

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

**MAKAS MOTORU ARAYÜZ DEVRESİ
TASARIMI VE GÜVENLİK BÜTÜNLÜK SEVİYESİ ANALİZİ**

YÜKSEK LİSANS TEZİ

Serhan SUBAŞI

Kontrol ve Otomasyon Mühendisliği Anabilim Dalı

Kontrol ve Otomasyon Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Salman KURTULAN

ARALIK 2016

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

**MAKAS MOTORU ARAYÜZ DEVRESİ
TASARIMI VE GÜVENLİK BÜTÜNLÜK SEVİYESİ ANALİZİ**

YÜKSEK LİSANS TEZİ

**Serhan SUBAŞI
(504131145)**

Kontrol ve Otomasyon Mühendisliği Anabilim Dalı

Kontrol ve Otomasyon Mühendisliği Programı

Tez Danışmanı: Prof. Dr. Salman KURTULAN

ARALIK 2016

İTÜ, Fen Bilimleri Enstitüsü'nün 504131145 numaralı Yüksek Lisans Öğrencisi Serhan SUBAŞI, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı “MAKAS MOTORU ARAYÜZ DEVRESİ TASARIMI VE GÜVENLİK BÜTÜNLÜK SEVİYESİ ANALİZİ” başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı : **Prof. Dr. Salman KURTULAN**
İstanbul Teknik Üniversitesi

Jüri Üyeleri : **Prof. Dr. Mehmet Turan Söylemez**
İstanbul Teknik Üniversitesi

Yrd.Doç Dr.Özgür Turay Kaymakçı
Yıldız Teknik Üniversitesi

Teslim Tarihi : **25 Kasım 2016**
Savunma Tarihi : **16 Aralık 2016**

Aileme ve İş Arkadaşlarıma,

ÖNSÖZ

Yüksek lisans bitime tezim boyunca bana yol gösteren ve projenin bütün aşamalarında benimle yakın olarak çalışan, yardımını ve zamanını benden esirgemeyen Sayın Prof. Dr. Salman Kurtulan’a teşekkürlerimi sunmayı bir görev bilirim.

Ayrıca bütün hayatım boyunca beni sürekli olarak destekleyen, her zaman el üstünde tutan ve mutlu bir aile hayatını yaşaamı sağlayan anne ve babama en içten sevgilerimi sunar ve teşekkür ederim.

Kasım 2016

Serhan SUBAŞI
Kontrol ve Otomasyon Mühendisi

İÇİNDEKİLER

Sayfa

ÖNSÖZ	vii
İÇİNDEKİLER	ix
KISALTMALAR	xi
ÇİZELGE LİSTESİ.....	xiii
ŞEKİL LİSTESİ.....	xv
MAKAS MOTORU ARAYÜZ DEVRESİ TASARIMI VE GÜVENLİK BÜTÜNLÜK SEVİYESİ ANALİZİ	xvii
ÖZET	xvii
SUMMARY	xix
1. GİRİŞ	1
2. MAKAS MOTORU ARAYÜZ PROBLEMİ.....	5
2.1 Makas Nedir?	5
2.1.1 Makasların sınıflandırılması	5
2.1.1.1 Yönlerine göre makaslar	5
2.1.1.2 Manevra yeterliliklerine göre makaslar	6
2.2 Makas Motoru Nedir?	7
2.3 Makas Motoru Arayüz Teknikleri.....	8
2.4 Dört Kablo Tekniği	9
2.5 Yedi Kablo Tekniği.....	12
3. ÜÇ FAZ DÖRT KABLO TEKΝİĞİ İLE SÜRÜLEN MAKAS MOTORU ARAYÜZ DEVRESİNİN TASARIMI.....	17
3.1 Giriş.....	17
3.2 Standartlar	18
3.3 Problemin Tanımlanması	20
3.4 Arayüz Devresinin İsterlerinin Çıkarılması	29
3.5 Makas Motoru Arayüz Devresinin Röle-Kontaktörlerle Gerçeklenmesi.....	31
3.5.1 Otomat tasarımı.....	31
3.5.2 Sezgisel tasarım.....	34
3.6 Fonksiyonel Güvenlik Kavramı ve Risk Analizi	39
3.6.1 Kabul edilebilir risk'i değerlendirme metotları olarak ALARP, GAME (GAMAP) ve MEM	41
3.6.2 Mevcut risk boyutunun belirlenmesinde "risk matrisi" metodu	43
3.6.3 Güvenlik bütünlük seviyesi (SIL)	45
3.7 Makas Motoru Arayüzünün SIL 4 Uyumluluğunun İncelenmesi	45
3.8 Arayüz Devresinin Elektronik Kontrolör ile Gerçeklenmesi	47
3.9 Sistemin Güvenlik Bütünlük Seviyesi Analizi	53
3.10 Hata Ağacı Analizi	57
3.10.1 Makas motoru arayüz devresi tasarımının tanımı	57
3.10.2 Sistem sınırları ve işletimi.....	58
3.10.3 Arayüz tasarımı ile ilgili varsayımlar.....	61

3.10.4 FTA için tepe olayın belirlenmesi	61
3.10.5 Arayüz devresi için hata ağacı analizi	62
4. SONUÇ	69
KAYNAKLAR.....	73
ÖZGEÇMİŞ	75

KISALTMALAR

AC/DC	: Alternatif Akım / Doğru Akım
ALARP	: As Low As Reasonably Practicable
EN	: Avrupa Normu
GAME	: Globalement Au Moins Equivalent
IRF/H	: Bireysel Ölüm Riski / Saat
I/O	: Giriş/Çıkış
MEM	: Minimum Endogenous Mortality
RAMS	: Güvenilirlik, Ulaşılabilirlik, Bakım Yapılabilirlik, Güvenlik
SIL	: Güvenlik Bütünlük Seviyesi
TIR/H	: Bağımsız Risk Oranı / Saat
THR	: Tolere Edilebilir Hata Oranı

ÇİZELGE LİSTESİ

Sayfa

Çizelge 3.1 : Ecostar 4 Makas Motoru Elektriksel Parametreler.....	17
Çizelge 3.2 : Pozisyonlara Göre S1 ve S2 Kontaklarının Durumu	21
Çizelge 3.3 : Arayüz Devresindeki Röle ve Kontaktörlerin İsimlendirmesi.....	30
Çizelge 3.4 : Risk Matrisi	44
Çizelge 3.5 : Doğrulama Tablosu	44
Çizelge 3.6 : SIL Değer Belirleme Tablosu	45
Çizelge 3.7 : IEC – EN Röle İster Karşılaştırma Tablosu	46
Çizelge 3.8 : FTA Sembol Tablosu.....	62
Çizelge 3.9 : FTA Lojik Kapı Tablosu	63

