İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

DEMİRYOLU SİNYALİZASYONUNDA GÜVENİLİRLİLİK EMRE AMADELİK SÜRDÜRÜLEBİLİRLİK VE EMNİYET (RAMS) YÖNETİMİ VE FMEA - FTA ANALİZİ UYGULAMASI

YÜKSEK LİSANS TEZİ

İsmail Yakın

Kontrol ve Otomasyon Mühendisliği Anabilim Dalı

Kontrol ve Otomasyon Mühendisliği Lisansüstü Programı

Tez Danışmanı: Prof. Dr. Mehmet Turan Söylemez

ARALIK 2014

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

DEMİRYOLU SİNYALİZASYONUNDA GÜVENİLİRLİLİK EMRE AMADELİK SÜRDÜRÜLEBİLİRLİK VE EMNİYET (RAMS) YÖNETİMİ VE FMEA - FTA ANALİZİ UYGULAMASI

YÜKSEK LİSANS TEZİ

İsmail Yakın

504091110

Kontrol ve Otomasyon Mühendisliği Anabilim Dalı

Kontrol ve Otomasyon Mühendisliği Lisansüstü Programı

Tez Danışmanı: Prof. Dr. Mehmet Turan Söylemez

15 Aralık 2014

İTÜ, Fen Bilimleri Enstitüsü'nün **504091110** numaralı Yüksek Lisans öğrencisi, "**İsmail YAKIN**", ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "**DEMİRYOLU SİNYALİZASYONUNDA GÜVENİLİRLİLİK EMRE AMADELİK SÜRDÜRÜLEBİLİRLİK VE EMNİYET (RAMS) YÖNETİMİ VE FMEA - FTA ANALİZİ UYGULAMASI**" başlıklı tezini, aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Prof. Dr. Mehmet Turan SÖYLEMEZ** İstanbul Teknik Üniversitesi	**……**
Jüri Üyeleri :	**Yrd. Doç. Dr. Özgür Turay KAYMAKÇI** Yıldız Teknik Üniversitesi	**……**
	Prof. Dr. Salman KURTULAN İstanbul Teknik Üniversitesi	**……**

Teslim Tarihi : 15 Aralık 2014

Savunma Tarihi : 4 Şubat 2015

ÖNSÖZ

Yüksek lisans eğitimimi tamamlamak üzere olduğum bugünlerde, Türkiye'nin güzide kurumlarından biri olan İstanbul Teknik Üniversitesi bünyesinde bulunmaktan dolayı çok mutluyum. Bu nedenle kuruluşundan günümüze kadar bu kurumun ayakta durmasında emeği geçen herkese teşekkür ederim.

Tez çalışmalarım esnasında, tez çalışmalarına başladığım andan itibaren, güler yüzü, anlayışı, destekleyici tavrıyla beni her zaman motive eden, iş yaşamımla beraber yürüttüğüm çalışmada zorlandığım anlarda bana anlayış gösteren, tez çalışmalarımız haricinde de değerli sohbetini benden esirgemeyen, değerli tez danışmanım, hocam Prof. Dr. Mehmet Turan Söylemez'e şükranlarımı sunarım. Ayrıca, çalışmalarım sırasında yardımlarını esirgemeyen değerli İstanbul Ulaşım AŞ yöneticilerine ve ekip arkadaşlarıma, Dr. Özgür Turay Kaymakçı'ya, Dr. Mustafa Seçkin Durmuş'a teşekkürlerimi sunarım.

Bugünlere gelmemde sayısız emekleri geçen, her anımda yanımda olan, her kararıma saygı duyan ve beni devamlı destekleyen aileme sonsuz şükranlarımı sunarım.

Aralık 2014

İsmail Yakın

Kontrol Mühendisi

İÇİNDEKİLER

Sayfa

KISALTMALAR

BS : İngiltere
CA : Kritik Analiz
CENELEC : Avrupa Elektrik Standartları Komitesi
EN : Avrupa Standardı
ETA : Olay Ağacı Analizi
FA : Fonksiyonel Analiz
FAST : Fonksiyonel Analiz Sistem Tekniği
FCA : Hata Sonucu Analizi
FDF : Bulanık Karar Fonksiyonu
FLA : Bulanık Mantık Analizi
FMEA : Hata Türü Etki Analizi
FMECA : Hata Türü Etki Kritik Analizi
FSP : Hata Şiddet Parametresi
FTA : Hata Ağacı Analizi
IEC : Uluslararası Elektro-teknik Komisyonu
PHA : Ön Tehlike Analizi
PRA : Olasılıksal Risk Analizi
RAMS : Güvenilirlilik Emre Amadelik Sürdürülebilirlik ve Emniyet
RBD : Güvenilirlilik Blok Diyagramı
RCM : Güvenilirlilik Merkezli Bakım
SADT : Yapısal Analiz ve Tasarım Tekniği
SCADE : Sistem Mühendisliği Yazılımı

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

DEMİRYOLU SİNYALİZASYONUNDA GÜVENİLİRLİLİK EMRE AMADELİK SÜRDÜRÜLEBİLİRLİK VE EMNİYET (RAMS) YÖNETİMİ VE FMEA - FTA ANALİZİ UYGULAMASI

ÖZET

Raylı sistem taşımacılığı özellikle gelişmiş ve gelişmekte olan ülkelerde çok önemli bir ulaştırma alternatifi oluşturmaktadır. Avrupa ve Asya'da bulunan birçok ülke yüksek hızlı demiryolu yapımına son yıllarda özel önem göstermektedirler. Bu özel önemin ana sebebi hızlı demiryolu sistemleri inşa edilerek yolcu ve yük taşımacılığının daha kısa sürede, daha güvenli şekilde ve daha ucuz şekilde yapılmak istenmesinden kaynaklanmaktadır.

Demiryolu teknolojisinin gelişmesiyle birlikte emniyet ve konfor kavramları daha da önem kazanmaya başlamıştır. Bu durum demiryolu sistem mühendisleri tarafından RAMS kavramının üzerinde durulmasına sebep olmuştur. Demiryolu sistemlerinde emniyet ve risk analizi konularında bugüne kadar birçok çalışma bulunmaktadır. Ancak ülkemizde ve bölgemizde hızla artan demiryolu altyapılarının teknik altyapıları ülkemizde herhangi bir sistem mühendisliği mevzuatı olmadığı için yeterince gelişememiştir.

Bu çalışma, İstanbul Ulaşım AŞ Bünyesindeki bir demiryolu işletmesinin yerel olarak sinyalizasyonunun yapılması sırasında karşılaşılan risklerden örnekler alınarak hazırlanmış ve ileriki çalışmalar için bir rapor haline getirilmiştir. Bu çalışmada öncelikle RAMS ve sistem mühendisliği kavramları üzerinde durulmuş, bu kavramlar hakkında özet bir literatür bilgisi verildikten sonra risk analizleri ve önemli risklerin nicel olarak hesaplanabilmesi için kullanılan yöntemler ele alınmıştır. Bu yöntemler arasında FMEA ve FTA analiz yöntemleri tercih edilmiş ve birbirlerini bütünleyici analizler olarak kullanımları detaylı olarak incelenmiştir. Sonuç olarak, yukarıda bahsi geçen demiryolu işletmesinde örnek bir çalışma sunulmuştur.

Bu çalışma bir raylı sistem projesinin planlanmasından başlayarak, tasarlanması, devreye alınması, işletilmesi, bakım yapılması ve nihayet sistemin sonlandırılmasına kadar bir başucu kaynağı olması gereken risk analizi yöntemlerini içermektedir. Daha sonra yapılacak olan çalışmalar, uluslararası sertifikasyon kuruluşları tarafından bir sistemin ne şekilde bu aşamalardan geçtiği ve uluslararası komisyonlarca yetkin bir sistemin nasıl elde edilmesi gerektiği sorusuna cevap bulmaya çalışmak olacaktır.

RELIABILITY AVAILABILITY MAINTAINABILITY SAFETY (RAMS) MANAGEMENT OF RAILWAY SIGNALLING SYSTEMS & FMEA-FTA ANALYSIS APPLICATION

SUMMARY

Today, high speed railway transportation systems are essential for countries because existing road and air transportation systems have become unable to carry the burden of excessive traffic. Special attention has been given to change this situation in many countries of Europe and Asia with high speed railway systems. Behind the main reason for constructing high speed railway systems in the world is to use potentiality of ability of carrying more passengers and loads in a short time safely and cheaply.

With the development of railway technology, safety and comfort concept has gained more importance. This is caused by the railway system engineers to focus on the concept, RAMS. In railway systems, there are many studies so far in safety and risk analysis. However, in our country and in our rapidly growing rail infrastructure technical infrastructure that our country has not developed sufficiently to be of any system engineering legislation.

Railway organizations have been a more wide-spread research area than any other transportation methods, in the manner of its characteristics and competition advantages. As a result, railway organizations have been interested in reengineering processes in order to develop innovative solutions on availability, reliability, efficiency in cost, and advanced technologies. For example, gradual liberalization in transportation and less auditing have yielded separation of management and infrastructure, competition among modes, and collaborative serviceability.

Reliability, availability, and efficiency in cost have been most important matter of railway industry. So, reliability, availability, and efficiency in cost for a railway system require to be developed continuously. Railway companies developed some specific engineering applications in their railway design and developed projects. For example, by many railway companies, RAMS management with system engineering has been used to build availability, reliability, and cost efficiency concepts in early project development phase.

RAMS management is an engineering area aiming to combine reliability, availability, sustainability, and safety with system engineering processes and to ensure to implement designated railway timetable. In recent years, implementing a designated railway timetable well-timed, reliably, and cost efficiently has become a fast growing area in engineering. Also, this area has an important potential in creating advantages in competition of railways against other means of transportation. So, RAMS management is a very crucial subject in today's global railway industry and its importance in local railway industries shows an increasing trend.

Railway RAMS standards were created based on BS IEC 61508 standards. BS IEC 61508 series are representative standards for safety management of electric/electronic related system.

3 railway RAMS management standard have been developed by CENELEC and they are based on BS IEC 61508 standards. BS EN 50126-1 was first published in 1999 as railway RAMS management basic principles and applications. BS EN 50128 is a RAMS management standard for the software used in operating, signalling, and communication of railway included systems and was developed in 2008. BS EN 50129 is a RAMS management standard on railway signalization system hardwares and was published in 2003.

Risk identification is the main part of system engineering and RAMS management. Risk is defined as results of a failure. Risk identification is the base of RAMS management application. Below are two definitions for concept of risk:

Risk is a combination of severity of results and expected frequency of occurrence.

Risk is negative effect occured according to its level.

In general, following 4 items are required to define the risk quantitatively and qualitatively.

- Main causes of potential failure
- Failure mode
- Damage or effect
- Occurrence possibility

Risk assessment is definition, identification and assessment process of a risk in quantitative and/or qualitative manner. Risk assessment generally seeks for the answers of following questions:

- What can happen and why? (By defining the risk)
- What are the causes of failure? (By defining the severity of results)
- What is the probability of a failure? (By specifying the frequency of failure)
- What is the risk level? Can the risk be tolerated or accepted? Or, is a specific control required? (By applying risk assessment techniques)

Risk assessment enables decision making in RAMS (risk assessment management systems) by enabling to deeply understand the risk, its causes, results, and occurrence probabilities. Risk assessment also enables applying RAMS management successfully in following 5 topics:

- Choosing from alternative risks and alternative options,
- Specifying risk priorities to identify decision making and risk management options,
- Choosing proper risk management strategies,
- Identifying risk activity to take the risk under control, and
- Specifying the risk level to be controlled.

This study was prepared for a local signalling system at Istanbul Ulasim Inc. examples of risks encountered during the course of the signaling .For further studies,

it was made into a report. This study focuses on RAMS and systems engineering concepts, risk analysis, a summary of the literature after the information about these concepts and the methods used to calculate quantitatively significant risks are discussed. These methods include FMEA and FTA was preferred for use in the analysis methods and analysis as complementary to each other were investigated in detail. Consequently, the working examples presented in the above-mentioned railway operation. The focusing case study is on FMEA and FTA analysis of the Mescid-i Selam Station Signaling System which is operated in fixed-block signaling system manner. Another aim of this study is to realize the application of the defined FMEA and FTA based risk assessment method and to establish the failure events & causes related to fixed-block signaling systems.

This study, includes a rail project starting with the planning, designing, commissioning, operation and, maintenance until the termination of the system. This study should be a basic source which includes risk analysis methods of the system. Studies to be carried out later, to try to find answers to the questions, such as; in what way a system passed through these stages by international certification bodies and, how it should obtain a system according to international commissions authority.

1. GİRİŞ

Otobüsler, kamyonlar, özel araçlar ve uçaklar gibi karayolu ve havayolu taşımacılığındaki gelişmelerle birlikte demiryollarının taşımacılık sektöründeki etkin rolü hızla azaldı ve sonuç olarak birçok ülkede demiryolu organizasyonları ulusallaştırılarak hizmete devam etme yoluna gitmiştir. Bu, demiryolu taşımacılığının nüfus hareketi ve ulusal ekonomi üzerindeki önemi dolayısıyla böyle olmuştur. Sonuç olarak, demiryollarının ulusallaştırılması demiryolu organizasyonlarında esnek olamamak, maliyet etkin olamamak, operasyonların dakiklikten uzaklaşması ve ray (rail service) hizmetinin kalitesizliği gibi birçok olumsuz etkiye sebep olmuştur. Ancak, demiryolu organizasyonları maliyet etkinlik, uygunluk ve teknik ve yönetimsel açılandan güvenlik beklentisi gibi problemler konusunda bir dönüm noktasına gelmiştir de diyebiliriz (Profilliids, 2007).

Demiryolu organizasyonları diğer ulaşım metodlarına kıyasla kendi özgünlükleri konusunda ve rekabet etme avantajları açısından uzun bir araştırma içerisinde olmuşlardır. Bu amaçla demiryolu organizasyonları, uygunluk, güvenlik ve maliyet etkinlik konusunda ileri teknolojilerin uygulama ve yönetimleri konusunda yeniliçi gelişmeler için özel bir yeniden yapılandırma süreci içerisine girmişlerdir. Örneğin, taşımacılıkta kademeli olarak serbestleşme ve denetimleri azaltma, işletme ile altyapının birbirinden dikey olarak ayrılmasına, modlar arası rekabetin ortaya çıkmasına ve birlikte işletilebilirliğin ortaya çıkmasına sebep olmuştur (Cantos & Compos, 2005; Profilliids, 2007).

Güvenlik, uygunluk ve maliyet etkinlik bugünün global ve yerel demiryolu sektöründe en önemli konular haline gelmiştir. Bundan ötürü, demiryolu sisteminin yüksek güvenlik, uygunluk ve maliyet etkinliğinin sürekli olarak geliştirilmesi gerekmektedir. Buna uygun olarak, demiryolu işletmeleri kendi demiryolu tasarım ve geliştirme projelerinde bazı özel mühendislikler ortaya koymuşlardır. Örneğin, sistem mühendisliğiyle beraber RAMS yönetimi, birçok demiryolu işletmesi tarafından erken proje aşamasında güvenlik, uygunluk ve maliyet etkinlik gibi mühendislik kavramlarını yerleştirmek için kullanılmıştır.

RAMS yönetimi güvenilirlik, uygunluk (emre amadelik), sürdürülebilirlik ve emniyet özelliklerini sistem mühendisliği süreçleriyle birleştirerek bir öz sistem tasarım özelliği ortaya koymaya yarayan ve belirlenen demiryolu tarifesini başarıyla sağlamaya çalışan bir mühendislik alanıdır. Son yıllarda, belirlenen bir demiryolu tarifesini zamanlı, güvenli ve maliyet etkin bir şekilde yerine getirmek hızla gelişen bir mühendislik alanı haline geldi. Ayrıca bu alan, demiryollarının diğer ulaşım sektörleri ile rekabetini geliştirmek için de önemli bir potansiyeldir. Bu sebeple, RAMS yönetimi bugünün global demiryolu sektöründe oldukça önemli bir konu haline gelmiş ve yerel demiryolu sektörlerinde ise gittikçe artan bir öneme sahiptir (BS EN 50126-1, 1999).

RAMS yönetimini demiryolu sistemleri mühendislik süreçleri ile birleştirmek için uzun zamandır gayret sarfedilmekle beraber yalnızca birkaç kuruluş demiryolu sistem mühendisliği için RAMS yönetiminin sistematik bir yaklaşımı olmaması münasebetiyle bu alanın mühendislik kavram, metod ve araçlarını kullanma fırsatı bulabilmiştir. Bu nedenle, bu araştırma projesi, RAMS yönetiminin demiryolu sistemler mühendisliği süreçlerine etkin bir şekilde entegrasyonunu sağlamak, bunun için sistematik bir yaklaşım geliştirmek ve demiryolu işletmelerinin bu alandaki güncel problemlerini araştırmak konularına odaklanmıştır.

Özellikle, demiryolu işletmeleri uzun dönem işletme yönünden RAMS yönetimini uygulayıp tanımlı işletme efektifliğini artırmayı sağlamışlardır. RAMS yönetimi genelde üç yönden demiryolu sistemleri mühendislik projelerine uygulanmıştır. Bunlardan ilki; güvenilirlik, uygunluk (emre amadelik), sürdürülebilirlik ve emniyet gibi RAMS gereksinimlerinin ve işletmeyle alakalı kavramların RAMS yönetimi özelliklerinin belirlenmesidir. İkincisi; demiryolu trafik hizmetinin kalitesini etkileyen problemlerin, hatalar ve yanlışlar gibi potansiyel tehlikelerin değerlendirmesi ve kontrol edilmesi ve son olarak; hata önlenmesi, hata toleransı, hatanın kaldırılması ve öngörülmesi gibi kontrol imkânlarının karşılanmasıdır (BS EN 50126-1, 1999).

Demiryolu hizmetinin kalitesini olumsuz manada etkileyen demiryolu riskleri demiryolu sistemleri mühendisliğinde RAMS yönetiminin ana odağında bulunmaktadır. Demiryolu sistemlerinin kendi doğasından kaynaklı birçok risk bulunmaktadır ve bunlar demiryolu sistem tasarımı ve geliştirme projelerinin erken dönem tasarımlarının üstüne sistemin yaşam döngüsü boyunca sürekli gelişmeyi

gerektirmektedir. Demiryolu riskleri görevli ve yolcuların yaralanma ve/veya yaşam kaybına, çevrenin bozulmasına demiryolu mallarının ve eşyalarının hasar görmesine ve olumsuz ekonomik etkileri içermektedir. Bu sebepten demiryolu riskleri sistematik bir yaklaşım gerektirmekte ve demiryolu sistemler mühendisliğinde önemli bir yönetimi içermektedir.

Demiryolu sistemler mühendisliğinde risk yönetimi yaklaşımı da bu doğrultuda RAMS yönetimi yönünden demiryolu risklerini etkin ve sürekli bir şekilde ortadan kaldırmak ya da azaltmak şeklinde değerlendirilebilir. RAMS yönetimi erken dönem sistem konsept tasarım aşamasında yapılmalı ve teknik yönden bütün riskleri tanımlamak değerlendirmek ve kontrol etmek amaçlı olarak kullanılmalıdır. Ayrıca mühendislik, teknolojiler, işleyiş ve/veya amaçlardaki değişikliklere hızlı yanıt almak için de yönetim perspektifini uygulamak önemlidir (BS EN 60300-1, 2014).

Bu tez RAMS yönetiminin demiryolu sistemler mühendisliğinde kullanım metodolojisini inceleyen beş bölümden oluşmaktadır. Bu araştırmanın temel katkısı Bölüm 3 ve Bölüm 4'te sağlanmıştır. Bu araştırmanın temel teorik bilgileri Bölüm 2 ve Bölüm 3'te anlatılmaktadır. Bölüm 4'te ise Mescidi Selam Lokal Sinyalizasyon Sistemi Uygulamasına ait bir risk değerlendirmesi çalışması yapılmıştır.

Birinci bölüm bu araştırma hakkında genel bir bakış ve bu araştırmaya bir giriş niteliğindedir. Bu bölüm öncelikle bu araştırmanın altyapısını ortaya koymakta ve demiryolu RAMS yönetiminin demiryolu hizmetine başarılı bir uygulaması, demiryolu sistemler mühendisliğine RAMS yönetiminin bir sistemler yaklaşımını içermektedir. Bu çalışmaya temel oluşturacak yaklaşımlar ele alınmaktadır. RAMS yönetiminin temel konuları ve problemleri de yine bu bölümde incelenmiştir.

Bölüm 2'de geniş bir literatür taraması ile sistemler mühendisliği yaklaşımının kavramsal bir açıklaması ile birlikte mühendislik kavramları, metod ve teknikleri RAMS yönetimi ile ilişkilendirilmiştir. Bu bölümde önce bir sistemi başarıyla anlamak için kullanılan mühendislik ve yönetim kavramları özetlenmiştir. Sistemlerin RAMS yönetimi kavramı üç yönden incelenmiş, demiryolu risklerinin tanımları ve değerlendirme yöntemleri gösterilmiş ve RAMS yönetimi için önemli teknikler de amaçları avantajları ve dezavantajları açısından kısaca incelenmiştir.

Bölüm 3'te FMEA ve FTA teknikleri ve bunların uygulamaları süreçleri kullanılarak raylı sistem risk değerlendirme metodlarının geliştirilmesi üzerinde durulacaktır.

FMEA ve FTA yaklaşımlarının temel prensipleri demiryolu risk tanımı için ayrıntılı olarak incelenecek ve iki FMEA-FTA komdinasyon modeli geliştirilerek sistem mühendisliği tasarım fazında uygulanması gösterilecektir. FTA yönteminin matematiğini göstermek amacıyla örnekler göstererek FMEA-FTA bazlı risk analiz süreci gösterildi.

Bölüm 4'te FMEA ve FTA Analizlerine örnek bir uygulama gerçeklenmiştir. Bu uygulama şu an devreye alma çalışmaları devam eden İstanbul Ulaşım AŞ bünyesindeki T4 Hattı Mescid-i Selam Bölgesinde bulunan Lokal Sinyalizasyon Sistemini kapsamaktadır. Bölüm 3'te ele alınan FMEA ve FTA Analiz yöntemlerinin bir uygulaması niteliğinde olan bu bölümde riskler nitel olarak belirlendikten sonra bir trenin deray olması riskiyle alınmış ve nicel olarak araştırması yapılmıştır.

Bölüm 5: Bu bölümde araştırma projesindeki sonuçları, amaç ve görevlerin seçilen araştırma yöntemleri ile nasıl başarıldığını anlatmaktadır. Ayrıca bu bölümün sonunda ileriye dönük araştırmalar hakkında tavsiyeler ve yönlendirmeler de bulunmaktadır.

2. RAMS ANALİZİ YÖNETİMİ

2.1 Giriş

Demiryolunda RAMS, demiryolu trafik hizmetinin genel kalitesini etkileyen bir sistem ürünüdür. Bir sistemin işletmesel hedeflerine ulaşılması için gerekli RAMS performansı, sisteminin ürün tasarımındaki RAMS özelliklerinin entegrasyonu ile elde edilebilir. Buna göre, sistemin konsept tasarımı aşamasındaki demiryolu sistemleri mühendisliği, en sağlıklı RAMS analizi ve RAMS yönetiminin başarılı bir şekilde uygulanması için gereklidir. (BS EN 60300-3-15, 2009)

Bu bölümde RAMS yönetiminin temel mühendislik konularını kurgulamak için, sistemler ve sistem mühendisliğinin tanımlamaları ile sistem mühendisliği yönetimi konsepti incelenecektir.

Demiryolu sistemi görev ve emniyet kritik bir sistemdir. Bu nedenle, bir demiryolu sisteminin operasyonel amaçlarına ulaşmak için, demiryolu sistemini etkileyen tüm olası potansiyel tehlikeler, tanımlanmış tespit edilmiş ve değerlendirilmiş olmalıdır. Bununla birlikte konsept tasarım aşamasından itibaren, sistem yaşam döngüsü aşamaları boyunca RAMS yönetimi ile kontrol edilmelidir. Risk kavramı etkin bir risk değerlendirmesi için tanımlanan ve elde edilen RAMS analizinin temelidir (BS EN 50126-1, 1999). Bu bölümde de, risk esaslı RAMS yönetimi kavramları ve RAMS yönetimini uygulamak için çeşitli yöntemler ve teknikler incelenecektir.

Bu bölüm altı alt başlıktan oluşmaktadır. 2.2'de sistemler kavramı; 2.3'de Sistem Mühendisliği Kavramı ele alınarak 2.4'te RAMS yönetimi konusu işlenecektir. 2.5'te ise RAMS analiz teknikleri üzerinde durulacaktır.

2.2 Sistemler Kavramı

'sistem ve sistemler' kavramı teknik ve yönetim yönü açısından sistem mühendisliği ve RAMS'ın önemli bir ilkesidir (BS EN 50126-1, 1999).

2.2.1 Sistemler

Uluslararası standartlarda ve literatürde 'sistem' teriminin birçok tanımı vardır, ancak bu tanımlar bazı farklılıklar içerir. Aşağıdaki üç tanım, bunlar arasındaki önemli farklılıkların anlaşılması bakımından güzel örnekler olacaklardır:

Sistem, belirtilen hedefe ulaşmak için sistem elemanlarını organize eden bir birleşim kümesidir (BS ISO 9000, 2014).

Sistem, tanımlanmış bir amaca ulaşmak için birbirine entegre edilmiş sistem elemanlarının bir kümesidir. Bu elementler donanım, yazılım ve firmware gibi ürünleri, süreçleri, insanları, bilgileri, teknikleri, tesisleri, hizmet ve diğer destek unsurlarını içerir. (Hasikins, 2007).

Sistem bireysel elemanlar tarafından elde edilemeyen ancak birlikte istenen sonuçları oluşturmak için bu elemanların birlikte oluşturduğu bir kümedir. Sistem elemanları; insan, donanım, yazılım, tesis, mevzuat ve belgeler içerebilir. Diğer bir deyişle, sistem düzeyinde istenen sonuçları elde etmek için gerekli tüm şeyleri içerebilir. Sistem seviyesinde ise sistem nitelikleri, sistem özellikleri, sistem işlevleri, sistem davranışları ve sistem performansı gibi sonuçlar elde edilir. Bağımsız elemanlar tarafından sağlanan bu değerler, elemanlar arasında ilişki ve etkileşim ile oluşturulur; dolayısıyla onların birbirleri ile nasıl bir etkileşim içerisinde oldukları çok önemlidir (Kapurch, 2010).

'sistemler' kavramı; yönetim açısından önemli bir yaklaşım olarak, yukarıda açıklanan 'sistem' kavramının genişletilmiş bir olgusudur ve genellikle 'sistemlerin sistemi' ya da 'sistemin sistemi' şeklinde ifade edilir. Sistemler kavramı, son zamanlarda, yönetim alanında sistem mühendisliğinin prensibi olarak uygulanmıştır. Uçak sistemi ve demiryolu sistemi gibi birçok bağımsız alt sistemlerden veya bileşenlerden yapılmış büyük, karmaşık sistemlerin yönetimine uygulanmaktadır (BS ISO / IEC 15288, 2002).

Genel olarak, sistem tedarikçileri sistemi geliştirmek için “teknik tasarım kriterleri”ni belirlerken, müşteriler de sistemin uyuglanması için sistemin tasarım ve geliştirme sürecini etkileyen “kabul kriterleri”ne ihtiyaç duymuşlardır. Sistem kavramı, işletmesel davranışların araştırılması ve sistem arayüzleri için tanımlanmıştır. Örnek olarak; görev tanımları, performans, emre amadelik, emniyet, maliyet vs gibi.

Ancak, “sistem” ve “sistemler” kavramlarının teknik açıdan herhangi bir farkları yoktur, ama sistem kavramı, sistemleri mühendisliği yönetimi açısından çok önemlidir (Clark, 2008). “sistem” kavramını açık bir şekilde anlamak için aşağıda üç farklı tanımları verilmiştir:

Sistem; dağıtık ve yüksek işbirliği yapan otomatik sistemlerin bir araya getirildiği organize kompleks bir birliktir; ki bu otomatik sistemlerin her biri bağımsız bir şekilde çalışabilme yeteneğine sahiptir.

Sistem; bireysel bir sistem tarafından ulaşılmaz sonuçlar üreten sistem elemanlarının bir birleşimidir. Sistemlerin yapısındaki bireysel sistem kendi başına faaliyete geçmesinin yanı sıra bazı üst düzey görev gereksinimine başarı olarak katkıda muhtemeldir. Herhangi bir sistem için, görev gereksinimleri karşılandığı sürece, bireysel sistemlerin yaşam döngüleri, farklı zamanlarda eklenmeler ve silinmeler olacağı için değişebilir. Böylece, diğer elemanların bertarafı için uzaklaştırıldığında, bazı yeni gelişmeler olabilir (Blanchard, 2012).

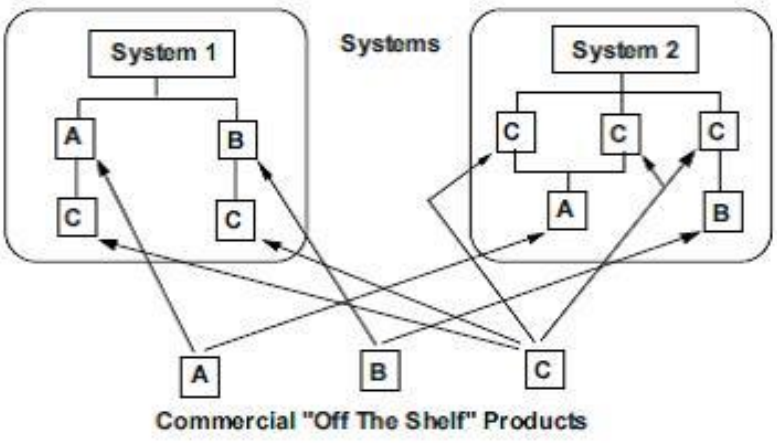
Sistemler, kullanıcılar ve diğer paydaşların yararına tanımlanan ortamlarda hizmet sunmak için oluşturulan ve kullanılan bir yapıdır. Bu sistemler, aşağıdakilerden biri veya daha fazlası ile yapılandırılmış olabilir: Donanım, yazılım, insanlarda, süreçler (örneğin, gözden geçirme süreci), prosedürler (örneğin, operatör talimatları), tesisler ve doğal olarak oluşan kuruluşlar (örneğin, su, organizmalar, mineraller). Uygulamada, onlar ürün veya hizmet olarak düşünülür. Belirli bir sistemin algısı ve tanımı, yani onun mimarisi ve sistem elemanları, bir gözlemcinin ilgi alanları ve sorumluluklarına bağlıdır; bir kişi için sistem ilgi odağı olurken; başka bir kişi için ise sistem elemanı ilgi çekici olarak görülebilir. Bunun aksine başka bir kişi için, işletme ortamının bir parçası olarak görülebilir (BS ISO / IEC 15288, 2002).

BS EN 50126-1 (1999) standardı, üç seviyede bir demiryolu sisteminin hiyerarşisini sınıflandırır ve Şekil 2.1’de gösterildiği gibi sistem düzeyinde yaklaşımının dikkate alınarak sistem, alt ve bileşenleri yönlerini açıklar. Sistem, alt sistemi ve bileşenin tanımı farklı düşünceler altında değişiklik gösterebilir:

Seviye 1: bir mühendislik disiplini içinde önemli ölçüde tanımlanan bir **alt sistem**. Örneğin, bir sürüş dişli kutusu, klima, vagon vb.

Seviye 2: **bir sistem** olup, iki veya daha fazla teknik disiplinleri içerir. Örneğin, tren, elektrik güç kaynağı, sinyal sistemi, vs.

Seviye 3: Birçok disiplini ve ekonomiyi; sosyal ya da çevresel faktörleri etkileyen veya bunlardan etkilenen **sistemler**. Örneğin, tüm bir demiryolu sistemi.



Şekil 2.1 : Sistem seviyeleri yaklaşımı.

2.2.2 Sistem yaşam dögüsü (life-cycle) kavramı

Sistem yaşam döngüsü, sistem mühendisliğinde çok önemli bir kavramdır. Bir sistem yaşam döngüsü kavramı tasarımdan demonte edilmeye kadar tanımlanmış sıralı aşamalarında gerekli olan çeşitli faaliyetleri kapsamaktadır (Çizelge 2.1). Her sistem, ne olursa olsun türü veya boyutu, tanımlanmış bir yaşam döngüsü aşaması izler. Yaşam döngüsü genellikle bir sistemin bütün hayatını kapsayacak şekilde değerlendirir, denetlenir, gözlemlenir ve bunlar; sistem mühendisliği için tüm faaliyetleri planlar. Bu durum Çizelge 2.1'de açıklandığı gibi, bir bütünlük sağlayan ardışık aşamadan oluşmaktadır. Bu nedenle, sistem mühendisliği sistem yaşam döngüsü fonksiyonlarını entegre etmek üzerinde odaklanır. Sistem mühendisliği yönetiminde kullanılan sistem yaşam döngüsü evreleri Çizelge 2.1'de göstermektedir (BS ISO / IEC 15288, 2002). Çizelge 2.1'de temel olarak ifade edilen aşamalar şu şekilde detaylandırılabilir:

Çizelge 2.1 : Sistem yaşam döngüsü aşamaları.

Sıralama	Aşamalar
1	Konsept Aşaması
2	Tasarım ve Geliştirme Aşaması
3	Üretim Aşaması
4	Kullanım Aşaması
5	Destek Aşaması
6	Demonte (retirement) Aşaması

- Konsept aşaması; müşteri ihtiyaçlarını ve beklentirlerini kabul etmek, konsepti incelemek ve uygun bir sistem çözümü önermek.
- Tasarım ve geliştirme aşaması; sistem isterlerini belirlemek, sistem çözümüne ait tanımlamaları geliştirmek, sistem ürünlerini tasarlamak ve bu tasarıları doğrulayıp onaylatmak.
- Üretim aşaması; sistem ürünlerini üretmek ve bu ürünleri gözlemleyip gerekli testlerini gerçekleştirmek.
- İşletme aşaması; sistemi müşteri ihtiyaçlarını karşılayacak şekilde işletmek.
- Destek aşaması; sistemin sürdürülebilirliğini sağlamak.
- Demonte aşaması; sistemi rafa kaldırmak veya tamamen sökmek.

2.2.3 Sistem mühendisliği tanımı

Sistem mühendisliği, bir sistemin sistem konsept tasarım aşamasında teknik tasarım kriterlerini geliştirmek için önemli bir ilkedir. Uluslararası mühendislik standartları ve literatürde sistem mühendisliği ile ilgili birçok farklı tanımlar vardır. Aşağıda üç farklı tanım ile sistem mühendisliği kavramını ifade etmek mümkün olacaktır. Sistem Mühendisliği (MIL-STD-499B, 1994):

sentez, tasarım, test ve değerlendirme gibi tekrarlayan bir sürecin kullanımı yoluyla, sistem performans parametrelerini ve sistem konfigürasyonunun tanımlamayarak bunları, işletmesel ihtiyaçlara dönüştürmek için;

ilgili teknik parametreleri entegre edecek ve toplam sistem tanımı ve tasarım optimize edecek bir şekilde tüm fiziksel, fonksiyonel ve program arayüzleri uyumluluğunu sağlamak için;

maliyet, zamanlama, desteklenebilirliği ve teknik performans hedeflerini karşılamak için toplam mühendislik çabası içine güvenilirliği, sürdürülebilirliği, emniyetli olmayı, mühendisliği ve diğer faktörleri entegre etmek için;

çabalayan, bilim ve mühendislik uygulamasıdır.

