July 2023

TECHNIQUES TO INCORPORATE NETWORK FAILURE EVENTS IN IMPACT ANALYSIS AND CRITICALITY ASSESSMENT MODELLING

Priyanka Bansal

Madhuri C

Sakshi Puri

Neha Nigam

TECHNIQUES TO INCORPORATE NETWORK FAILURE EVENTS IN IMPACT ANALYSIS AND CRITICALITY ASSESSMENT MODELLING

AUTHORS:
Priyanka Bansal
Madhuri C
Sakshi Puri
Neha Nigam

ABSTRACT

Criticality assessment is a process that typically involves assigning assets with a criticality rating based on the effects of asset failure on a system and/or operation of the system as a whole. Presented herein are techniques that provide for the ability to incorporate network failure events in impact analysis and criticality assessment processes utilizing a five-dimensional formula, referred to herein as an Aggregated Risk Priority Number (ARPN), which can be derived using various parameters representing the severity of a network failure, the probability of occurrence of the network failure, the probability of detection of the network failure, the time of occurrence of the network failure, and a deployment knowledge factor (DKF).

DETAILED DESCRIPTION

Criticality assessments are often provided for assets within a system in order to determine how the system may be affected by the failure of different assets and/or how operation of the system may be affected, as a whole, by the failure of different assets. There may be many reasons for performing criticality assessments for a system such as for determining the availability and/or impact of asset failure(s) on an enterprise entity (e.g., loss of revenue due to downtime, etc.), determining the safety and/or environmental impact of asset failure(s), determining whether a single point of failure(s) can be isolated, prioritizing assets for maintenance and/or upgrades, prioritizing leads based on maintenance history (e.g., for estimating a mean time between failures of a same asset, for sourcing spare parts, for determining service contracts, etc.), and/or the like.

There are many models that can be utilized for assigning a criticality rating for an asset, such as failure modes and effects analysis (FMEA); failure modes, effects, and criticality analysis (FMECA); hazard and operability study (HAZOP); and others. Such models have been applied to assembly/production lines across different industries and often consider design, process, and functional failures for failure analysis and assigning criticality ratings to assets. Figure 1, below, provides a general overview of criticality assessment processes.

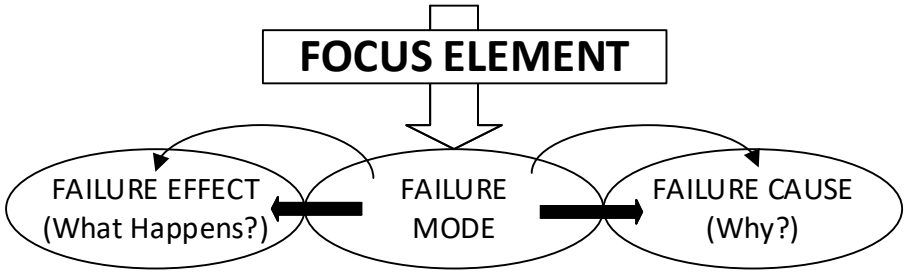

Figure 1: Overview of Criticality Assessment Processes

With the recent upsurge of industrial automation and connected factories, networking systems can play a critical role and may be a prominent part of such industrial/connected ecosystems. Currently, however, network failures/events are not factored into or otherwise considered within criticality assessment models. Yet, it would be advantageous to account for network failures/events in assigning criticality scores for assets within a system.

This proposal provides techniques through which network failure events can be incorporated into impact analysis and criticality assessment models. In particular, an Aggregated Risk Priority Number (ARPN) can be generated for assets that considers network failures and their impact analysis for criticality assessment modeling. For example, FMEA has different failure modes that are considered for effect analysis and criticality assessment for models that consider design, process, and functional failures.

In accordance with this proposal, a Networking Failure Mode can be added as an extension to a criticality assessment model (e.g., FMEA) such that impact analysis for assets can be augmented to consider various network failures that may impact a system. Assessments of network failures can consider various parameters, as follows:

- Severity: Category of a failure, depending on what is broken. For Example : Network or Application failure which is of a higher Severity (S1) vs Informational level Log Collection broken which could be of a lower severity (S10));
- Occurrence: Probability of an event occurring;
- Detection: Probability that a failure will be detected;
- Time of Occurrence: time and day of the event (e.g., business hours vs. non-business hours, Mon-Fri vs Sat-Sun, etc.); and
- Deployment Knowledge Factor (DKF): an administrator provided prioritization value or weighting that can be based on operator/administrator knowledge/experience, asset category (e.g., PLC vs logging host), etc.

Each of the parameters may be normalized to represent a numerical value such that an ARPN can be calculated as:

ARPN = Severity * Occurrence * Detection * Time of Occurrence * DKF

The ARPN may provide a realistic and quantifiable value for characterizing network failure events that considers knowledge factors as well as information relating to the actual occurrences of failures and can be readily incorporated as another mode for any existing criticality assessment modeling process. In some instances, the ARPN and/or parameters of the ARPN could also be used to train a machine learning model that could be utilized to automate/adopt network failure assessments as a factor for impact analysis and criticality assessment modeling processes.

Accordingly, this proposal provides for the ability to incorporate network failure mode information within impact analysis and criticality assessment processes utilizing the ARPN through which five network failure related parameters (severity of a network failure, the probability of occurrence of the network failure, the probability of detection of the network failure, the time of occurrence of the network failure, and the DKF) can be utilized to quantify/characterize network failure events such that the ARPN can be incorporated into any impact analysis and criticality assessment modeling process.