ŞEKİL LİSTESİ

Sayfa

Şekil 2.1 : Sağ Basit Makas	6
Şekil 2.2 : Makas Motoru	8
Şekil 2.3 : Makas Motorunun 3 Faz ile Sürülmesi	10
Şekil 2.4 : Sağ Son Pozisyon Konumu için Kurulmuş 4 –Kablo Tekniği.....	11
Şekil 2.5 : Sol Son Pozisyon Kurulmuş için Kurulmuş 4-Kablo Tekniği.....	12
Şekil 2.6 : Sağ Son Pozisyon Konumu için Kurulmuş 7 –Kablo Tekniği.....	13
Şekil 2.7 : Motorun Hareket Halindeki Devre Şeması	14
Şekil 2.8 : Sol Son Pozisyon Konumu için Kurulmuş 7 –Kablo Tekniği.....	15
Şekil 3.1 : Motorun Sağ Son Pozisyonda İken	22
Şekil 3.2 : Motor İlk Enerji Aldığı An.....	23
Şekil 3.3 : Motor Sağ Pozisyondan ve Sol Pozisyona Hareket Ederken	24
Şekil 3.4 : Motor Sol Son Pozisyona Ulaştığı An	25
Şekil 3.5 : Motor Sol Son Pozisyonda İken	26
Şekil 3.6 : Motor Sağ Son Pozisyonda	27
Şekil 3.7 : Motorun Harekete Başladığı İlk An	27
Şekil 3.8 : Motor Hareket Halinde	28
Şekil 3.9 : Motor Sol Son Pozisyona Ulaştığı An	28
Şekil 3.10 : Motor Sol Son Pozisyonda	28
Şekil 3.11 : Arayüz Devresi Otomat Modeli	32
Şekil 3.12 : 3 Faz 4 Kablo Arayüz Güç Devresi.....	36
Şekil 3.13 : 3 Faz 4 Kablo Arayüz Güç Devresi.....	37
Şekil 3.14 : Elektronik Kontrolörlü Arayüz Güç Devresi	49
Şekil 3.15 : KMR-KML Kontaktörlerinin Sürülmesi ile İlgili Yazılım Parçası..	51
Şekil 3.16 : DCR-DCL Rölelerinin Sürülmesi ile İlgili Yazılım Parçası	51
Şekil 3.17 : RP-LP Rölelerin Okunması ile İlgili Yazılım Parçası.....	52
Şekil 3.18 : Arayüz Devresi için Hazırlanan Yazılım	52
Şekil 3.19 : Mimari A Gösterimi	54
Şekil 3.20 : Mimari B Gösterimi	54
Şekil 3.21 : Mimari C Gösterimi	55
Şekil 3.22 : Mimari D Gösterimi	55
Şekil 3.23 : Nitel Hata Ağacı (Metot A).....	67
Şekil 3.24 : Nicel Hata Ağacı (Metot B).....	68

MAKAS MOTORU ARAYÜZ DEVRESİ TASARIMI VE GÜVENLİK BÜTÜNLÜK SEVİYESİ ANALİZİ

ÖZET

Demiryolu sistemlerine duyulan ihtiyaç dünyanın her bölgesinde gün geçtikçe artmaktadır. Bunun sebebi demiryolunun mevcut ulaşım sistemleri içerisinde ulaşılabilir, güvenli, hızlı ve çevreyi kirletmeyen ulaşım şekli olarak diğerlerinden ayrılmasıdır. Gelişmiş ülkelerde olduğu gibi ülkemizde de demiryolu ağına yapılan yatırımlar her geçen gün artmaktadır. İnşası süren şehirlerarası hızlı tren hatları, metro ve tramvay projelerinin tamamlanması ile beraber demiryolu günlük hayatın içerisinde insanlar tarafından daha fazla tercih edilen öncelikli ulaşım şekli olacaktır.

Türkiye’de demiryolu inşası konusunda elde edilen sonuçlar ve başarılar ne yazık ki teknoloji geliştirme alanında çok fazla karşılık bulmamıştır. Bunun altında yatan sebepler olarak demiryolu sistemlerinde kullanılan teknolojilerin katı olarak standartlara bağlanması ve talep edilen yüksek güvenilirlik, ulaşılabilirlik, bakım yapılabilirlik ve güvenlik değerleri olduğu söylenebilir. Tasarlanan sistemler sadece problemin çözümüne yönelik olarak değil aynı zamanda uzun ürün hayat döngüsü, çevresel faktörlere dayanım ve yoğun kullanıma karşı hatasız bir şekilde çalışmayı sürdürmelidir.

Trenlerin yönlendirmesini yapmak üzere makasları süren elektrik motorlu üniteye makas motoru denir. Motor kendi içerisinde özel bağlantılar içermektedir. Daha basit yöntemler ile motorun sürülmesi ve konum bilgisi okunması yapılabilecek iken motora çekilen kablo sayısını azaltmak amacı ile özel bir yöntem geliştirilmiştir. 4 kablo tekniğinde makas motorunu sürmek için ve indikasyon bilgisi elde etmek için aynı bağlantıların kullanılması nedeni ile bir arayüz devresi oluşturma zorunluluğu oluşmuştur.

Tasarımı gerçekleştirdikten sonra arayüz devresinin demiryolu standartlarına uygunluğu araştırılmaya başlanmıştır. Makas motoru, sinyalizasyon sisteminin doğrudan kontrolü altında olan bir ekipmandır. Makas motoru üzerinde elde edilen

bilgilerde bir hata yaşanması durumunda ölümle sonuçlanacak kazalara yol açabilir. Tasarım bu doğrultuda ele alınarak güvenlik öncelikli aynı zamanda ise güvenilirlik ve ulaşılabilirlik etmenlerini de göz ardı etmeden gerçekleştirilecektir.

Yapılan tasarımın başarılı bir şekilde uygulandığı gözlemlendikten sonra, arayüz devresinin kullanımı hakkında risk analizi gerçekleştirilecektir. Buradan elde edilen sonuçlar ile sistemin karşılaması gereken güvenlik bütünlük seviyesi ortaya çıkacaktır. Tasarımı yapılan sistem üzerinde istenilen güvenlik seviyesine ulaşılabilirlik kontrolü gerçekleştirildikten sonra tasarım revize edilecektir. Nihai tasarım, ilgili standartlarla uyumlu ve istenilen güvenlik bütünlük seviyesine uygun olacaktır. En son olarak tasarım ile ilgili eksik veya zayıf bir nokta olup olmadığını kontrol etmek amacı ile tehlike analizi gerçekleştirilecektir. Seçilen tehlike analiz metotlarından biri tasarım üzerinde uygulanarak tez tamamlanacaktır.

DESIGN OF POINT MACHINE INTERFACE AND SAFETY INTEGRITY LEVEL ANALYSIS

SUMMARY

Demand for railway systems is increasing day by day at all around the world. The reason for that railway is differentiated with respect to other existing transportation methods in terms of accessibility, safety, being fast and non-polluting alternative for transportation. Railway investments are growing in our country as well as at developed countries. People will choose railway as a preferred option for transportation in daily life with completion of intercity high-speed lines and metro and tramway lines in cities.

Unfortunately, the results and successes of construction of railways could not find any response at technology development on railway systems at Turkey. It can be explained that the railway technology development is strictly linked with standards moreover, the systems are required with high reliability, availability, maintainability and safety levels. The systems are not only designed to solve the problem but also consider to reach long product lifecycle, resisted against environmental factors and reliable functioning under frequent usage.

