Bayesian Decision and Risk Analysis
Semester 6, 2019

Coursework 2 – System Safety Analysis

Deadline: Friday 29th March 2019

Coursework Instructions

Your answer should be prepared using a word processor (preferably MSWord) and submitted electronically. Any BN modelling should be done using AgenaRisk and diagrams and results pasted as pictures directly into your word-processed document.

This coursework counts for 15% of the final mark. The total marks that can be achieved in this coursework is 70.

The Problem

You are the safety manager on a railway project with the responsibility to determine assess the safety of a Train Protection and Warning System (TPWS). Your primary concern is determining the chance of a Signal being Passed At Danger (SPAD) and the chance of an accident should this occur. A SPAD occurs when a train passes a stop signal without authority to do so.

General information on the system can be found here:

http://en.wikipedia.org/wiki/Train_Protection_%26_Warning_System

Part I – Fault Tree [50]

Use AgenaRisk to develop a Bayesian Network model of a fault tree with a SPAD as the "top event".

The following components form the TPWS under study; other factors such as human reliability or operation under degraded conditions are excluded from the analysis:

- Components in trackside equipment sub-system:
  - Power
  - Overspeed sensor electronic loop on track
  - Train stop electronic loop on track

    - Computer controlling trackside equipment

- Components in train borne equipment sub-system:
    - Brakes on train
    - TPWS receiver to detect signals from electronic loops
    - Power
    - Computer controlling train equipment

The following assumptions are relevant:

- Each component has only one mode of failure and that it operates successfully or fails to operate.
- All power supplies are composed of four partially redundant power units and sufficient power will be available operate the system if at least two units are operating.
- The probabilities of failure for each primary event (component) are:

    - Train computer: 0.001
    - Train receiver: 0.002
    - Brakes on train: 0.005
    - Train power unit: 0.02
    - Trackside power unit: 0.01
    - Trackside computer: 0.002
    - Train stop sensor: 0.03
    - Overspeed sensor: 0.05

As part of your fault tree analysis report you need to:

1. Show a graph of the fault tree with the fault tree logic clearly shown alongside meaningful node names [20]
2. Show the marginal probability risk graphs for each node in the fault tree [10]
3. Document all NPTs or expressions used [10]
4. Calculate the probability of the top event [5]
5. Identify which is the least safe: the trackside or train subsystems? [5]

Tip: Be careful to set the model graph properties to display small probability values on the risk graphs.

Part II – Event Tree [20]

Use AgenaRisk to develop a Bayesian Network model of an event tree assuming a SPAD has occurred and using this information:

The following accident scenario is envisaged:

- Assume the SPAD event has occurred
- Assume the train committing the SPAD is a passenger train.
- Peak times occurs for 6 hours in each 24-hour operational period (assume 24 hours operation). Passenger trains travel at peak and off-peak times whilst freight trains only use the track during off peak hours.
- A train committing a SPAD will collide with another train sharing the same track junction. When a collision occurs, there is a:
    - 90% chance that that both trains involved in the accident will both be passenger trains and a
    - 10% chance of one being a freight train and the other a passenger train.
    - If a passenger train is involved in the collision, we expect that in peak time such a train will carry 200 passengers, otherwise during off peak time it will be carrying 50 passengers.
    - A freight train will always have two crew members.
    - The chance of each passenger or train crew being killed in any train collision is 20%.

As part of your event tree analysis report you need to:

1. Show a graph of the event tree as a Bayesian Network [6]
2. Show the marginal probability risk graphs for each node in the event tree [4]
3. Document any NPTs or expressions used [5]
4. Calculate the expected casualty rate [5]

Tip: Consider using partitioned expressions, simulation, continuous type and arithmetical functions to declare casualty numbers.

Tip: For an easier to read graph of the casualty node change the graph to histogram from area.