Advanced SIS Analysis using FTA – Virtual Class

Audience:	Experienced Process Safety Risk Analysts
Time:	9 hours: 8:00 am to 12:30 pm, 2 consecutive days
CEUs:	0.75

Overview

Advanced SIS Analysis using FTA is a 9-hour virtual course designed to familiarize experienced risk analysts with the quantitative techniques used to evaluate the risk reduction achieved by process hazard protection strategies that create additional challenges for safety system design. These include strategies in which a very large amount of risk reduction (RR>10,000) is being claimed for instrumented protections and strategies in which the instrumented safety systems will not be physically and functionally separate from both the cause of the hazard and the other layers of protection.

The quantitative analysis of a simple, physically independent, SIS design is usually performed with standardized commercially available SIS design tools. The typical risk assessment methodologies used in the process sector (e.g., LOPA or risk graph) depend on the chance of a failure causing the hazard and breaking a protection layer or the chance of a failure causing the loss of multiple protection layers being negligible. However, when the SIS design is not physically independent from the cause of the hazardous event or other instrumented protection layers, the hardware in common between the functions can cause a significant decrease in the overall safety performance achieved. Likewise, when the protection strategy depends on a large amount of risk reduction from instrumented protections in total (i.e., “stacking” IPLs), even relatively small common cause failures related to using the same instrument technology across the different functions can significantly constrain the overall result.

In such cases, an advanced fault tree calculation method is often needed. When the quantitative analysis involves more than one instrumented function from a hazardous event scenario, it is also important that the FTA model reflects the limitations for instrumented protection layers based on the recognized and generally accepted good engineering practices documented in industry standards (e.g., ISA 61511-1). Failure to do so can result in overly optimistic conclusions regarding the amount of functional safety provided by the protection strategy as a whole.

This class will cover modeling approaches for addressing common cause and dependent cause failures between instrumented functions, common design pitfalls to be aware of when modelling more complicated SIS architectures, and typical FTA simplifications to avoid when modeling instrumented protection layers.

Pre-requisites

The Advanced FTA class is intended for engineers who are already familiar with the basic practices of SIL verification calculations and the use of Reliability Workbench or analogous FTA tool. While the class will summarize some of the fundamental principles of both SIL verification and FTA modeling for convenience of discussion, this course will not develop these more foundational skills for someone without this background experience.

Objectives

The course participants will gain an understanding of the following:

- Common situations for using FTA in SIS design
- Use of simplifying assumptions in the SIS FTA model and which ones to avoid
- Modeling dependent failures between functions
- How to ensure the SIS FTA model conforms to prescriptive requirements from the SIS standard
- RWB calculation setup options
- Use of RWB reports/views to troubleshoot the FTA

Course Outline:

<u>Session 1</u>:

1. Common situations for using FTA in SIS Analysis
    a. Complex architectures
    b. Lack of independence
    c. RRF>10,000
    d. Why not FTA for everything?

2. What to include in FTA and what NOT to include
    a. What is really in the function?
    b. Target: Frequency or PFDavg
    c. Device selection and HFT come BEFORE doing the FTA
    d. Why not include systematic failure or PM?
    e. Caveats on data selection

3. Math vs. Proscriptive/Prescriptive Requirements
    a. Limits on BPCS Demand Frequency
    b. Limits on BPCS Protection Layers
    c. Boundaries of SIL Ranges
    d. Other prescriptive requirements

4. Deciding what simplifying assumptions to use
    a. $1 – β ≈ 1$
    b. Where to apply frequency/RRF “caps”
    c. Using FTA Boolean vs. Markovian models
    d. Excluding low frequency causes from dependency/HFT analysis
    e. Significantly non-conservative simplifications to avoid

<u>Session Two</u>:

5. RWB setup nuances
    a. Overall tool setup
    b. Conceptualizing the gate/event skeleton
    c. Setting up generic failure models (and beta models if used)
    d. Setting up events

6. Examples of advanced SIS FTA analyses
    a. Sharing hardware between two protection layers
    b. Sharing hardware between a Protection Layer and the Demand Cause
    c. Sharing hardware between two protection layers AND the demand cause

7. Reports and views
    a. RWB view options for troubleshooting
    b. Reporting for advanced FTA