background – NuDE**

- **Nuclear development environment (NuDE)**
  - Development environment for safety-critical software of nuclear power plant.
  - Includes tools NuSRS, NuFTA, NuSCRtoSMV, NuSCRtoFBD, FBD Tester, FBDtoVerilog, and FBD_FTA.
Fault tree templates
Fault Tree Templates

- Generating FT needs FT templates for each FB.
  - Each FB has their characteristics.

- Template selection is depending on FB’s output.
  - The output value to three types; “0,” “1,” and unspecified value.

- The case “0,” and “1,” expressed by the connection of FB and logical gates.
  - Unspecified value is cannot represented by AND and OR gates.

- Templates can be connected to another template.
  - Connecting to leaf node of other template.

- Generate intermediate nodes for visualization.
  - Visualization for translation of fault tree.
Fault Tree Templates – Bit-string and Bitwise boolean

- Bit-string and bitwise FBs
  - It used to manipulate one or more bit patterns or binary numerals for comparisons and calculations.
  - AND_BOOL behaves like a logical AND operation.

- Template for output value:
  - “0”, “1”: Represented by logical gate and input variables.
  - Unspecified value: Use INORDER gate to represent the template.

FT templates for AND_BOOL
Fault Tree Templates – Bit-string and Bitwise boolean

- **Case A**
  - Output value is 0.
  - Output is determined by one false value.

- **Case B**
  - Output value is 1.
  - Output needs that all input value become 1.

- **Case C**
  - Output value is unspecified.
  - It cannot be represented by logical gates.

FT templates for AND_BOOL (a), (b)

FT templates for AND_BOOL (c)
Fault Tree Templates – Type conversion

INT_TO_BOOL function block

- **Type conversion FBs**
  - It transforms input data to another data type.
  - INT_TO_BOOL change int type value to boolean type value.

- **Template for output value:**
  - Always same form.

- **Reflecting type conversion to formula is difficult.**
  - Integer “0” and boolean “0” are same form in formula.

FT templates for INT_TO_BOOL
Fault Tree Templates – Selection and Comparison

- Selection and comparison FBs
  - It selects one of each values between inputs.
  - SEL_BOOL outputs selectively IN0 or IN1 depending on G value.

- Template for output value:
  - Always same form.

- Regardless of the output value, selection is determined by G value.
Fault Tree Templates – Numerical

- Numerical FBs
  - It performs operations like arithmetic and trigonometric functions.
  - ADD_INT returns an output sum of the input values.

- Template for output value:
  - Always same form.

- Representing the result of ADD_INT using AND or OR gate is difficult.
  - If return value is “2,” it is hard to express using “0,” “1,” and logical AND, OR gates.
  - Use INORDER gate to describe the template.
Fault Tree Templates – Timer

- Timer FBs
  - It decides output value by check on the input value and determination of input value.
  - TOF receives the timer value of the whole system to ET. The value of IN is to be output to the Q value of time coming to the PT.

- Template for output value:
  - Always same form.

- For temporal properties, temporal gate is used in template.

- TFT expression
  \[(C==1) \Rightarrow \Box_E (A==1)\]
FBD_FTA – Implementation of FBD_FTA

• Input :
  • Standard FBD defined in IEC 61131-3
  • Input file is generated from NuSCRtoFBD.

• Development environment :
  • Eclipse plug-in for extension and NuDE.

• Automatic generation of FT from FBD.
  • Manual generation of FT takes lots of cost and time.

• Two view for FBD and FTA.
  • FBD View shows the whole FBD program.
  • FTA View shows generated FT from selected FB in FBD View.
FBD_FTA – Generation of fault tree

- **Generate fault tree**
  - Make root from output value.
  - If sub FB of current FB is not input value, FBD_FTA finds appropriate FT template and repeat this sequence recursively.
  - If sub FB of current FB is input value, FBD_FTA ends FT generation.

- **Make FT Template From FBD**
  - Make FT template from FB’s name.
  - Use each defined template of FB.

- **FBD_FTA does not care about the probabilities of nodes.**
  - Generally, FTA assign probabilities to each node.
  - Probability of logics in software is basically meaningless.
FBD_FTA – Finding cut-sets

- Cut-sets are another representation of FT using formula.
  - Intermediate nodes are meaningless in the formula.

- FBD_FTA find cut-sets using inorder traversal.

- Formula of AND_BOOL
  - If C == 1,

\[
( \text{A} == 1 \land \text{B} == 1 ) \rightarrow ( \text{C} == 1 )
\]

- Input value A and B affects to the output value C.
FBD_FTA – Fault tree data structure using xml

- No standards of general file formats to save the result of FT.
- Define xml schema for save the FT information.
  - Other tools can use this information.
  - Saving the FT helps to understand generation sequence of TF.
- Attributes
  - data: Actual information of each node in FT like formula or definition.
  - desc: Description of the information that using data only is difficult to express.
  - id: Integer value for identification and order of each node.
  - type: Gate or leaf node values for the classification of node types.
Case study
Case study

Our target:
- A part of reactor protection system (RPS) Bistable Processor (BP).
- This program is written by FBD.

Output
- cond_C

Input
- K_LO_SG1_LEVEL_Ptrp_Dly
- F_LO_SG1_LEVEL_Val_Out
- K_LO_SG1_LEVEL_Ptrp_Set

FB
- TOF
- GT_INT
Case study

- Fault:
  - cond_C == 1

- Leaf nodes:
  - k_LO_SG1_LEVEL_Ptrp_Dly == 1
  - IN2 ==
  - f_LO_SG1_LEVEL_Val_Out > k_LO_SG1_LEVEL_Ptrp_Set
  - f_LO_SG1_LEVEL_Val_Out <= k_LO_SG1_LEVEL_Ptrp_Set

- Cut-sets

  ( ( k_LO_SG1_LEVEL_Ptrp_Dly == 1 ) \* ( IN2 ==
    ( ( f_LO_SG1_LEVEL_Val_Out > k_LO_SG1_LEVEL_Ptrp_Set ) |
      ( f_LO_SG1_LEVEL_Val_Out <= k_LO_SG1_LEVEL_Ptrp_Set ) ) )
  )

  \rightarrow ( cond_C == 1 )

- Significant input value
  - k_LO_SG1_LEVEL_Ptrp_Dly
  - f_LO_SG1_LEVEL_Val_Out
  - k_LO_SG1_LEVEL_Ptrp_Set
Conclusion and Future work
Conclusion and Future work

- Conclusion
  - Generating FT from FBD needs FT templates for each FB.
  - FBD_FTA uses backward analysis to make FT and find cut-sets.
  - Automatic FT generation will help analysts perform hazard analyze of FBD program.

- Future work
  - Formalize the translated formula
  - Find minimal cut-sets
Reference
Reference