Sistem Mühendisliği parçalardan farklı olarak bütün (sistem) tasarım ve uygulama üzerinde yoğunlaşan bir disiplindir. Bu, tüm gerçekleri ve tüm değişkenleri ve teknik açıdan sosyal koşulları da göz önüne alarak, bütünüyle bir sorun bakmayı da kapsar (Hasikins, 2007).

Sistem Mühendisliği, disiplinler arası bir yaklaşımdır ve başarılı sistemlerin gerçekleşmesini sağlamak anlamına gelir. Sistem mühendisliği, geliştirme döngüsü kapsamında erken müşteri ihtiyaçlarını ve gerekli işlevselliği tanımlayan, gereksinimleri belgeleyen ve sorunu göz önüne alarak daha sonra tasarım sentezi yapılmasına ve sistem doğrulamasına odaklanır. Sistem mühendisliği kullanıcı ihtiyaçlarını karşılayan ürünün kalitesini sağlamak amacı ile tüm müşterilerinin ticari ve teknik ihtiyaçlarını düşünmektedir (BS ISO / IEC 26702, 2007).

Sistem mühendisliği ile mekanik, elektrik, inşaat mühendisliği gibi geleneksel mühendislik disiplini arasındaki fark aşağıdaki şekilde açıklanabilir: (Kossiakoff 2011)

Sistem mühendisliği bir bütün olarak sistemde odaklanmıştır,

Sistem mühendisliği müşteri ihtiyaçlarına ve işletmesel içeriklere odaklanmıştır;

Sistem mühendisliği bir sistemin kavramsal tasarım sağlar, ve;

Sistem mühendisliği geleneksel mühendislik disiplinleri arasında bir köprü olarak rol alır.

Ayrıca, sistem mühendisliği, projenin bir parçası olarak sistem mühendisliğinin genel faaliyetlerini planlar ve bu planlara kılavuzluk eder (Daup, 2001). Bu nedenle, sistem mühendisliği bazen sistem mühendisliği projesi veya sistem mühendisliği yönetimi olarak da adlandırılır.

2.3 Sistem Mühendisliği Kavramı

Sistem mühendisliği, bir sistemin tasarımı ve geliştirilmesi için bir temel oluşturur. RAMS yönetimi ise sistem mühendisliği dalının bir parçasıdır. Bu nedenle, RAMS yönetimi sistem mühendisliğinin ayrılmaz bir parçası olarak uygulanır (BS EN 60300-3-15, 2009). Bu bölümde öncelikle RAMS yönetimi teorik arka plan oluşturmak için sistem mühendisliği kavramını incelenecektir.

'sistem' kelimesi Yunanca 'sustēma' kelimesinden türemiştir (Blanchard, 2012). Türk Dil Kurumu Sözlüğünde ise “bir sonuç elde etmeye yarayan yöntemler düzeni” olarak ifade edilmiştir. Oxford sözlüğü ise, “bir mekanizmanın parçası olarak birlikte çalışan şeylerin bir kümesi "olarak sistemini tanımlar. sistem kavramı büyük,

karmaşık görev veya emniyet kritik sistemlere ilişkin, birçok mühendislik disiplinlerinde uygulanmıştır.

Bilimsel alanda öncelikle 19. yüzyılda Sadi Carnot (1796-1832), bir Fransız doktorun önerisi üzerine 'sistem kavramını' uyguladı. Daha sonraları, 1945 yılında Bertalanffy tarafından yayınlanan 'Genel sistem teorisi' ile bilim ve mühendislik alanında genel sistem kuramı bir ilke olarak uygulandı. Günümüzde genel sistem teorisi bir sistem tasarlayan ve geliştiren bir prensip olarak daha geniş bir şekilde uygulanmaya başlandı (Elphick , 2010; Blanchard, 2012).

Amerika Birleşik Devletleri'nde Bell Şirketi, ilk olarak 1940'larda sistem işlerliğini geliştirmek için 'sistemler mühendisliği ilkeleri' uygulamaya aldı. Sistem mühendisliği ilkesi ileri teknolojiye ve yönetime giriş yapmak nedeniyle bir sistemin karmaşıklığını ve belirsizliğini çözmek ve rekabet gücünü artırmak için birçok alanda uygulanmıştır. Her şeyden önce, 1960'larda 'Apollo uzay gemisi Projesi'nin başarıyla uygulanması, sistem mühendisliği dünya çapında benimsenmesinde büyük bir katkı sağladı. Birçok demiryolu kuruluşunda 1980'lerden beri sistem mühendisliği uygulaması denenmiştir, ancak hala başlangıç aşamasında kalmıştır.

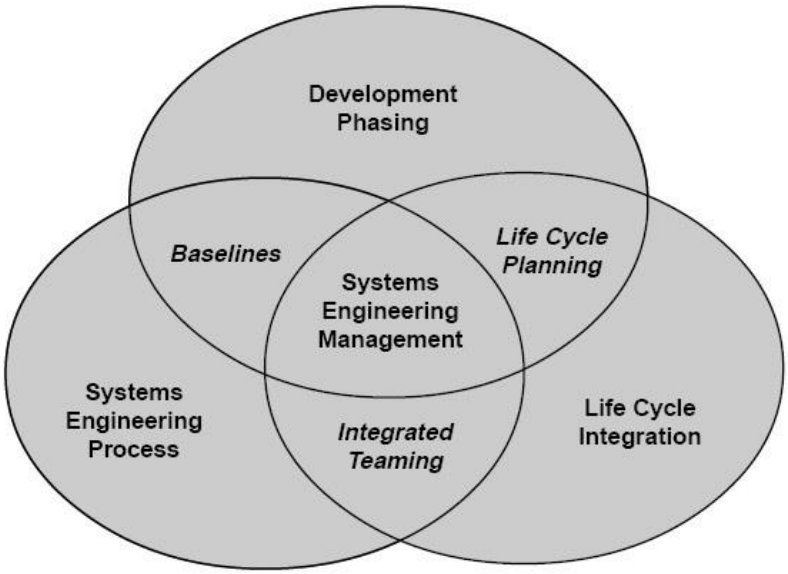
2.3.1 Sistem mühendisliği aşamaları

Sistem mühendisliğinin başarıya ulaşması için, yalnızca teknik bilgiye erişilmesi yeterli değildir, aynı zamanda sürecin yönetilebilmesi de gereklidir. Etkin ve verimli bir yönetim yapısı ile birlikte uygun bir işbirliği ortamının kurulması, sistem mühendisliğinin başarılı bir şekilde uygulanması için gerekli kriterlerdendir. Bu durumda, müşterinin ihtiyaçlarını ve sistemin beklentilerini karşılayacak şekilde optimum teknik tasarım ve kabul kriterleri gelişimi sağlanır (Blanchard, 2012).

Genel olarak, sistem mühendisliği yönetiminin rolü aşağıdaki üç farklı mühendislik faaliyetinin tam entegrasyonu ile tanımlanır:

- Tüm tasarım ve geliştirme aşamalarının genel hatlarıyla kontrolü,
- Sistem mühendisliği sürecinin uygulanması
- Sistemin yaşam döngüsü fonksiyonlarının entegrasyonu.

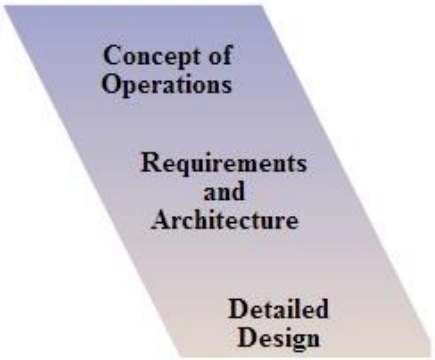
Şekil 2.2'de sistem mühendisliği faaliyetleri arasındaki ilişkiler gösterilmektedir:



Şekil 2.2 : Sistem mühendisliği faaliyetleri.

2.3.1.1 Tasarım aşamasının kontrolü

Tasarım ve geliştirme aşamasında sistemin ana hatlarıyla kontrolünde, sistemleri mühendisliği yönetiminin önemli bir rolü vardır. Genel olarak, bir sistem çeşitli tasarım aşamalarından geçerek tasarlanmış ve gelişmiştir. Şekil 2.3'de gösterildiği gibi sistemin tasarım sonuçları tertip edilip ana hatları kontrol edilir.



Şekil 2.3 : Sistem tasarım ve geliştirme hiyerarşisi.

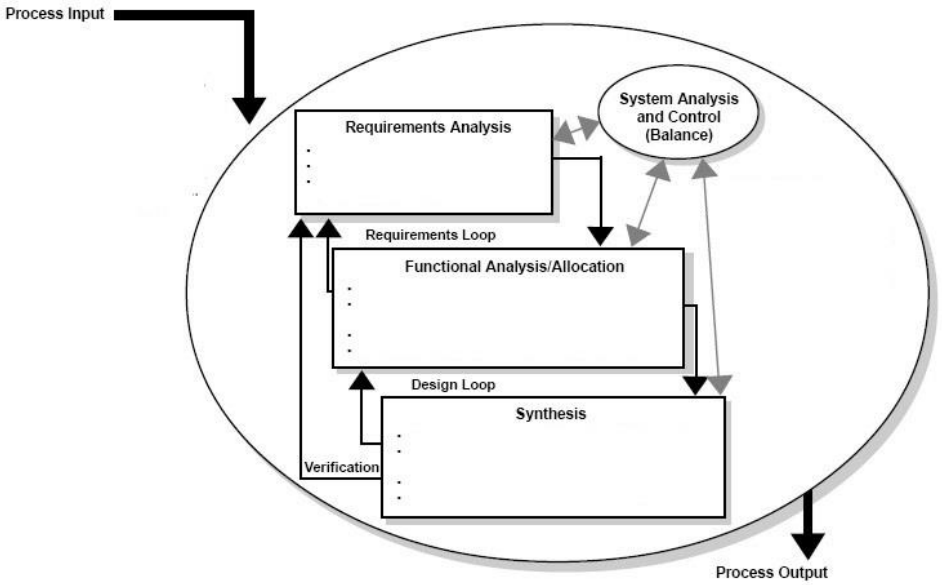
Şekil 2.3'de gösterildiği gibi; sistemin konsept aşaması, tasarım ve geliştirme için sistem kavramları oluşturur ki buna genellikle fizibilite çalışması aşaması denir. Sistem gereksinimleri ve mimarisi aşaması, sistem fonksiyonları ve performansları açısından ister tanımlamalarını sağlar ve fonksiyonel mimariden oluşur. Son olarak, ön (preliminary) ve detaylı tasarım aşamaları, sistem ürünlerinin karakteristiklerinin

ve performans özelliklerinin oluşturulmasını sağlar. Ön tasarım aşaması sistemin, yüzeysel ve ayrıntılı tasarım aşaması formları içermektedir. Tüm ana hatlar, sistem mühendisliğinin bir yönetim kontrol noktasıdır (MIL-STD-499B, 1994).

2.3.1.2 Sistem mühendisliği sürecinin başlatılması

Teknik mühendislik sürecinde sistem mühendisliği, bir sistemin başarılı gelişimi için gerekli olan sorunlara etkili çözüm bulmak için yönetir. Teknik mühendislik süreci, tasarım ve geliştirmenin tüm aşamalarında uygulanabilir. Bu sürecin ana fonksiyonları aşağıda tarif edilmiştir (Daup, 2001). Sistem mühendisliği süreci aşağıdaki üç temel görevi içerir:

- Sistem gereksinimlerini, Sistem tasarım çözümleri ve süreç tanımları şekline dönüştürme;
- Karar vermek için gerekli bilgi ve kaynakları üretme;
- Bir sonraki tasarım ve geliştirme aşamasında katkı sağlama.



Şekil 2.4 : Sistem mühendisliği süreci (MIL-STD-499B, 1994).

MIL-STD-499B ve ISO / IEC 15288 gibi uluslararası standartlarda ve literatürde birçok türde sistem mühendisliği süreç modelleri vardır. Şekil 2.4, 1994'de askeri bir standart olarak yayınlanan MIL-STD-499B standardından alınan bir süre. modeli açıklanmaktadır. Sistem mühendisliği süreci üç temel fonksiyonu vardır:

- İsterlerin (requirements) analizi
- Fonksiyonel analiz ve ayrıştırma
- Tasarım sentezi

Şekil 2.4'de gösterildiği gibi, her işlem aşaması; tanım, belirleme, analiz, değerlendirme, kontrol etme ve doğrulama faaliyetleri yürütülmektedir.

Süreç, isterler döngüsü ve tasarım döngüsü şeklinde iki işlem döngüsü tarafından tekrarlanarak uygulanmaktadır. Her işlem aşaması Şekil 2.4'de gösterildiği gibi tüm süreç aşamaları; tanımlama, belirleme, analiz, değerlendirme, kontrol ve doğrulama faaliyetleri olarak yürütülür.

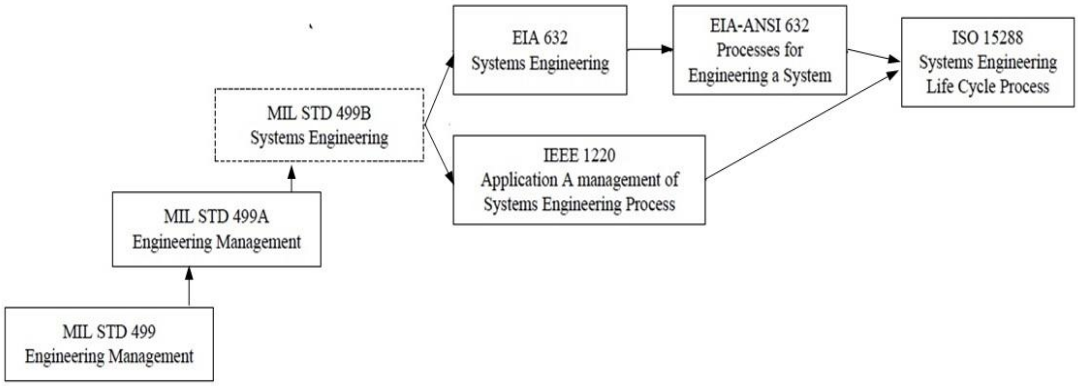
2.3.1.3 Yaşam döngüsü fonksiyonlarının entegrasyonu

Sistem mühendisliği yönetiminin bir diğer faydası da yaşam döngüsü süresince ortaya çıkabilecek olası tüm problemleri etkin bir şekilde çözmek için, sistem mühendisliği sürecine, bir sistemin tüm yaşam döngüsü süresince gerekli tüm fonksiyonları entegre etmektir. Sistem yaşam döngüsü sekiz temel işlevleri şunlardır (Daup, 2001): tasarım & geliştirme, imalat, dağıtım, işletme, destek, bertaraf etme (disposal), eğitim ve doğrulama.

2.3.2 Sistem mühendisliği standartları

Askeri ve sivil alanlarda geliştirilen birçok sistem mühendisliği standartları vardır. Birçok sistem mühendisliği standartlarının gelişmesi sebebiyle, sistem mühendislerinin bir sistemin tasarımı ve geliştirilmesi için temel olarak bir standart seçmesi kolay olmayabilir.

Sistem mühendisliği standardı ilk kez ABD Askeri tarafından "MIL-STD- 499 (1969) - Mühendislik Yönetimi," standardı isminde geliştirildi ve yayımlandı. Daha sonraları çeşitli standartlar ticari alanlarda geliştirildi (Şekil 2.5). İlk standart 1974 ve 1994 yıllarında olmak üzere iki kez revize edildi. Ancak, MIL-STD-499B standardı 1994 yılında revize edildi, ama yayınlanmadı. Bununla birlikte MIL-STD-499B standardının prensip ve konsepti IEEE-1220 (1995), (1998) EIA 632 ve EIA / IS-632 (1999) sivil standartlarına uygulandı. Son zamanlarda, EIA / IS-632 ve IEEE 1220 standartları ISO / IEC 15288-2008 standardını refere ederek, tek bir konsepte uyumlu hale getirilmiştir.

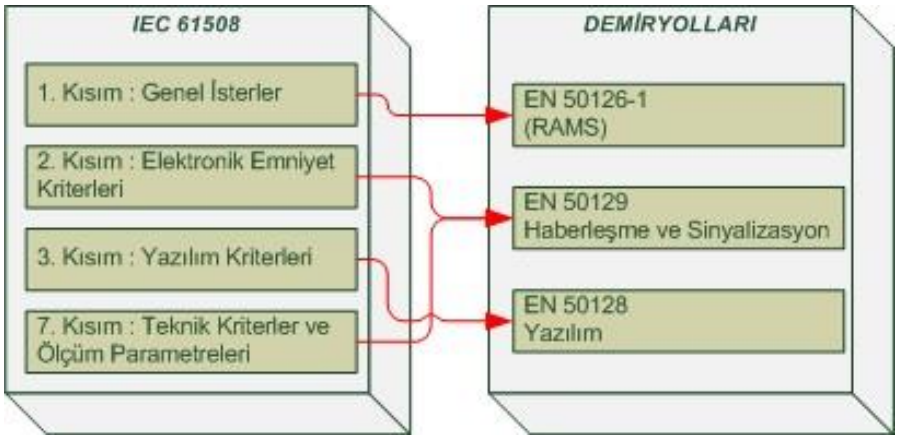


Şekil 2.5 : Sistem mühendisliği ile ilişkili standartlar.

2.4 Sistemlerde RAMS Yönetimi

Demiryolu RAMS standartları, Şekil 2.6'da belirtildiği gibi BS IEC 61508 standardına (2002 ve 2005) dayanarak geliştirilmiştir. BS IEC 61508 serileri elektrik/elektronik sistemlerle ilgili güvenlik yönetimi için örnek standartlardır.

CENELEC tarafından 3 demiryolu RAMS yönetimi standardı geliştirilmiştir ve bunlar Şekil 2.6'da belirtildiği gibi BS IEC 61508 serilerine dayanır. BS EN 50126-1 ilk defa 1999 yılında demiryolu RAMS yönetimi temel prensipleri ve uygulaması olarak yayınlanmıştır. BS EN 50128, demiryolu sistemi içeren sistemlerin çalışması, sinyalizasyonu ve iletişiminde kullanılan yazılımlar için RAMS yönetimi standardıdır ve 2008'de geliştirilmiştir. BS EN 50129 ise demiryolu sinyalizasyon sistemleri donanımları ile ilgili RAMS yönetimi standardıdır ve 2003'te yayınlanmıştır. Bu RAMS yönetimi standartları her 5 yılda bir revize edilir (Lundteigen, 2009; Nordland, 2003; Braban et al., 2003; Pasquale, 2003).



Şekil 2.6 : Demiryolu standartları.

2.4.1 RAMS kavramı

"Sistemlerde RAMS" güvenlik ve güvenilirlik kavramlarını temel alan geniş bir mühendislik disiplinidir. Güvenlik ve güvenilirlik kavramları 1930'larda ilk olarak havacılık sektörü ile ön plana çıkmıştır. Bu kavramlar sistem hata analizinde istatistik tekniklerinin uygulanması sayesinde 1950'lerde havacılık sektöründe önemli bir mühendislik disiplini olmuştur.

Güvenlik ve güvenilirlik mühendisliği ürünlerin hataya düşmesini ve insan hatalarını belirlemek üzere ortaya çıkmıştır. Hata türü ve etkilerinin analizi (FMEA) güvenlik ve güvenilirlik belirlemesi için kullanılan ilk yöntemdir ve 1940'larda geliştirilmiştir. Boeing FMEA ifadesini 1960'lı yıllarında 'Kritiklik Analizi(CA)' ekleyerek FMECA olarak ileriye taşımıştır. CA ile tek nokta hatalarının analizi üzerinden sistemlerin güvenliğini doğrudan etkileyen nicel güvenlik belirleme desteklenir.

1970'lerde havacılık sektöründe güvenlik ve güvenilirlik riskine dair "Event Tree Analysis(ETA)", "Fault Tree Analysis(FTA)" ve "Probabilistic Risk Analysis(PRA)" gibi birçok ileri belirleme yöntemleri geliştirilmiştir. Bu ileri yöntemler kimya, demiryolu gibi birçok farklı sektörde uygulanmaktadır.

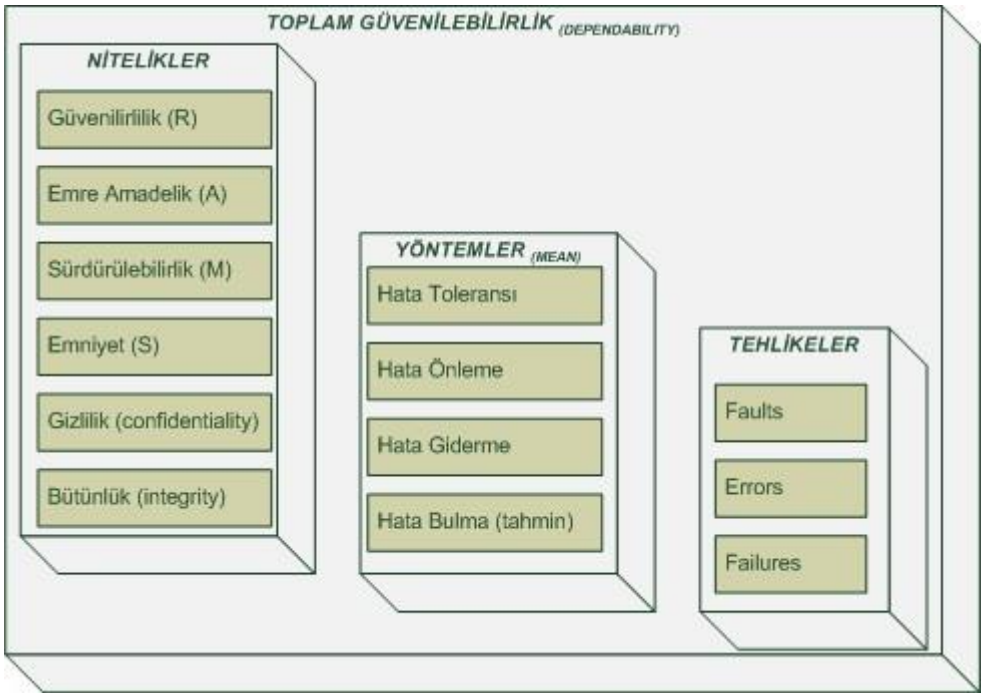
Systems RAMS yönetimi, güvenlik ve güvenilirlik için ulaşılabilirlik ve sürdürebilirlik kavramlarının oluşturulması ve sistem mühendisliğinin 1980'lerin başından bu yana gelişmesiyle benimsenmiştir. Bu yapı bütün bir sistemi etkileyecek tüm tehlikelerin tanımlanması, belirlenmesi ve kontrol edilmesiyle başarıya ulaşır ve özellikle görev ve güvenlik kritik sistemlere uygulanmıştır. Systems RAMS yönetimi 1990'ların başından bu yana sistem mühendisliğinin ayrı bir disiplini olarak gelişmiştir ve oturmuş mühendislik kavramları, yöntemleri, teknikleri, ölçülebilir parametreler ve matematiksel araçlara ihtiyaç duyar.

Özellikle demiryolu organizasyonları, sistemin uzun dönemli çalışmasının güvenlik, ulaşılabilirlik ve maliyet yönetimi açısından başarıya ulaşması için RAMS yönetimini uygular. Demiryolu sistem mühendisliği için RAMS yönetimi uygulaması 1980'lerin başında A.B.D demiryolu sektöründe başladı. Avrupa'da ise 1990'ların başında sistem mühendisliğinin demiryolu sektöründe yer almaya başlamasıyla bu sistem uygulanır oldu.

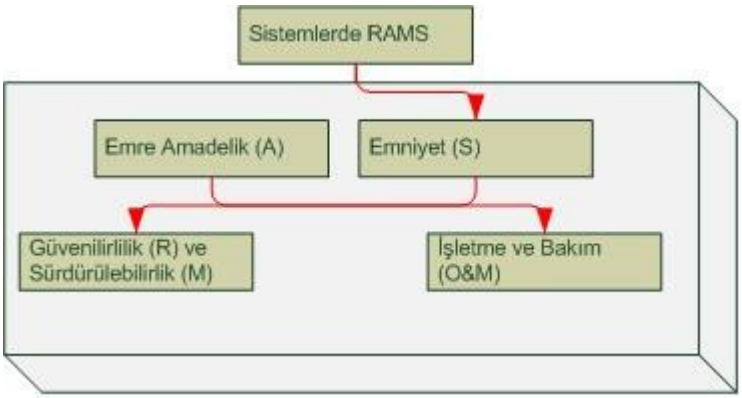
Demiryolu RAMS yönetimi ilk defa CENELEC tarafından 1999'da standartlaştırıldı. Bu standart 2002'de uluslararası demiryolu RAMS yönetimi standardı "IEC62278"

olarak benimsenmiştir. Bu aileden olan BS EN50128(2009) ve BS EN50129 (2003) standartları da CENELEC tarafından sonradan yayınlanmıştır. Bu standartlar birçok global demiryolu projesinde önemli bir rol üstlenmiştir.

BS EN 50126-1 (1999), sistemlerde RAMS yönetimini Şekil 2.7'de görüldüğü üzere 3 noktada tanımlamışlardır. Bunlardan ilki RAMS teriminin açılımı olan tanımlardır. İkincisi RAMS gerekliliklerinin başarımını ters yönde etkileyecek potansiyel tehlikelerin belirlenmesi ve kontrolüdür. Son olarak da Sistemlerde RAMS gerekliliklerini başarımı için gerekli yöntemlerin içeriğidir (Ucla, 2000).



Şekil 2.7 : Bağıllık ağacı gösterimi.



Şekil 2.8 : Sistemlerde RAMS.

Sistemlerde RAMS yönetimi sistemin işletmesel görevlerinin başarılı bir şekilde tamamlandığına emin olmak için sistem ürün tasarımı için doğal birer unsur olan

ulaşılabilirlik, güvenilirlik, sürdürebilirlik ve güvenlik olmak üzere 4 karakteristik tanımlar. BS EN 50126-1 standardında, Sistemlerde RAMS'ın karakteristikleri arasındaki genel bağlantı Şekil 2.8'deki gibi gösterilmektedir.

Güvenilirlik karakteristiği bir sistemin kendisine atanmış fonksiyonunu belirli bir süre zarfında, tanımlanmış bir hataya düşmeden gerçekleştirebilme yeteneğidir. Sürdürebilirlik ise sistemin yapısına dair bir bakım işleminin kolay olmasını sağlamaya yönelik bir sistem karakteristiğidir. Ulaşılabilirlik karakteristiği de operatör tarafından istenildiği zaman bir sistemi gerekli bir görevin başlangıç noktasında kullanabilme yeteneği anlamına gelir. Son olarak güvenlik ise işletme, bakım, insan, çevre ve ekipmana dair kabul edilemeyecek risklerden kurtulmayı sağlayan sistem tasarım karakteristiğidir. Güvenilirlik ve sürdürebilirlik karakteristikleri ürün tasarım performansına dair karakteristikler olarak sistem veya operasyonel ulaşılabilirlik ve/veya güvenlik ihtiyaçlarınca belirlenir. Ayrıca ulaşılabilirlik ve güvenlik, Şekil 2.8'de gösterildiği üzere güvenilirlik ve sürdürebilirlik karakteristikleri ile sağlanabilir.

Sistemlerde RAMS yönetimi sisteme dair potansiyel tüm tehlikeleri tanımlar ve kontrol eder. Potansiyel tehlikeleri sistem, işletme ve bakım kaynaklı olmak üzere 3 başlıkta toplayabiliriz. Bu faktörler özellikle risk belirleme girdisi olmak üzere RAMS yönetim sürecinin önemli girdileri olarak değerlendirilmektedir.

Son olarak Systems RAMS yönetimi, yerine getirilmesi beklenen operasyonel görevleri yapabilmek için hata önleme, hata toleransı, hata giderme ve hata öngörme gibi yöntemler önerir. Bu yöntemler RAMS performansını etkileyen tehlike faktörlerini kontrol etmekle doğrudan ilişkilidir. Demiryolu RAMS yönetimi EN BS 50126-1'de aksaklık ihtimalini minimize edecek uyarılar üzerine kuruludur. Uyarı, önlem ve koruma kavramlarının birleşimidir ama bir demiryolu sisteminin RAMS yönetiminde önlem koruma yerine tercih edilmelidir. Sistemlerde RAMS yönetimi aşağıdaki 3 maddeyi uygulayan bir süreçtir.

- RAMS yönetimi içeriğinin stratejik yöneliminin bilinçli seçimi
- RAMS yönetimi fonksiyonlarının etkili kontrolü
- Tüm RAMS yönetimi faaliyetlerinin koordinasyonu

RAMS yönetiminin maliyet etkinliğine, sistem etkinliğine, riske ve çevresel etkilere dair işlevleri de vardır.

Demiryolu RAMS yönetimi, etkin sistem mühendisliği için aşağıda sıralanmış 5 faaliyeti destekler:

- RAMS gereklerini tanımlama
- Demiryolu RAMS'e yönelik tüm tehlikeleri belirlemek ve kontrol etmek
- RAMS görevlerini planlama ve uygulama
- RAMS gereklerine uyumluluk sağlama
- Sürekli gözetim ve gözden geçirme işlemlerini yönetme

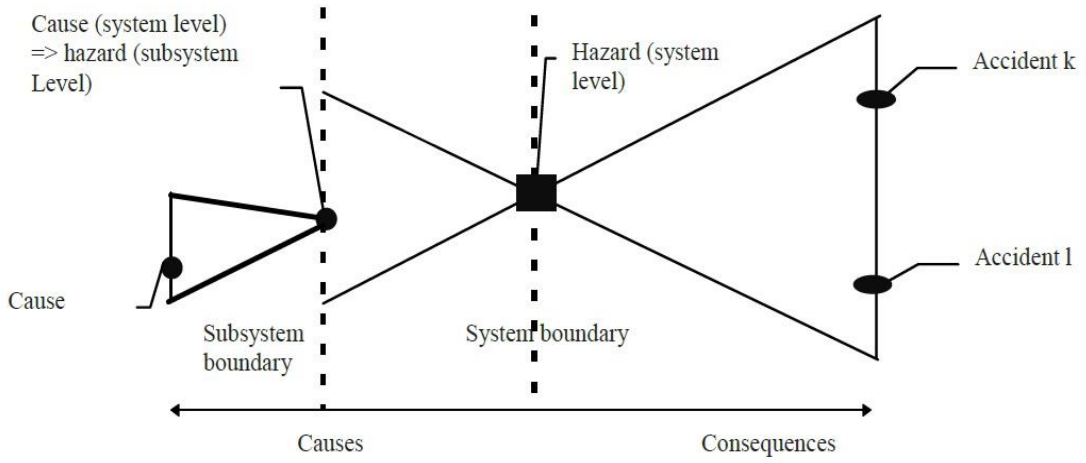
2.4.2 Risk değerlendirme kavramı

Risk belirleme, sistem mühendisliği ve RAMS yönetiminin temel kısmını oluşturur. Bu kısımda sistem riski ve bunun belirlenmesi kavramları işlenmiştir.

Risk bir hata durumunun sonuçları olarak tanımlanır. Risk belirleme RAMS yönetimi sürecinin temel parçasıdır ve RAMS yönetiminin uygulanması için temel oluşturur.

Aşağıda risk kavramı için iki tanım bulunmaktadır:

- Risk, getireceği sonuçların vahametinin ve götürülerinin beklenen gerçekleşme sıklığının birleşimidir (BS EN 50126-1, 1999).
- Risk, seviyesi ile birlikte sebep olduğu ters etkileridir.



Şekil 2.9 : Risk tanımlama diyagramı (BS EN 50129, 1999).

Genellikle riski nitelik ve nicelik olarak tanımlamak için aşağıdaki 4 madde gereklidir. Şekil 2.9'da bu 4 maddenin ilişkisi verilmiştir.

- Potansiyel hatanın temelinin sebepleri
- Hata modu
- Götürüleri ya da etkileri
- Olma olasılığı

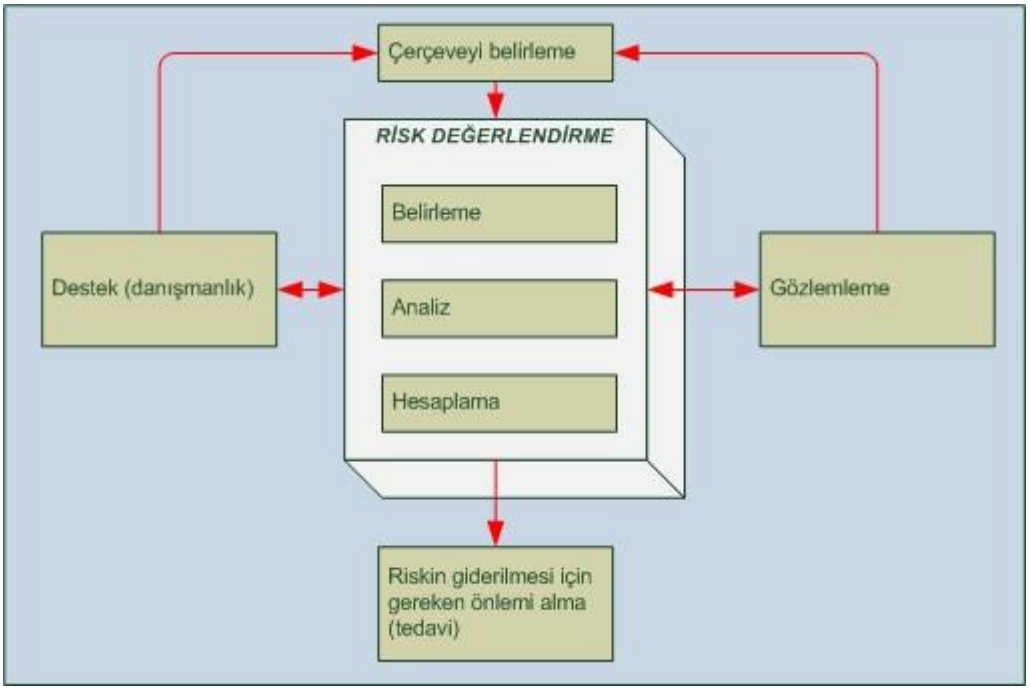
Risk değerlendirme bir riski, nitelik ve/veya nicelik açısından, tanımlama belirleme ve değerlendirme sürecidir. Risk değerlendirme genelde şu sorulara yanıt arar (BS EN 31010,2010):

- Ne meydana gelebilir ve neden olabilir? (Riski tanımlayarak)
- Başarısızlık sebepleri nelerdir? (Sonuçların ciddiyetini tanımlamayarak)
- Başarısız olma ihtimali nedir? (Başarısız olma sıklığını belirleyerek)
- Risk seviyesi nedir? Risk tolere edilebilir veya kabul edilebilir midir? Yoksa ayrıca kontrol gerekli midir? (Risk değerlendirme teknikleri uygulayarak)

Yukarıdaki sorulara cevap arayabilmek için bir sistem bütün potansiyel zararları tanımlamak, belirlemek, analiz etmek ve değerlendirmek amacıyla Şekil 2.10'da görülen süreci takip etmek gerekir.

Risk değerlendirmesi riski, sebeplerini, sonuçlarını ve olma ihtimalini derinlemesine anlamayı sağlayarak sistemlerin RAMS (risk değerlendirme yönetme sistemleri) yönetiminde karar verme için imkân sağlar. Risk değerlendirmesi, ayrıca aşağıdaki beş konuda da RAMS yönetiminin başarıyla uygulanmasına imkan sağlar:

- Değişik riskler arasında değişik seçenekler arasında seçim yapmak
- Karar verme ve risk yönetim seçeneklerinin belirlenmesi için risk önceliklerinin belirlenmesi
- Uygun risk yönetim stratejilerinin seçilmesi.
- Undertak için risk aktivitesinin belirlenmesi ve
- Kontrol edilecek olan risk seviyelerinin belirlenmesi.