Main technological component of railway systems is the Interlocking System that uses for safety train movement on the line. The Interlocking system connects to Control Centre and the field equipment on the line. Status of the field equipment are monitored continuously by the system. Control Centre takes the decisions for train movements in the station and as well as the train operation between stations. Control Centre commands are executed by the Interlocking as long as the safety principles are guaranteed. The logic found on the Interlocking always works to provide the safety at all time. Therefore, the interlocking never executes non-safe logic that might causes a collision of train even the Control Centre demands a non-safe command.

In order to provide safe logic and execute commands for train operation, the Interlocking System should have proper interfaces with field equipment. The

Interlocking System should control and monitor the field equipment such as wayside signals, level crossings, axle counters or track circuits and point machines.

Trains are navigated by switches which is driven by electric powered point machine. The point machine has most complicated interface other than all field equipment. Other interfaces usually established over dry contacts and moreover power line and control line are strictly separated. AC power will be either one phase or three phase or DC voltage fed to drive point machine. Monitoring status of the point machine is again realised over dry contacts that have special behaviour while point machine is moving one position to another.

A special method was developed in order to reduce to cable core quantity even there are some existing methods allow that the motor can be driven and position indications can be read over separate cables. The method is called 4 wire technique that only 4 cable core connections are made between the point machine and the Interlocking System. There is a necessity to develop an interface because of the same connections are used at the 4-wire technique to drive point machine as well as to obtain position indications.

Two important issues should be considered during the design of the interface. One of them is that precise transitions between power and control circuit connections are established over point machine. Any fault during the transition or connection of the power and control circuits at the same time might be resulted with extreme damage over the equipment or even false information can be read by the interlocking. Second is that the interface never provides a false indication to the Interlocking System. This could be lead a fatal accident. Therefore, safety concerns should be fulfilled by the interface system.

In order to meet with safety requirements, related standards must be defined and studied. Research activities started over compliance of the interface design with the railway standards after the design had been completed. The point machine is a device that is placed under direct control of the signalling system. In case a fault occurs while obtaining position information of the point, it might be resulted with fatal accident. Therefore, the design is carried out with safety considerations that is the prior parameter for the design without ignoring reliability and availability considerations.

First design is carried out with basic electric components such as relays and contactors. Logic itself pays attention to realize a smooth transition between control circuit connection to motor and power circuit connection to motor. The results show that the interface is working properly and safely. However later studies show that the interface is not compliant with the standards and regulations. Therefore, the design had to be rethought in terms of compliance with the related railway standards.

Logic of the interface is moved to an electronic controller which has a certification for appropriate safety integrity level for a railway application. Some relays and contactors have to be kept as a part of the interface. Therefore, the safety integrity level check for these parts of the interface must be realized as well. Relays were searched and selected as appropriate safety integrity level according to standards. But there wasn't any contactor that meets with an appropriate safety integrity level. The additional calculations should be done in order to prove that the proposed designed with selected contactors correspond to appropriate safety integrity level. The calculations show that contactors are reached the level as well as the controller and relays. Moreover, overall interface will be participated into a safety critical system such as an Interlocking System in terms of safety

A risk analysis is the last issue that must be realized in order to be sure that there is not any missing or weak point placed in the design. Fault Tree Analysis method is one of the suggested methods by the standards for risk analysis. In addition to that it is most suitable method to realize a risk assessment for our interface design. The analysis carried out together with the design in order to find non-compliant or weak points of the design. In thesis, it used to check that the interface meets with corresponded safety integrity level. It is required that the design requirements and border conditions must be considered once again before start to the analysis. Afterwards, top event should be defined to realize the analysis. In our case, it is obvious that false indication signal is selected as top event. The thesis was completed after realize quantitative and qualitative risk analysis. Results of the analysis can be used justify the interface design quality. The interface can be updated after the design checked whether compliant with defined safety integrity level. Final design is compliant with the standards and corresponded the required safety integrity level.

Studies of the thesis show that even a small system development for the safety critical railway system requires a lot of effort in terms of compliance with the standards and

corresponded safety integrity level. Before starting the design process all related standards should be found and studied carefully. The requirements of the problem and standards are fulfilled by the engineers at the design. The design must be strengthened by the calculations in necessity points in order to reach corresponded safety integrity level that is defined before the design process. All in all, the thesis would be a guidance for engineers who will be worked over safety critical areas.

1. GİRİŞ

Giderek artan nüfus ve yerleşik şehir hayatına geçiş ile beraber, kalabalık insan gruplarının günün her saatinde kullanabileceği esnek, hızlı ve güvenli ulaşım ihtiyacı ortaya çıkmıştır. Şehirlerde, günün belli saatlerinde, çok sayıda insanın ortak noktalardan aynı yönlere doğru seyahat etme amacı taşıdığı görülmektedir. Aynı zamanda artan kaynak ve materyal ihtiyacı yüksek miktarlarda yükün uzun mesafelerde güvenli, hızlı ve ucuz olarak taşınma problemini de doğurmuştur. Şuan için dünya üzerinde en yaygın dört ulaşım yöntemi içerisinde demiryolu taşımacılığı, şehir içi ve şehirlerarası insan ve yük taşımacılığı için en iyi alternatif olarak son yıllarda ön plana çıkmıştır.

Geçtiğimiz yüzyılda demiryolu taşımacılığı ihtiyaca yönelik olarak gelişimini sürdürmüş ve farklı şekillerde insanlara hizmet etmeye devam etmiştir. Şehir içerisinde toplu taşıma yöntemi olarak metro, tramvay ve banliyo trenleri; Şehirler arası taşımacılıkta ise konvansiyonel hatlar ve hızlı tren hatları olmak üzere çeşitlilik göstererek gelişmiştir.

Demiryolu sistemlerinin son yıllarda ön plana çıkmasının en önemli sebeplerinden biri sürdürülebilir olmasıdır. Demiryolu projelerinin ilk yatırım maliyetleri yüksek olmasına karşın, orta vadede yapılan yatırımın karşılığı alınıp uzun vadede kar ettiren projeler haline gelmektedir. Bunun altında yatan en önemli sebep sistemlerin yüksek güvenilirlik, ulaşılabilirlik, bakım kolaylığı ve güvenlik değerlerinin çok yüksek olmasıdır

Projelerin yürütülmesi iki ana başlık altında toplanabilir. Bunlar, inşaat işleri ve elektromekanik işler olarak listelendirilebilir. İnşaat işleri projenin yapısına bağlı olarak bütün altyapı ve üstyapı işlerini kapsayacak şekilde oluşturulur. İnşaat bölümü en genel haliyle trenin ilerleyeceği hattın oluşturulması, rayların döşenmesi ve bütün yolcu ve ekipman binalarının oluşturulmasından sorumludur.

Elektromekanik işlerin altında ise sinyalizasyon, telekomünikasyon ve güç sistemleri başlıkları bulunmaktadır. Buradaki en kritik sistem olarak sinyalizasyon sistemi ön

plana çıkmaktadır. Sinyalizasyon sistemini oluşturan ana bileşenler genel haliyle anlaşılan sistemi, saha elemanları ve kumanda merkezidir. Söz edilen sistemler trenlerin güvenli bir şekilde işletilebilmesi için yüksek güvenlik standartlarına sahip olmalıdır. Demiryolunda sinyalizasyon içerisinde kullanılan bileşenlerin güvenlik standardı, güvenlik bütünlük seviyesi üzerinden değerlendirilmektedir. Anlaşılan ana sistemi, alt sistemler, anlaşılan yazılımı ve saha elemanları için güvenlik bütünlük seviyesi 4 istenmektedir. Bu seviyedeki sistemlerin hata yapma oranı 10^8 saatlik operasyona karşılık bir seferden daha düşüktür.

