Option #2: Factory Machines Faults Detection

Scott Miner

Colorado State University – Global Campus

**Option #2: Factory Machines Faults Detection**

The student proposes a two-page outline for his portfolio project, utilizing all headings

from the Functional Requirements Document (FRD), incorporating five scholarly resources.

# General

## Project Description

The project description provides a general project overview.

### Background

The background provides historical context as well as who authored the FRD and why.

### Purpose

The purpose of the FRD is to present the stakeholder needs accurately and consistently.

### Assumptions and Constraints

Assumptions indicate future situations affecting system success; constraints are conditions affecting system development.

### Interfaces to External Systems

This section describes the details of all applications interfacing with the system.

## Points of Contact

This section presents the names, titles, and occupations of key stakeholders in the project.

## Document References

Supporting references and key documents identified by author, title, version, and date.

# FUNCTIONAL REQUIREMENTS

## Data Requirements

A logical data model using ERDs to illustrate the business data needs of the system.

## Functional Process Requirements

Information on what the system must do, including context and additional detail.

# OPERATIONAL REQUIREMENTS

## Security

Security refers to who can control, view, and alter system data. Gifty et al. (2019) describe how security measures, including network design defenses, encryption, and physical access controls, are used to eliminate vulnerabilities in network communications. Warren (1998) classifies data into three classes: (a) public, (b) confidential, and (c) most sensitive. We use the principle of “least privilege” to limit data access.

## Audit Trail

The Audit Trail describes activities recorded in the audit trail of the system.

## Data Currency

Data currency measures data recency. The requirements call for real-time processing.

## Reliability

An online survey of IT executives found 75% of respondents suffered from “unrecoverable loss of corporate data they thought was backed up” (Marshall & Heffes, 2005, p. 34). Reliability refers to the system’s ability to work uninterrupted.

## Recoverability

Ryan & Ryan (2005) describe reasons for system failures including, wearing out, suffering from design defects, network attacks, and environmental stresses. Recoverability represents the capability of the system to restore functions in the incident of crashes.

## System Availability

The availability of the system refers to the time and schedule the system is available for use.

## Fault Tolerance

Fault Tolerance refers to the system’s ability to continue operating during malfunctions.

## Performance

Performance requirements may be indicated in response time units or data volumes.

## Capacity

System capacity states the number of applications the system will process.

## Data Retention

Data Retention describes the amount of time the system retains data.

# REQUIREMENTS TRACEABILITY MATRIX

Goknil et al. (2011) define requirement traceability as “the ability to relate requirements back to stakeholders” (p.23). The Requirements Traceability Matrix (RTM) tracks functional requirements throughout the development process.

# Glossary

Glossary of business terms, acronyms, and abbreviations related to the system.

References

Gifty, R., Bharathi, R., & Krishnakumar, P. (2019). Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection. Neural Computing & Applications, 31(1), 23–34. https://doi.org/10.1007/s00521-018-3635-6

Goknil, A., Kurtev, I., Berg, K., & Veldhuis, J.-W. (2011). Semantics of trace relations in requirements models for consistency checking and inferencing. Software & Systems Modeling, 10(1), 31–54. https://doi.org/10.1007/s10270-009-0142-3

Marshall, J., & Heffes, E. M. (2005). Tape-Based Backup of Data Seen Unreliable. Financial Executive, 21(9), 12–12.

Ryan, J. J. C. H., & Ryan, D. J. (2005). Proportional Hazards in Information Security. Risk Analysis: An International Journal, 25(1), 141–149. https://doi.org/10.1111/j.0272-4332.2005.00573.x

Warigon, S. (1998). Data warehouse control & security. Internal Auditor, 55(1), 54.