Şekil 2.10 : Risk değerlendirme süreci (BS EN 31010,2010).

2.4.3Risk değerlendirme yöntemleri

Risk değerlendirme, istenen risk değerlendirmesi amaçlarını ve toplanan bilgi ve kaynakların kullanımında gerekli olan risk seviyesinin karar verilmesi yerine getirir. Risk değerlendirme metodu 2 gruba ayrılır: genel grup ve özel grup. Genel grup, analitik şartlar, bilgi ve kaynaklara göre, nitel, nicel ve yarı-nicel değerlendirme olarak üç ana kategoriye ayrılır. Özel grup ise sistem tasarım sürecinin analitik yönlendirilişine göre, tepeden tabana ve tabandan tepeye olmak üzere iki gruba ayrılır. Tepeden tabana değerlendirme, fonksiyonel tasarım aşamasında, tabandan tepeye değerlendirme ise fiziksel ürün tasarım aşamasında uygulanır (BS EN 31010, 2008).

Sistem mühendisliğinin tasarım aşamasında nitel değerlendirme metotları sıklıkla tanımlanan riskin genel seviyesini saptamak ve tüm potansiyel muhtemel riskleri belirlemek ve tahmin etmek amacıyla ön risk değerlendirme olarak kullanılır. Bununlar birlikte, nitel değerlendirme sistem mühendisliğinin her bir tasarım süreç aşamasında tanımlanmış risklerin yarı-nicel ya da nicel risk değerlendirmesi için gerekli bir evre olabilir. Örneğin, FMEA nitel risk değerlendirme olarak uygun bir örnektir (BS EN 60300-3-1, 2004).

Nitel değerlendirme, fonksiyonel (sub-sistem) tasarım aşamasında tüm muhtemel arıza etkilerini tanımlamak ve güvenlik fonksiyonları oluşturmak için uygundur. Nicel veri kullanımı yerine böyle bir nitel yaklaşım, arıza sonuçlarının sıklığını ve şiddetini ölçmek için sözel aralıklardan faydalanabilir. Genellikle, 'felaket, kritik, marjinal ve önemsiz' gibi 4 sözel aralık arıza şiddetini sınıflandırmak için ve 'sık, muhtemel, bazen, pek az ve muhtemel olmayan' gibi 5 sözel aralık da arıza sıklığını sınıflandırmak için kullanılabilir (MIL-STD-882D, 2000).

Yarı-nicel risk değerlendirmesi yukarıda anlatılan nitel risk değerlendirmesine benzer olmakla birlikte, ondan daha geniş sıralama aralığı kullanır. Nitel metotların avantajlarından birçoğunu içerir. Bununla birlikte böyle bir metot, nitel metotlar kadar kesin ve hassas olmayabilir. Eğer bütüncül bir nitel değer elde değilse, nitel bilgiyi nicel ölçülere dönüştürmek için FMECA gibi risk değerlendirme metrikleri kullanan sıralama parametreleri kullanılabilir. FMECA yarı-nicel risk değerlendirme metodu olarak uygun bir örnektir.

Nicel risk değerlendirme metodu, sistem ve RAMS tasarımcılarına nicel ölçülerle sistem tasarım çözümlerinin alternatiflerini belirleme imkanı sağlamayı amaçlar. Nicel değerler riskleri anlamada, uygulamada ve karşılaştırmada çok önemli avantajlar sağlar. Bununla birlikte, nicel değerlendirme metodu istatistiksel analiz için veri ve teknikleri gerektirir.

Nicel metodun uygulanması tasarlanacak sistemin daha derin bir şekilde anlaşılmasını ve sistem tasarımını geliştirebilecek daha detaylı enformasyonu gerektirir. Hata ağacı analizi (FTA) ve Olay ağacı analizi (ETA) nicel risk değerlendirme için uygun örneklerdir.

Tepeden tabana ve tabandan tepeye risk değerlendirme metotları, arıza etkilerinin sonuç senaryolarını tanımlamak ve analiz etmek için kullanılır. Metodun seçimi, eldeki veri ve bilgiye, risk değerlendirmesinin sözleşme seviyesine, değerlendirilecek sistemi oluşturan sub-sistemlerin ve bileşenlerin ilişkilerinin karmaşıklığına ve sistemin teknik inovasyon seviyesine bağlıdır (BS EN 31010, 2008).

Şekil 2.11, geçmiş hata verilerini kullanarak kök arıza sebeplerini ve istenilen düşük risk seviyesine inebilmek için arıza sebepleri arasında hiyerarşiyi tanımlayan tepeden tabana risk değerlendirme sürecini gösterir. Tepeden tabana risk değerlendirme tüm kök arıza sebepleri belirlenene kadar devam eder. Nicel ve nitel risk

değerlendirmenin her ikisi de tepeden tabana değerlendirmede kullanılabilir fakat bunun için derin bir bilgi ve birçok geçmiş tecrübeye ihtiyaç vardır. FTA tepeden tabana risk değerlendirme metodu olarak uygun bir örnektir (BS EN 60300-3-4, 2008).

Şekil 2.11 : Yukarıdan aşağıya risk değerlendirme süreci (Url-2).

Tabandan tepeye risk değerlendirme yaklaşımı Şekil 2.12'de gösterilmiştir. Tüm muhtemele hata türlerini tanımlamak için sistemin detaylı dağılımına ihtiyaç duyan tümevarımsal bir risk değerlendirme metodudur. Hata türleri taban seviyeden tepe seviyeye doğru tanımlanır ve arıza sonuçlarının şiddeti ile arıza sıklığı değerlendirmesi yürütülür. Tabandan tepeye risk değerlendirmesi, tepeden tabana değerlendirmeye kıyasla aşağıdaki özelliklere sahiptir (Url-1):

Kesin hata modlarını ve sebeplerini analiz edebilir;

Bilgisayar programı ile kullanımı daha kolaydır;

Büyük ölçekli karmaşık sistemlerin risk değerlendirmelerinde kullanılmak için uygundur.

Şekil 2.12 : Aşağıdan yukarıya risk değerlendirme süreci (Url-2).

Risk değerlendirmesi için gerekli veri uygun bilgi kaynaklarından elde edilebilir. En yaygın bilgi kaynakları ve çeşitleri risk olasılığını hesaplamak için kullanılabilir. Bilgi, aşağıdaki kaynaklardan toplanabilir (BS EN 31010, 2008):

- Geçmiş arıza/kaza kayıtları (saha verisi)
- Pratik ve konuyla ilgili veri (olay verisi)
- Deneyler ve prototipler
- Mühendislik ve diğer modeller
- Uzman yorumu (uzman görüşü)

Çizelge 2.2 : Temel risk değerlendirme teknikleri**.**

Teknik	Risk Tanımlama	Sıklık	Olasılık	Şiddet	Risk Ölçülmesi
FMEA			-	-	-
FTA	-	+	+	+	+
HAZOP			-	-	
PHA		-	-	-	-
ETA	-			+	-
RBD		+	+	+	+

("+": yönteme ait karakteristik özellik, "-": yönteme ait olmayan özellik)

BS EN 31010 (2008) ve BS EN 60300-3-4 (2008), şu iki açıdan risk değerlendirme tekniğini seçme metodunu içerir: risk değerlendirme süreç aşaması ve risk seviyesini etkileyen faktörler. Çizelge 2.2 ve Çizelge 2.3, BS EN 31010 (2008) ve BS EN 60300-3-4 (2008)'den alıntılanmıştır ve 8 tipik risk değerlendirme tekniğinin tahmini sonuçlarını özetler. Çizelge 2.2 tipik risk değerlendirme tekniklerinin risk değerlendirme sürecinde uygulanabilirliklerini gösterir. Çizelge 2.3 ise bu teknikleri sistemin risk seviyesini etkileyen üç faktöre göre açıklar.

Çizelge 2.3 : Risk değerlendirme tekniklerinin hesaplanabiliriliği.

Teknik	Kaynaklar	Belirsizlik Derecesi	Karmaşıklık	Nicelik Hesaplama
FMEA	Orta	Orta	Orta	Orta
FMECA	Orta	Orta	Orta	Orta
FTA	Yüksek	Yüksek	Yüksek	Yüksek
HAZOP	Orta	Yüksek	Yüksek	Orta
RCM	Orta	Orta	Orta	Yüksek
PHA	Düşük	Yüksek	Orta	Düşük
ETA	Orta	Orta	Orta	Yüksek
RBD	Yüksek	Yüksek	Yüksek	Yüksek

Birçok risk değerlendirme tekniği geliştirilmiş ve birçok farklı endüstride kullanılmıştır. Bununla birlikte, sistem mühendisliği tasarım aşamasında risk değerlendirme metotları ve tekniklerinin kullanımı ile ilgili bazı zorluklar da mevcuttur. An (2005) risk değerlendirmedeki bazı zorlukları şu şekilde belirtir:

- Eldeki kaynaklar, veriler ve bilgiler çok sınırlıdır ve istatistiksel olarak yanlıştır;
- Sistem performansını etkileyen birçok tehdit, sistemin fonksiyonel davranışını değerlendirecek matematiksel modelin uygulanmasını zorlaştırır;
- Nicel risk değerlendirme, sistem tasarım analizinde asıl bir unsurdur fakat maliyetlidir ve doğru veri gerektirir. Dolayısıyla, risk değerlendirmesinin derinliğini ve kapsamını belirlemek oldukça zordur.
- Arıza sonuçlarının nicel risk değerlendirmesi yanlış veriden dolayı büyük belirsizlikler içerebilir;
- Nitel değerlendirme, birçok varsayım, tahmin, görüş ve yorumla birlikte birçok analitik tecrübeler gerektirir fakat değerlendirme sonuçları sıklıkla analiste bağlı olacak şekilde öznel olabilir.

2.5 RAMS Analiz Teknikleri

Bu bölümde RAMS yönetim sürecinin etkin desteklenmesi için geliştirilen bir kısım RAMS yönetim tekniği gözden geçirilmiştir.

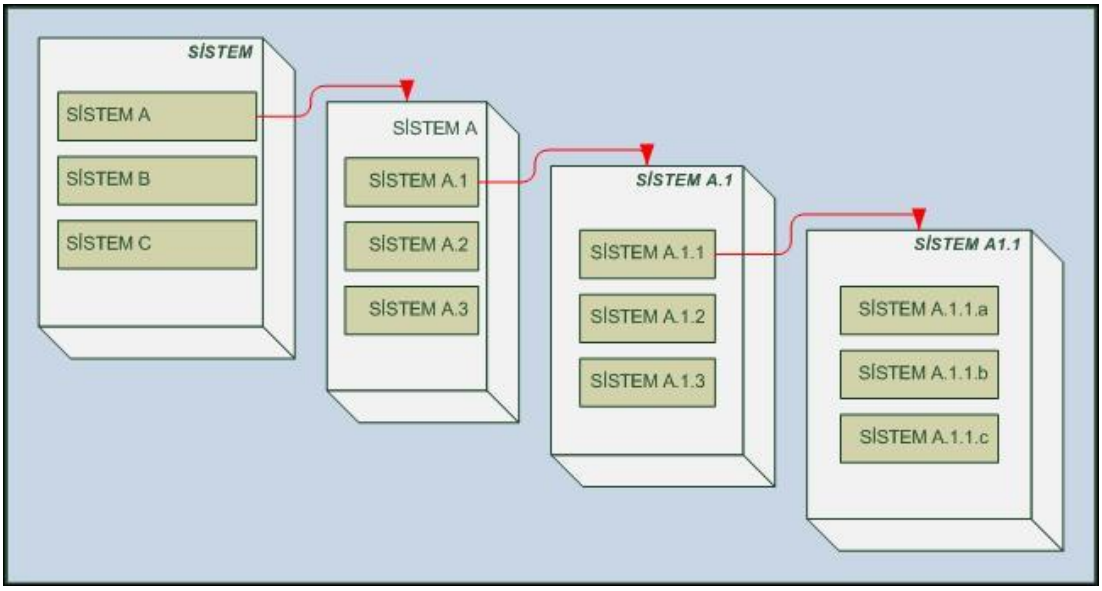
2.5.1 Fonksiyonel analiz

Fonksiyonel analiz arzu edilen sistemin performans ve kritik fonksiyonlarının tasarlanması ve anlaşılması için temel bir tekniktir. Fonksiyonel analizin, RAMS yönetimi ve sistem mühendisliğinde kullanılması gereklidir. Dolayısıyla fonksiyonel analiz, risk analizi ve RAMS yönetiminin temeli ve başlangıç noktası olup fonksiyonel davranışların analizinde kullanılmaktadır. Fonksiyonel analizin amacı sistem fonksiyonlarını ve performansını etkileyen temel bilgiyi sağlamak ve RAMS yönetiminin temelini tesis etmektir. Fonksiyonel analiz ayrıca spesifikasyon, modelleme, simule etme, doğrulama ve gerçekleme için de kullanılmaktadır. Bunla bağlantılı olarak fonksiyonel analiz genellikle sistemin fonksiyonel yapısını tasarlamak için kullanılan önemli bir etmendir. Fonksiyonel analiz genellikle şağıdaki iki yöntemi kullanmaktadır:

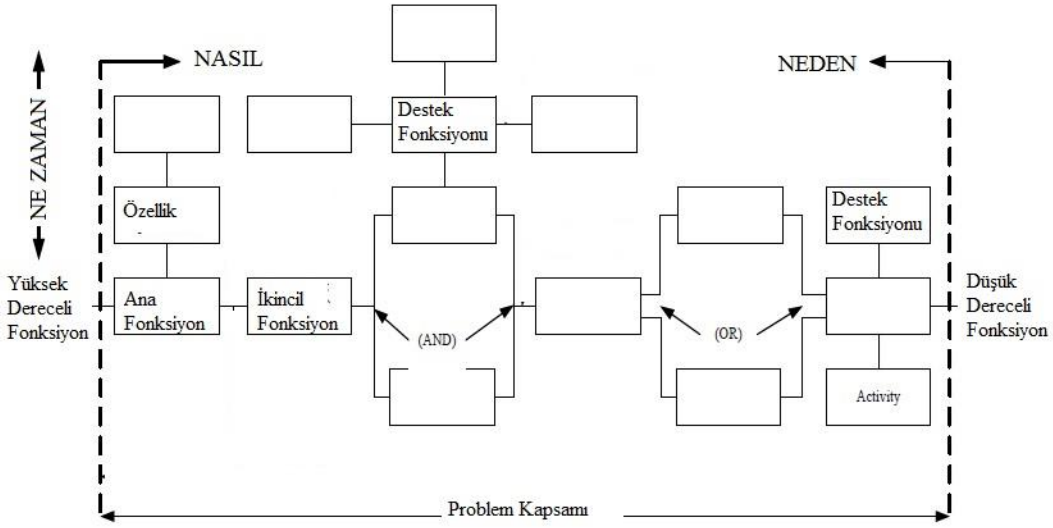
- Yapısal analiz ve Tasarım Tekniği (Structured Analysis and Design Technique)
- Fonksiyonel Analiz Sistem Tekniği (FAST)

SADT birçok endüstriyel alanda kullanıla gelmektedir. sistemin fonksiyonel davranışları ve arayüzünü anlayıp tarif etmek için tasarlanmış diyagramlı bir kavramdır. Bilgi akışı ve aktivitesini temsil eden bloklar ve bloklar arası ilişkiyi gösteren birçok oktan oluşup, Şekil 2.13‘te SADT için verilmiş bir örnek görülmektedir.

FAST Charles Bytheway tarafında 1964 yılında geliştirilmiştir ve birçok endüstriyel alanda kullanılmıştır. FAST fonksiyonel temsil ile mantık silsilesinin fonksiyonlarını betimlemek, önceliklendirmek ve bağımsızlıklarını sınamak için yaralı olabilir. Fonksiyonel problemlerin çözümünü yapamaz fakat sistemin temel karakteristiğini açıklayabilir. Şekil 2.14 Kaufmann tarafından 1982’de tasarlanmış FAST modelleme örneğidir.



Şekil 2.13 : SADT modeli.



Şekil 2.14 : FAST modeli.

2.5.2 Ön risk analizi

Ön risk analizi sistem seviyesinde tariflenmiş riskleri değerlendiren bir tekniktir. PHA'nın amacı muhtemel riskleri, onların neden faktörlerini, etkilerini ve risk seviyelerini tespit etmek ve tespit edilen riskleri kontrol etmektir. Ayrıca PHA, sistem tanımlama safhasında tüm muhtemel riskleri değerlendirici bir yöntem olmayı hedefler ve sistem gereksinimlerini P2nın sonuçları üzerinden belirler. Birçok modifiye edilmiş PHA bazen değişik aslar ile de kullanılmaktadır. Örneğin Hızlı Risk Değerleme (RRR) ve risk tanılama (HAZID).

PHA tekniği ilk olarak amerikan ordusunun 1960‘larda füze sistemlerinde emniyet risk değerlendirmei için kullanılmıştır.Daha sonra endütriyel alanlarda yaygınlamiştır. PHA tekniği genel olarak sistem mühendisliği prosesinde gereksinim analizi safhasında kullanılmıştır. sistem sınırlarından sonra da arayüz ve operasyonel bağlam tanımlanmıştır. PHA resmi olarak geşitiricisi olan MIL-STD-882 tarafından tanıtılmış ve duyurulmuştur. aslında ön tasarım safhasında kullanıldığında dolayı gross risk analizi olarak adlandırılmıştır.

PHA sistemin genel fonksiyonel davranışında risklere başlangıç olarak bir genel bakış sağlamaktadır. ayrıca genel olarak detaylandırılmamış ve spesifik olmayan geniş risk değerlendirmesi sağlamaktadır. Fakat, PHA düşük risk sistemlerinde total riski tamımlayıcı olarak uygulanmaktadır. Diğer yandan, uçak ve demiryolu gibi yüksek riskli sistemlerde, tim risk aralığının sağlanması için risk önceliklendirmesi yapılmaktadır. PHA sistemin konsept tasarım safhasına uygulanabildiği gibi alt sistemlere ve komponentlere de uygulanabilmektedir.

2.5.3 Hata türü ve etki analizi

Hata türleri ve etki analizi (FMEA) komponentleri belki de tüm sistem performansını etkileyen tüm potansiyel hata türleri ve hata etkilerini değerlendiren, emniyet ve güvenilirlik değerlendiren tekniktir. Ayrıca arıza önleme ve hata türlerinin etkisini azaltan bir yöntemdir. FMEA sistem tasarımında ve üretiminde veya sürecinde olabilecek tüm potansiyel hata türlerini tanımlayan, açıklayan, önceliklendiren ve kontrol eden bir tekniktir.

Daha önceleri FMEA, FMECA olarak bilinirdi. Buradaki “C” harfi sistemde arızanın kritik seviyelendirilmesinin kısaltması olarak kullanılmıştır. FMEA, FMECA ile eşanlamalı olarak kullanılmasına karşın fonksiyonu tamamen farklıdır. genel olarak FMEA bir arıza modunun etkilerinin şiddetini seviyelendirici olarak kullanılırken, FMECA arıza şiddeti yanısıra arıza etkisinin oluşma frekansının seviyelendirmesini de kapsamaktadır. arıza şiddeti ve frekansının kombinasyonu sistemin krtikliği ya da riski olarak bilinmektedir.

FMECA sistem tasarım prosesinde arıza analizi için kullanılan bir sistematik teknik idi ve genel olarak karmaşık sistem projelerinde sistem tasarım prosesinin temel bölümü olarak uygulanmıştır. FMECA amerikan ordusunda 1950‘lerde geliştirilmiş olup, ilk kullamım prosedürü 1950‘lerde “Mil-P-1629 olarak yayınlanmıştır.FMECA

yaygın olarak tüm potansiyel arızaların dikkate alındığından emin olmak amacıyla sistem konsept tasaarımıında güvenilirlik ve emniyet değerlendirmesi için kullanılmıştır.

FMECA konsept tarasrım fazında yüksek güvenilirlik ve emniyetle alternatif sistem tasarım çzöümlerinin bulunmasında kullanılabilir. ayrıca sistemin başarılı olması için tüm muhtemel arıza modları ve etkilerini refere etmeyi ve listelemeyi garanti eder. FMECA sistem gereknimlerinin test planı ve test kabul kriterlerini geliştirebilir ve sistem bakımının palnı, fonksiyonları ve aktivitileri için temel oluşturabilir. Son olarak, FMECA, RAMS değerlendirme için temel teşkil eder.

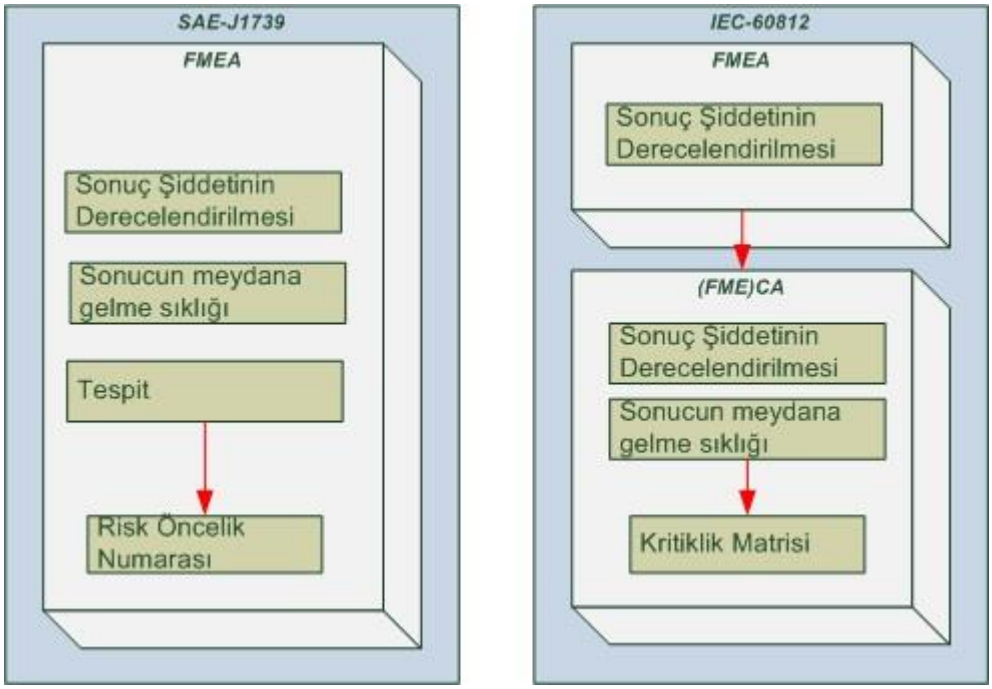
Aşağıda bulunan altı temel soru FMECA'nın etkin kullanımı için gereklidir:

- Bir sistem nasıl arıza verir?
- Oluşan arıza modlarının mekanizması nedir?
- Bir arıza modunun sonucu nedir?
- Bir arıza modunun emniyeti için etkileri nelerdir?
- Arıza modu nasıl tespit edilir?
- Arıza modu için tasarım nasıl desteklenir?

FMECA iki analitik yaklaşım methodu için uygulanabilir: alt-üst ve üst-aşağı yaklaşımları. alt-üst yaklaşımı sistem konseptinde karar almak için kullanılmaktadır. komponent seviyesinden, genel sistem seviyesine kadar uygulanmaktadır. üst-aşağı yaklaşımı ise bazen hardware yaklaşımı olarak bilinir. diğer taraftan, üst-aşağı yaklaşımı ana olarak tüm sistem yapısı ile alakalı karar verme işlemi öncesi fonksiyonel analizlerde kullanılmaktadır. analizler fonksiyonlar, önemli etkisi bulunan önceliklendirilmiş foksiyonel arızalar üzerinde tasarım çözümlerini seçme amacıyla odaklanmıştır. Fonksiyonel yaklaşım bir tam analiz olmamasına rağmen, emniyet fonksiyonlarında karar verirken , halihazırda bulunan bir sistemin problemli alanlarını belirlemede kullanılabilir.

Özet olarak, FMECA (1) tüm sistem döngüsü sırasında oluşabilecek bütün potansiyel arızların dikkate alınmasıyla, tasarım prosesi esnasında potansiyel arızayı geliştimek amacıyla yürütülen, FMECA tasarımı (2) üretim, bakım ve operasyon prosesi esnasında oluşabilecek problemlerim çözümü, FMECA prosesi, ve son olarak (3)

Potansiyel problemleri ve zayıf noktaları geniş proseslerde arayan, FMECA sistemi analizleri için kullanılmaktadır.



Şekil 2.15 : FMEA standartları arasındaki farklılıklar.

FMECA analizi için birçok standart vardır; örneğin MIL-STD-1629A (1980), BS IEC 60812 (2006) ve SEA-J 1739 (1970), fakat bunların analiz metodları birbirinden biraz farklı olduğunu Şekil 2.15'de göstermektedir. Tablo 3.4 ise FMECA analizlerine arıza modu uygulanmasında kullanılan üç standardın ana farklılıklarını özetlemektedir. Bu araştırma risk tanımı bakımından MIL-STD-1629A (1980) metodunu uygulayacaktır.

Çizelge 2.4 : FMEA standartları arasındaki farklılıklar.

Aşamalar	BS EN 60812	SAE-J1739
Analiz	FMEA ve FMECA	FMEA
Kritiklik Analizi	Şiddet ve Frekans	Şiddet, Frekans ve Tespit
Kritiklik	Kritiklik Derecelendirmesi	Risk Öncelik Numarası (RPN)
Kritiklik Belirleme	Hata Türü	Hata Sebebi
Şiddet ve Olma Sıklığının Önemi	Şiddet	Şiddet - Frekans
Hata Etkisi Analizi	Komponent ve Son Etki (end Effect) Seviyesinde	Hata Etkisi Seviyesinde

2.5.4 Hata ağacı analizi

Arıza ağacı analizi (FTA) bir hata olayına neden olabilecek veya emniyet, güvenilirlik, sürdürebilirlik ve maliyet ile ilgili sistem performansını etkilemesi muhtemel faktörlerin açıklanması, modellemesi, analizi ve değerlendirilmesi için kullanılan sistematik, çıkarımsal ve sembolik mantık analitik tekniğidir. FTA ayrıca bir arıza olayının emniyet değerlendirmesi ve güvenilirliğinin mantıksal değerlendirilmesi açısından en güvenilir tekniklerden bir tanesi olarak da kabul edilebilir.

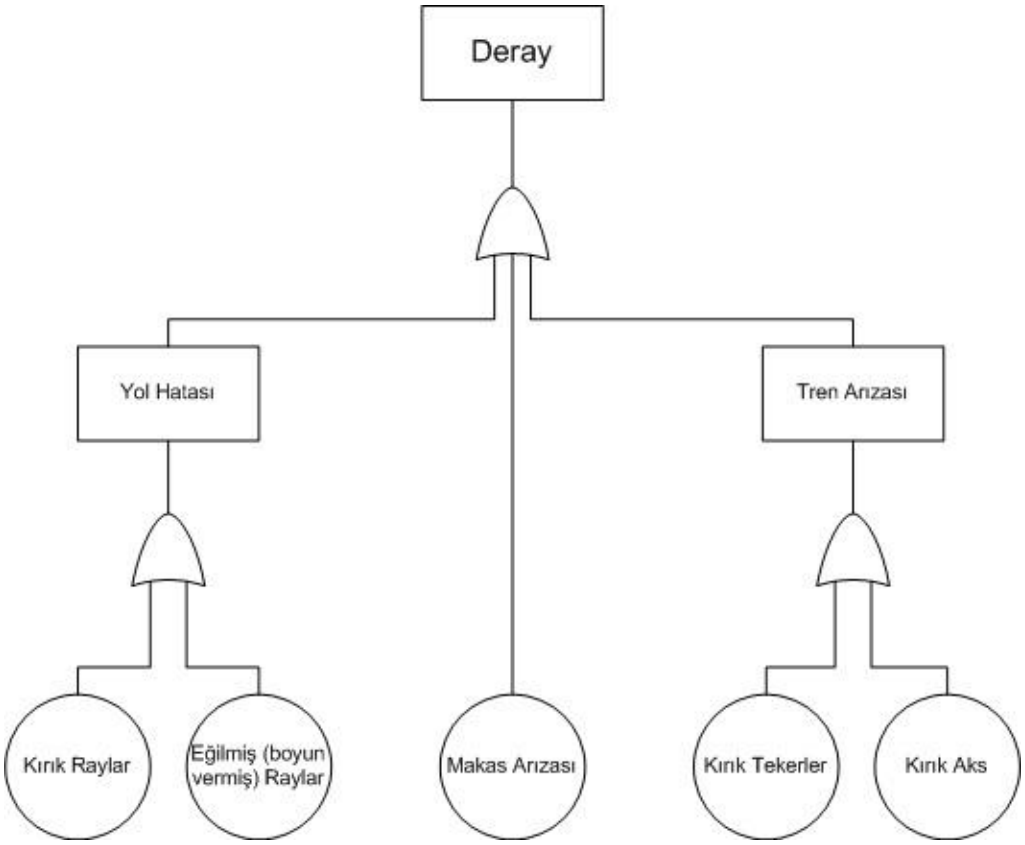
FTA, H. Watson ve Allison B. Meams tarafından 1962'de geliştirilmiştir. Bu ikili US Bell şirketinin ve Boeing şirketinin laboratuvarlarında çalışmış ve sonrasında FTA tekniğini silah sistemlerinde emniyet faktörlerini nicelemek için uygulamışlardır. İlave olarak, birçok endüstriyel alanda, örneğin; ticari uöak endüstrisi (1960'lar), ulaşım (1990'lar), kimya endüstrisi (1980'ler), nükleer güç endüstrisi (1970'ler) emniyet ve güvenilirlik değerlendirmelerini yaygın olarak FTA tekniği ile yapmışlardır.

FTA özellikle yıkıcı etkisi bulunan arıza etkileri olmak üzere, tüm arıza modlarına odaklanmıştır. Kapı, olaylar ve kesme setleri FTA'nın genel analitik elementleridir. matıksal diyagram, "VE" ve "VEYA" kapıları, FTA'nın analitik sonuçlarını teşkil etmektedir. Arıza etkileri kapılara girişi (input) göstermekte, kesme setleri ise sistem arızasına neden olabilecek arıza etki selerini temsil etmektedir. FTA, FTA'nın arıza analizinde yaşayabileceği limitasyonları aşmak için FMECA, Markov ve Olay ağacı analizi (ETA) ile beraber kombinasyon halinde kullanılabilir.

FTA sistem mühendisliğinin tüm proses evrelerine, konsept tasarım fazında, yetersiz bilgi ve data ile ilgili tasarım detaylarına bağlı olarak oluşan potansiyel tarasım problemlerini de kapsayacak şekilde etkin geliştirme için analitik bir teknik olarak uygulanabilir. daha önceki analitik aktiviteler, gelişen bilgi ve data ile daha da genişletilebilir. FTA ayrıca ürün tasarımı, çevre ya da operasyon, üretim ve operasyonel, bakım şartlarından kaynaklanabilecek potansiyel problemleri tanımlar ve değerlendirir.

Şekil 2.16 bir hızlı trenin deray olması üzerine oluşturulmuş bir FTA analiz örneğini göstermektedir. Norveç Demiryollarına ait Hızlı Tren Risk Değerlendirmesi Dökümanından (2012) alınan bu örnekte deray vakası, iki adet ara olay ve beş adet

temel olay VEYA kapısı ile bağlanmasından oluşmaktadır. Ara olaylar, en üst olayın temel sebeplerini göstermektedir. Temel olaylar ise ara ve ana olaya sebebiyet veren sorunların nedenlerini göstermektedir.



Şekil 2.16 : Tren deray olmasına ait hata ağacı modeli örneği.

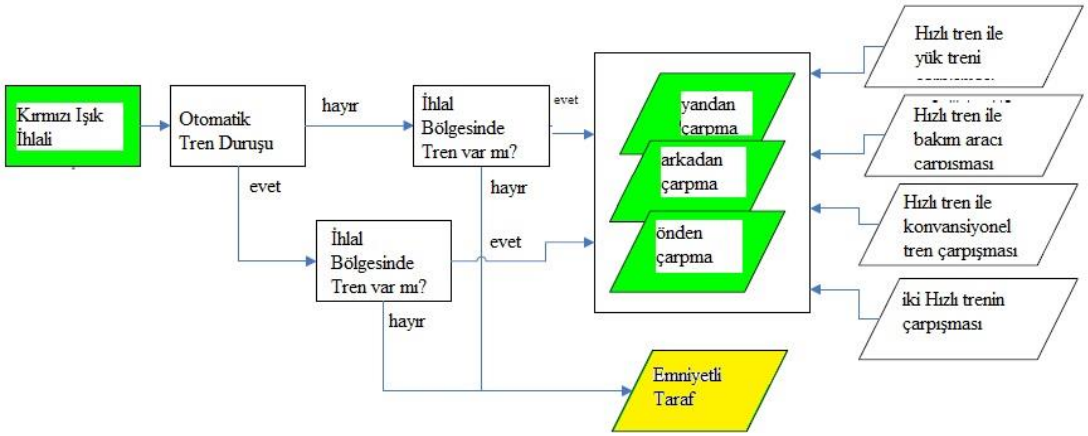
2.5.5 Olay ağaç analizi

Olay ağaç analizi (ETA) bir potansiyel arıza olayının sonuç senaryo analizindeki arızaların gelişimini tahmin eden tekniklerden bir tanesidir. ETA, mantık ağaç modeli grafiğini kullanır. Bu ağaç modeli arıza olayının emniyet sistemleri tarafından kontrol edilip edilmediğini belirleyen, ciddi hasarları temsil etmektedir. ETA başlayan bir olaydan birçok olası çıktıya (outcome) yol açabilir. Şekil 2.17'de herbir çıktı için bir olasılığı sağlayabilir.

ETA, Şekil 2.17'de gösterilen, çoklu karar yollarının belirlendiği bir karar ağacının ikili formundan oluşmaktadır. ETA, nükleer tesis emniyet çalışması olarak 1974'te WASH-1400 tarafından yayınlanmıştır. WASH-1400 bir nükleer güç tesisinin PRA'sının, ETA kullanılarak tariflenebileceğini göstermiştir. Fakat FTA'nın arıza analiz ağacı kullanılarak oluşturulsaydı çok karmaşık ve geniş olurdu. ETA, halen

FTA'yı bütünleştirmekle beraber analizleri daha yönetilebilir resimlere özetlemeyi sağlamıştır.

ETA genel olarak tüm risk değerlendirme çeşitlerinde uygulanabilir olmasına karşın etkin olarak, koruyucu unsur olarak çoklu koruyucuların bulunduğu kazaları modellemede kullanılır. ETA, Şekil 2.17'de Norveç Demiryollarından (2012) alınan bir örneğe yer verilmiştir. Şekil 2.17'de görüldüğü gibi bu model; birbirleriyle ilgili birçok kazaların başlangıç olaylarının belirlenmesinde oldukça etkilidir. Olay ağacı modeli; sıcaklık, basınç ya da tehlikeli madde salınımı gibi bir komponent arızası belirlenerek, başlatıcı olayın oluşturulması ile başlamaktadır. Olayların sonuçları birbirlerine bağlı olarak ortaya çıkmaktadır. Her bir yol FTA'nın uygulanması sırasında oluşacak olası bir oluşum ile tahsis edilir ve tüm olası çıkarımların olasılığı hesaplanabilir.



Şekil 2.17 : Trenin kırmızı ışık ihaline ait olay ağacı modeli örneği.