Sistemlerin güvenlik derecesinin yüksek olmasının yanı sıra, güvenilirlik ve ulaşılabilirlik değerleri de bir o kadar yüksek olmalıdır. Çünkü demiryolundan talep edilen her an yüksek verimli, hızlı ve hatasız bir operasyon gerçekleştirmesidir. Güvenlik standartlarının karşılandığı ancak işletmede sürekliliği sağlanamayan bir sistem kullanıcılar ve operatörler tarafından tercih edilmemektedir. Bu sebeple bu iki kavram da en az güvenli değerleri kadar önemlidir.

Sistemler sürdürülebilir ve uzun bir ürün hayat döngüsü gözetilerek tasarlanır ve üretilmektedir. Sistemlerde mükemmellik amaçlanırken aynı zamanda sistemlerin ulaşılabilir bir maliyete sahip olması da ayrıyetten önem taşımaktadır. Bu sebeple sistemlerin maliyet ve teknoloji kıstasları düşünülerek belli sürelerde bakımlar gerçekleştirerek, sistemlerin çalışır durumda tutulması amaçlanmaktadır. Bu nedenle demiryolu sistemlerinde yer alan bir diğer önemli kriter de bakım kolaylığı olarak ortaya çıkmaktadır. Demiryollarında sinyalizasyon ve diğer elektriksel sistemler için belirlenen hayat döngüsü en az 20 yıldır. Bu süre içerisinde altsistemlere uygulanan periyodik önleyici bakımlar ve arıza durumunda yapılan hızlı müdahaleleri ile sistemin çalışması aksamadan sürdürülebilmektedir. Bu sürenin ardından sistemlerin ağır bakımları yapılarak daha da uzun yıllar sistem kullanılmaya devam edebilmektedir.

Demiryolu sinyalizasyon sistemin işleyişine daha yakından bakmak gerekirse; kumanda merkezi, saha elemanları üzerinden gelen bütün indikasyonları yansıtır ve operatör sahadan gelen bilgiler doğrultusunda tren işletimi yapmak üzere uygulamak istediği komutları anlaşılan sistemine buradan gönderir. Anlaşılan sistemi her zaman güvenlik koşullarını göz önünde tutarak, güvenlik için tehlike içermeyen durumlarda komutları işletir, aksi takdirde ise komutları reddeder. Anlaşılan sistemi, tren algılayıcısı, makas motoru, sinyal, hemzemin geçit, derayman gibi bütün saha elemanlarından veri okuyabilir ve onları istenilen şekilde kumanda edebilir. Bu

elemanlar, anlařman sistemine baęlı dijital I/O üniteleri ile saha elemanları arasında oluşturulan arayüzler ile komut gönderebilmekte ve indikasyon alabilmektedir.

Arayüzler içerisinde en karmařık olanı makas motoru için gerekli olan arayüzdür. Makas motorları AC veya DC olarak sürülen yüksek torklu ancak verimi düşük motorlardır. Motor, anlařman sisteminden alınan komut doęrultusunda sürülür. Motor son konuma ulařtıktan sonra tasarlanan arayüz üzerinden son konum bilgisi okunur. Oldukça kritik öneme sahip makas motoru arayüz devresi yukarıda belirtilen genel kıstasları gerçekleřtirecek řekilde tasarlanmalıdır. Bütün bu kıstaslar göz önüne alınarak geliştirilen ürünler yüksek bir mühendislik ve özel bir bilgi birikimi gerektirmektedir. Projelendirme, isterlerin hazırlanması, tasarımın aşaması, ürünün gerçeklenmesi, test yapılması ve en sonunda doęrulama ve geçerleme faaliyetlerinin yapılması ile beraber ürün nihai aşamaya getirilmektedir. Süreç içerisinde geliştirilen ürünün ilgili bütün standartlara uyumluluęu karřılanarak ilerlenmelidir.

Bitirme projesi kapsamında, öncelikle makas motoru arayüz problemi açıklanacaktır. Problemin isterleri ortaya çıkarıldıktan sonra otomat tasarımı yapılan modelin, röleler ve kontaktörler kullanılarak lojik tasarımı gerçekleştirilecektir. Uygulama için risk analizi yapılca ve sistem için bulunan risk deęeri için yapılan tasarım gözden geçirilecektir. Tasarımda yapılan iyileřtirmelerin ardından istenilen güvenli seviyesine karřılık düşüp düşmedięi kontrol edilecektir. Nihai tasarım için anahtarlama elemanlarının güvenilirlik ve ulařılabilirlik deęerleri hesaplanaca en sonunda ise tehlike analizi gerçekleştirilerek tez tamamlanacaktır.

Bu tez sayesinde demiryolu projesinde yer alan gerçek bir problem aktif bir biçimde ele alınmış olacaktır. Standartlarda ifade edildięi řekilde bir proje yönetim prosedürü uygulanacaktır. İsterlerin hazırlanmasından dizayn sürecinin sonucuna kadar detaylı olarak söz edilecektir. Testlerin aşamalarının belirtilmedięi sadece sonuç olarak söz edilen tezde doęrulama ve geçerleme aktivitelerinden söz edilmeyecektir.

Güvenlik, güvenilirlik ve ulařılabilirlik açısından oluşturulan arayüz deęerlendirmeye alınaca ve gerçek bir problem üzerinde bu kavramların nasıl uygulandıęı örneklendirilecektir. Normalde motor sürülmesi gibi görünen basit bir problemin endüstriyel demiryolu sistemlerinde uygulanma istenildięinde ne gibi zorluklarla karřılıřılabileceęi tezin ana yaklařımını oluřturmaktadır. Özellikle endüstriyel

koşullarda uyulması ve takip edilmesi gereken standartların yoğunluğu bu tez süresince fazlası ile üzerinde çalışılan bir konu haline gelmiştir.

2. MAKAS MOTORU ARAYÜZ PROBLEMİ

2.1 Makas Nedir?

Trenler diğer yaygın kullanılan ulaşım araçlarının aksine herhangi bir yönlendirme mekanizmasına sahip değildir. Makinistin tren yolu seçme hakkı veya yönlendirme yapması söz konusu değildir. Trenlere yönlendirme hatta bulunan makaslar üzerinden gerçekleştirilir.

Ulaştırma terimleri sözlüğü “makas” terimi için “İstasyon ve saydingerde bir yoldan diğer bir yola geçişi sağlayan yol donanımları” [1] tanımına yer vermektedir. Genel anlamda bakacak olursak, makaslar birer kesişim noktasıdır. Makaslama işlemi iki farklı yoldan aynı yola bağlanma şeklinde veya ortak uçtan gelindiğinde sapan ya da normal yöne olan hareket makasın konumuna bağlı olarak yol seçme şeklinde gerçekleşir.