Şekil 2.17 bir olayın arıza sonuç senaryolarının anlizini ETA modeli ile göstermektedir. Arıza senaryoları ayrıca FMEA ile de gösterilerek, FTA analizi ile de arıza olasılığı değerlendirilebilir.

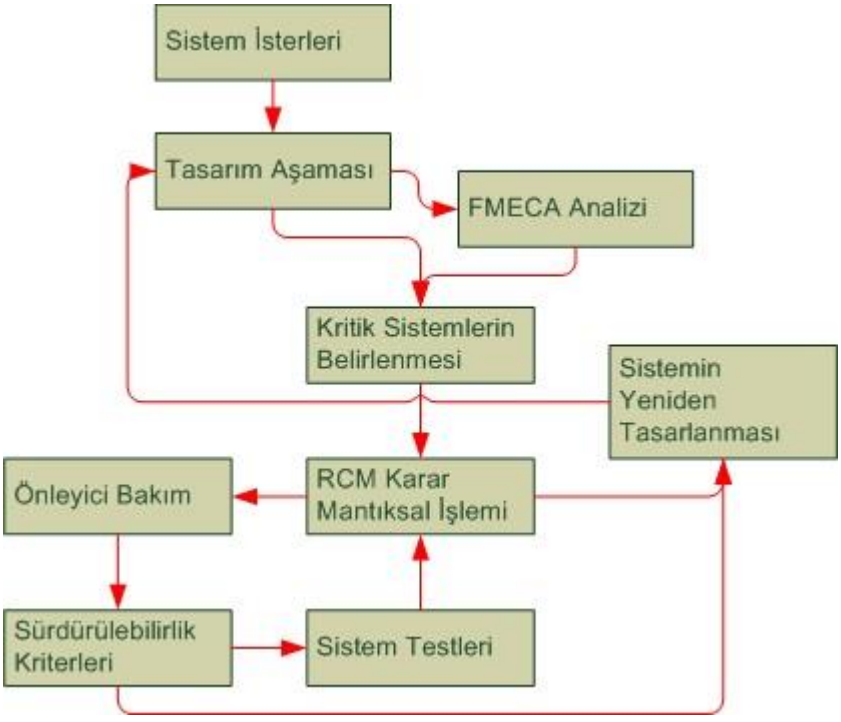
2.5.6 Güvenilirlik merkezli bakım (reliability center maintenance)

Güvenilirlik merkezli bakım, işletmesel amaçlar olan emniyet, uygunluk ve maliyetin sağlanmasında arıza yönetim uygulamalarının belirlenmesi ve sağlanması için mantıksal yapılandırılmış bakım analiz tekniğidir. arıza yönetim uygulamaları genellikle, bir arıza modunun sonuçlarını kontrol etmek için bakım stratejileri, operasyonel değişimler, tasarım modifikasyonları içermektedir. Fakat sistemin

emniyeti ve uygunluğunu korumak amacıyla efektif ve ekonomik bakım yöntemlerine odaklanır.

1960'ların başlarına kadar, önleyici bakım, periyodik değişim ve bakım gibi tüm bakım şemaları , bakım organizasyonlarının operasyonlar esnasında elde ettikleri deneyim ile planlanır ve uygulanırdı. Problemi çözmek için , RCM programı ilk önce ticari havacılık endüstrisi tarafından geliştirilmiştir. Bu program havacılık bakım-planlama dökümanı ATA MSG-3'e dayalıdır. RCM şimdilerde havacılık, yakıt endüstrisi, demiryolu, denizcilik gibi birçok geniş endüstriyel alanda kendini ispatlamış bir bakım metodolojisidir.

RCM; FMECA, FTA gibi analizler ile desteklenerek gerekli önleyici bakım yöntemleri, tasarım geliştirmeleri ya da gerekli emniyet, operasyonel sonuçlar ve potansiyel fonksiyonel arızaların azaltılması alternatiflerini oluşturucu, yapısal mantıklı karar prosesidir. RCM'nin tasarım sürecinde uygulanması genellikle en etkili olduğu kısımdır, fakat halihazırdaki bakım uygulamalarının geliştirilmesi için operasyon ve bakım aşamalarında da uygulanabilir.



Şekil 2.18 : RCM modeli örneği.

Şekil 2.18 sistem mühendisliği sürecinde FMECA ile beraber uygulanabilir RCM prosedürünü göstermektedir. RCM genellikle, önleyici bakım stratejileri ile risk değerlendirmesinin kontrol etmek için uygulanır.

2.5.7 Tehlike ve işletilebilme çalışması

Tehlike ve İşletilebilme çalışması (HAZOP) analizi, bir sistemin potansiyel tehlike ve işletilebilme problemlerini açılayan ve analiz eden sistematik bir değerlendirme tekniğidir. Organize, yapılandırılmış ve metodolojik bir proses kullanmaktadır.

Birleşik krallık Kimya endüstri enstitüsü, HAZOP'u 1970'de resmileştirmiştir. Kimyasal endüstri gibi emniyetin kritik olduğu birçok alanda yaygın olarak kullanılmaktadır. İlk olarak 1974 yılında Herbert G. Lawley, HAZOP tekniğini, HAZOP teknniğinin risk değerlendirmelerindeki pratiklerde nasıl kullanılacağını, kılavuz olarak yayınlamıştır.

Çizelge 2.5 : HAZOP örneği.

Parametre	Sapma	Sebep	Etki
Hayır / Değil (no)	Kapıların açılamaması	Mekanik arıza	Yolcu tahliyesinin mümkün olmaması
Fazla	Tren istasyona gelmeden kapılarının açılması	Araç bilgisayarı arızası	Yolcuların zarar görmesi ihtimali
Az	Bir kapının açık kalması	Mekanik Arıza	Trenden yolcu düşme tehlikesi

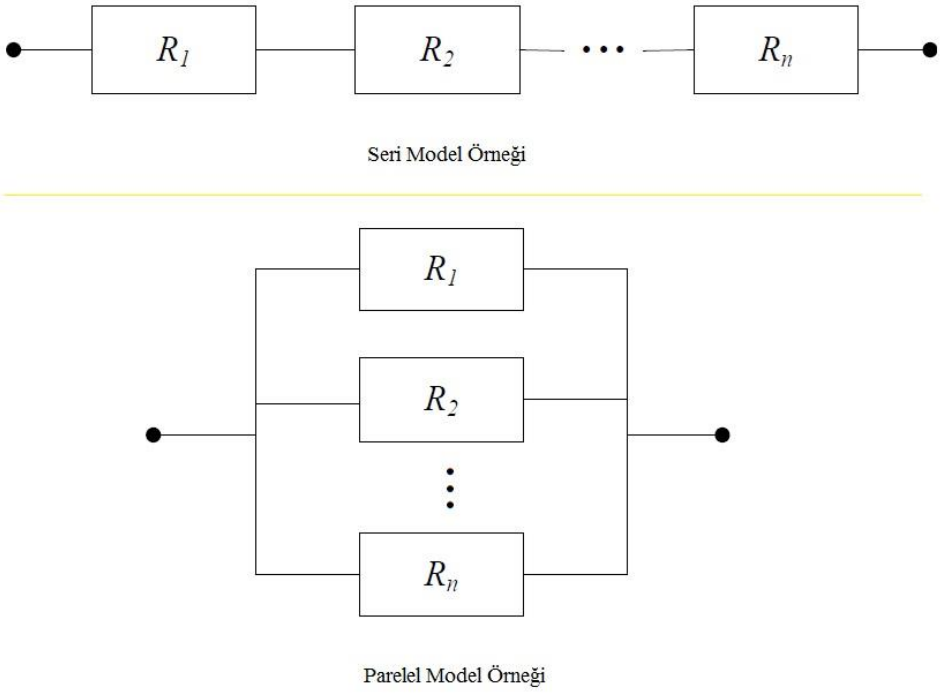
HAZOP, analistlere yardım etmek amacıyla; sistem tasarım amacından neyin saptığını bulmak amacıyla çeşitli kelimeler kullanmaktadır. Tasarım sapmaları bu kelimeleri kullanarak sorulan bir süreç ile açığa çıkarılmaktadır; Çizelge 2.5'te görüleceği üzere bu kelimeler "hayır/değil", "fazla", "az" gibi kelimelerdir. Bu kelimeler çalışmanın etkinliğini maksimize etmek için hayali-imgesel düşünceyi teşvik edici bir role sahiptir. HAZOP, işletmesel problemleri sorgulamak amacıyla, detaylı tasarım fazından sonra en uygun halini alır. Çizelge 2.5 platformlardaki tren kapılarının işletmesel problemlerini analiz için örnek HAZOP uygulamasını göstermektedir.

2.5.8 Güvenilirlik blok diyagramı (RBD)

Güvenilirlik blok diyagramı (RBD) matıksal bağlanmış sistem yapısının güvenilirliğini temsil eden grafiksel analiz tekniğidir. RBD blokları, sistemin başarı yollarını temsil eder. Nitel ve nicel analiz kullanımında çeşitli değişik seviyelerde oluşturulur.

RBD doğrudan sistem fonksiyonel diyagramında oluşturulur ve fonksiyonel yolları sistematik olarak temsil eder. Değişik tipte sistem konfigürasyonlarını açıklayabilir,.

Buna örnek olarak, Şekil 2.19'da seriler ve paraleller gösterilmiştir. RBD sistem performans parametrelerinin varyasyonları ve mübadelelerini analiz etmekte kullanılır ve güvenilirlik ve uygunluk değerlendirmesi için model oluşturur. Fakat, RBD sebep-sonuç analizi gibi belirli bir arıza analizinde kullanılmaz ve sistem performansının olasılık modeli için uygulanır.



Şekil 2.19 : RBD modeli örneği (EN 61078, 2006).

2.5.9 Bulanık mantık analizi (FLA)

Bulanık küme (FS) etkin bir şekilde sorunları çözme teorisidir. Sorunları kesin olarak tanımlanmış ve yetersiz bir yöntem aracılığıyla bilgi işlenir. Bu yöntem, sistemlerdeki uzman görüşünü geliştirir ve belirsizlikleri kontrol eder. FS çakışan yönetim ortamında karar verme için mükemmel bir araç sağlar. Bu etkili derece belirsiz ve muğlak bilgilerden daha güvenilir sonuçlar elde etmek için risk değerlendirme sürecine entegre edilebilir. (Url-1).

FS 1920'lerde Lukasiewicz tarafından geliştirilmiştir. Zadeh ise 1969 yılında matematiksel bulanık mantık formel bir sistem haline FS genişletmiştir. Bu setleri üyelik dereceleri kullanan mantık bir dalıdır. Örneğin, düşük risk, makul risk veya yüksek risk buna örnektir. Bulanık mantık belirsiz, dilsel terimler kümesi tanımlar.

Bu terimler, tek bir değerle sabit, ama FS teorisi matematiksel mantık tarafından araç sağlar değildir. (An, 2013).

İki dinamik teknik, yani Bulanık Karar Fonksifonu (FDF) ve bulanık çıkarım (FI), karar verme ve modelleme için sağlanmaktadır. FDF karar vericinin tercihlerini teyit etmek için karar amaçları ve kısıtlamaları birleştiren bir araçtır. Dil kuralları FI için şeffaflık sağlar. İstenilen bu tesis bulanık kural tabanlı sistemde tanımlanan girdi ve çıktılardan arasında bir eşleme sağlar. Yukarıdaki iki bulanık teknikler aracılığıyla bir risk değerlendirme aşamaları Şekil 2.20'de gösterilmiştir.

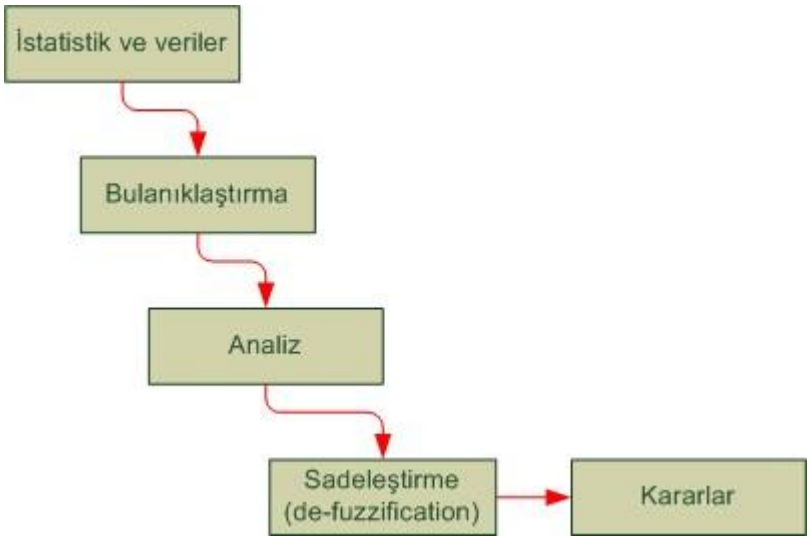
Yeni bulanık risk değerlendirme modeli ilerleyen aşamaları aşağıdaki şekilde açıklanabilir: (Url-1)

- Adım: Araştırın ve risk ile ilgili veri ve bilgileri kontrol edin;
- Adım: Risk kriterleri belirleyin;
- Adım: risk kriterlerini ölçün;
- Adım: iki ana eylemin FDF'na risk kriterleri girdisini işleyin: toplama ve bulanıklaştırma;
- Adım: Önerilen FI sistemi içine toplanan kriterler girdisini işleyin;
- Adım: Eşleşen net değeri (Durulaştırma) içine bulanık sonuç dönüştürün.

2.5.10 RAMS ihtiyaç paylaşımı

RAMS ihtiyaç paylaşımı düşük sistemlerin (örneğin altsistemler) tasarımı için gerekli bir bölümüdür. İhtiyaç paylaşımının amacı sistem düzeyinde RAMS ihtiyacını elde edebilen ve fonkisyonel davranışların analizi ile yapılan tahsisin en etkili fiziksel tasarım mimarisini bulmaktır. Bir RAMS tasarımı gerektiğinde güvenilirlik, kullanılabilirlik, sürdürülebilirlik ve güvenlik için her performans karakteristiğinin tahsisi gereklidir ve dört RAMS karakteristiğinin tahsisi benzerdir (BS EN 60300-3-1, 2004).

RAMS ihtiyaç paylaşımı alt sistemlerin karmaşıklığına bağlıdır, karşılaştırılabilir alt sistemler ile deneyime dayalıdır. Gereksinimlere ilk tasarım aşamasında ulaşılamazsa tasarım süreci tekrar tekrar yapılmalıdır. Tahsisi de sık sık karmaşıklık, kritiklik, operasyonel profili ve çevre koşulu gibi düşünceler temelinde yapılır (Ebeling, 2010).



Şekil 2.20 : Bulanık mantık analiz modeli aşamaları.

RAMS ihtiyaçları paylaşımı normalde erken tasarım aşamasında yapılırken mevcut bilgiler yetersiz ise, tahsisin fonksiyonel analizi yoluyla sürekli olarak güncellenmesi gerekmektedir. Düşük sistem seviyelerinde RAMS gereksinimleri tahsisi sistem ürün tanımı aşaması için gerekli ve amaçları aşağıda belirtilmiştir (BS EN 60300-1,2014):

- Tüm sistem için RAMS gereksinimleri uygulanabilirliğini onaylamak ,
- Düşük seviyelerde doğrulanabilir RAMS tasarım gereksinimlerini belirlemek,
- Alt sistemler ve bileşenler için açık ve uygulanabilir RAMS gereksinimlerini belirlemek.

Genel olarak, RAMS Sistem Analizi aşağıdaki basamaklar ile icra edilmektedir:

- Bilinen ve RAMS özellikleri ile ilgili mevcut veya hazır değerlendirilmiş bilgi tasarım alanlarını belirlemek;
- Uygun ağırlıkları saptamak ve;
- Üst düzey RAMS ihtiyacına katkılarını belirlemek.

MIL-HDBK-388B (1998) aşağıda belirtildiği şekilde RAMS ihtiyaç paylaşımı için dört teknik sağlar:

- Eşit ayırma tekniği;
- ARINIC (Aeronautical Radio, Incorporated) ayırma tekniği;
- Nesnel teknik fizibilitesi ve;
- AGREE (Advisor Group on Reliability of Electronic Equipment) tekniği.

Eşit ayırma tekniğinin tüm alt sistemlerin güvenilirlik ihtiyacını eşit olarak ayıran bir ayırma tekniği olduğunu belirtmek gerekir. Altsistemleri tasarlamak için ulaşılabilir bir bilgi olmadığında genellikle kullanılır. Mevcut tek altsistemlerin başarısızlık oranı olduğunda ARINIC tekniği kullanılır. Paylaştırma sistem yetmezliğine katkıda bulunan altsistemin ağırlık faktörü ile yapılır. Fizibilite tekniği alt sistemleri ile ilgili tasarımcıların uygun tecrübe ve bilgisine göre kullanılır ve bu teknikler sistem karmaşıklığı, çevre ve operasyon gibi başarısızlık oranı üzerinde durur. Son olarak, AGREE tekniği altsistemin karmaşıklığı ve altsistemlerin neden olduğu tüm sistemin başarısızlığı ile sistem güvenilirliği gereksinimlerini ayırır. Karmaşıklık, bir alt sistemin oluşturduğu hata oranı üzerinden tüm sistemin oluşturduğu hata oranı ile hesaplanabilen alt sistem ve katkı içeren bileşenlerin sayısı olarak uygulanabilir.

2.5.11 Güvenilirlik büyüme değerlendirmesi

Güvenilirlik Büyüme Değerlendirmesi (RGA) başarısızlık mekanizmasının sistematik ve kalıcı kaldırılması yoluyla güvenilirlik performansının geliştirilmesi için uygulanır. RGA, sistemin tasarım değişiklikleri ile zamanla güvenilirlik performansını değerlendirmeyi amaçlamaktadır. RGA sistemi, sistem prototipi için test-fix-test-fix döngüsünün gerçekleştirilmesi yoluyla gerçekleştirilir. Literatürde birçok güvenilirlik büyüme modelleri vardır ancak Duane ve Güç Kanunu modeller genellikle kullanılır (MIL-HDBK-189C, 2011).

Duane modeli grafiksel güvenilirlik büyümesini analiz etmek en sık kullanılan modeldir. Model J.T. Duane tarafından 1964 yılında geliştirildi ve hızlı, basit ve kolay anlaşılır bir modeldir. Duane modeli 'log-log kağıt' üzerinde çizilen zaman işletim zamana karşı sistemin MTBF yaklaşık düz çizgi olarak temsil edilir şekilde güvenilirlik büyüme bir deterministik yaklaşım kullanır (MIL-HDBK-781A, 1986).

Güç kanunu modeli yani AMSAA (Army Material Systems Analysis Activity) modeli L.H. Crow tarafından 1970 yılında geliştirildi. Güç kanunu modeli büyüme paterni Duane modeli ile aynıdır, ancak Güç Kanunu modeli istatistiksel tabanlıdır. Güç Kanunu modelinin istatistiksel yapısı Weibull başarısızlık oranı fonksiyonlu Homojen Olmayan Poisson Süreci (NHPP) modeline eşdeğerdir. Bunun birkaç avantajı vardır çünki NHPP parametreleri istatistiksel olarak katı temelleri olduğu tahmin edilerbilir; güven aralıkları elde edilebilir; ve Fit Testi İyiliği (GFT) uygulanabilir (Ebeling, 2010; BS EN 61164, 2004).

2.5.12 RAMS güvenilirlik (reliability) testi değerlendirmesi

BS EN 60300-3-5 (2001) tahmin, uyum ve karşılaştırma testleri gibi güvenilirlik testlerini sınıflandırır. Güvenilirlik tahmin testi, garanti maliyetler ve güvenilirlik tahmini için güvenilirlik ölçülerini değerlendirmeyi amaçlamaktadır. Karşılaştırma testi, aralarındaki güvenilirlik performans ölçüleri tahmin etmek yerine işlevsel olarak benzer iki sistemin güvenilirlik performansı arasında A sisteminin B sisteminden daha güvenilir olup olmadığına karar vermek için karşılaştırır.

Uygunluk testi (veya ispat testi) belirtilen parametreler ile uyumu tanımlamak için kullanılır. Testin sonucu ya "kabul" (uygun) ya da (uyumsuz) "reddedildi" şeklinde karar verilir. Test istatistiksel hipotez testi ilkesine dayanmaktadır. Güvenilirlik ispat testi sistem güvenilirlik tasarımının kabulünün kararı için önemlidir. Genel olarak, iki güvenirlik ispat yöntemleri raylı sistem testlerine uygulanabilir: kesik sıralı testi ve sabit süre testi (BS IEC 61124, 2012; MIL-HDBK-781A, 1986).

2.5.13 RAMS sürdülülebilirlik (maintainability) testi değerlendirmesi

Sistem mühendisliği tasarımı sırasında performans sistemi testi parçası olarak, bir idame testi idame gereksinimlerinin sistem tasarımı ile karşılandığını doğrulamak için yapılır. BS EN 60300-3-10 (2001) standardı idame testini iki kategori olarak sınıflandırır: idame yeterlilik testi ve idame ispat testi.

İdame yeterlilik testi, ilk çalışmalarda ve prototipin geliştirilmesinde prototipin müşterinin ihtiyaçlarını karşıladığını doğrulamak için yapılabilir. Bu test şart değildir ancak idame şartlarının yerine getirilmiş olduğundan emin olmak için çok etkili bir yöntemdir. İdame ispat testi gelişmiş prototipin idame şartlarının gerçekleştirmesini doğrular bir testtir. Test değerlendirmesi istatistiksel hipotez testi teorisine dayanmaktadır ve nihai tasarım tamamladıktan sonra uygulanır.

2.6 Özet

Bu bölüm RAMS sistemleri yönetimi ile ilgili kuramsal mühendislik altyapısı kurmak için genel kavramlar, yöntemler ve sistemler mühendisliği teknikleri sunar. Demiryolu RAMS yönetiminin uygulanması için sistemler, risk ve sistem yaşam döngüsü temelli yaklaşım, bu bölümün odak noktasıdır. Bu nedenle, bu bölümde

demiryolu RAMS yönetiminin başarılı bir şekilde uygulanması ile ilgili tanımlar, süreçleri, yöntemleri ve teknikleri tartışmıştır.

Bu bölümde öncelikle, bir sistemin başarıyla gerçekleşmesi amacıyla mühendislik kavramları kurmak için sistem / sistemler ve sistem mühendisliğinin birkaç tanımlarını gözden geçirildi. Sistem mühendisliği yönetim faaliyetleri üç şekilde gözden geçirilmiştir: RAMS özellikleri, tehditler ve araçlar, yönetim perspektifinde RAMS sistemleri anlayışına yardımcı olmak. Bununla birlikte, sistem mühendisliği raylı sistemler mühendisliği uygulamalarında üstesinden gelmek için birkaç zorlukları olan nispeten yeni bir mühendislik kavramdır. Buna göre RAMS yönetimini raylı sistemler mühendisliğine entegre etmek için daha çok çalışmaya gerek olduğu ortaya çıkar.

Bu bölüm RAMS sistemleri yönetiminde şu bakış açılarını kazandırmayı amaçlamıştır: Bunlar; Risk yönetimi, RAMS performans özelliklerinin tanımı, RAMS performansını etkileyen tehlikeli faktörlerin değerlendirilmesi ve tehdit unsurlarını önleme çalışması olarak sıralanabilir.

Bu bölümde ayrıca risk değerlendirmesini harekete geçirmek ve risk tanımı ile yetersiz bilgi nedeniyle problemlerin üstesinden gelmek için çeşitli RAMS risk değerlendirme yöntemleri araştırılmıştır. RAMS yönetimini desteklemek için tipik değerlendirme teknikleri çeşitli incelenmiş ve tartışılmıştır.

3. FMEA & FTA TEKNİKLERİYLE RİSK DEĞERLENDİRİLMESİ

3.1 Giriş

Raylı sistemler ve uçak gibi görev ve emniyet kritik sistemlerde, mühendisler sistem performansı için bir tehdit oluşturabilecek tüm potansiyel tehlikelerin kontrolünü dikkate almak zorundadır. nitekim, tehlikeler için risk değerlendirmesi, RAMS yönetiminin ana konusudur. Demiryollarında tehlikeler, hata sonucu, hata şiddeti ve sıklığı birleşimi ile belirlenir. Bu tehlikeler, risk düzeyini belirlemek için, nitel nicel ya da yarı-nicel yöntemlerle değerlendirilir. Hata şiddeti, niteliksel bir değerlendirme parametresi olarak, aşağıdan yukarıya doğru bir yaklaşım yöntemi ile belirlenir. Hata frekansı ise bir nicel değerlendirme parametresi olarak, yukarıdan aşağıya doğru bir yaklaşım yöntemi ile değerlendirilir. Bu nedenle, raylı sistemler sistemlerinde risk değerlendirmesi, yukarıda belirtilen yöntemlerle sağlanan birçok risk değerlendirme tekniklerini gerektirir (Url-1).

Birçok risk değerlendirme teknikleri geliştirilmiştir ve bu teknikler görev ve emniyet kritik sistemlerde geniş bir uygulama alanı bulmuştur. Raylı sistemler sektörü de uzun süre boyunca raylı sistemler tehlikelerinin risk değerlendirmelerine uygun çeşitli tekniklerin uygulanmasını irdelemiştir. Risk değerlendirme tekniği için yapılan çalışmaların çoğu, risk değerlendirmesi tekniklerinin bireysel uygulamaları üzerinde durmuşlardır. Ancak, bu bireysel uygulamalar, tüm sistem mühendisliği sürecinde risk değerlendirmesinin kesin analitik hedefleri ile uyuşmamış olabilir. Bu yüzden, çeşitli risk değerlendirme tekniklerinin kombinasyonu gerekli olmuştur, ancak pratik uygulama yöntemleri verilmemiştir. Bu bölümde, sistem mühendisliği tasarım aşamasında, belirlenen analitik hedefleri, mevcut bilgi ve verilere göre, risk değerlendirme teknikleriyle birleştiren bir yöntem anlatılacaktır.

Bu bölümde; kısa girişten sonra, risk değerlendirmesi FMEA-FTA tekniklerinin birleştirilerek modellenmesi işlenecektir. Daha sonra bu iki tekniğin sistem mühendisliği sürecinin genel olarak tüm aşamalarını kapsayacak şekilde risk değerlendirme aşamaları anlatılacaktır.

3.2 Risk Değerlendirme Modelinin Oluşturulması

3.2.1 Raylı sistemlerde risk değerlendirme tekniği

İşletmesel hedeflere ulaşmak için tasarlanan RAMS özellikleri performansını tehdit eden tüm riskler, RAMS yönetiminin odak noktasıdır. Bu risk yönetim sistemi, niteliğine uygun süreçler ve tekniklerle desteklenir. Raylı sistemlerde birçok doğal riskler tespit edilmiştir ve raylı sistem geliştirme projelerinden kaynaklanan sorunların, daha en başından, yani sistem konsept tasarım aşamasından itibaren sürekli iyileştirilmesi gerekmektedir. Raylı sistemlere ait riskler, yaralanma veya yolcu yaşam kaybına neden olabilecek büyüklükte bir potansiyele sahiptir. Bu nedenle, raylı sistemlerde risk değerlendirmesi uygun teknik ve süreçlere sahip bir sistematiğe ihtiyaç duyar ki bu dolayısıyla sistem mühendisliği tasarım aşamasında, olası tüm riskleri başarılı bir şekilde kontrol altında tutabilecektir.

Halihazırda, açık ve etkili bir şekilde bir demiryolu riskleri değerlendirmek için birçok teknikler üzerinde çalışılmaktadır. Önceki bölümde incelendiği üzere bunlara örnek olarak; Hata Ağacı Analizi (FTA), Olay Ağacı Analizi (ETA), Hata Türü ve Etkileri Analizi (FMEA), Hata Tütü, Etkileri ve Kritik Analizi (FMECA), Tehlike ve İşletilebilme Analizi (HAZOP), Bulanık Mantık Analizi (FLA) verilebilir. Ancak, risk değerlendirme tekniklerinin sistem mühendisliği sürecine uygulanması henüz sağlanmıştır değildir. Tipik bir risk değerlendirme tekniği genellikle mevcut sistem mühendisliği süreci fazında gereken çok özel analitik amaç tarafından geliştirilmiştir. Bu teknikler, önceki bölümde belirtildiği gibi belirli doğal özelliklere sahiptirler. Bu nedenle, risk değerlendirme teknikleri uygun analitik hedefler, veriler ve mevcut bilgiler ve sistem tasarım aşaması için kullanılabilir olacaktır.

Raylı sistemlerde artan karmaşıklık, kendine has riskli doğası ve bilgi kaynaklarının sınırlı sayıda olması, çeşitli analitik yöntemler ve teknikler gerektirir. Bu, uygun gerekli risk değerlendirme tekniklerini birleştirmek için esas teşkil eden bir durumdur. Bu nedenle, FMEA ve FTA tekniklerin birleşimi önerilmiştir ve demiryolu risk değerlendirmesi için temel teknik olarak uygulanması aşağıdaki gibi tarif edilmiştir.

3.2.2 FMEA ve FTA risk değerlendirme modelleri

Önceki bölümde, FMEA ve FTA tekniklerin özellikleri ayrıntılı olarak incelenmişti. Bu bölümde ise FMEA ve FTA birleşimine olan ihtiyacı göstermek için analitik hedefleri, uygulamaları, avantajları, dezavantajları tekrar gözden geçirilecektir.

FMEA risk değerlendirmesi için yararlı bir tekniktir ve raylı sistemleri etkileyen hata sonuçlarına neden olabilecek sistemleri detaylı arıza analizi için etkin bir şekilde kullanılmıştır.

FMEA'nın analizi prosedürü tüm potansiyel hata türleri ve sistemin etkilerini tanımlamak için temel bir mühendislik tasarım süreci olarak da uygulanabilir. Ancak, FMEA'nın büyük ölçekli raylı sistemlerde olduğu gibi çok fonksiyonlu ve emniyetli karmaşık sistemlerin risk değerlendirmesinde aşması gereken birçok zorlukları vardır. Bu teknikte, sistem mühendisliği tasarım aşamasında kusurları veya zayıf noktalarını yargılamak için sistem elemanlarının birbirleriyle olan ilişkilerinde nitelik ve mantıksal ifade zorlukları bulunmaktadır (BS EN 60812, 2006).

FMEA; birçok yedekleme yapıları ile çeşitli hiyerarşi seviyeleri olan bir sistemin analizi için uygulandığında çok karmaşık hale gelir ve hatta yanlış anlaşılma veya hataları neden olur. FMEA bireysel ve grup olarak incelenen hata türleri veya nedenleri arasındaki ilişkiyi etkili bir şekilde temsil edemez. Bu yüzden, sistem tasarımı sürecini yeterince desteklemekte zorluklar olacaktır. Ayrıca, FMEA'daki bir noksanlık; sistem mühendisliği tasarım bileşenleri tanımlarında açıkça görülür. Bununla birlikte, FMEA bu eksiklikleri ortadan kaldırılabilir ve daha fazla mantıksal sistem bileşenleri arasındaki ilişkiyi göstermek için iki veya daha fazla farklı tekniklerin entegrasyonu ile tamamlanmaktadır. Bunlara örnek olarak, FTA ve ETA verilebilir. FTA ise FMEA entegrasyonu için en sık tavsiye edilen yöntemlerden birisidir (BS EN 60300-1, 2004).

FTA, hata ağacının bir nicel ve nitel minimal kümesi temsillerini sağlayarak ve mantıksal ve grafiksel hata ağacı inşa ederek tehlikeli başarısızlık sonuçlarını kestirebilmek için düşük seviyeli arıza nedenlerini etkin bir şekilde takip edebilir. FTA, özellikle önemli emniyet kazalarına direkt olarak yol açan tekil hata noktalarının senaryolarını modellemek için yararlı bir tekniktir. Bu nedenle, FTA emniyet ve izleme fonksiyonları tanımlanmasında ve tasarımında kullanılabilir.

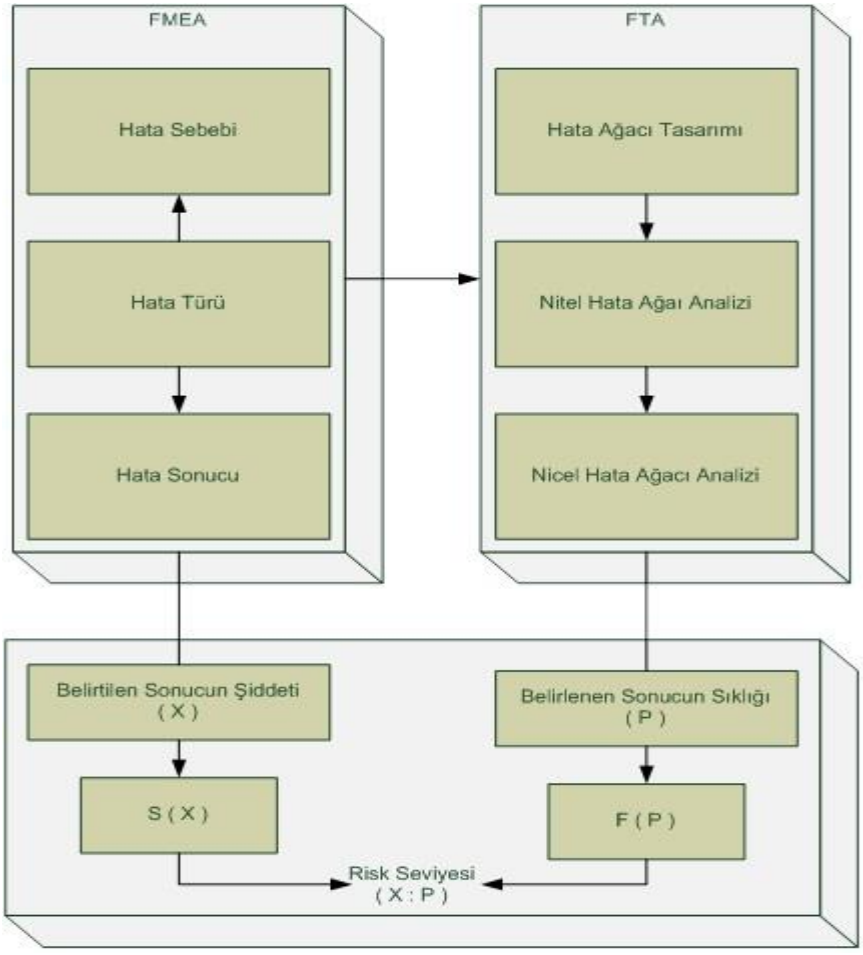
FTA, hata nedenleri mantıksal analizi yoluyla nicel değerlendirme için en sık kullanılan bir tümdengelim tekniğidir. Bununla birlikte; FMEA ise başarısızlık sonuçları nitel değerlendirilmesi için kullanılan sistematik bir tümevarım risk değerlendirme tekniğidir. Sistem mühendisliği tasarım süreci çeşitli risk değerlendirme yöntemleri gerektirir. Etkin bir mühendislik tasarım hedeflerine ulaşmak için nitel, nicel veya yarı-nicel değerlendirmeler de dahil olmak üzere bütün tümevarım veya tümdengelim yaklaşımları bunlara örnektir. Bu nedenle, FMEA ve FTA'nın birlikte ele alınması ile sistem tasarım aşamasına bağlı olarak, tüm analitik gereksinimleri sağlamak için yararlı bir risk değerlendirme yöntemi oluşturabilir (Gofuku, 2006).

Şekil 3.1 : Demiryolu risk değerlendirme kavramı.

3.2.3 FMEA & FTA temelli risk değerlendirme modelleri

Önceki bölümde belirtildiği üzere, raylı sistemlerde risk bir hata sonucu ve tanımlanır; frekans veya olasılık şiddeti derecesi kombinasyonu ile belirlenir. Raylı Sistemlerde hata şiddeti ve hata sıklığı düzeylerini belirlemek üzere risk değerlendirmesi için aşağıdaki dört soru için net cevaplar bulunması gerekir (Şekil 3.1). Bu nedenle, raylı sistemlerde risk seviyelerini saptayan bir süreç önerilebilir. Her adımi verilen soruları tatmin edecek şekilde yanıtlayacak uygun risk değerlendirme teknikleri seçimini yapmak durumundadır.

Şekil 3.2'de FMEA ve FTA'ya dayalı risk değerlendirme tekniği (Şekil 3.1 modeline uygun formda) gösterilmiştir. FMEA tekniği, tüm olası hata türleri, bu hataların etkileri & nedenleri ile hata sonuçları & nedenleri senaryo geliştirme gibi sistem elemanlarının nitel hata analizi için kullanılır.

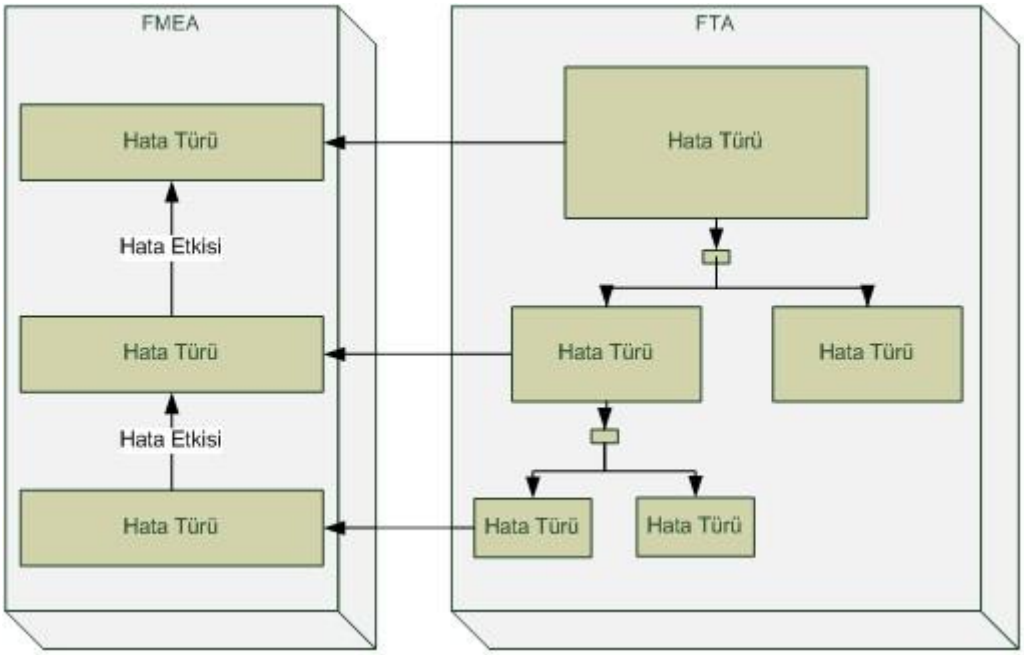


Şekil 3.2 : FMEA – FTA modellerinin birleşimi ile risk değerlendirme kavramı.

Diğer yandan FTA, hata nedenlerinin mantıksal analizi yapılırken, hata sonuçlarının nicel analizi için kullanılır. Bu hata nedenleri, hata ağacının mantıksal yapıları, Bool

Cebri kuralları, geliştirilen hata senaryoları ve yukarıdan aşağı yaklaşımı tarafından analiz edilir; dolayısıyla 3. Sorunun cevabı aranır.

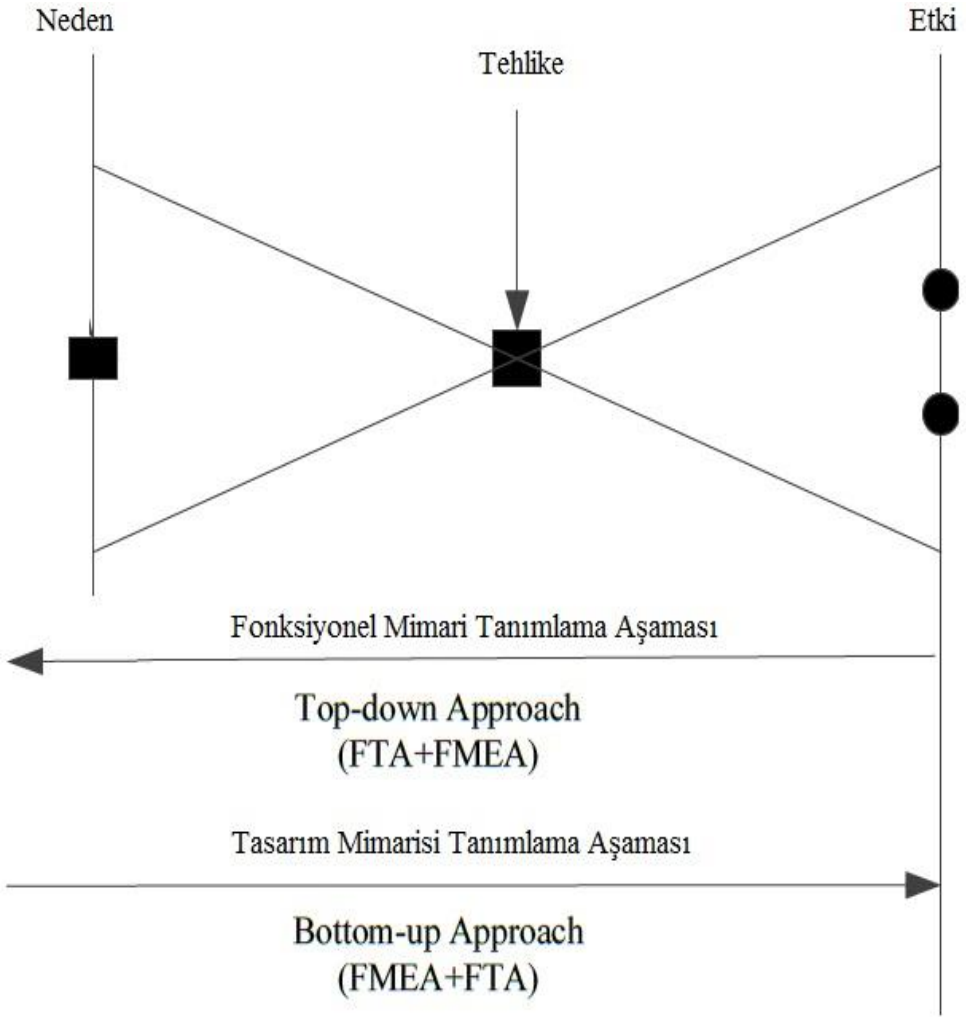
Şekil 3.3, herhangi bir risk analitik noktasında, FMEA ve FTA tekniklerinin birbirleriyle bütünleşme yöntemini göstermektedir. İlk olarak, tüm sistem elemanları için FMEA analizi yapılır ve bu sonuçlar hata ağacı oluşturulmasında etkin bir şekilde kullanılır. Sonra, Bool Cebri kuralları ve olasılık kanunları kullanılarak hata ağacının nitel ve nicel analizleri gerçekleştirilir. Bu kombinasyon, Şekil 3.5 ve Şekil 3.6 'da gösterildiği gibi, sistem mühendislik tasarım aşamalarında farklı şekillerde uygulanabilir.



Şekil 3.3 : FMEA ve FTA modellerinin birlikte değerlendirilmesi.

FMEA ve FTA kombinasyonu modeli Şekil 3.4'de gösterildiği gibi sistem mühendisliği tasarım aşamasında bağlı olarak yukarıdan aşağıya bir yaklaşım ve aşağıdan yukarıya yaklaşım şeklinde, iki yöntemle uygulanabilir. Alt sistem tanımı aşaması alt sistemlerin fonksiyonel mimarisi tanımlamak için yapılır. Buna göre, hata analizi emniyet ve bunların izleme fonksiyonlarının tanımlanması ve hesaplanması amacıyla objektif kök hata nedenlerini izlemek için yukarıdan aşağıya bir yaklaşım olarak yapılır. Komponent tanımlama aşaması fiziksel tasarım mimarilerini tanımlamaktır. Böylece, hata analizi hata sonucu senaryoları izlemek için nicel olarak aşağıdan yukarıya bir yaklaşım şeklinde yapılır. Şekil 3.4, bir hata tehlikesi için FMEA-FTA yöntemleriyle risk değerlendirme yaklaşımını açıklar. Ancak, Şekil

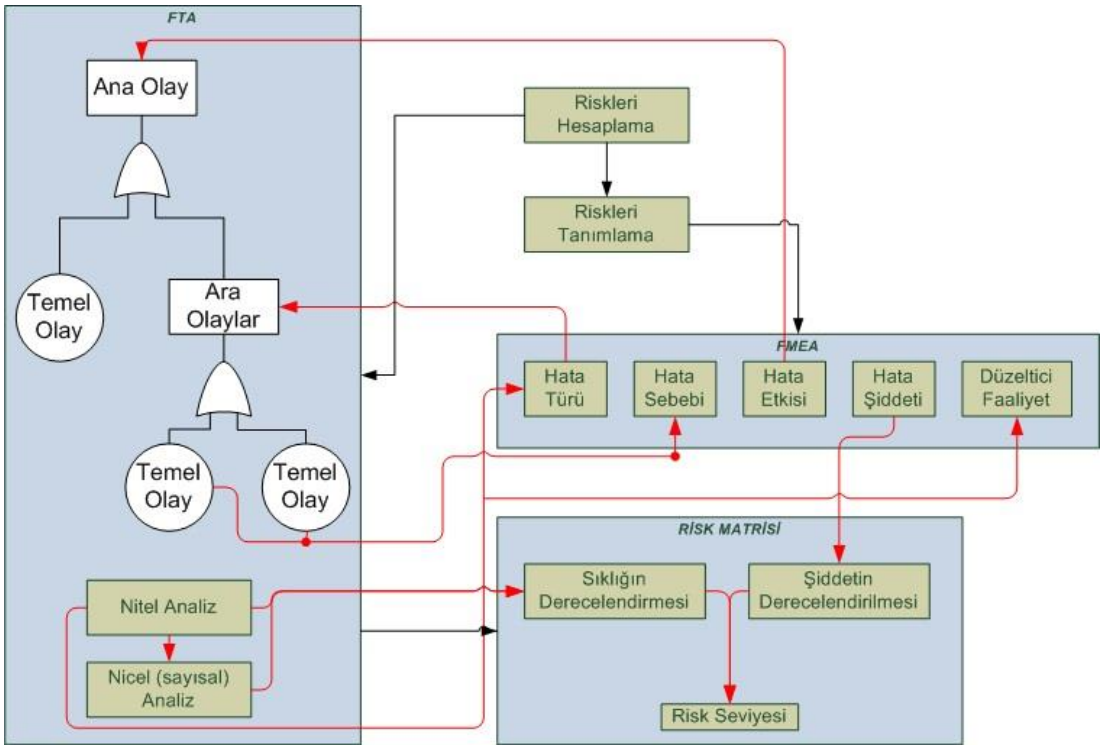
3.4'de gösterildiği gibi, FMEA-FTA modellerinin kombinasyonu aynı anda iki yaklaşım için de uygulanabilir. Bu nedenle, her tasarım aşamasında, hata sonuçları ve nedenleri analizi tek seferde uygulanabilir.



Şekil 3.4 : FMEA ve FTA modellerine dayalı risk değerlendirme yaklaşımları.

3.2.3.1 Top-Down model

Şekil 3.5'de entegre FTA-FMEA yaklaşım modelinin prensip şeması gösterilmiştir ve bu model sistem mühendisliği sürecinde yukarıdan aşağıya (backward/geriye doğru) risk değerlendirmesi için uygulanır. Bu modelde, FTA, hata türünün kök sebebini irdelemek için kullanılan ana değerlendirme tekniği olarak aktif rol oynar. Bunun yanında, FMEA ise olası tüm hata türleri, nedenleri, etkileri ve sonuçlarını detaylı olarak inceler.



Şekil 3.5 : FTA – FMEA tabanlı yukarıdan aşağı risk değerlendirme modeli.

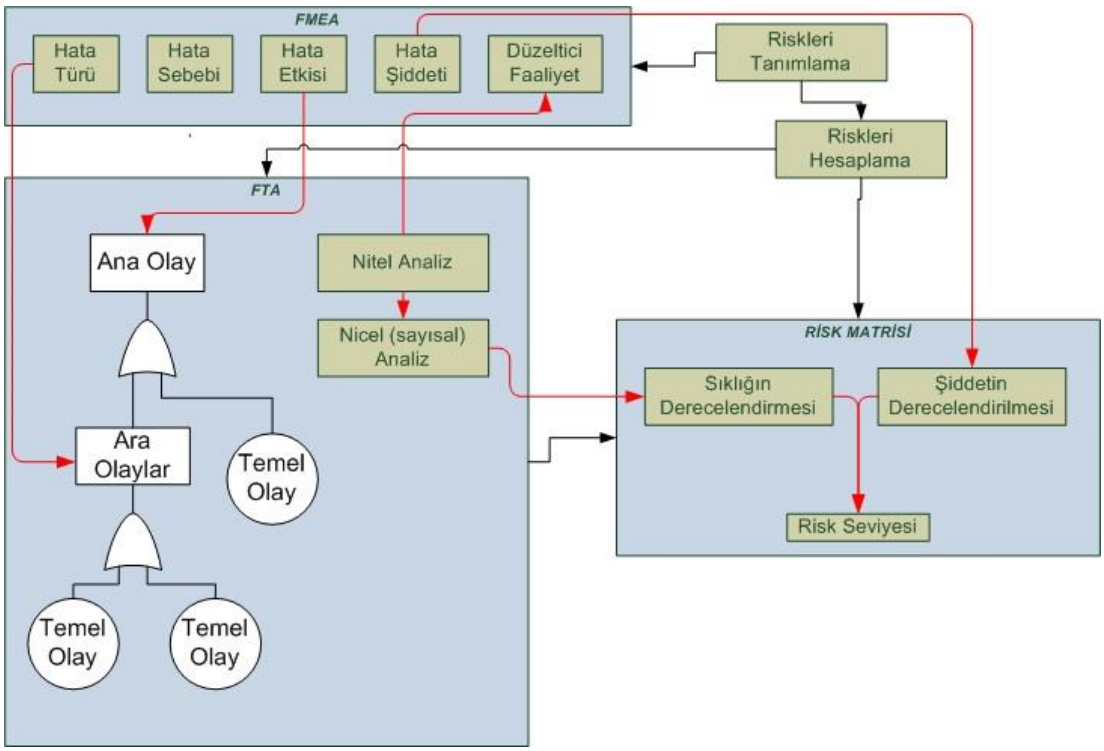
FTA-FMEA modeli tasarımında öncelikle bir ana olay (top event) seçilmelidir. Ana olay çeşitli analitik yöntemlerle belirlenebilir. Bunlara örnek olarak; ön tehlike analizi (preliminary hazard analysis), tehlike ve işlerliğini analizi (HAZard and OPerability analysis), geçmiş tehlike kayıtları, farklı tasarım aşamalarındaki emniyet gereksinimleri gibi yöntemler verilebilir. Ama seçilen ana olaylar FMEA tarafından analiz edilmelidir, çünkü FMEA bu riskleri değerlendirmek için gerekli tüm analitik öğeleri belirleyebilir ve bir hata ağacının oluşturulmasını ve hata sonucu senaryoları modelleme destekler.

Şekil 3.5 de gösterildiği gibi, önemli alt olaylar sistem tasarım aşamasında nitel hata ağacı analizi tarafından tanımlanır ve daha sonra sistem düzeyinde FMEA analizi yapmak için hata türleri olarak uygulanır. Fonksiyonel mimariyi kurmak için dengeleme karşılığı çok önemlidir. Emniyet fonksiyonlarının ve emniyet izleme fonksiyonlarının belirlenmesi için büyük bir avantaja sahip olan bu model; alt sistemlerin uygun fonksiyonel yapısına ait tasarım ve analizini destekleme konusunda çok yararlıdır.

3.2.3.2 Bottom-Up model

Aşağıdan yukarıya (forward/ileriye doğru) risk değerlendirme modeli için FMEA-FTA yaklaşımı, raylı sistemlerin tasarım mimarisine ait hata analizinde kullanılan etkin bir uygulamadır (Şekil 3.6). Bu modelde, FMEA ana analiz tekniği olarak ele alınır. FTA ise sistem tasarımı ve hata nedenleri nicel değerlendirilmesi mantıksal yapısını sağlayarak daha detaylı hata nedenleri nitel ve nicel analiz için FMEA analizini destekler.

FTA analizi, hatası sebeplerini tespit etmek için herhangi bir sistem tasarımı aşamasında hata etkilerinin şiddetinin belirlenmesi için yapılan nicel bir hesaplamayı içerir. Şekil 3.6'da gösterildiği gibi hata modları, hata ağacında ara olaylar olarak kullanılmaktadır. Bu modelde FTA, sistem tasarımı ve bakım politikasını desteklemek için hata nedenlerini telafi edecek koşullar sağlayacak daha kapsamlı uygulamadır. Bu yaklaşım modeli, tasarım belirleme aşamasında komponent mertebesinden sistem mertebesine kadar uygulanabilir.



Şekil 3.6 : FMEA - FTA tabanlı aşağıdan yukarı risk değerlendirme modeli.

RAMS yönetimi, sistem mühendisliği sürecinde tüm potansiyel tehlikeleri ve ilgili risklerin değerlendirilmesi ve bu risklerin azaltılarak ortadan kaldırılması veya risklerin kontrol edilebilir seviyelere indirgenmesine uygun bir uygulama belirlemek için gerekli temel bilgiyi sağlayacak bir sürece sahip olacaktır. Etkin bir risk

değerlendirme sürecinde RAMS yönetimi raylı sistemlere ait riskleri en aza düşürür hatta mümkünse ortadan kaldırır. Rasyonel kararlar verilmesini sağlamak amacıyla raylı sistem riskleri tüm yönleriyle ele alır. Bu nedenle, hata türlerinin (ALARP) risk seviyesini mümkün olduğunca düşük kabul edilebilir ve uygulanabilir (As Low As Reasonably Practible) düzeye çekmek için risk değerlendirme süreci yeterli yöntemleri ve teknikleri kapsar (Umar, 2010).

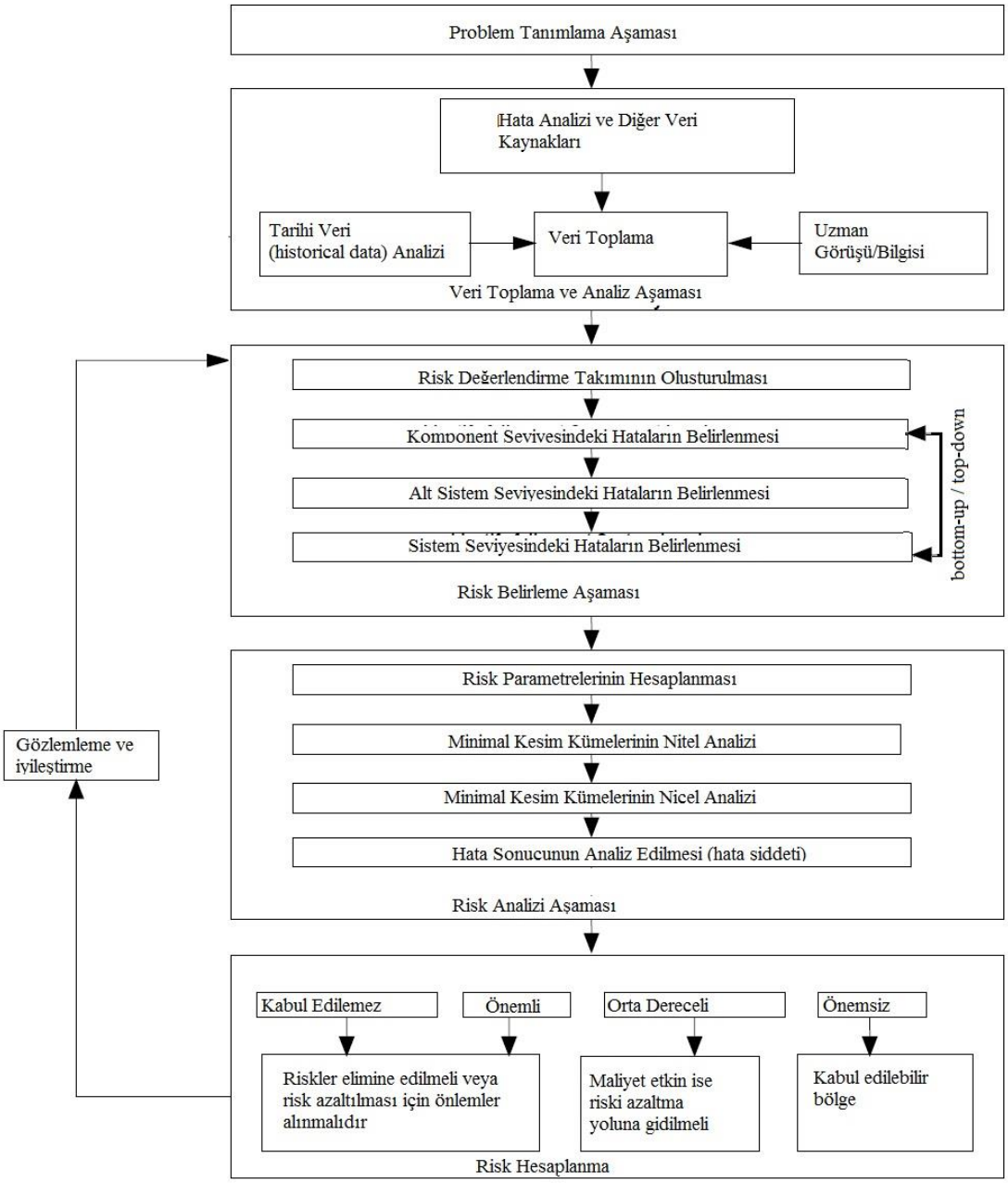
RAMS yönetimi ihtiyacını belirlemek için tavsiye edilen FMEA ve FTA ortaklığına dayalı raylı sistem risk değerlendirme süreci, geçmiş olaylar ve benzer sistem kazalarından toplanan bilgi ve verilerin karşılaştırılması ve analizi yoluyla RAMS ihtiyaçlarının belirlenmesi şeklinde başlar. RAMS isterleri, yasal düzenlemeler, ürün yaşamı, hata türleri yanı sıra olası elde edilen hata sonuçları ile kurulur. Ancak, yetersiz risk bilgileri ve veri kaynağının yüksek karmaşıklık içermesi; risk değerlendirmesi uzmanları ve sistem mühendisliği tasarımı aynı anda risk değerlendirmesi niceliğini karşılamak için raylı sistem risk değerlendirme tekniklerinin kombine kullanımını gerektirebilir. Önemli hata sonuçları daha sonraki analizler için kullanılır. Bunu kullanmak için aşağıdan yukarıya veya yukarıdan aşağıya doğru çalışma modelleri benimsenebilir (Umar, 2010).

3.3FMEA Analizi

3.3.1 İster tanımlama aşaması

Bu süreç, fizibilite çalışmalarıyla, raylı sistem mühendisliği projesinde RAMS yönetim etkilerinin ihtiyaçlarını ve bunların belirlenmesini içerir. Ayrıca sistem sınırları, işletmesel kriterler, ortamlar ve yaşam döngüsü sürecinin tanımı ile RAMS tasarım çözümleri ve bunların kabul performans kriterlerini tanımlar. RAMS tasarım çözümü ve kabul kriterleri farklı sistem hiyerarşisi seviyeleri ile tanımlanmalı ve belirtilmelidir. Şekil 3.7 de gösterildiği gibi; sistem seviyesi, alt sistem seviyesi ve sistem komponent seviyesini içerir. Bu aşamada, tespit edilmesi ve tanımlanması gereken öğeler şunlardır: (BS IEC/ISO 26702, 2007)

- Tasarım kısıtlamaları (mevzuat ve standart düzenlemeleri gibi)
- İşletmesel senaryolar ve RAMS etkinliğinin ölçüsü
- Sistem sınırları, işletmesel ortamlar ve yaşam döngüsü süreci;
- Fonksiyonel gereksinimler, deterministik veya olasılıklı RAMS gereksinimleri;
- RAMS kabul performans kriterleri.



Şekil 3.7 : FMEA ve FTA modelleri ile önerilen risk değerlendirme süreci.

3.3.2 Risk parametreleri ve ölçüm matrisi aşaması

RAMS gereksinimleri belirlendiğinde; yani, tasarım ve kabul kriterleri ile sistem ve işletmeye ait kriterler oluşturulduğunda, tanımlanan risk değerlendirmesi için gerekli olan veri ve bilgiler toplanır; risk parametrelerine ve risk değerlendirme sürecine girdi sağlamak için analiz edilir.

Risk değerlendirme sürecinin ikinci aşaması, toplanan verilerin ve bilgilerin analizi ile başlar; risk parametresi ve risk değerlendirme matrisi indeksi aralığını belirlemek ve risk değerlendirme sürecinde bir girdi sağlamak için kullanılabilir. Şekil 5.7 de gösterildiği gibi veri ve bilgiler; tarihsel verileri, test verileri, uzman görüşü ve diğer bilgi kaynaklarından derlenmiştir.

Toplanan veri ve bilgi analizlerinin amaçları, geçmiş kazalar ve benzer sistemlerin tüm olası riskleri açık bir anlayış tanımlamak ve toplanan verilerden bilgi kümesi elde etmektir. Verilerin istatistiksel doğru olmaması veya yetersiz kalması durumunda, veriler uzman görüşü veya mühendislik kararları ile belirlenebilir. Tespit ve analiz edilen bilgi ve veri göstergesi parametre sıralamasını belirlemek ve niteliksel bir indeksleme matrisi için kullanılabilir (Umar, 2010).

Birçok ortak istatistiksel teknikler kendi içsel eksikliklerin üstesinden gelmek ve pekiştirmek için kombine edilebilir. Örneğin, istatistiki veri ve bilgi analizi, insan tecrübesi ve mühendislik bilgilerinin analizi, kavramsal haritalama gibi olgular bilgi ve 'know-how' toplamak için kullanılabilir. Bu tekniklerin iki veya daha fazlası kendi içsel çevre özelliklerinin üstesinden gelmek için uygulanabilir (An, 2013).

Toplanan verilerden belirlenen bilgi ve veriler; indeks (dizin) sıralamasını belirlemek ve niteliksel bir indeksleme matrisi oluşturmak için kullanılabilir. Raylı sistemlerdeki risk tanımı gereği, önerilen FMEA-FTA temelli risk değerlendirme modeli iki risk indeksi parametresini gerektirir; bunlar: hata şiddeti parametresi ve arıza sıklığı parametresidir. Bu hata bileşenlerinin sonuçlarını ve alt sistemler üzerindeki etkilerini belirlemek ve aynı zamanda raylı sistem seviyesinde risk düzeylerini belirlemek için bir değerlendirme matrisi gerekmektedir (BS EN 50126-1, 1999).

3.3.2.1 Hata şiddet parametreleri

Bir hata sonucunun hata şiddeti parametresi (Failure Severity Parameter); sistemin hata sonucunun olası büyüklüğünü bir bütün olarak anlatır. Çizelge 3.1 de anlatıldığı

gibi önemsiz düşük (marjinal), kritik ve yıkıcı şeklinde tanımlanan kelimeler ile ifade edilebilir. Demiryolu sisteminin hata sonuçları; insan, çevre ve işletme hizmeti olmak üzere üç koşulda değerlendirilebilir. Çizelge 3.1, demiryolu risk değerlendirmesinde önemli olan tüm hata sonuçlarının olası büyüklük derecelerini; yani hata şiddet parametrelerini göstermektedir (BS EN 50126-1, 1999).

Çizelge 3.1 : Hata şiddet parametreleri (severity).

Seviye	Şiddet Kategorisi	İşletmeye Etkisi
4	Yıkıcı	Sistemin 1 hafta devre dışı kalması / Trenin raydan çıkması
3	Kritik	Sistemin 1 gün devre dışı kalması (işletme anında giderilemeyen hata)
2	Düşük	Sistemin 1 saat devre dışı kalması (işletme esnasında giderilebilen hata)
1	Önemsiz	Sistemin 20 dakika devre dışı kalması (anında müdahale ile giderilebilen hata)

3.3.2.2 Hata sıklık parametreleri

Çizelge 3.2, risk seviyesini ölçmek için mümkün olan tüm hata sonuçlarının hata frekans parametrelerinin (Failure Frequency Parameter) sınıflandırılmasını açıklar. Uluslararası standartlar ve literatürde genellikle önerilen sınıflandırmalar; sık, muhtemel, ara sıra, uzak, imkansız ve olağanüstü olarak ve Çizelge 3.2'de görüldüğü gibi belirlenir. Bu parametrelerin sayısal aralıkları ise 100/yıl ve 10-6/yıl arasında tanımlanır (Kim, 2008).

Çizelge 3.2 : Hata sıklık parametreleri (probability).

Seviye	Kategori	Tanım	Sıklık (1/yıl)
A	Sık	Büyük ihtimalle olması beklenen	100'den fazla
B	Muhtemel	Birçok kez tekrarlanacak	1 ; 100
C	Ara sıra	Birçok kez tekrarlanma ihtimali bulunan	10^{-2}; 1
D	Uzak	Sistem işletmede olduğu sürece (life cycle) birkaç kez olması beklenen	10^{-4} ; 10^{-4}
E	İmkansız	Olma ihtimali bulunmayan ancak istisnai olarak olması beklenen	10^{-6} ; 10^{-4}
F	Olağanüstü	Olma ihtimali bulunmayan ve olmaması beklenen	10^{-6}'dan az

3.3.2.3 Risk seviyesi

Risk düzeyinin en yaygın şekli Çizelge 3.3'de gösterildiği gibidir. BS EN 50126-1 (1999) standardı, sinyal sistemi için bu tabloyu önemsiz tahammül edilebilir, sakıncalı/istenmeyen ve kabul edilemez şeklinde sınıflandırarak tanımlar. Çizelge 3.3, türetilmiş risk düzeyinin nitel tanımlayıcı kategorilerini düşük, makul, olarak uygulanabilecek (As Low As Reasonability Practible) şekilde göstermektedir.

Çizelge 3.3 : Risk seviyesi parametreleri (risk).

Seviye	Risk Sınıfı	Risk Kontrolü
R1	Kabul edilemez	Risk giderilmeli
R2	Sakıncalı	Risk, mümkünse giderilmeli
R3	Tahammül edilebilir	Risk kontrol altında tutulmalı
R4	Önemsiz	Kabul edilebilir risk

Risk değerlendirmesi matrisi, yatay eksende FFP (Failure Frequency Parameter); dikey eksende ise FSP (Failure Severity Parameter) içinde seviyelerini içerir (Çizelge 3.4). Bu tabloda, demiryolu risk düzeyini belirleyen risk hesaplama matrisi gösterilmektedir. Her dizin parametresi karşılıklı buluştuğu nokta, bir hata sonucuna ait risk seviyesi olduğunu göstermektedir. Örneğin; Çizelge 3.4'de gösterildiği gibi, FFP seviyesi: sık ve FSP seviyesi: önemsiz ise; risk seviyesi istenmeyen (yüksek riskli) olarak belirlenmiştir. FFP seviyesi: olağanüstü ve FSP: felaket ise risk seviyesi önemsiz olarak belirlenmiştir (BS EN 50126-1, 1999).

Çizelge 3.4 : Risk hesaplama matrisi.

Hata Sıklıkları	A	R2	R1	R1	R1
	B	R3	R2	R1	R1
	C	R3	R2	R2	R1
	D	R4	R3	R2	R2
	E	R4	R4	R3	R3
	F	R4	R4	R4	R4
		1	2	3	4
		Hata Şiddeti			

3.4 FTA Analizi

Risk tanımı genellikle fonksiyonel mimari kurulduktan sonra yapılır. Bu nedenle, daha önceki bölümde tarif edildiği üzere SADT (Structured Analysis and Design Technique) veya FAST (Functional Analysis System Technique) gibi fonksiyonel blok diyagramları, olası risklerin diğer toplanmış veri ve bilgiler ile tanımlanması

için gereklidir. Risk tanımlama, farklı sistem hiyerarşi seviyelerinde tüm potansiyel hata türleri, hata nedenlerini ve hata etkilerini tanımlayan bir süreçtir. Örneğin, komponent seviyesinden alt sistem seviyesine kadar bu süreci sistematik bir şekilde belirler. Risk tanımlama; tüm sistem düzeyinde performansını etkileyen arıza sonuçlarını ve nedenlerini belirler daha sonra da onların iki modelini kurar. Bu nedenle; risk tanımlama, işletme gerekleri, fonksiyon ve tasarım tanımı süreçleri olmak üzere üç işlem adımında gerçekleştirilir. İşletme gerekleri (operasyonel) tanım aşaması büyük riskler onaylamak için yapılır. Fonksiyonel tanımı riskleri tanımlamak ve karşılaştırmak için yukarıdan aşağı yaklaşımı ile yapılır. Tasarım tanımlama ve sentez aşaması ise önceki aşamalarda tespit edilen risklerin aşağıdan yukarıya yaklaşımı güncelleştirilmesi ile yapılır. Risk tanımlama, hata türlerinin tanımlanmasından, bu hataların etkilerinin ve nedenlerinin analizinden ve son olarak bunların hata etkisi ve neden senaryolarında oluşmaktadır.

Bu süreç aşamasında; beyin fırtınası, kontrol listesi ve HAZOP (HAZard and OPerability analysis) gibi tipik risk değerlendirme teknikleri, demiryolu risklerini açıkça belirlemek için FMEA ile birlikte kullanılabilir.

Risk tanımlama başlangıçta sistem düzeyinde başlamıştı ve sürdürülerek komponent seviyesine kadar uzatılmıştır ki; Şekil 3.7'de gösterildiği gibi komponent düzeyinden sistem düzeyine döngüsel bir şekilde tekrarlanarak tamamlanır. Bu aşama, sistem tasarımı mantıksal mimarilerini türeterek, hata nedenlerinin ve hata sonuçlarının senaryo modellemesine katkı sağlar (BS EN 31010, 2010).

3.4.1 Hata sonucu senaryosunun oluşturulması

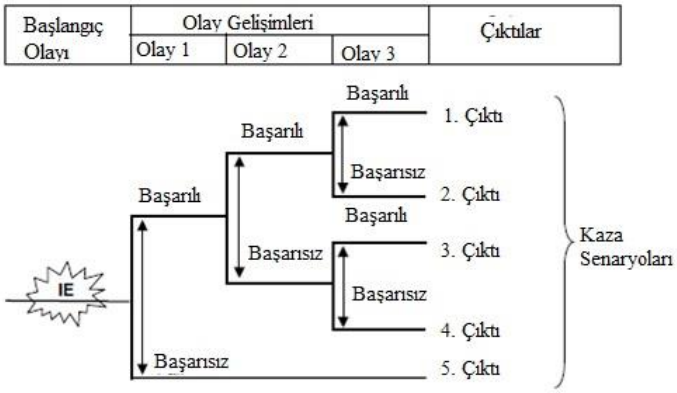
Farklı hata şiddetinin seviyesi aralığı olan hata sonuçlarına ait senaryoların geliştirilmesi, hata olaylarının durumlarının veya koşullarının etkilerini tahmin etmektir. Hata sonuçları, bir veya birden çok hata etkisinin veya deneysel çalışmalardan elde edilen kabullerin şiddetini belirlemek için modellenir.