2.1.1 Makasların sınıflandırılması

Makasın sınıflandırılması iki farklı duruma göre gerçekleştirilir.

Yönlerine göre makaslar:

- Sağ Makas
- Sol Makas
- Simetrik Makas
- Münhani Makas

Manevra yeterliliklerin göre makaslar:

- Basit Makas
- Bileşik Çift Makas
- Çapraz Makas

2.1.1.1 Yönlerine göre makaslar

Sağ Makas: Trenin makasın ortak ucundan girdiğinde çıkış tarafında sapan yolun sağ tarafta kaldığı makaslardır.

Sol Makas: Trenin makasın ortak ucundan girdiğinde çıkış tarafında sapan yolun sağ tarafta kaldığı makaslardır.

Simetrik Makas: Trenin makasın ortak ucundan girdiğinde çıkış tarafında normal yön mevcut değildir. Çıkış tarafındaki her iki yönde sapan olarak kabul edilmektedir.

Münhani Makas: Kurp üzerinde bulunan özel tip makaslardır.

2.1.1.2 Manevra yeterliliklerine göre makaslar

Basit Makas: Makas üzerinde üç adet bağlantı yolu mevcuttur. Ortak uçtan, sapan veya normal yola hareketi sağlamak için ya da tam tersi hareketi sağlamak için kullanılan en yaygın tip makaslardır. Şekil 2.1’de sağ basit makasa bir örnek bulunmaktadır.



Şekil 2.1 : Sağ Basit Makas

Bileşik (Çift) Makas: En temelde iki basit makasın ardışık olarak yerleştirilmesinden oluşur. Ortak uçtan yaklaşan tren iki ayrı sapan veya doğru yola ilerleyebilir. Genellikle depo ve manevra alanlarında kullanılan makasın işletim altında olan hatlarda uygulaması yoktur.

Çapraz Makas: Bu makaslarda iki adet yolun çapraz kesişmesi sonucu farklı doğrultulardan gelen trenlerin doğrultu değiştirmeden ilerlemesi sağlanır. 4 adet ile makas ile sağlanacak geçiş bu sayede tek bir makas üzerinden gerçekleştirilir.

Genellikle istasyon ve manevra alanlarında yer tasarrufu yapmak için bu makaslar kullanılmaktadır.

2.2 Makas Motoru Nedir?

Makasların pozisyon deęişimlerini sağlamak ve makasın son konumuna oturduęunu denetlemek için elektrikli makas motorları kullanılır. Arayüz devresi anklařman sisteminden gelen komut doęrultusunda makası, makas motoru vasıtası ile bulunduęu konumdan dięer konuma sürer. Makas motoru son konuma ulařtıęında, arayüz devresi pozisyon kontrolünü gerekleřtirerek, makas son konuma oturmuř ise bunu anklařman sistemine bildirir.

Makas motorları kullanım řekline göre farklılık gösterirler. Motorların gücü ve montaj řekilleri kullanıldıkları farklı demiryolu tipleri için özelleřtirilmiřtir. Tramvaylarda operasyon yoğunluęu yüksektir ve hat řehir ierisinde yer aldıęı için makas motorunun monte edileceęi alan her zaman dardır. Bu sebeple tramvaylarda makas motorları ray arasına monte edilir. Enerji temini ve tařınması sorun teřkil etmeyeceęi için DC gerilim altında hızlı alıřan motorlar tercih edilir. Konvansiyonel hatlarda makaslar enerji temin noktalarından uzakta yer alabilir. Bu sebepten motorlar AC gerilim altında alıřan ve rayın dıřına monte edilen tipte olur. řekil 2.2’de konvansiyonel hatlarda kullanılan bir makas motoru örneęi bulunmaktadır.

Anklařman sistemi makası iki řekilde kumanda edebilir. Birincisi tren hareketi için operatör tarafından kurulan rotanın kabulü ile ilgili makasların anklařman tarafından otomatik kumanda edilmesi řeklinde, ikinci olarak ise operatör sahayı istedięi gibi hazırlamak için makasları rota kurmadan baęımsız olarak kumanda edebilir. Anklařman sistemi her iki durumda da olabilecek bütün güvenlik fonksiyonlarını göz önüne alarak makasın evrilme kararını verir. Makasın bulunduęu ray bölgesinde meřguliyet veya belirsiz durum bir bařka deyiř ile hata olması gibi durumlarda hatada-güvenli konumda kalarak makasın hareketine izin vermez.

Makas motoru üzerinden konum okuma problemi hayati öneme sahiptir. ünkü makası olduęu konumun dıřında bir konumda göstermek veya oturmamıř bir makastan pozisyon bilgisi üretmek sonucu trenin deray etmesi veya iki trenin arpıřması gibi kazalara yol aılabilir. Sonucunda yaralanma hatta can kaybına neden olabilecek

durumlardan ötürü makas motoru arayüzü demiryolunda istenen yüksek güvenlik seviyelerine sahip olmalıdır.



Şekil 2.2 : Makas Motoru

Makas motorları birçok uygulamada güvenlik bütünlük seviyesi 4'e sahip olacak şekilde talep edilmektedir. Makas motoru, içerisinde özel bir yapı barındırır. Makas rayları her iki pozisyonda otuduğunu mekanik olarak algılayan makas motoru bu işareti üzerinde bulunan röleler yardımı ile arayüz devresine bildirir. Söz edilen rölelerde ürünün SIL4 sertifikası dahilinde yer almaktadır. Dolayısı ile arayüz devresinin görevi röleler üzerinde doğru zamanda doğru bir şekilde okumaktır. Genel olarak makas dilinin ana raya oturma (normal veya sapan pozisyon) bilgisi iki rayın birbirine 2mm'den daha yakın olduğu konumlarda üretilmelidir. Makas motoru üreticisi bunu garanti etmektedir. Ancak bazı özel uygulamalarda, örneğin hızlı tren hattı uygulamalarında oldukça uzun ve kurplu makaslara rastlanılmaktadır. Burada ekstra bir cihaz olarak son konum dedektörleri kullanılır. Bu dedektör makas üzerindeki rölelere ekstra olarak 2mm'den az olmama durumunu kendi üzerindeki kontaklardan da kontrol ederek garanti altına almış olur. Makas motoru üreticisi arayüz devresinin değişmemesi için iç bağlantıları ayarlarak iki sistemin kontaklarının seri bağlanılmasını garanti altına alır.

2.3 Makas Motoru Arayüz Teknikleri

Makas motorlarının sürülmesi ve indikasyon okunabilmesi için arayüz devrelerine ihtiyaç duyulmaktadır. En temel seviyede ihtiyaç, motor sürme için güç devresinin

bağlanması ile AC veya DC enerjinin beslenmesi ve motor son konuma ulaştığında ise indikasyon okumak için kontrol devresinin bağlanması ile beraber motor üzerinden pozisyon okunmasıdır. Arayüz devresinin bir başka amacı ise motoru yüksek akım, faz kısa devreleri veya farklı karakteristikteki gerilimlerin aynı anda motora iletilmemesi gibi istenmeyen ve zararlı durumlardan korumaktır.