Şekil 3.8'de gösterildiği gibi, hata sonuçlarının senaryo geliştirilmesi, bir başlangıç olayının nihai hata sonucu ile başlar. FMEA analizi sonuçlarına göre hem ETA hem de FTA hata sonuçlarının mantıksal ve grafiksel senaryo geliştirme modeline uygulanabilir. Ancak, Olay Ağacı Analizi Bölümünde belirtildiği üzere FTA; birden çok güvenceleri olan sistemlerin hata sonuçlarını modellemek için kullanıldığı takdirde, senaryo çok karmaşık ve büyük olacaktır. Bu nedenle, demiryolu sistemi

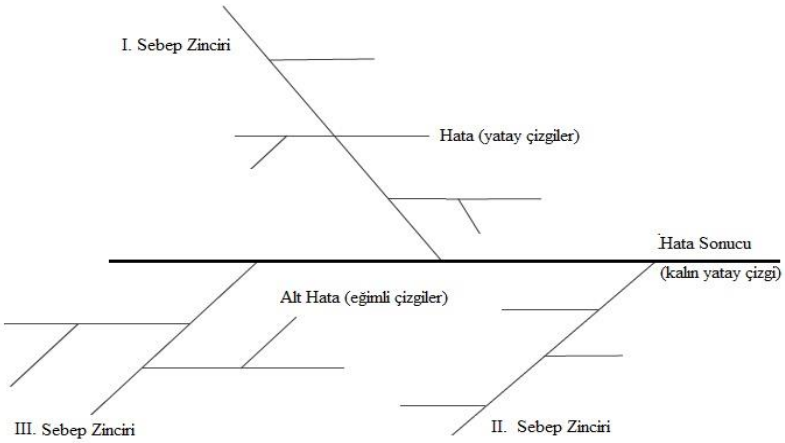
gibi birden çok güvenceleri olan sistemleri ETA tarafından modellenmektedir. Şekil 3.8'de bu yönteme bir örnek gösterilmektedir (Ericson, 2005).

3.4.2Hata sebebi senaryosunun oluşturulması

Risk tanımlama, istenmeyen bir sistem yetmezliğine sebep olabilecek tüm olası nedenlerini belirlemek için yapılandırılmış bir yöntem olmalıdır. Dolayısıyla geniş kategoride olası katkı faktörleri düzenlemek gerekir. Bu, sadece toplanan veri ve deneysel test verileri ile belirlenebilir. Ancak, muhtemel hata nedenlerinin bazıları fiili bir katkıda bulunabilir. Buna göre, bir balık kılçığı diyagramı tüm olası nedenleri daha etkili inceleyebilir ki bu temsil bir hata sonucu yol açan hata nedenleri arasındaki ilişkiyi anlamak için çok kullanışlı bir tekniktir. Dolayısıyla bir balık kılçığı diyagramı hassas bir hata nedenlerini belirlemek için FMEA analizi etkin bir şekilde destekleyebilir ve Şekil 3.9'da gösterildiği gibi FTA analizi, hata nedeni senaryoları modellemek için yardımcı olabilir.

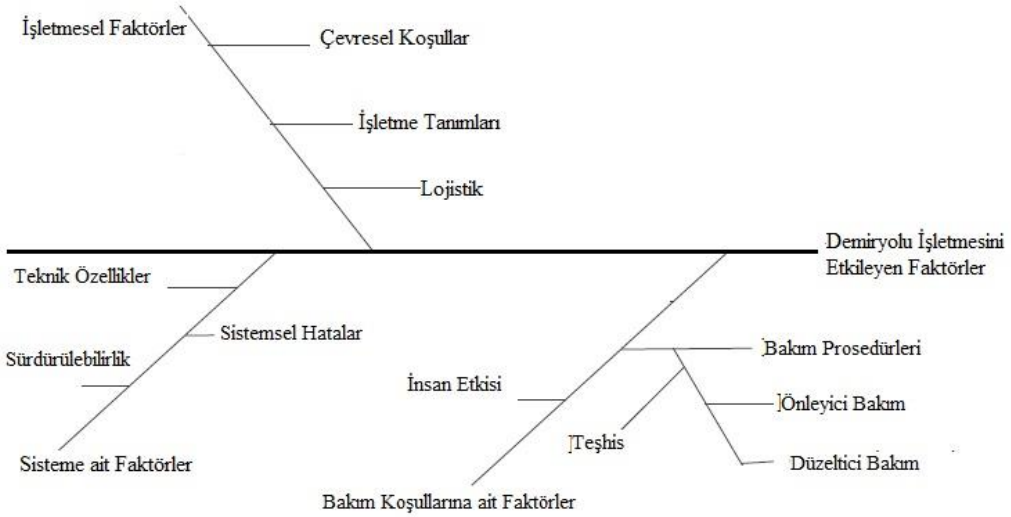


Şekil 3.8 : Hata Sonuçları senaryosunun olay ağacı analizi ile gelişimi.



Şekil 3.9 : Balık kılçığı diyagramı ile hata sebeplerinin analizi.

Balık kılçığı diyagramı kolayca hata ağacına dönüştürülebilir. Şekil 3.10'da EN 50126-1 (1999) standardından türetilen, bakım ve işletme koşullarına göre raylı sistemleri etkileyen faktörleri kullanan bir balık kılçığı diyagramı, RAMS performansını göstermektedir.



Şekil 3.10 : Demiryolu işletmesini etkileyen faktörler.

Hata nedenleri senaryoları bir mantıksal yapısı kullanılarak modellenebilir. Mantıksal modelleme bir hata ağacı kullanılarak uygulanır. Mantıksal modelleme bir ana olay (top event) ile başlar tekrarlanan bir şekilde kök hata nedenlerine ulaşıncaya kadar sürekli ağaç yapıları ile devam ettirilir. Bu hata ağacı modellemesi aşağıda gösterildiği gibi iki aşama kullanılarak gerçekleştirilmiştir:

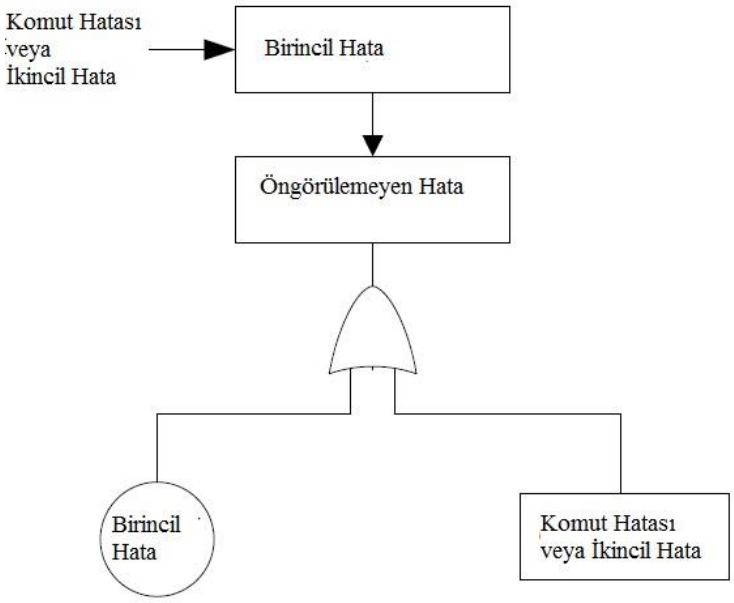
3.4.2.1 Aşama I: Ana olay (top event) belirlenmesi

Bir hata ağacı hata ağacı, bir arıza durumunda kök başarısızlık nedenleri tespit böylece bir başarısızlık olayı neden olabilir sistem koşulları sembolik bir temsilidir. Bir hata ağacının inşaat bir üst olayı ve üst olaya neden tüm olayları tanımlayan başlar. Şekil 3.11'de gösterildiği gibi iyi etkinlik üç başarısızlık nedenleri ile belirlenir.

Birincil hata, tasarım sınırları çerçevesinde komponent hatalarına bağlı olan bir olaydır. Yani olay, komponent kararkteristiklerinden birisidir.

İkincil hata, tasarım sınırları dışında bir komponentin hatalarını gösterir. Yani olay, komponentin çevresel veya işletmesel koşullardan dolayı etkilenmesi neticesinde gerçekleşmiştir.

Komut hatası, yanlış bir zamanda işletme komutu iletilmesi nedeniyle komponentin istenmeyen şekilde çalışmasıdır (Ericson, 2005; MIL-HDBK-764, 1990).



Şekil 3.11 : Hata ağacı oluşturma yöntemi.

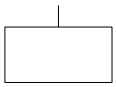
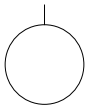
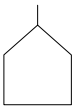
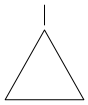
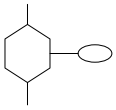
3.4.2.2 Aşama II: Hata ağacı sembollerinin belirlenmesi

Bir sonraki adım, hata ağacının yapımı için hata ağacı sembolleri tespit etmektir. Çizelge 3.5 de gösterildiği gibi bir hata ağacı oluşturmak için sembollerin iki türü vardır. Bunlar; mantık sembolleri ve olay sembolleri olarak isimlendirilebilirler. Mantık sembolleri; belirli ana olaya (top event) sebep olan hata olaylarının birbirleriyle ilişkilendirilmesi içindir. Temel mantık sembolleri 'VEYA' ve 'VE' kapılarıdır. Olay sembolleri ise sistem hiyerarşisi tarafından tanımlanan hata olaylarını temsil eder. Çizelge 3.5 sık kullanılan hata ağacı sembolleri kısa bir açıklamasını içerir.

3.4.3 Risk analizi aşaması

Risk analizi hata sonucu risk düzeyini belirlemek için önceki aşamada geliştirilen hata nedenleri ve sonuçları senaryosunu nicel olarak tahmin eden bir süreçtir. Şekil 3.12 Hata olaylarının hata nedeni senaryoları için FTA analizi ile yapılan hata sonucunun modelinin nicel olarak ölçülmesini göstermektedir. Her hata sonucunun sıklığı ve şiddetine ait yapılan ölçüm seviyeleri, risk düzeyini belirlemek için Çizelge 3.4'de belirtilen risk değerlendirme matrisi uygulanır (Ericson, 2005).

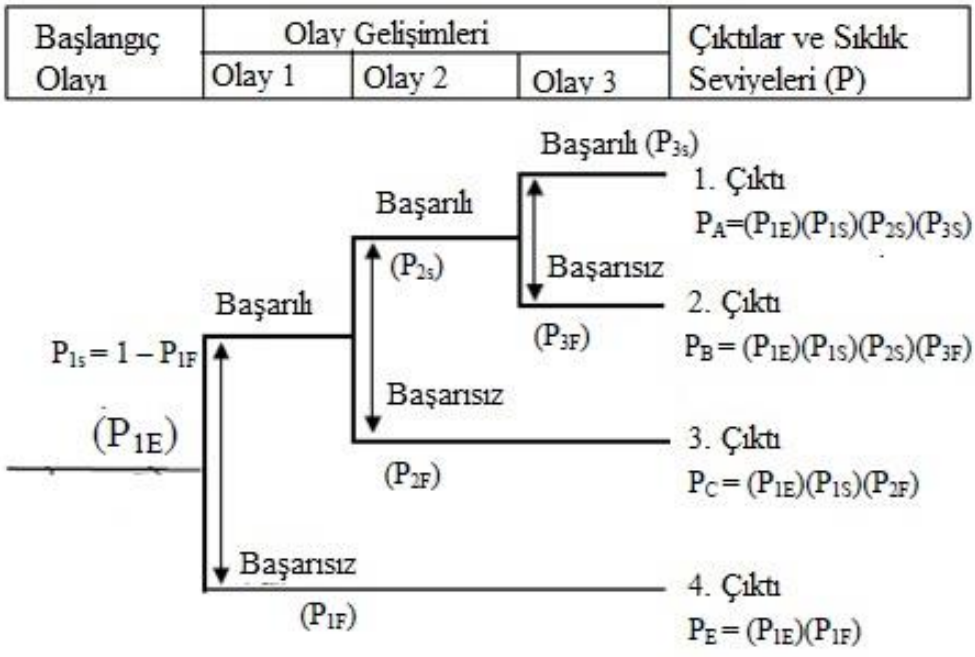
Çizelge 3.5 : Hata ağacı sembollerinin tanımları.

Sembol Türü	Sembol Gösterimi	Sembol İsmi	Sembol Açıklaması
Olay Sembolü		Ana olay (top event) veya ara olay (intermadiate event)	
		Temel olay (basic event)	
		Ev olay (house event)	
		Tanımlanmamış olay (undeveloped event)	
		Bağlayan olay (connecting event)	
Mantıksal Sembol		VE kapısı	
		VEYA kapısı	
		Kısıtlama (inhibit) kapısı	

3.4.4 Hata sebeplerinin sayısal olarak hesaplanması

Bir hata ağacı, ana olayı etkileyebilecek komponentlerin hata kombinasyonlarını içerir. Hata ağacı ana olaya ulaşan bir mekanizma kurulmasını sağlar. Bu nedenle, bir arıza ağacın kesim kümesi (cut set) analizi; emniyetle ilgili (safety related) olasılığı yüksek kesim kümeleri bileşenlerini belirleyerek sistem tasarımındaki komponentlerin kritik veya zayıf bağlantılarını ortaya çıkarır. Küçük/minimal kesim kümeleri (minimal cut set) belirlenmesi için yapılan kesim kümesi analizi Boole cebri kuralları tarafından belirlenir (STAMATELATOS ve Caraballo, 2002).

Boole cebri kuralları çok önemli kuralladır. Minimal kesim kümeleri, belirlemek amacıyla kullanılan Boole cebri kuralları Boole cebri ilişkisinin şematik bir ifadesidir. Çizelge 3.6 genel olarak kullanılan Boole cebri kurallarını göstermektedir.



Şekil 3.12 : Hata sebep-sonuç hesaplama modeli.

Bir hata ağacı, bir veya daha fazla minimal kesim kümeleri (MCS) tarafından bir ana olayı oluşturur. Bir temel olay (basic event) yani dolayısıyla bir minimal kesim kümesi (MCS), ana olayın (top event) gerçekleşmesine neden olabilecek bir hata noktası (single point failure) anlamına gelir. Iki temel olayın yani dolayısıyla iki minimal kesim kümesinin (MCSs) birlikte üst olayın meydana gelmesine neden olması durumunda ise çift hata noktaları (double point failures) terimi ortaya çıkmış olur. Dolayısıyla "n" adet temel olayın ana olayı oluşturması durumunda "n" adet temel olayın meydana gelmesini sağlayacak hataların tamamının birleşmesi söz konusu olacaktır. Yukarıda açıklanan bu durumun matematiksel ifadesi olarak (3.1) denklemiyle ifade edilen bir düzenleme yapılabilir:

$$T = M1 + M2 + \ldots + Mk \qquad \textbf{(3.1)}$$

(3.1) denkleminde; T ana olayı (top event), Mn ise minimal kesim kümelerini (MSC) ifade etmektedir. Her MSC, spesifik olayların birleşiminden oluşmaktadır. Bu yüzden, "n" adet temel olay (3.2) denklemiyle ifade edilebilir:

$$Mn = X1 + X2 + \ldots + Xn \qquad \textbf{(3.2)}$$

Bu denklemde; temel olayların her biri X terimi ile ifade edilir. Dolayısıyla nihai (3.3) denklemi elde edilir.

Çizelge 3.6 : Bool cebri kuralları.

Matematiksel Sembol	Mühendislik Sembolü
$X \cap Y = Y \cap X$	$X \cdot Y = Y \cdot X$
$X \cup Y = Y \cup X$	$X + Y = Y + X$
$X \cap (Y \cap Z) = (X \cap Y) \cap Z$	$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z$
$X \cup (Y \cup Z) = (X \cup Y) \cup Z$	$X + (Y + Z) = (X + Y) + Z$
$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$	$X \cdot (Y + Z) = X \cdot Y + X \cdot Z$
$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$	$X + (Y \cdot Z) = (X + Y) \cdot (X + Z)$
$X \cap X = X$	$X \cdot X = X$
$X \cup X = X$	$X + X = X$
$X \cap (X \cup Y) = X$	$X \cdot (X + Y) = X$
$X \cup (X \cap Y) = X$	$X + (X \cdot Y) = X$
$X \cap X' = \phi$	$X \cdot X' = \phi$
$X \cup X' = \psi = I^*$	$X + X' = \psi = I^*$
$(X')' = X$	$(X')' = X$
$(X \cap Y)' = X' \cup Y'$	$(X \cdot Y)' = X' + Y'$
$(X \cup Y)' = X' \cap Y'$	$(X + Y)' = X' \cdot Y'$

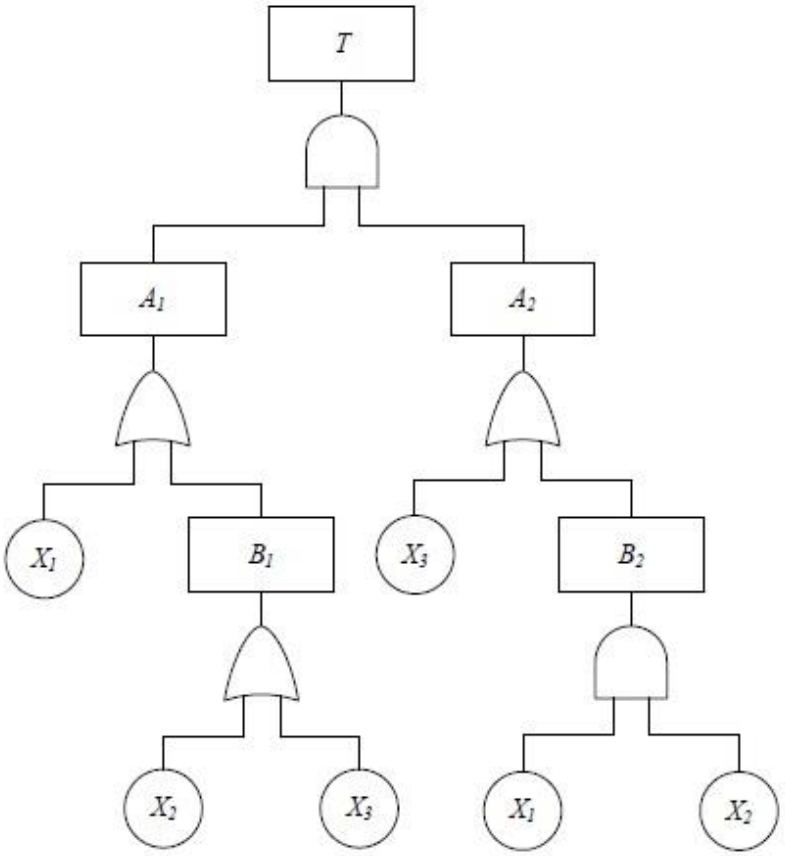
$$T = X1 + X2 + \ldots + Xn \qquad \textbf{(3.3)}$$

3.4 denklemi, ana olayı ifade eden bir örnek olarak aşağıda verilmiştir:

$$T = X1 + X2 \,.\, X3 \qquad \textbf{(3.4)}$$

Bu denklemde; “X” terimlerinin herbiri temel olay hatalarıdır. Ana olay (T) bir temel olay (X1) “ve” iki temel olaydan (X2 . X3) meydana gelmiştir.

Hata ağacının minimal kesim kümelerini belirlemek için, hata ağacı kendisine eşlenik olan Bool cebri denklemine çevrilir. Bool cebri denklemlerini kesim kümelerine çevirmek için çeşitli algıritmalar mevcuttur. Genel uygulama yöntemlerinden birisi yukarıdan aşağıya ve aşağıdan yukarıya metodlarının yer değişikliğidir. Bu metodlar anlaşılması kolay ve açık ifade edilebilir metodlardır. Ayrıca, bunlar Bool cebri ifadelerinin dönüştürülmesine ve genişletilmesine katkı sağlarlar. Şekil 3.13 eşlenik Bool cebri denklemlerini gösteren bir hata ağacı örneğini ifade etmektedir (STAMATELATOS ve Caraballo, 2002).



Şekil 3.13 : Hata ağacı örneği.

Şekil 3.13'te gösterilen hata ağacı aşağıdaki denklemlerle ifade edilebilir:

$$T = A1 \cdot A2 \quad \textbf{(3.5)}$$

$$A1 = X1 + B1 \quad \textbf{(3.6)}$$

$$B1 = X2 + X3 \quad \textbf{(3.7)}$$

$$A2 = X3 + B2 \quad \textbf{(3.8)}$$

$$B2 = X1 \,.\, X2 \qquad \textbf{(3.9)}$$

3.4.4.1 Yukarıdan aşağı (top-down) değiştirme yöntemi

(3.5) denklemi, (3.6) ve (3.8) denklemleri kullanılarak tekrar yazıldığında ve yutma özelliği ile düzenlendiğinde 3.10'daki denklem elde edilir:

$$T = (X1+B1).\,(X3+B2) = (X1.X3) + (B1.X3) + (B2.X1) + (B1.B2) \qquad \textbf{(3.10)}$$

Daha sonra 3.7 denklemi ile tekrar düzenlendiğinde aşağıda belirtilen 3.11a denklemi elde edilir:

$$T = X1+X3 + (X2+X3).\,X3 + B2.X1 + (X2 + X3).\,B2$$

$$= X1.X3 + X2.X3 + X3.X3 + B2.X1 + B2.X2 + B2.X3 \qquad \textbf{(3.11a)}$$

Yukarıdaki denklemde verilen ifadelerin eşlenik olanları aşağıdaki gibi birleştirilebilir:

$$X1.X3 + X2.X3 + X3.X3 + B2.X3 = X3 \qquad \textbf{(3.11b)}$$

3.11b denklemi 3.11a denklemine uygulanacak olursa;

$$T = X3 + B2.X1 + B2.X2 \qquad \textbf{(3.12)}$$

denklemi elde edilir. Bu denklem 3.9 denklemi ile birleştirildiğinde;

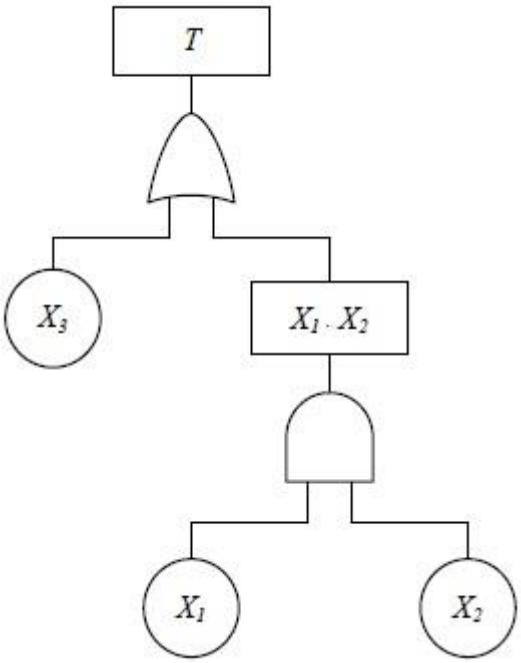
$$T = X3 + (X1 \,.\, X2\,).X1 + (X1 \,.\, X2\,).X2 \qquad \textbf{(3.13)}$$

$$T = X3 + (X1 \,.\, X2\,) + (X1 \,.\, X2\,) \qquad \textbf{(3.14)}$$

3.14 denklemi elde edilir. Bu denklemde yutma özelliği kullanıldığında 3.15 denklemi elde edilmiş olur. Dolayısıyla 3.5 denkleminin minimal kesim kümesi şeklindeki ifadesi 5.15 denklemi olacaktır.

$$T = X1 \,.\, X2 + X3 \qquad \textbf{(3.15)}$$

Ana olayın (top event) minimal kesim kümeleri; tekil olay olan X3 ve çift olay olan X1. X2 şeklinde ifade edilebilir. Dolayısıyla 3.15 denklemi şematik olarak Şekil 3.14 ile gösterilecektir.



Şekil 3.14 : Eşlenik FTA modeli.

3.4.4.2 Aşağıdan yukarı (bottom-up) değiştirme yöntemi

Şekil 3.13'de gösterilen hata ağacı için aşağıdan yukarıya değiştirme yöntemi aşağıda açıklanacaktır. 3.7, ve 3.9 denklemleri yeniden düzenlenerek aşağıdaki denklemlere dönüştürülecektir:

$$A1 = X1 + X2 + X3 \quad \textbf{(3.16)}$$

$$A2 = X3 + X1 .X2 \quad \textbf{(3.17)}$$

Daha sonra 3.5 denklemi düzenlenerek 3.18 denklemi elde edilecektir:

$$T = (X1 + X2 + X3).(X3 + X1 .X2) \quad \textbf{(3.18)}$$

Nihai olarak, yutma özelliği kullanıldığında, 3.19 denklemi elde edilir:

$$T = X1.X3 + X1.X1 .X2 + X2.X3 + X2.X1 .X2 + X3.X3 + X3.X1.X2$$
$$= X1.X3 +X1 .X2 + X2.X3 + X1 .X2 + X3 + X1.X1.X3$$
$$= (X1.X3 + X2.X3) + (X1.X2 +X3)+ (X1.X2 + X1.X2.X3)$$
$$= (X1.X2 + X3) + (X1.X2 +X3)+ (X1.X2 + X3)$$
$$= X1.X2 +X3 \quad \textbf{(3.19)}$$

Dolayısıyla, 3.15 ve 3.19 denklemlerinin eşit olduğu ve her iki yöntemin de minimal kesim kümelerini oluşturmak için kullanılabileceği görülmüş olur.

Bir hata nedeni senaryosu modeli olasılık yasası veya hata oranı ile ölçülebilir. Bu hesaplama yöntemleri aşağıda tarif edilmektedir:

3.4.4.3 Olasılık kanunu ile hesaplama

Bir hata ağacının minimal kesim kümeleri belirlendikten sonra, ana olayın olasılığı değerlendirilebilir. Olasılık yasalarının temel kavramları FTA mantık kapılarına uygulanır. Olasılık yasasının iki temel özelliği 'VEYA' ve 'VE' kapısı için şu şekilde temsil edilir:

VEYA kapısının olasılık ifadesi 3.20 denkleminde gösterilmektedir:

$$P(T) = P(a) + P(b) - P(a.b) \quad \textbf{(3.20)}$$

“a” ve “b” bağımsız olaylar ise ve “P (a.b)” çok küçük ise 3.20 denklemi yaklaşık olarak 3.21 denklemine eşit olacaktır.

$$P(T) = P(a) + P(b) \quad \textbf{(3.21)}$$

VEYA kapısına “n” adet giriş olması durumunda P (T) olasılığı şu şekilde düzenlenebilecektir:

$$P(T) = P(a + b + \ldots) = P(a) + P(b) + P(c) + \ldots \quad \textbf{(3.22)}$$

VE kapısının olasılık ifadesi ise 3.23 denklemi ile gösterilebilir:

$$P(T) = P(a.b) = P(a) \,.\, P(b) \quad \textbf{(3.23)}$$

Dolayısıyla, “n” adet giriş için VE kapısının olasılık ifadesi 3.24 denklemiyle gösterilebilecektir:

$$P(T) = P(a.b.c. \ldots) = P(a) \,.\, P(b) \,.\, P(c). \ldots \quad \textbf{(3.24)}$$

3.4.4.4 Hata oranı ile hesaplama

Mantıksal olarak VEYA kapısı seri bir sisteme karşılık gelmektedir. Dolayısıyla bu durumda güvenirlilik (reliability) fonksiyonu şu şekilde ifade edilebilecektir.

$$R_s(t) = \prod_{i=1}^{n} R_i\ (t) \tag{3.25}$$

Bu denklemde "n" komponentlerin miktarını, Ri i. komponentin güvenilirlilik değerini ve Rs ise seri sistemin güvenilirlik değerini belirtmektedir.

Hata oranı, yani F(t) değeri 3.26 denklemiyle ifade edilmektedir. Bu yüzden, seri sistemin hata oranı denklemi 3.27'de belirtildiği şekilde düzenlenecektir.

$$F\ (t) = 1 - R\ (t) \tag{3.26}$$

$$F_s(t) = 1 - \prod_{i=1}^{n} (1 - F_i\ (t)) \tag{3.27}$$

Bu denklemde; "n" komponentlerin miktarını, Fi i. komponentin hata oranını ve Fs ise seri sistemin hata oranını belirtmektedir.

VE kapısı mantıksal olarak paralel bir sisteme karşılık gelmektedir. Dolayısıyla bu durumda güvenirlilik (reliability) fonksiyonu şu şekilde ifade edilebilecektir.

$$R_p(t) = 1 - \prod_{i=1}^{n} (1 - R_i(t)) \tag{3.29}$$

3.29 denkleminde "n" komponentlerin miktarını, Ri i. komponentin güvenilirlilik değerini ve Rp ise paralel sistemin güvenilirlik değerini belirtmektedir. Dolayısıyla bu paralel sistemin hata oranı 3.30 denklemiyle ifade edilebilecektir:

$$F_p(t) = \prod_{i=1}^{n} (F_i(t)) \tag{3.30}$$

Bu denklemde; "n" komponentlerin miktarını, Fi ise "i." komponentin hata oranını ve Fp ise paralel sistemin hata oranını belirtmektedir. Şekil 3.12 önceki aşamada geliştirilen sonuç senaryoları aracılığıyla her hata olayının hata sıklığı olasılığını analiz yöntemleri gösterir (Ericson, 2005).

3.4.5 Risk hesaplama aşaması

Risk değerlendirme aşaması; hata şiddeti ve risk değerlendirme matrisi ile frekans seviyelerinin birleşimi şeklinde, risk düzeyini belirlemek için uygulanır. Bu aşamada elde edilen sonuçlar uygun risk işleme ve kontrol seçenekleri seçimi için önemli bilgiler sağlayacaktır. Değerlendirilen sonuçlar bakım, lojistik destek ve işletme planları sistemi ürünlerini tasarlamak ve geliştirmek için sistem mühendislerine veya RAMS mühendislerine yardımcı olacaktır. Eğer risk yüksek ölçülerde ise, bu riskin hata sıklığının düşürülmesi veya olası hata sonuçlarından muhafaza edilmesi için kontrol altında tutulması gerekmektedir. Riskler kabul edilebilir düzeyde ise, herhangibir işleme gerek kalmayacaktır; ancak sertifikasyon süreçleri için, sağlanan analiz sonuçlarının kayıt altına alınması gerekecektir (Umar, 2010).

3.5 Özet

Bu bölümde demiryolu hizmetinin görev ve emniyetini etkileyen demiryolu RAMS risklerin kontrolünü desteklemek için FMEA-FTA kombinasyonuna dayalı, demiryolu risk değerlendirme yöntemi sunulmuştur. Tehlikeler, bilgiler, mevcut veriler ve sistem tasarım aşaması, demiryolu risk değerlendirme tekniklerinin seçimi için karar vermek (decision making) için önemli faktörlerdir.

Öncelikle demiryolu risk tanımı ve FMEA-FTA kombinasyonu uygulamaya dayalı, demiryolu risk değerlendirme modelleri incelenmiştir. Demiryolu risklerinin tanımı, risk senaryolarının oluşturulması ve risk değerlendirme tekniklerinin seçimi için soruların belirlenmesini sağlamış; ve aynı zamanda demiryolu riski senaryosuna FMEA-FTA kombinasyonunu uygulama yöntemi sağlamıştır. Yukarıdan aşağıya (top-down) ve aşağıdan yukarıya (bottom-up) olmak üzere, fonksiyonel ve tasarım mimari tasarım aşamalarında uygulanabilir iki FMEA-FTA temelli risk değerlendirme modelleri incelenmiştir.

Bu bölüm ikinci olarak, sistem mühendisliği sürecine dayalı demiryolu risk değerlendirmesinin tüm yönlerini kapsayacak şekilde sistem tasarım aşamasında uygulanabilen FMEA-FTA tabanlı demiryolu risk değerlendirme süreci üzerinde durmuştur. Süreç, RAMS tasarım ve kabul kriterlerinin tanımı ile başlatılır. Risk tanımlama aşamasında, süreçteki olası tüm riskleri etkin bir şekilde tespit etmek için olay ağacı analizi (ETA) ve balık kılçığı diyagramı yöntemlerinin kullanımı

önerilmiştir. ETA, hata sonuç senaryolarının şematik (yani grafiksel) gösterimi için kullanılırken; balık kılçığı diyagramı hata nedenlerinin tam olarak belirlenmesi ve bir hata ağacı tasarımının etkin bir şekilde desteklenmesi için kullanılabilir.

Belirlenen demiryolu riskleri hata sonuçlarının sıklığını ve şiddetini ölçmek için nitel ve nicel olarak analiz edilir. Bir hatanın sonucuna ait nedenleri açık bir şekilde tanımlayan nitel analiz, minimum kesim kümelerini belirlemek amacıyla yapılır. Bu nitel analiz, özellikle emniyet fonksiyonlarını ve onların izleme fonksiyonları belirlemek ve nicel analiz hatası olasılığı veya hata oranı tarafından belirlenen minimal kesim kümesini ölçmek için yapılır.

Sonuç olarak, demiryolu risk değerlendirmesi, demiryolu risklerin etkin kontrolü için tam bir anlayış ve yeterli bilgi veren RAMS yönetimi ve sistem mühendisliğinin temel bir parçasıdır. Önerilen risk değerlendirme yöntemleri sistem tasarımı aşamasında kolayca kullanılabilecek ve sistem emniyet fonksiyonlarını tasarlamak için büyük bir potansiyele sahip olacaktır. Özetle; risk değerlendirme süreci; demiryolu sistem fonksiyon ve hatalarını, demiryolu işletme koşullarını, uygun risk veri kaynaklarını ve birçok deneyim ve bilgiyi anlamayı gerektirir.

4. MESCİDİ SELAM LOKAL SİNYALİZASYON SİSTEMİ UYGULAMASI

4.1 Giriş

Bir demiryolu hattında makas ve sinyal lambaları hat üzerindeki önemli bölgelerde bulunmaktadır. Bunlar manüel olarak işletildiklerinde sinyal operatörü hattın işletilmesini bu makas ve sinyal lambalarına tek tek giderek yapmak zorunda kalır. Herhangi bir rota yalnızca bir araca tahsis edilebileceğinden, böyle bir durumda hızlı bir işletim mümkün olmayacaktır. Sinyalizasyon tek bir merkezden manüel olarak yapılması durumunda ise makas kollarının hangi makasa ait olacağı konusunda bir yanılma olabilir. Ayrıca, operatör makaslardan uzakta olacağından, makas konumlarının tam olarak gözlenebilmesi mümkün olmayacaktır.

Büyük şehirlerde karayolu taşımacılığında yaşanan sorunların yol açtığı trafik sıkışıklığının hafifletilmesi için raylı toplu taşıma sistemlerine yapılan yatırımların giderek artmasıyla birlikte metro sistemlerinde, istasyona gelecek iki tren arasında dakikalar, hatta saniyeler kadar bir fark söz konusu olmaktadır. Eğer trenler zamanında istenilen istasyona varmış olsalardı belki sinyalizasyona ihtiyaç kalmayabilirdi. Ancak, her ne kadar dakik olunması istenilse de trenlerin kara taşıtları gibi anında hareket edebilmeleri ve durabilmeleri mümkün olmamaktadır. Demiryolu trafiğinin düzenlenmesinde, karayolu trafiğine göre daha hassas bir trafik kontrol mekanizması geliştirilmelidir. Bu nedenle, raylı sistemlerin sinyalizasyonu, işletmenin emniyeti ve en yüksek verimde kullanılabilmesi için hayati önem taşımaktadır.

Anklaşmanın amacı, tehlikeden emin olmak için, makasları ve sinyal lambalarını birbirleriyle bağlamaktır. Bunun sonucunda hat işletmesinin yapılması da daha hızlı olmaktadır. Anklaşman donanımı, bağlantı bölgelerinde ve hattın diğer kısımlarında tren çarpışmalarından koruyacak şekilde sinyalizasyonu düzenler. Rayda bir tren varsa, o ray bölgesine girişleri kontrol eden sinyal hiçbir zaman yeşil olamaz. Sistem, ray bölgesinde bir trenin bulunup bulunmadığını fark etme kabiliyetinde olmalıdır ki, o bölge hakkındaki kararların bir tehlike arz etmediğinden emin olunabilsin.

Bu bölümde, genel sinyalizasyon sistemi bilgileri verildikten sonra, İstanbul Ulaşım AŞ'de işletme altındaki bir demiryolu bölgesinin lokal sinyalizasyon sistemi mevcut durumu incelenecek ve akabinde bu bölgeye uygulanacak çözüme ait tasarım kriterleri ile ve bu sisteme ait FMEA ve FTA analizleri üzerinde durulacaktır.

4.2 Sinyalizasyon Sistemi

Sinyalizasyon denilince genellikle akla yalnızca trafik sinyalleri gelebilir. Tabii ki bunlar makinisti bilgilendirmek için hayati önem taşımaktadırlar. Ancak emniyeti garanti edebilmek için bu sinyallerin doğruluğunun da sağlanması gerekmektedir. Genel anlamda demiryolu sinyalizasyonu, trenlerin emniyetli bir şekilde seyretmelerini ve demiryolunun az bir masrafla maksimum kapasitede kullanılmasını, yani en verimli bir şekilde çalıştırılmasını sağlamak için yapılan çalışmaların bütünüdür.

Sinyalizasyonun esas problemi demiryolunda tren karşılaşmalarını göz önüne alarak trafiği düzgün ve ekonomik bir tarzda yönetmektir. Demiryolu sinyalizasyonu bugünkü modern şekle gelinceye kadar birçok aşamalardan geçmiştir, öncelleri demiryolunun bazı noktalarında görevlendirilen operatörler yolun belirli kısımlarındaki trenlerin durumlarını değişik anlamlara gelen el kol işaretleriyle bildirirlerdi. Daha sonra bunların yerini alan ve trenlerin hareketleri için değişik manaları olan kırmızı, yeşil, sarı, beyaz ve mavi renkli bayraklar ve lambalar kullanılmıştır. Bugünkü modern sinyalizasyonun temelini oluşturan bu kıstaslar, manevra bölgelerinde ve bazı ana yollarda halen kullanılmaktadır.

Demiryolu emniyetini garanti edebilmek için bazı donanımsal elemanlara ihtiyaç vardır. Bunlar vasıtasıyla sinyalizasyon daha güvenli hale getirilebilir. Donanımın işleyişinin doğru olabilmesi için emniyet tedbirlerinin bir kontrol merkezi tarafından belirlenmesi ve yürütülmesi gerekebilir. Bu merkezde bir operatör olabileceği gibi, bunun yanında bir sinyal işletme sistemi de olabilir.

4.2.1 Sinyalizasyon sistemi bileşenleri

Trafik kontrol merkezleri; (TCC) demiryolu ağının tüm donanımlarından bilgilerin alındığı ve bu bilgilere göre trenlerin konumlarının izlendiği ve rota tanzimlerinin yapıldığı birimlerdir. Bu merkezlerde bulunan operatörler daha önceden trenlerin sevkiyatını buradan kontrol etmekte ve yönlendirmekte iken, günümüzde yalnızca

anklaşmanın işletme komutları bu merkezden verilmektedir. Bu komutlar rota tanzimlerinden ibarettir. Asıl işletmeyi anklaşman mekanizması düzenlemektedir. Diğer yandan herhangi bir hata veya arıza durumunda da TCC operatörleri sisteme müdahalede bulunma imkânına sahiptirler. Anklaşman ise, demiryolu sinyalizasyonunda, sinyal tertibatının ve trenler arasındaki mesafelerin güvenli kontrol edilebilmesi ve aynı zamanda seferlerdeki aksamaların da önlenebilmeleri amacıyla kurulan bir kontrol & kumanda mekanizmasıdır.

Nesne Kontrol Üniteleri (Object Control Units), hat boyu ekipmanları ile kontrol merkezi (TCC) arasındaki iletişimi sağlayan haberleşme üniteleridir. Bu üniteler sahadan gelen verileri anklaşman sistemine iletirler, bununla birlikte anklaşman sisteminden gelen komutları sahaya yönlendirirler.

Hat boyu ekipmanları, demiryolu hattına ait saha elemanlarını kapsamaktadır. Bunlar tren algılama sistemleri, makas kontrol sistemleri, renkli ışık bildirimleri, lokal kumanda butonları şeklinde detaylandırılabilir.

Tren algılama sistemleri olarak, çok farklı teknolojiler kullanılmaktadır. Algılamadaki amaç, ray hattı üzerinde trenlerin net konumlarının belirlenebilmesidir. Günümüzde daha ileri teknoloji algılama sistemleri olmasına rağmen, nispeten daha eskiye dayanan ray devresi sistemi ve aks sayıcı sistemi yaygın bir kullanım alanı bulmaktadır.

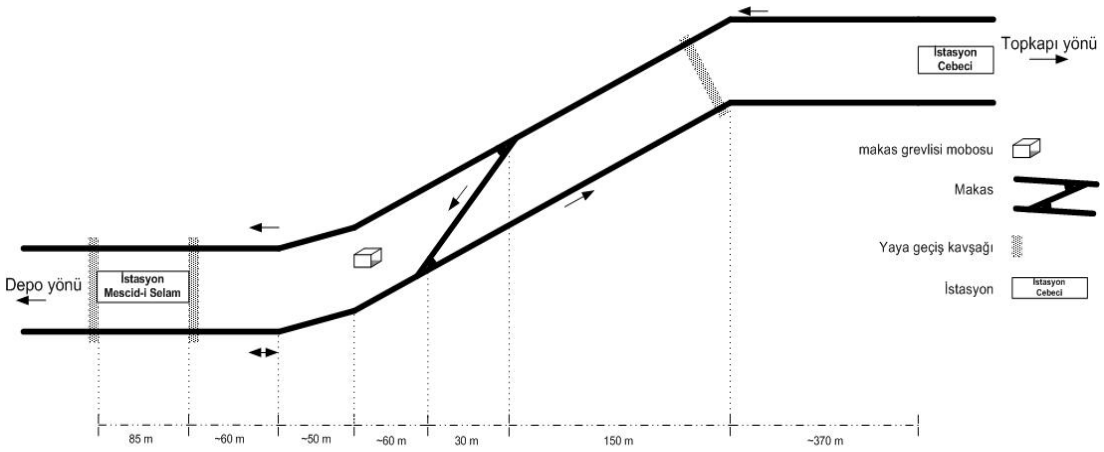
Demiryolu araçlarının seyirlerine devam ettikleri yoldan başka bir yola geçişleri için kullanılan ray elemanlarına makas denilmektedir. Makas motorları da bu makasların demiryolu üzerinde hareketini sağlayan saha ekipmanlarıdır.

Sinyalizasyon sistemlerinde makinisti bilgilendirmek ve yönlendirmek için hayati önem taşıyan bir bileşen de renkli aydınlatma sinyalleri mevcuttur. Bu sinyaller için kullanılan çok çeşitli standartlar vardır. Ancak genel olarak renkli aydınlatma sinyallerinin makinist için iki anlamı vardır; bunlardan ilki sinyalin rengi, ikincisi ise birden fazla sinyal aydınlatıldığında bu sinyallerinin sıralamalarıdır. Bazen de sinyallerin kuvvetli aydınlatılmaları veya yanıp sönmeleri de bir anlam taşır.

4.3 Mescidi Selam Lokal Sinyalizasyon Sistemi

T4 İşletmesinin aktif olarak kullandığı Mescidi Selam döngü makaslarının elle işletilmesinden dolayı emniyetsiz ve düşük verimli bir işletme yapılmaktadır.

Bölgede tren manevraları makas görevlileri tarafından yapılmaktadır ve vardiyalı olarak toplamda 4 adet makas görevlisi bölgede çalışmaktadır. Makas görevlilerinin gün boyunca makasları çevirmeleri gerektiğinden dolayı gün boyunca tren geçişinin olduğu hat içerisinde beklemek zorunda olmaları risk unsuru oluşturmaktadır. Bu risk unsurunu ortadan kaldırmak için trenler makas bölgesinden çok düşük hızla geçmektedirler. Bu durum enerji verimli sürüşü ve işletme hızını olumsuz etkilemektedir. İlgili bölgenin genel şematik görünümü Şekil 4.1'de gösterilmiştir:

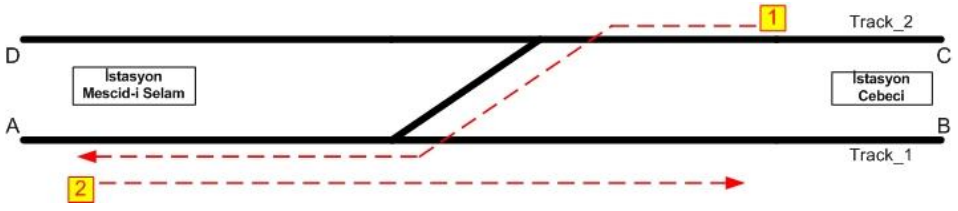


Şekil 4.1 : Mescidi selam istasyonu makas bölgesi hat şeması.

4.3.1 Genel Bilgiler

T4 Hattında Cari işletme yapılan hat Topkapı - Mescid-i Selam İstasyonları ve arasındaki yaklaşık 14 km'lik bölgeyi kapsamaktadır. Mescid-i Selam istasyonunun devamındaki bölge depo/atölye sahası olup bakım ve depolama alanı olarak kullanılmaktadır.

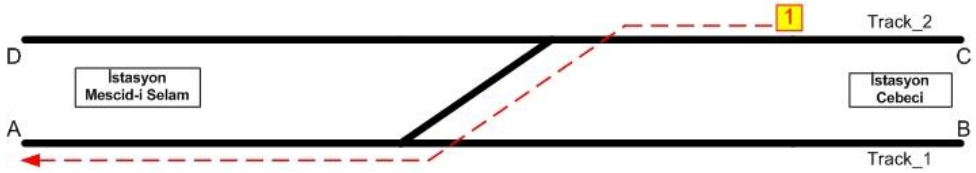
Bölgede tek yönde günlük ortalama 170 tren geçişi olmaktadır. Bu geçişlerin minimum %90'ı Şekil 4.2'de belirtilen senaryoda gerçekleşmektedir.



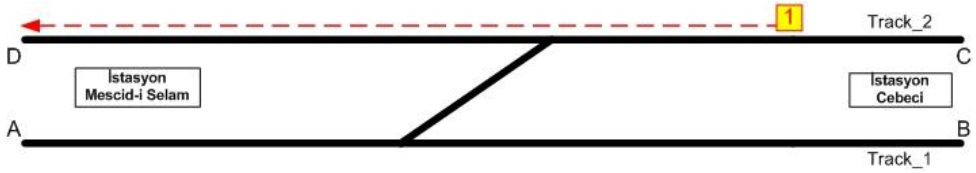
Şekil 4.2 : Ana işletme senaryosu.

Trenler herhangi bir hız veya kırmızı ışık ihlali korumasına sahip olmayıp tamamen makinist kontrolünde işletilmektedir.

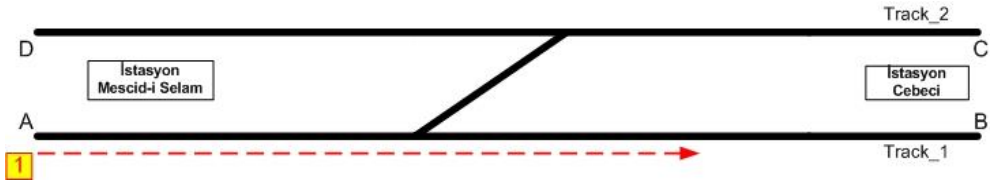
Cari hattaki trenlerin herhangi bir nedenle 2. yoldan depoya alınması sırasında Şekil 4.3 ve Şekil 4.4 ile gösterilen senaryolar uygulanmaktadır. Depo alanından cari hatta tren alma veya herhangi bir nedenle depodan manevra ihtiyacı durumlarında Şekil 4.5 ve Şekil 4.6 ile gösterilen senaryolar uygulanmaktadır.



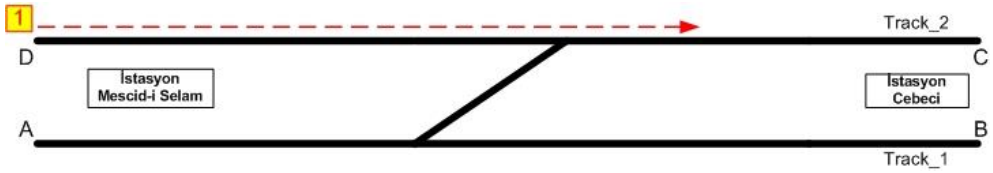
Şekil 4.3 : Treni cari hattan depo alanına alma senaryosu 1.



Şekil 4.4 : Treni cari hattan depo alanına alma senaryosu 2.

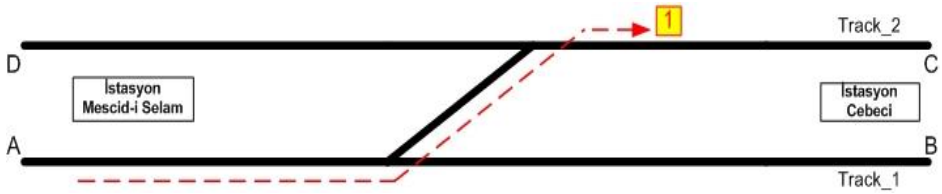


Şekil 4.5 : Treni depodan cari hatta alma senaryosu 1.



Şekil 4.6 : Treni depodan cari hatta alma senaryosu 2.

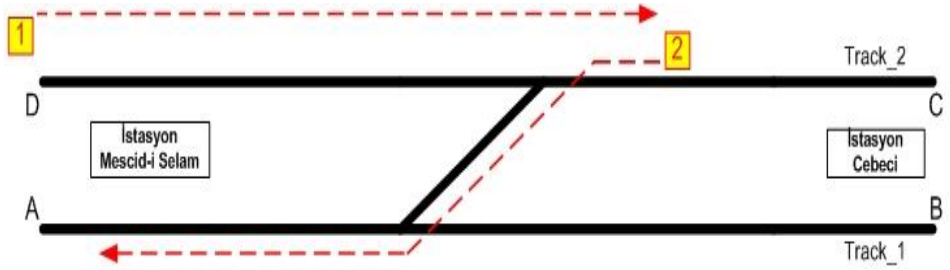
Cari hatta 1. yolda herhangi bir engel nedeniyle 2. yoldan işletme yapılması durumunda Şekil 4.6 ve Şekil 4.7 ile gösterilen senaryolar uygulanmaktadır.



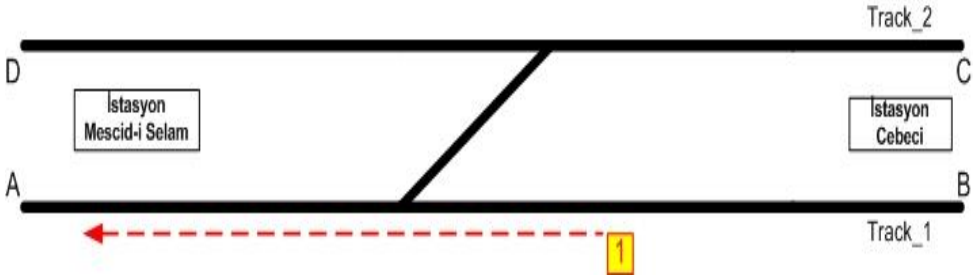
Şekil 4.7 : I. yoldaki engel nedeniyle 2. yoldan işletme yapılması senaryosu 1.

Depodaki herhangi bir sorundan dolayı ya da Mescid-i Selam istasyonu 1. peronunda tren arızasından dolayı 2. peron üzerinden işletmeyi sürdürme zarureti durumlarında ise Şekil 4.8 ile gösterilen senaryo uygulanmaktadır.

Bununla birlikte cari hat üzerindeki herhangi bir arıza/sorun sebebiyle trenler 1. yolu kullanarak depoya alınması da Şekil 4.9 ile gösterilen senaryo ile tanımlanmıştır.



Şekil 4.8 : İşletmenin II. peron üzerinden sürdürülmesi senaryosu.



Şekil 4.9 : Trenlerin I. yolu kullanarak depoya alınması senaryosu.

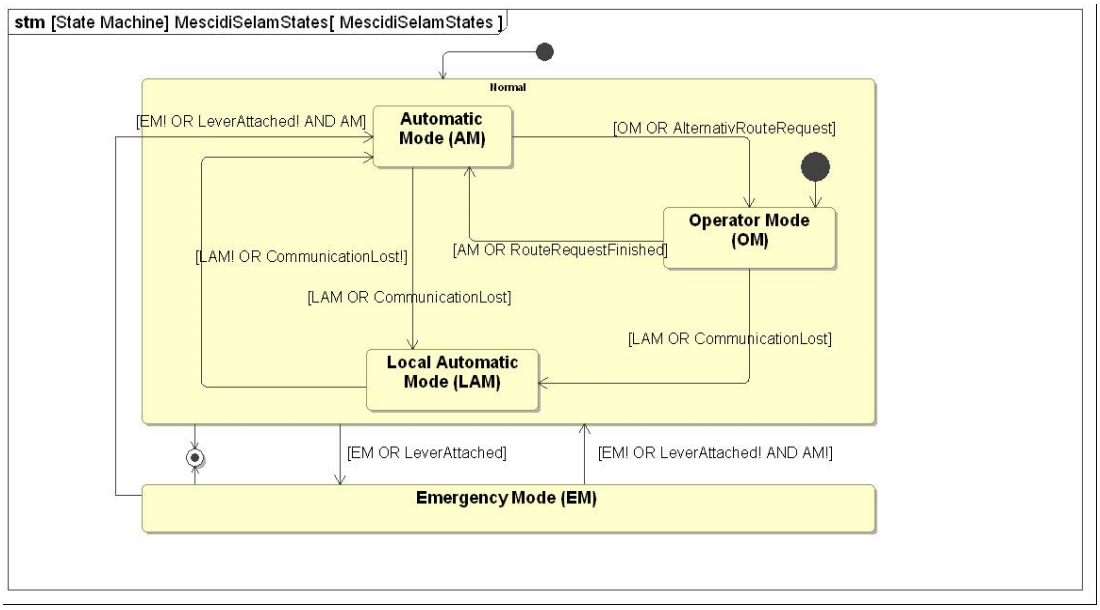
4.3.2 Sisteme Ait İşletme Tanımları

Bölgeyi kontrol edecek olan sistem dört farklı çalışma moduna sahip olacaktır. Bu modlar ve sistemde çalıştırılacak öncelik seviyeleri Çizelge 4.1'de listelenmiştir.

Çizelge 4.1 : Sistem çalışma modları.

Çalışma Modu	Öncelik Seviyesi
Otomatik Mod (AM)	4
Operator Modu (OM)	3
Lokal Otomatik Mod (LAM)	2
Emniyet Modu (EM)	1

Sistemin öncelik sırasına göre çalışma modları (düşükten yükseğe) yukarıda listelendiği gibi 4, 3, 2, 1 şeklinde tasarlanacaktır. Sistem normal (default) çalışma modu AM'dir. Sistem belirtilen tüm bu modlardan herhangi birisini aktive edemediği durumlarda kendisini EM'ye alacak ve hiçbir kontrol & kumanda fonksiyonunu yerine getiremeyecektir. Çizelge 4.1'de belirtilen tüm modlar Kumanda Merkezi tarafından yönetilecektir. Modlar arası geçiş şartları Şekil 4.10'da gösterilmektedir.



Şekil 4.10 : Mod geçişleri.

4.3.2.1 Otomatik mod (AM)

Bu mod, Şekil 4.2 ile gösterilen ana işletme senaryosunun geçerli olduğu durumlarda kullanılacak çalışma şeklini kapsamaktadır. C yönünden gelen trenler makaslardan sapan geçiş yaparak A yönünde Mescid-i Selam İstasyonuna ulaşacaktır. İstasyonda tüm yolcuları indirip yeni yolcularını aldıktan sonra makaslar düz konumda olduğu halde B yönüne ilerleyecektir. Bu şekildeki işletme modunda makas hareketleri ve demiryolu trafik sinyalleri tam otomatik olarak çalışacaktır.

Bu senaryo durumunda C yönünden gelen trenler makaslardan sapan geçiş yaparak A yönünde Mescid-i Selam İstasyonunu geçerek depo yönüne gidecektir. Şekil 4.3 ile gösterilen işletme senaryosunun geçerli olduğu durum Şekil 4.2 ile gösterilen senaryo tarafından kapsanmaktadır. Dolayısıyla yukarıda, AM olarak tanımlanan işletme modu geçerli olacaktır.

Kumanda Merkezi (KM) yazılımı eklendiği takdirde, tren trafiği sinyalden sinyale rota tanzimi ile yönlendirilecektir. Bu durumda AM geçerli olmaya devam edecektir. Otomatik Mod'da özetle; Kumanda Merkezi aktiftir. Günlük işletme senaryosu interlock (PLC) içerisinden aktiftir. Günlük işletme senaryosuna bağlı rotalar tanzim edildiğinde ilgili sinyal lambaları sürekli yeşil ışık verirler. Lokal Kumanda Butonları devre dışıdır.

4.3.2.2 Operator modu (OM)

OM, AM ile aynı özelliklere sahiptir. Ancak, Kumanda Merkezinde bulunan operatörün alternatif bir rota tanzim etmek istemesi durumunda kendi kendine bu moda geçiş yapacaktır. Bu modda;

- Kumanda Merkezi aktiftir.
- KM yazılımı ile günlük işletme senaryosu dışındaki alternatif rotalar PLC'ye gönderilir ve uygunluk durumuna göre alternatif rotalar aktif edilir. İlgili rotalar tanzim edildiğinde ilgili sinyal lambaları sürekli yeşil ışık verirler.
- Lokal Kumanda Butonları devre dışıdır.

4.3.2.3 Lokal otomatik mod (LAM)

Bu mod, Şekil 4.4, Şekil 4.5, Şekil 4.6, Şekil 4.7, Şekil 4.8 ve Şekil 4.9 ile gösterilen senaryoların herhangi birisi geçerli olduğu durumlarda kullanılacak çalışma modunu kapsamaktadır. Bununla birlikte Kumanda Merkezi ile haberleşme bağlantısı koptuğunda sistem kendi kendini bu moda alacaktır.

Ana işletme senaryosu haricindeki tüm tanımlı senaryolar; makinist/kullanıcı tarafından makas bölgesindeki veya Mescid-i Selam İstasyonundaki lokal kumanda butonlarından herhangi birisine basılarak işletilebilecektir.

Bu şekildeki işletme modunda makas hareketleri ve demiryolu trafik sinyalleri lokal kumanda butonlarına basıldıktan sonra otomatik olarak çalışacaktır. Bu modda;

- Kumanda Merkezi devre dışıdır. Sistem sahadaki PLC üzerinden lokal olarak çalışır.
- Günlük işletme senaryosu interlock (PLC) içerisinden aktiftir. Günlük işletme senaryosuna bağlı rotalar tanzim edildiğinde ilgili sinyal lambaları sürekli yeşil ışık verirler.
- Lokal kumanda butonları aktiftir. Lokal kumanda butonlarına basıldığında tanzimli rotalar iptal edilir ve yalnızca makaslar tanzim edilir. Tanzimden sonra ilgili sinyal lambası kesikli kırmızı (flashing red) ışık verir.

4.3.2.4 Emniyet modu (EM)

Sistem AM, OM veya LAM'dan birisini aktive edemediği durumda EM'na geçiş yapacaktır. Bu mod, makas bölgesi üzerinde sisteme ait ekipmanlarda veya alt sistemlerde bir arıza meydana gelmesi durumunda veya sistemin çalışmasını olumsuz etkileyecek herhangi bir dış etki durumunda aktive olacaktır. EM'nda lokal kumanda butonlarıyla sadece makas hareketleri yapılabilecektir. Tren makaslar üzerinden geçiş yaparken makas motorları kesinlikle hareket etmeyecektir. Bu modda;

- Tüm rota talepleri ve aktif rotalar iptal edilir.
- Lokal kumanda butonları devre dışıdır.
- Tüm sinyal lambaları sönüktür.

4.3.3 Sisteme ait kullanıcı arayüzleri

Bölgeyi kontrol edecek olan sistem aşağıdaki arayüzlere sahip olacaktır:

4.3.3.1 Lokal kumanda butonları

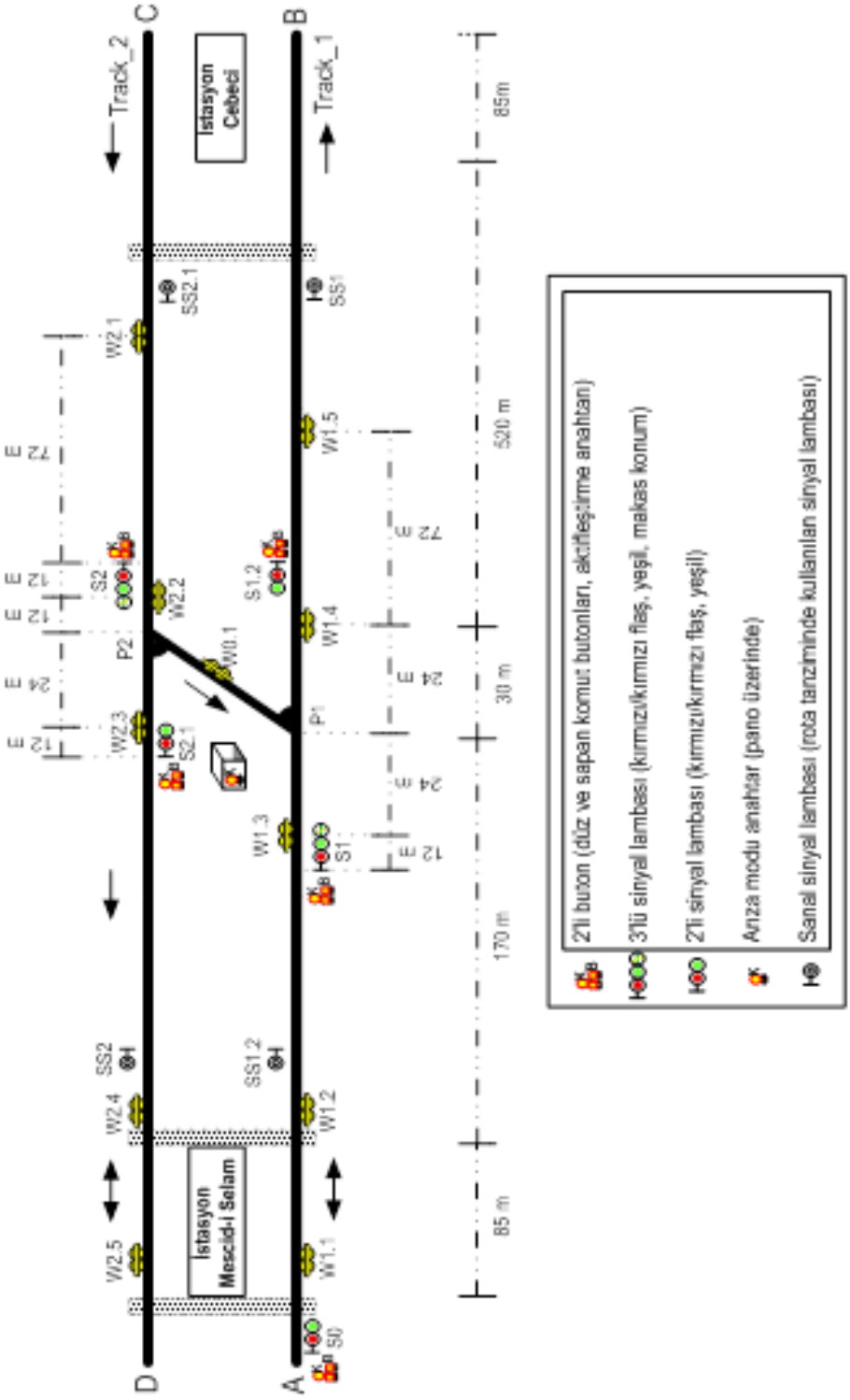
Her bir sinyal direği üzerinde makas konumlarını gerektiğinde (OM veya LAM) ayarlayabilmek amacıyla butonlar bulunacaktır. Tekli sinyaller üzerinde tek buton (makası normal konuma alabilmek için), üçlü sinyaller üzerinde ise çift buton (makası normal veya sapan konuma alabilmek için) yerleştirilecektir.

OM veya LAM'da butonlar yardımıyla makas konumlarını ayarlayabilmek için makinist/kullanıcı sinyal direği üzerinde bulunan güvenlik anahtarını çevirerek butona basacaktır. Anahtar çevrilmeden butona basıldığında makaslar hareket etmeyecektir.

Butonlar vasıtası ile tren hareketi gerçekleştirmeden önce makinist KM ile görüşerek kontrollü geçiş yapacaktır. KM'ye haber verilmeksizin LAM kesinlikle kullanılmayacaktır.

4.3.3.2Trafik sinyal lambaları

Mescid-i Selam makas otomasyonu projesinde 3 adet ikili sinyal, 2 adet üçlü sinyal kullanılacaktır. İkili sinyaller kırmızı, yeşil ve kırmızı flaş bildirimi verecektir. Üçlü sinyallerde ikili sinyaller ile aynı renk bildirimlerini verecek olup en üstte bulunan lamba makasın konum bilgisini (normal veya sapan) makiniste bildirmek amacıyla



Şekil 4.11 : Mescidi selam lokal sinyalizasyon sistemi ekipman yerleşimi.

kullanılacaktır, eğer makas herhangi bir konumda değil ise ilgili lamba hiçbir bildirim vermeyecektir. Sinyal renk bildirimleri aşağıdaki gibi tanımlanmıştır:

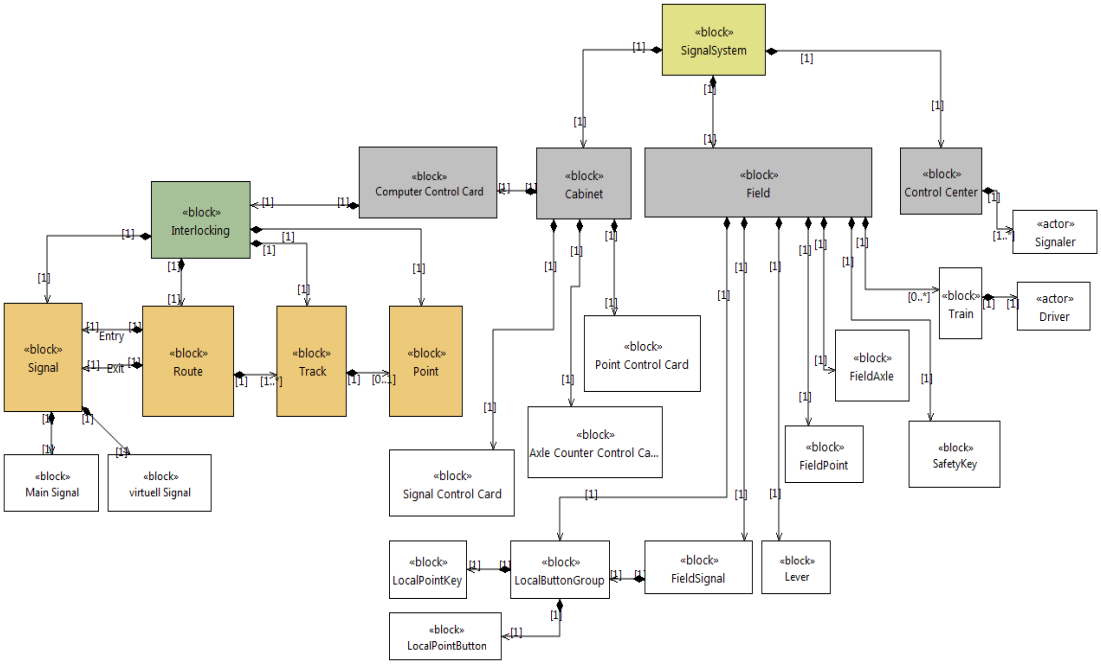
- Kırmızı: Dur, bir sonraki blok dolu.
- Yeşil: İzin verilen hız ile ilerleyebilirsin.
- Flaş Kırmızı: Her an duracakmış gibi ilerleyebilirsin.
- Saha ekipman yerleşimleri Şekil 4.1'de gösterilmektedir.

4.3.3.3 Kumanda merkezi yazılımı

Kumanda Merkezi Yazılımı operatör ile anklaşman sistemi arasındaki bir arayüz yazılımıdır. Bu arayüz, sahanın kontrol ve kumandar edilmesi için tasarlanmıştır. Operatör, sahadaki ekipmanların durumlarını tanımlı grafikler aracılığı ile izleyebilecektir. Bununla birlikte sistemi uzaktan kumanda edebilecektir.

4.3.4 Sistem Mimarisi

Mescidi Selam Lokal sinyalizasyon Sistemine ait mimari şu şekilde tarif edilebilir: saha ekipmlanları, kabinet sistemi (yani OCS, nesne kontrol sistemi) anklaşman sistemi, kumanda merkezi yazılımı. Şekil 4.12'de SCADE yazılımı aracılığı ile tasarlanan sistem mimarisi görülmektedir.



Şekil 4.12 : Mescidi selam lokal sinyalizasyon sistemi hiyerarşik şeması.

Anklaşman sistemi sisteme ait tüm komponentleri kontrol ve kumanda edecektir. Kabinet alt sisteminde, sinyal kontrol kartları, aks sayıcı sistemi, makas motoru

kontrol kartları bulunmaktadır ki bu komponentler anklaşman sistemi ile saha ekipmanları arasındaki arayüzlerdir.

Sinyal kontrol kartı, anklaşman sisteminden aldığı komutlar neticesinde sahadaki lambalara kırmızı, yeşil ve yanıp sönen kırmızı ışık bildirimlerini gönderecek; bunun yanında sahadaki lambaların arızalarına karşın uyarı ve hata geri bildirimlerinde bulunacaktır.

Aks sayıcı sistemi, bölgedeki trenleri varlığını tesbit ederek, belirlenen ray bölgesinin meşgul veya serbest bilgisini anklaşman sistemine gönderecektir.

Makas motoru kontrol kartı ise bölgede bulunan makasların emniyetli çalışmasını sağlayan anklaşman sisteminden gelen komutlara göre makas konumlarını düz veya sapan olarak değiştirecektir. Bununla birlikte makas motoruna manivela takılması bilgisini de anklaşman sistemine iletecektir.

Saha üzerinde bulunan ekipmanlar (way side equipments) aks sayıcı sistemine bağlı olarak ray bölgesi (track section), sinyal kartına bağlı olarak sinyal lambaları ve de makas kontrol kartına bağlı olarak makas motorlarından oluşmaktadır. Bunlara ek olarak, direkt anklaşman sistemi ile bağlantılı olan emniyet butonları (Safety Key) ve lokal kumanda butonları bulunmaktadır.

4.4 Mescidi Selam Lokal Sinyalizasyon Sisteminin Risk Değerlendirmesi

Mescidi Selam Lokal Sinyalizasyon Sistemine ait sistem ve alt sistem tablosu Çizelge 4.2'de gösterilmektedir. Bu çizelgede sistem bileşenlerine ait fonksiyonel tanımlar belirlenmiş ve sınıflandırılmıştır.