Bu amaçlar doğrultusunda motor üreticileri ve anklaşman sistemi sağlayıcıları arasında uluslararası kabul görmüş iki adet genelleşmiş arayüz metodu mevcuttur. Bunlar, arayüz devresi ile makas motoru arasında çekilen kablo damar sayısı ile orantılı olarak isimlendirilen 4 kablo tekniği ve 7 kablo tekniğidir.

2.4 Dört Kablo Tekniği

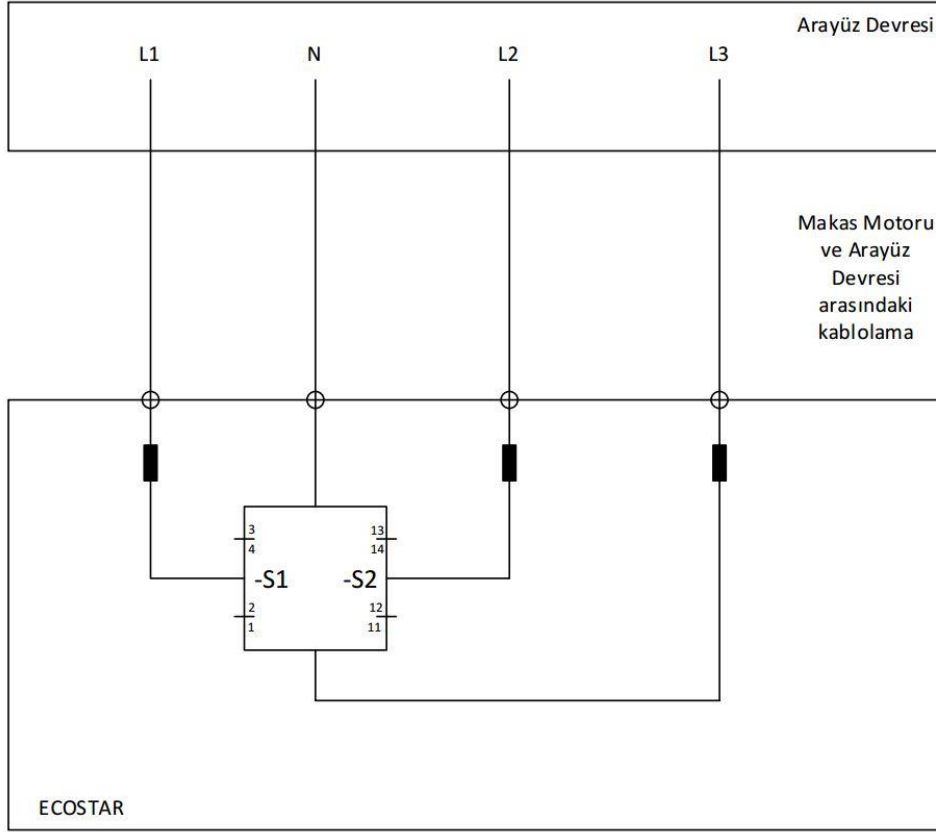
4 Kablo tekniğinde 4 adet kablo arayüz devresi ile makas motoru arasında bulunmaktadır. 4 kablo üzerinden makas motoru 1 faz veya 3 faz olarak sürülecek aynı zamanda yine aynı kablolar kullanılarak motorun üzerinde yer alan kontaklardan konum bilgisi okunacaktır. 4 kablo arayüzü iki ayrı devreden oluşmaktadır. Bunlardan birincisi fazların motora iletilmesi ve motorun sürülmesi için kullanılan güç devresidir. Diğeri ise makastan son pozisyon indikasyonlarının alınması için kullanılan kontrol devresidir. İleride anlatılacak 7 kablo tekniğinde ise motoru sürmek ve indikasyon okumak için farklı kablolar kullanıldığı için arayüz çok daha basittir.

Tek faz ile üç faz makas motorlarının sürülmesinde güç devresi açısından büyük bir fark yoktur. Tek faz sistemlerde makas motorunun zıt yönlerle sürülmesi için fazlar farklı kablolar üzerinden motora iletilir ve her iki tarafa sürüş içinde aynı nötr hattı kullanılır. Üç fazlı sistemlerde de benzer şekilde üç kablo motora fazların beslenmesi için kullanılırken, geriye kalan dördüncü kablo ise motorun nötr hattına bağlanması için kullanılır. Motorun diğer tarafa sürülmesi istenildiğinde motora iletilecek iki fazın yeri değiştirilir.

Arayüz devresi, motorun nötr hattındaki akım karaktestiğini gözlemlemektedir. Motorun sürülmesi esnasında makas son konuma ulaştığında motor akımı üzerindeki değişiklik gözlemlenerek motora güç iletilmesi kesilir. Güç devresinin ayrılmasından sonra motora kontrol devresi bağlanır ve motorun son konuma ulaşp ulaşmadığı kontrol edilir. Bu bilgi motor içerisinde yer alan rölelerin son konum bilgisini aktaracak pozisyona gelip gelmediği kontrol edilerek sağlanır. Makas pozisyonun

anlaşılması için bir kablodan iletilen gerilim motor içerisindeki konum rölelerinden geçerek bir başka damar üzerinden geri dönüş alınıyor ise motor beklenen son pozisyona ulaşmış demektir.

4 kablo tekniğinin 3 faz için uyarlanmış halinin görünümü aşağıda verilen görseller üzerinden daha detaylı anlatılmıştır.