Çizelge 4.2'de belirtildiği gibi; Besleme Sistemi (PS) ana güç/besleme kaynağından gelen enerjiyi sistem içerisinde kullanılabilecek seviyeye indirgemek, LED aydınlatmaları için gerekli gücü sağlama ve sistemin aşırı gerilime karşı korunması için topraklama fonksiyonunu yerine getirmektir.

Anklaşman Sistemi (IS), sisteme ait tüm saha elemanlarını kontrol ve kumanda etmek, sahadan veya kullanıcıdan gelen mantıksal verileri değerlendirip sistemin emniyetli bir şekilde işletilebilmesini sağlamaktır. Bununla birlikte tren algılamasının emniyetli bir şekilde yapılması ve Kumanda Merkezi ile haberleşme sağlanması da yine bu alt sistemin fonksiyonlarındandır.

Çizelge 4.2 : Sinyalizasyon sisteminin fonksiyonel tanımı.

No:	Alt Sistem	No:	Komponent	Fonksiyon Tanımı
A1	Besleme (PS)	A1.1	750V/24V DC besleme (PS24a)	Katener Hattından gelen 750 V DC gerilimini 24V DC'ye çevirmek. Sistemin beslemesini sağlamak.
		A1.2	24/48V DC besleme (PS48)	24V sistem besleme girişini 48V DC'ye çevirmek. Lambaların beslemesini sağlamak.
		A1.3	Topraklama Ünitesi (EU)	Aşırı gerilime karşı sistemi korumak
A2	Anklaşman (IS)	A2.1	İşlemci (CPU)	Tüm sistemlerin işlerliğini denetlemek. Saha kontrol ve kumandasını sağlamak.
		A2.2	Giriş/Çıkış Modülü (IOM)	Tüm mantıksal giriş ve çıkışları işlemciye iletmek. Tren varlığını algılayıp, anlık durumu logic olarak işlemciye bildirmek.
		A2.3	Haberleşme Modülü (CM)	HMI alt sistemi ile sürekli haberleşmeyi sağlamak. IOMile CPU arasındaki haberleşmeyi sağlamak.
A3	Makas Kontrol Modülü (PCM)	A3.1	Motor Tahrik Modülü (PDM)	Makas elektrik motorunu tahrik etmek. Makas mekanizmasını çalıştırmak.
		A3.2	Konum İndikatörü (PI)	Makasın konumunu izlemek.
A4	Lamba Kontrol Modülü (LCM)	A4		Lamba durumlarını izlemek. Lambaları aydınlatmak.
A5	Kullanıcı Arayüzü (HMI)	A5.1	Kumanda Merkezi (GUI)	Sistemin tesis edildiği bölgeyi uzaktan izlemek. Dispeçer kullanıcısının sistemi yönetmesini sağlamak. Sisteme ait tüm verileri arşivlemek.
		A5.2	Buton/Anahtar ve LED lamba (MMI)	Makinist/bakımcı kullanıcısının sahadan sistemi yönetmelerini sağlamak. Makiniste tren hareket yetkisini (kırmızı/yeşil) bildirmek.

Makas kontrol modülü (PCM), makasların konumlarını değiştirmek yani hareket ettirmek ve makasların mevcut bulundukları konumları izlemektir. Lamba kontrol modülü (LCM) de benzer bir fonksiyona sahip olup, LED lambaların durumlarını sürekli takip ederek gerektiğinde enerjilendirerek ışık vermesini sağlamaktır.

Kullanıcı arayüzü (HMI) modülünde ise saha veya Kumanda Merkezindeki tüm kullanıcı arayüzleri bulunmaktadır. bunlar, operatör bilgisayarı (kumanda merkezi yazılımı), lokal kontrol butonları ve LED lambalardır.

Çizelge 4.3'de bu sistemin işletdildiği hatta ait işletmesel veriler bulunmaktadır. sistemin tesis edildiği bölgenin bir tren tarafından meşgul edilme oranı X_1; sisteme ait anklaşman yazılımının hata sıklığı X_2; ilgili bölgeden geçen trenlerin kırmızı ışık ihlali yapma oranı X_3; makasın konum değiştirirken hareketini standart sürede tamamlayamaması durumu X_4 ve son olarak ilgili bölgede tren algılanamaması durumu ise X_5 ile ifade edilmiştir. Bu bilgiler İstanbul Ulaşım AŞ birimlerinin işletme ve arıza kayıtları baz alınarak elde edilmiştir.

Çizelge 4.3 : Mescidi selam lokal sinyalizasyon sistemi işletme istatistikleri.

Olay	Olay Açıklaması	Değer	Birim
X_1	bir trenin bölgeyi meşgul etme oranı	5,90E-03	birimsiz
X_2	yazılım hatası (SIL 2 olduğu varsayılarak); (dolayısıyla, hatalı yeşil ihtimali…)	3,00E-03	birimsiz
X_3	herhangibir trenin bölgeden kırmızı ışıkta geçme ihtimali	4,03E-06	birimsiz
X_4	makas hareketinin standart sürede tamamlanamaması	2,28E-04	1/saat
X_5	makas bölgesinde tren algılanamaması (aks sayıcı arızası)	5,71E-06	1/saat

Bölüm 3'te anlatılan FMEA-FTA Tabanlı Risk Analizi için, Bölüm 2'de detaylı açıklanan, Hata Şiddet Parametreleri (Çizelge 4.4), Risk Seviyesi Parametreleri (Çizelge 4.5), Hata Sıklık Parametreleri (Çizelge 4.6) ve EN Standardına göre tanımlanmış Risk Hesaplama Matrisi (Çizelge 4.7) aşağıda verilmiştir.

Çizelge 4.4 : Hata şiddet parametreleri.

Seviye	Şiddet Kategorisi	İşletmeye Etkisi
4	Yıkıcı	Sistemin 1 hafta devre dışı kalması /Trenin raydan çıkması
3	Kritik	Sistemin 1 gün devre dışı kalması (işletme anında giderilemeyen hata)
2	Düşük	Sistemin 1 saat devre dışı kalması (işletme esnasında giderilebilen hata)
1	Önemsiz	Sistemin 20 dakika devre dışı kalması (anında müdahale ile giderilebilen hata)

Çizelge 4.5 : Risk seviyesi parametreleri.

Seviye	Risk Sınıfı	Risk Kontrolü
R1	Kabul edilemez	Risk giderilmeli
R2	Sakıncalı	Risk, mümkünse giderilmeli
R3	Tahammül edilebilir	Risk kontrol altında tutulmalı
R4	Önemsiz	Kabul edilebilir risk

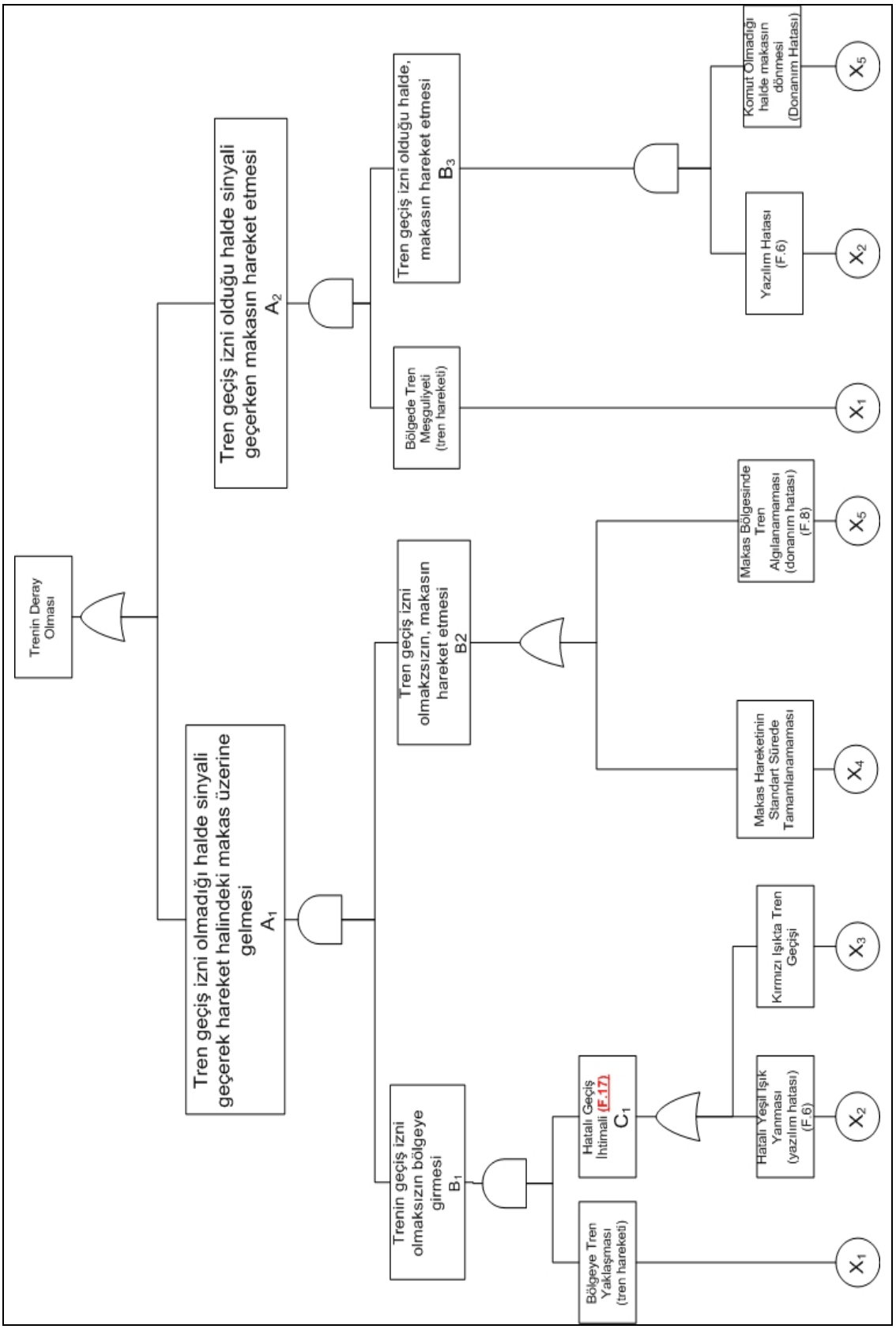
Çizelge 4.6 : Hata sıklık parametreleri.

Seviye	Kategori	Tanım	Sıklık / yıl başına
A	Sık	Büyük ihtimalle olması beklenen	100'den fazla
B	Muhtemel	Birçok kez tekrarlanacak	1 ; 100
C	Ara sıra	Birçok kez tekrarlanma ihtimali bulunan	1E-2 ; 1
D	Uzak	Sistem işletmede olduğu sürece (life cycle) birkaç kez olması beklenen	1E-4 ; 1E-2
E	İmkansız	Olma ihtimali bulunmayan ancak istisnai olarak olması beklenen	1E-6 ; 1E-4
F	İnanılmaz	Olma ihtimali bulunmayan ve olmaması beklenen	1E-6'dan az

Çizelge 4.7 : Risk hesaplama matrisi.

Hata Sıklıkları	A	R2	R1	R1	R1
	B	R3	R2	R1	R1
	C	R3	R2	R2	R1
	D	R4	R3	R2	R2
	E	R4	R4	R3	R3
	F	R4	R4	R4	R4
		1	2	3	4
		Hata Şiddeti			

Çizelge 4.4, Çizelge 4.5, Çizelge 4.6 ve Çizelge 4.7'de belirtilen parametrelere göre hazırlanan FMEA Çalışması Ek A'da gösterilmektedir. Ek A'da belirtilen bu FMEA çalışmasından yola çıkarak oluşturulacak FTA Modelinde üst olay olarak, FMEA'da "Trenin Deray Olması" hata sonucu incelenmiştir. Bu olayın meydana gelme olasılığını hesaplamak için Şekil 4.13'te gösterilen FTA Modeli oluşturulmuştur.



Şekil 4.13 : Mescidi selam lokal sinyalizsyon sistemi için hazırlanmış FTA modeli.

Şekil 4.13'te gösterilen FTA Modelinde iki ana unsur göz önünde bulundurulmuştur. Bunlardan 1.'si, Trenin, sistem tarafından, geçiş izni olmadığı halde sinyali geçerek hareket halindeki makas üzerine gelmesi (A_1); 2.'si ise sistem tarafından trene geçiş izni verildiği halde sinyali geçerken makasın hareket etmesidir (A_2). Bu iki durum da trenin başlıca deray olma sebepleridir. A_1 olayının olabilmesi için makas bölgesine tren girişi olmalı ve makas hareket etmelidir. A_2 olayının meydana gelebilmesi için ise yine bölgeye tren girişi olmalı ve bu durumda makas motoru hareket etmelidir. Verilen FTA Modelinin Bool Cebri ile ifadesi aşağıdaki denklemlerle açıklanmış ve sadeleştirilmiş Bool Denklemi (4.4) denkleminde verilmiştir.

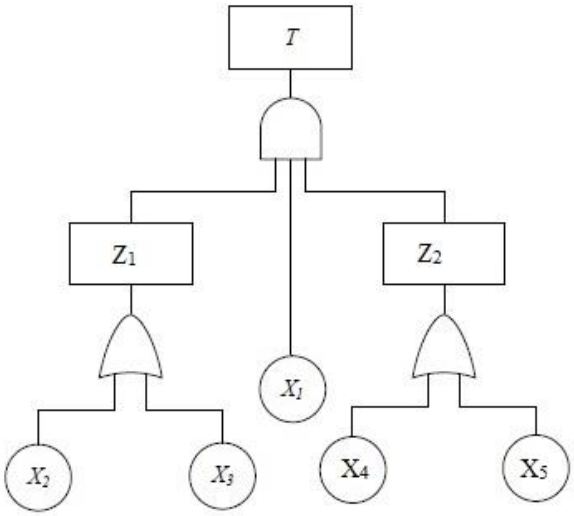
$$T = A_1 + A_2 \quad \textbf{(4.1)}$$

$$A_1 = B_1 \,.\, B_2 = (X_1.X_2 + X_1.X_3) + (X_4 + X_5) \quad \textbf{(4.2)}$$

$$A_2 = X_1 .\, B_3 = X_1.X_2.X_5 \quad \textbf{(4.3)}$$

$$T = X_1 .\, (X_2 + X_3) .\, (X_4 + X_5) \quad \textbf{(4.4)}$$

elde edilen deklem ile sadeleştirilmiş FTA modeli Şekil 4.14'de verilmiştir.



Şekil 4.14 : İndirgenmiş FTA modeli.

Bu durumda Çizelge 4.3'te verilen işletme istatistiklerinden yararlanarak F(T) değeri hesaplanabilir. Şekild 4.14'de verilen indirgenmiş FTA modeli Çizelge 4.3'deki veriler yardımıyla şu şekilde hesaplanacaktır:

$$F(T) = F(Z_1) .\, F(Z_2) .\, F(X_1) \quad \textbf{(4.5)}$$

$$F(Z_1) = 1 - \{1 - F(X_2)\}.\ \{1 - F(X_3)\} \quad \textbf{(4.6)}$$

$$F(Z_2) = 1 - \{1 - F(X_4)\}.\ \{1 - F(X_5)\} \quad \textbf{(4.7)}$$

$$F(T) = \sim 6x10^{-7}\ /\text{saat} \quad \textbf{(4.8)}$$

4.5 Özet

Bölüm 3'te verilen risk değerlendirme yöntemlerinden FMEA – FTA birleşimi yöntemi kullanılarak bir uygulama yapılmıştır. Uygulama, şu an devreye alma çalışmaları süren Mescidi Selam Lokal Sinyalizasyon Sistemine ait risk değerlendirmesini kapsamaktadır. Dolayısıyla FMEA modeli, ilgili sistem baz alınarak oluşturulmuş; ardından en önemli risk sonucu olan "trenin deray olması" alınarak FTA modelinde ana olay (top event) olarak belirlenmiştir. Bu olayın meydana gelmesi durumları irdelenmiş ve elde edilen temel olaylar işletme istatistikleri ile sisteme ait komponentlerin hata oranları alınarak işlem yapılmıştır. Nihai olarak; (4.8) denkleminde elde edilen değer Mescidi Selam Makas Bölgesinde 1 saat boyunca deray hadisesinin yaşanması ihtimalini ortaya koymaktadır. Bu değer PFH olarak bilinen 1 saatte hata yapma ihtimali terimi ile benzerlik göstermektedir.

5. SONUÇ VE ÖNERİLER

Günümüzdeki demiryolu projelerinde, kent içi taşımacılık veya şehirler arası taşımacılık türleri fark etmeksizin emniyetli bir işletmenin sağlanabilmesi amaçlanmaktadır. Bu projelerin kısıtlı süre içerisinde ve belirli maliyet seviyelerinde emniyetli bir şekilde işletme sağlamak için RAMS yönetiminin uygulanması gerekliliği hâsıl olmuştur. Bununla birlikte, demiryolu sektöründe sistem mühendisliği kapsamına RAMS yönetimi de girmek durumundadır.

Bu çalışma, çeşitli risk değerlendirme modelleri ve süreçleri üzerinde durmuş; RAMS yönetimi için kabul görmüş teknikleri incelemiştir. Raylı sistemler mühendisliği kapsamına RAMS yönetiminin başarılı bir şekilde entegrasyonunun sağlamak için hedefler belirlemiş ve bunları incelemiştir. Bu çalışma, önerilen yönetim modellerini, süreçleri ve teknikleri demiryolu kuruluşları için ve sistem kavramı tasarım aşamasında RAMS yönetiminin uygulanması için faydalanılabilecek bir rapor halinde sunulmuştur.

Çalışmanın incelediği konular; RAMS Yönetimi ve RAMS yönetiminde kullanılan risk değerlendirme yöntemlerini kapsamaktadır. Kapsamlı bir standart araştırması niteliğine de sahip olan bu çalışma sistem mühendisliği alanında çalışma yapmak isteyen araştırmacılar için faydalı bir rapor olacaktır. İncelenen konular belirli bir uygulama sahasında gerçeklenmiş ve sunulmuştur.

Bu araştırma öncelikle sistemleri ile ilişkili teorik mühendislik dağarcığı oluşturarak RAMS yönetimi kurma hedefini elde etmektedir.. Sistem RAMS yönetim sistemleri mühendisliği dalı yönetimi disiplinidir. Böylece, bu araştırma RAMS yönetimi genel fonksiyonları ve yaşam döngüsü faaliyetleri için temel bir dayanak oluşturduğuna sistemleri mühendisliği kavramlarını tanımlanmıştır. Bu araştırma sistemlerinin kavramı üç açıdan incelenmiştir. Bunlar; işletme kriterlerinin tanımlanması, risklerin belirlenmesi için gerekli bilgilerin toplanması ve işletmeyi tehdit eden tüm potansiyel risklerin değerlendirilmesi ve kontrol altında tutulması olarak özetlenebilir. Bu çalışmada kurulan risk değerlendirme yöntemleri; yukarıdan aşağıya ve aşağıdan yukarıya değerlendirme yaklaşımı ile nitel ve/veya nicel kombine yaklaşımı

şeklindedir. Bu çalışmada, etkin bir sistemleri mühendisliği uygulaması için demiryolu RAMS yönetimi, demiryolu sistemleri mühendisliğine sistematik bir şekilde entegre edilmiş ve önerilen risk analiz yaklaşımı sağlanmıştır. Raylı sistemler mühendisliği süreci ve çeşitli süreç modelleri aracılığıyla süreç faaliyetleri RAMS yönetimi ile ilgili süreç, fonksiyonlar, etkinlikler ve teknikleri temel dayanak oluşturması sağlanmıştır. Aynı zamanda RAMS temelli demiryolu değerlendirilmesi ve tüm demiryolu RAMS riskleri kontrol üzerinde RAMS yönetimi odaklanmak için yönetim sürecini oluşturmuştur. Önerilen RAMS yönetim sistemleri, demiryolu sistemleri mühendisliği süreci ve risk bazlı RAMS yönetimi süreci demiryolu mühendisliği projesinde RAMS yönetimini uygulamak için gerekli unsurlar olacaktır. Demiryolu risk değerlendirme süreci için FMEA ve FTA gibi tipik risk değerlendirme teknikleri, hedefleri, avantajları, dezavantajları, incelenmiştir. Bu sonuçlar farklı kaynaklardan kapsamlı bir inceleme yoluyla elde edilmiştir.

Bu araştırma sonunda önerilen FMEA-FTA temelli risk değerlendirme yöntemi ile Mescidi Selam Lokal Sinyalizasyon Sistemine ait riskleri incelemiş ve "tren deray" olması riski üzerinde durmuştur. Bu örnek çalışmada, Mescidi Selam Lokal sinyalizasyon Sistemi için ayrıntılı yapısal ve işlevsel açıklamalar sunulmuş; tüm olası hatalar analiz edilmiştir. Hata sonuçlarını belirlemek için sahadan toplanan işletme verileri ile hata analizi desteklenmiştir. Bu işlevsel bilgiler kapsamında, risk parametreleri, risk seviyeleri ve risk değerlendirme matrisi kurulmuştur. "tren dray" olması olayının Bool Cebri ile FTA modeli sayısal olarak hesaplanmıştır.

Önerilen modeller, süreçler ve teknikler tasarlanmış ve raylı sistemler mühendisliği için RAMS yönetim sistematik bir yaklaşım sağlamak üzere geliştirilmiştir. Bu çalışma, RAMS yönetimini tanıtma açısından ülkemiz demiryolu işletmecilerine katkı sağlayacaktır. Bununla birlikte, bir sonraki çalışma alanı olarak, araştırmacılar, bu süreçleri derinlemesine inceleyebilir ve ülkemizde henüz önemini kavrayamamış bu konunun anlaşılmasına katkı sağlayabilirler. Raylı sistemlerle ilgilenen mühendislik disiplinleri; emniyeti geliştirmek ve ülkemizin demiryolu yatırımlarında teknik altyapımızın üst seviyelere taşınmasına katkı sağlamak için sistem mühendisliği ve RAMS Yönetimi konularını araştırmalıdırlar. Hızla artan demiryolu yatırımlarının sürekliliği ve vatandaşlarımızın daha konforlu bir hayat yaşamalarını garanti etmek için biz mühendislere çok büyük görevler düşmektedir.

KAYNAKLAR

An, M. (2005). A review of design and maintenance for railway safety - the current status and future aspects in the UK railway industry. World Journal of Engineering, Vol.2 (3), pp.10-22.

An, M. Lin ve W., Huang, S (2013). An Intelligent Railway Safety Risk Assessment Support System for Railway Operation and Maintenance Analysis. The Open Transportation Journal, Vol.7, pp.27-42.

Blanchard, B. S. (2012). System engineering management, Wiley

BS EN 31010 (2010). Risk Management – Risk Assessment Techniques. London: British Standards Institution (BSI).

BS EN 50126-1 (1999). Railway applications – The Specification and Demonstration Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic Requirements and Generic Process. London: British Standards Institution (BSI).

BS EN 50126-2 (2007). Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 3: Guide to the Application of EN 50126-1 for Safety. London: British Standards Institution (BSI).

BS EN 50126-3 (2006). Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 3: Guide to the application of EN 50126-1 for Rolling Stock RAMS. London: British Standards Institution (BSI).

BS EN 50128 (2009). Railway Applications - Communication, Signalling and Processing Systems - Software for Railway Control and Protection Systems. London: British Standards Institution (BSI).

BS EN 50129 (1999). Railway Applications - Communication, Signalling and Processing Systems - Safety related Electronic Systems for Signalling. London: British Standards Institutionm(BSI).

BS EN 60300-3-1 (2004). Dependability Management – Part 3-1: Analysis Techniques for Dependability – Guide on Methodology. London: British Standards Institution (BSI).

BS EN 60300-3-4 (2008). Dependability Management – Part 3-4: Application guide — Guide to the specification of dependability requirements. London: British Standards Institution (BSI).

BS EN 60300-3-5 (2001). Dependability Management – Part 3-5: Application guide — Reliability test conditions and statistical test principles. London: British Standards Institution (BSI).

BS EN 60300-3-15 (2009). Dependability management - Part 3-15: Guidance to engineering of system dependability. London: British Standards Institution (BSI).

BS EN 60812 (2006). Analysis Techniques for System Reliability – Procedure for Failure Mode and Effects Analysis (FMEA). London: British Standards Institution (BSI).

BS EN 61025 (2007). Fault tree analysis (FTA). London: British Standards Institution (BSI).

BS EN 61124 (2012). Reliability testing - Compliance tests for constant failure rate and constant failure intensity. London: British Standards Institution (BSI).

BS EN 61164 (2004). Reliability Growth - Statistical test and estimation methods. London: British Standards Institution (BSI).

BS EN 61508-1, 2, 3, 4, 5, 6, 7 (2002 - 2005). Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1 to 7: Functional safety and IEC 61508. London: British Standard Institution (BSI).

BS IEC 61882 (2001). Hazard and Operability studies (HAZOP studies – Application guide. London: British Standards Institution (BSI).

BS ISO 9000 (2014). Quality Management Systems – Fundamentals and Vocabulary. London: British Standards Institution (BSI).

BS ISO 15288 (2002). Systems Engineering – System Life cycle Processes. Lodon: British Standards Institution (BSI).

BS ISO/IEC 26702 (2007). Systems Engineering – Application & Management of the Systems Engineering Process. London: British Standards Institution (BSI)

Haskins, K. F. a. M. K. (2007). Systems Engineering Handbook: A Guide for System Life Cycle Process and Activities. International Council on Systems Engineering (INCOSE).

Cantos, P. & Campos, J. (2005). Recent changes in the global rail industry: facing the challenge of increased flexibility.

Daup (2001). Systems Engineering Fundamentals, Vergina, USA, Defense Acquisition University Press.

Ebeling, C. E. (2010). An Introduction to Reliability and Maintainability Engineering, Canada, Waveland Press, Inc.

Elphick, J. (2010). Railway Systems Engineering Why is Water Wet? *In:* Railway Signalling and Control Systems (RSCS 2010), IET Professional Development Course on, 2010. IET, 250-270.

Ericson, C. A. (2005). Hazard analysis techniques for system safety, Wiley-

Gofuku, A., Koide, S. & Shimada, N. (2006). Fault tree analysis and failure mode effects analysisnbased on multi-level flow modeling and causality estimation. *In:* SICE-ICASE, 2006.nInternational Joint Conference, 2006. IEEE, 497-500.

Kapurch, S. J. (2010). NASA Systems Engineering Handbook, DIANE Publishing

Kaufmann, J. J. (1982). Function analysis system technique (FAST) for management applications.nValue World, Vol.5.

Lundteigen, M. A., Rausand, M. & Utne, I. B. (2009). Integrating RAMS engineering and management with the safety life cycle of IEC 61508. Reliability Engineering & System Safety, Vol.94, pp.1894-1903.

MIL HDBK 189c (2011). Handbook of Reliability Growth Management. Washington DC: Department of Defense.

MIL HDBK 781A (1996). Handbook for Reliability Test Methods, Plans, and Environments for Engineering, Development Qualification and Production. Washington, DC: Department of Defense.

Mil Std 499a (1994). Systems Engineering (Draft). Washington, DC: Military Standard, Notice 1.

Mil Std 882d (2000). Standard Practice for System Safety. Washington, DC: Department of Defense.

Profillidis, V. A. (2007). Railway management and engineering, Ashgate Publ., Ltd.

Stamatelatos, M. & Caraballo, J. (2002). Fault tree handbook with aerospace applications, Office of safety and mission assurance NASA headquarters.

Ucla, A. A., Avizienis, A., Laprie, J.-C. & Randell, B. (2001). Fundamental concepts of dependability.

Umar, A. A. (2010). Design for safety framework for offshore oil and gas platforms. University of Birmingham

Url-1 <http://www.dttas.ie/sites/default/files/publications/public-transport /english/review-rail-safety-ireland/review-rail-safety-ireland.pdf>. alındığı tarih: 15.11.2014

Url-2 <http://www.jernbaneverket.no/PageFiles/17329/P%C3%B6yry%20 Report%20HSR%20Phase%203,%20Risk%20and%20safety%20rev%20 1.pdf>. alındığı tarih: 10.11.2014

EKLER

EK A: Mescidi Selam Lokal Sinyalizasyon Sistemi FMEA Özet Tablosu

Hata Kodu (failure code)	Alt Sistem	Komponent Hata Türü (failure mode)	Muhtemel Hata Sebepleri	Hata Sıklığı (P) (failure frequency)	Hata Şiddeti (S) (failure severity)	Risk Seviyesi (R)	Hata Etkisi (failure consequence)	Hatanın Teşhisi	Riskin Kontrolü için Alınması Gereken Önlemler
F.1	PS	Ana Besleme Arızası	Katener Hattında Enerji kesintisi	C	1	R3	sistemin devre d	Sistem ile tüm haberleşmenin kesilmesi	
F.2	PS	A1.1 modullerinden birinin arızalanması	Donanım Hatası	E	3	R3	sistem fonksiyo	Alarm log'ları ile takip edilmesi	Periyodik bakımlarla yedekli olarak çalışan güç

Hata Kodu (failure code)	Alt Sistem	Komponent Hata Türü (failure mode)	Muhtemel Hata Sebepleri	Hata Sıklığı (P) (failure frequency)	Hata Şiddeti (S) (failure severity)	Risk Seviyesi (R)	Hata Etkisi (failure consequence)	Hatanın Teşhisi	Riskin Kontrolü için Alınması Gereken Önlemler
F.3	PS	A1.2 arızası	Donanım Hatası	D	2	R3	LED lambaların	Alarm log'ları ile takip edilmesi	yukarıdaki maddede yedeklilik eklenince bu maddenin hata sıklığı D'ye
F.4	PS	Topraklama Kablosunun devre dışı kalması	Kablo Hatası	E	2	R4	Sistemin aşırı g	Rutin bakımlarla elektriksel ölçümler alınması	
F.5	IS	CPU Arızası	Donanım Hatası	C	3	R2	sistem fonksiyo	Sistem ile tüm haberleşmenin kesilmesi veya arıza bildirimi	

Hata Kodu (failure code)	Alt Sistem	Komponent Hata Türü (failure mode)	Muhtemel Hata Sebepleri	Hata Sıklığı (P) (failure frequency)	Hata Şiddeti (S) (failure severity)	Risk Seviyesi (R)	Hata Etkisi (failure consequence)	Hatanın Teşhisi	Riskin Kontrolü için Alınması Gereken Önlemler
F.6	IS	Anklaşman Arızası (Sinyal ihlali riski)	Yazılım Hatası	E	3	R3	sistem fonksiyonlarının azalması (dolaylı deray riski)	Arıza bildirimi	Tüm işletmesel senaryolar test edilmiştir.
F.7	IS	IOM Arızası	Donanım Hatası	C	3	R2	sistem fonksiyonlarının azalması (saha komutlarının iletilememesi	Sistem ile tüm haberleşmenin kesilmesi veya arıza bildirimi	
F.8	IS	Tren algılamasının yapılamaması (Sinyal ihlali riski)	Donanım Hatası / Algılayıcı Hatası / Algılayıcı pozisyonu	C	3	R2	sistem fonksiyonlarının azalması (dolaylı deray riski)	Aks sayıcı sisteminin hataya düşerek uyarı bildirimi yapması	Bakım periyotları artırılarak hata sıklığı azaltılmalıdır.

Hata Kodu (failure code)	Alt Sistem	Komponent Hata Türü (failure mode)	Muhtemel Hata Sebepleri	Hata Sıklığı (P) (failure frequency)	Hata Şiddeti (S) (failure severity)	Risk Seviyesi (R)	Hata Etkisi (failure consequence)	Hatanın Teşhisi	Riskin Kontrolü için Alınması Gereken Önlemler
F.9	IS	CM arızası	Donanım Hatası	D	2	R3	sistemin lokal n	moda geçiş yapması	Sistemin lokal
F.10	IS	CM kablo arızası	Fiber Optik Kablo Hatası (Yedekli)	C	1	R3	sistemin lokal n	moda geçiş yapması	Sistemin lokal
F.11	PCM	PDM Tahrik Arızası	Elektrik Motoru Hatası / Makas Motorunun Tahrik Kolunun	C	3	R2	sistem fonksiyo	Makas motorunun hareket etmemesi	Makas motoruna ait yedek malzemeler hazırda tutulmalıdır ve

Hata Kodu (failure code)	Alt Sistem	Komponent Hata Türü (failure mode)	Muhtemel Hata Sebepleri	Hata Sıklığı (P) (failure frequency)	Hata Şiddeti (S) (failure severity)	Risk Seviyesi (R)	Hata Etkisi (failure consequence)	Hatanın Teşhisi	Riskin Kontrolü için Alınması Gereken Önlemler
F.12	PCM	PDM kablo arız	Kablo Hatası	D	2	R3	sistem fonksiyo	Makas motorunun hareket etmemesi	
F.13	PCM	PDM Yön Arızası	Kontaktör Arızası	D	2	R3	sistem fonksiyo	Makas motorunun hareket etmemesi	hatanın hızlı giderilmesi için koltuk ambarında yedek komponent
F.14	PCM	PI belirsizlik arızası	Sensör Arızası / Kablo Hatası / Makas Motoru Tespit Kolunun Kırılması	B	4	R1	deray riski (makas motorunun hareketini tamamlayamaması)	Makas motorunun konumunun tespit edilememesi (alarm logları	Bakım periyotları artırılarak hata sıklığı E'ye düşürülecektir. Ayrıca

Hata Kodu (failure code)	Alt Sistem	Komponent Hata Türü (failure mode)	Muhtemel Hata Sebepleri	Hata Sıklığı (P) (failure frequency)	Hata Şiddeti (S) (failure severity)	Risk Seviyesi (R)	Hata Etkisi (failure consequence)	Hatanın Teşhisi	Riskin Kontrolü için Alınması Gereken Önlemler
F.15	LCM	LCM arızası	Donanım Hatası / Kablo Hatası	B	2	R2	sistem fonksiyo	alarm logları veya arıza bildirimi	Hata risklerini ortadan kaldırmak için LCM komponenti geliştirilmelidi
F.16	HMI	GUI arızası	Donanım Hatası / Hatalı Komut Talebi	B	1	R3	sistem fonksiyonlarını n azalması işletme gecikmesi	Sistemin lokal moda geçiş yapması	Sistemin etkilenmemesi için bu hata durumunda lokal modda çalışma
F.17	HMI	MMI kullanıcı hatası	Kırmızı ışıkta tren geçişi	C	4	R1	deray riski	Görsel olarak, operator kontrolü	Makinistlere işletmesel yaptırımlar konularak kırmızı ışıkta geçiş kesin

Hata Kodu (failure code)	Alt Sistem	Komponent Hata Türü (failure mode)	Muhtemel Hata Sebepleri	Hata Sıklığı (P) (failure frequency)	Hata Şiddeti (S) (failure severity)	Risk Seviyesi (R)	Hata Etkisi (failure consequence)	Hatanın Teşhisi	Riskin Kontrolü için Alınması Gereken Önlemler
F.18	HMI	MMI Arızası	Kablo Hatası / LED arızası	D	1	R4	sistem fonksiyo	alarm logları veya arıza bildirimi	Bu riskin indirilmesine çözüm olarak 2 beslemeli akım kontrollü LED

ÖZGEÇMİŞ

Ad Soyadı: İsmail Yakın

Doğum Yeri ve Tarihi: Konya 16 Ağustos1986

E-posta: ismailyakin@hotmail.com

Lisans Üniversite: İstanbul Teknik Üniversitesi - Kontrol ve Otomasyon Mühendisliği