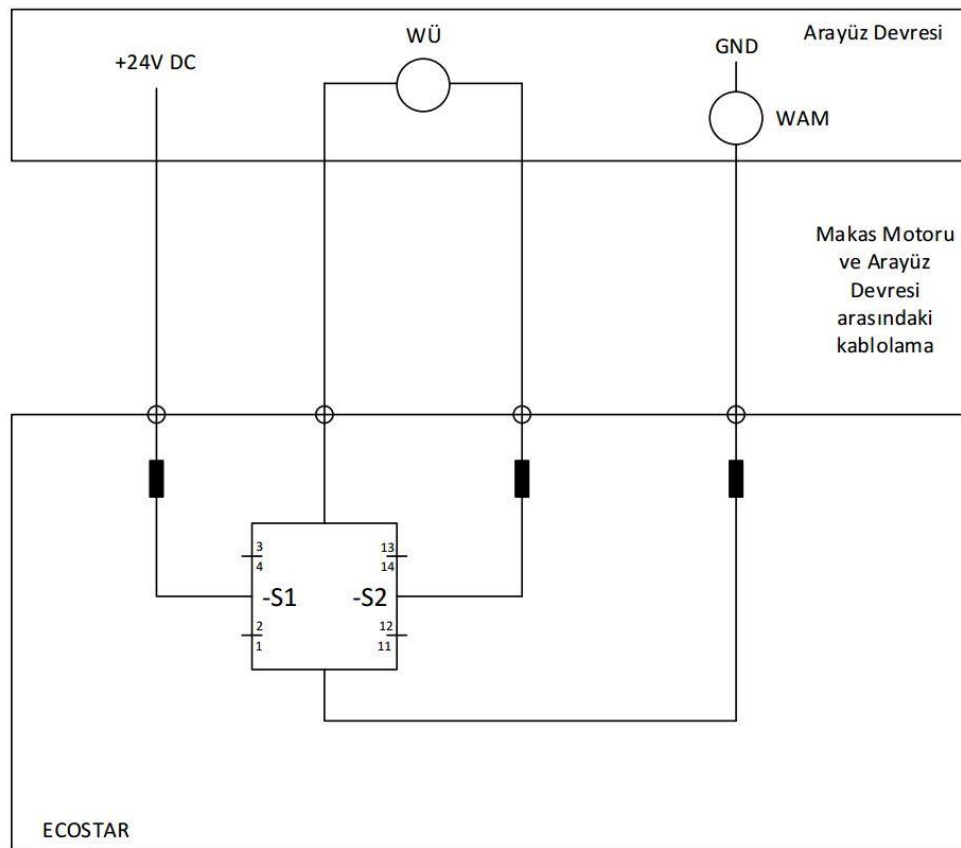


Şekil 2.3 : Makas Motorunun 3 Faz ile Sürülmesi

Şekil 2.3’de verilen kablolar sol baştan sırası ile L1 fazı, nötr hattı , L2 fazı ve L3 fazı şeklindedir. Şu anki konumda görüldüğü gibi güç kontakları bağlı değildir. Son pozisyon bilgisinin alınabilmesi için Makas L1 fazının bağlandığı uçtan DC olarak beslenmektedir. Beslenen gerilim son pozisyon bilgisinin sağlayan önce S1 kontağından geçerek neutral wire kolundan geri döndürülür. Bu kolda bulunana WÜ rölesinin çekmesi makasın sağ konumda olduğunun ispatıdır.

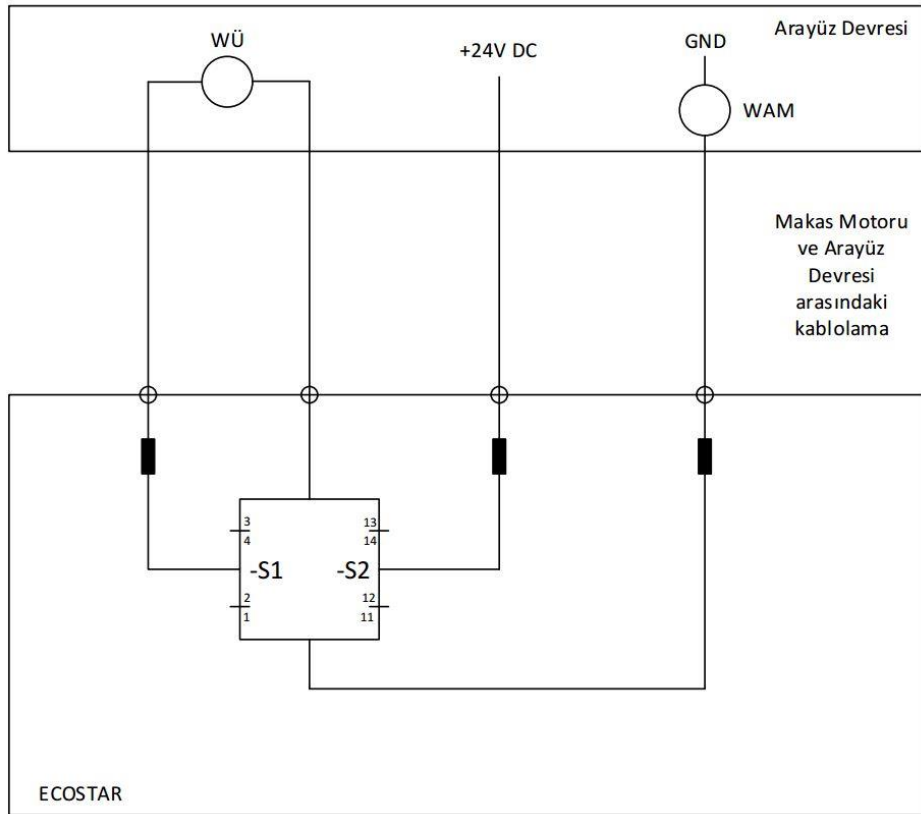
Şekil 2.4’deki devre üzerinde görülebileceği gibi L3 fazının bağlandığı yerde WAM rölesi vardır. Bu röle indikasyon devresi bağlanıldığı durumda bobinin enerjilendirilmesi durumunda çıkış vermektedir. Bu sayede makasta tersten girme yaşandığı bilgisi anlaşılabilir. Çünkü bulunmaması gereken bir pozisyon için makas

Makas sağ pozisyonunda iken anlaşılacağı gibi L1-N uçları ve L2-L3 uçları birbirine bağlı şekilde iki ayrı yol vardır. Makas harekete başlayacağı zaman önce kontrol devresi makastan izole edilir, ardından ilgili fazlar doğru şekilde bağlanır. Motora enerji verildiği anda S1 kontağı konum değiştirir ve 3 faz bir araya gelerek makas yıldız şeklinde maksimum tork ile sürülür.



Makas motoru hareketini tamamladığında S2 kontağı konum değiştirerek motor üzerine iletilen fazlardan birini yıldız bağlantı şekilinden ayırmış olur bu sayede nötr hattı üzerinden akım akmaya başlar. Nötr hattı üzerinde bulunan akım sensörü yardımı ile bu durum tespit edilir ve doğru zamanda güç kesilerek, kontrol devresi bağlantısı kurulur.

Bu sefer kontrol devresinin sağladığı DC gerilim L2 fazının bağlandığı koldan verilmektedir. Beslenen gerilim son konum bilgisini sağlayan S2 kontağından öncelikle geçer. Buradan geçen gerilim nötr hattına ait koldan geri döndürülür. Burada bulunan WÜ rölesinin çektirilmesi ile makasın sağ pozisyonda olduğu bilgisi alınmış olur. L3 fazının bağlandığı yerde sol pozisyon indikasyonu kontrol edilirken kullanıldığı gibi WAM rölesi vardır. Bu röle sol pozisyonda olan makas içinde tersten girme yaşandığı bilgisi üretmek için kullanılır. L2 fazının bağlandığı uçtan verilen DC gerilim beklendiği gibi nötr hattının bağlandığı noktadan geri dönüş sağlamaz WAM rölesinin bulunduğu yerden geri dönüş sağlar. Makas sol pozisyonda iken Şekil 2.5’de görülebileceği gibi L1-L3 ve L2-N uçları birbirine bağlıdır. Makas tekrar ters yöne sürülecek iken daha önce açıklanan olaylar dizisi ters olacak şekilde tekrar uygulanır.



Şekil 2.5 : Sol Son Pozisyon Kurulmuş için Kurulmuş 4-Kablo Tekniği

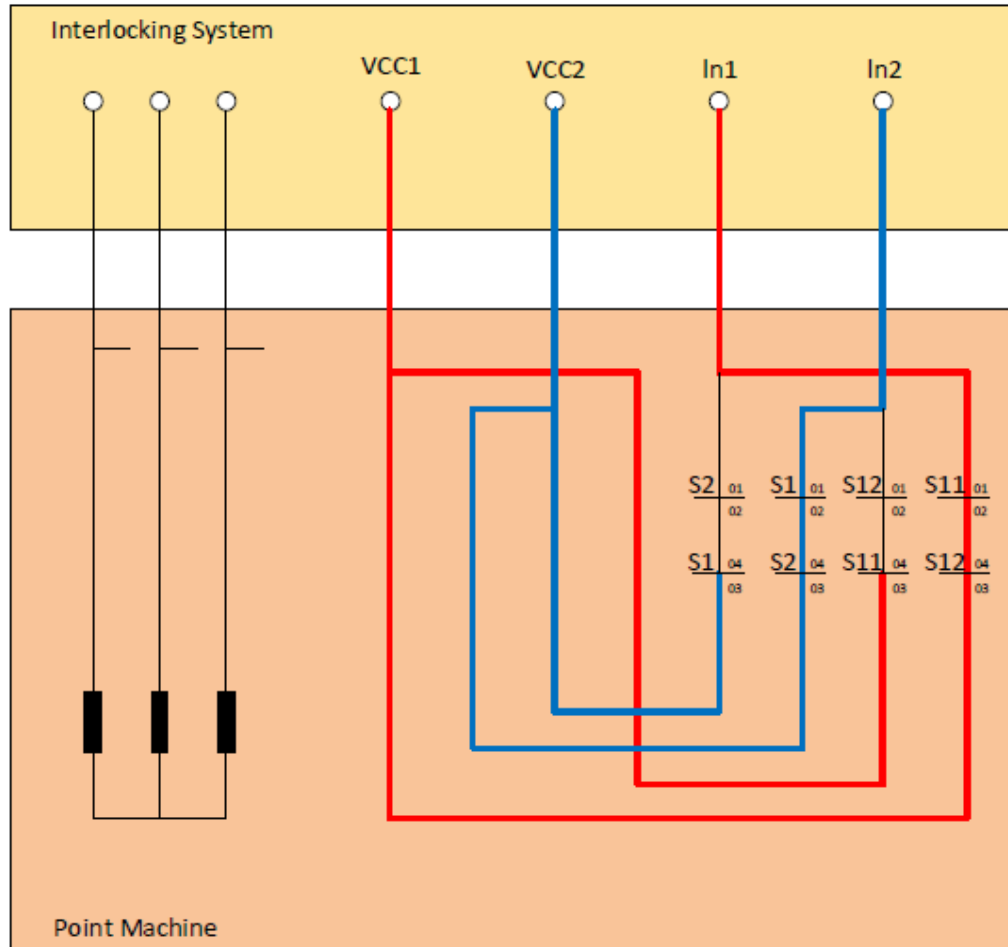
2.5 Yedi Kablo Tekniği

7 Kablo tekniğinde 7 adet kablo arayüz devresi ile makas motoru arasında bulunmaktadır. 4 Kablo tekniğinin aksine güç devresi ve kontrol devresi farklı uçlar üzerinden makas motoruna bağlıdır. Üç kablo, motorun üç faz veya tek faz alternatif

gerilim altında sürülmesi için ayrılmıştır. Dört kablo ise motorun son konum bilgisini okumak amacı ile ayrı olarak motora bağlıdır.

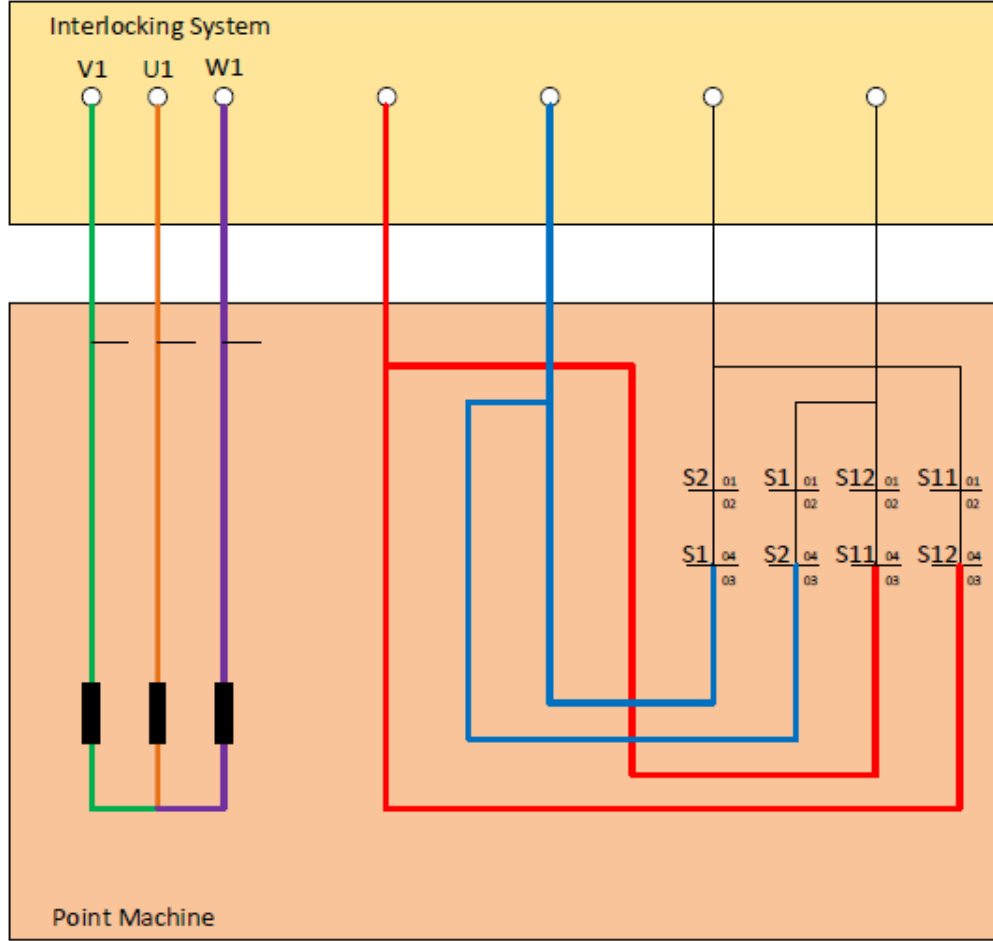
Bu yöntemde ayrı kablo uçlarının kullanılması güç devresinin ve kontrol devresinin aynı zamanlarda izole bir şekilde bağlanma problemini ortadan kaldırmıştır. Aynı zamanda güç devresinin arayüzden doğru zamanda ayrılmasını sağlamak için nötr hattının akımını gözleme zorunluluğu ortadan kalkmıştır.

Sağ son pozisyon indikasyonu için güç devresi kesilmiş ve kontrol devresi aktif durumda olmalıdır. VCC1 ve VCC2 gerilimi daha önce belirlenmiş uçlardan makasa gerilim uygulanmaya başlanır. Şekil 2.6'da görülebileceği gibi eğer makas sağ son pozisyona oturmuş ise uygulanan gerilimlerden VCC1 makasın son pozisyon kontaklarından geçerek IN1 bağlantısı üzerinden geri dönüş sağlanmış olmalı ve aynı zamanda uygulanan VCC2 gerilimi ise IN2 bağlantısı üzerinden geri dönmelidir. Bu iki durumun gerçekleşmesi makasın sağ pozisyona oturduğunun kanıtıdır.



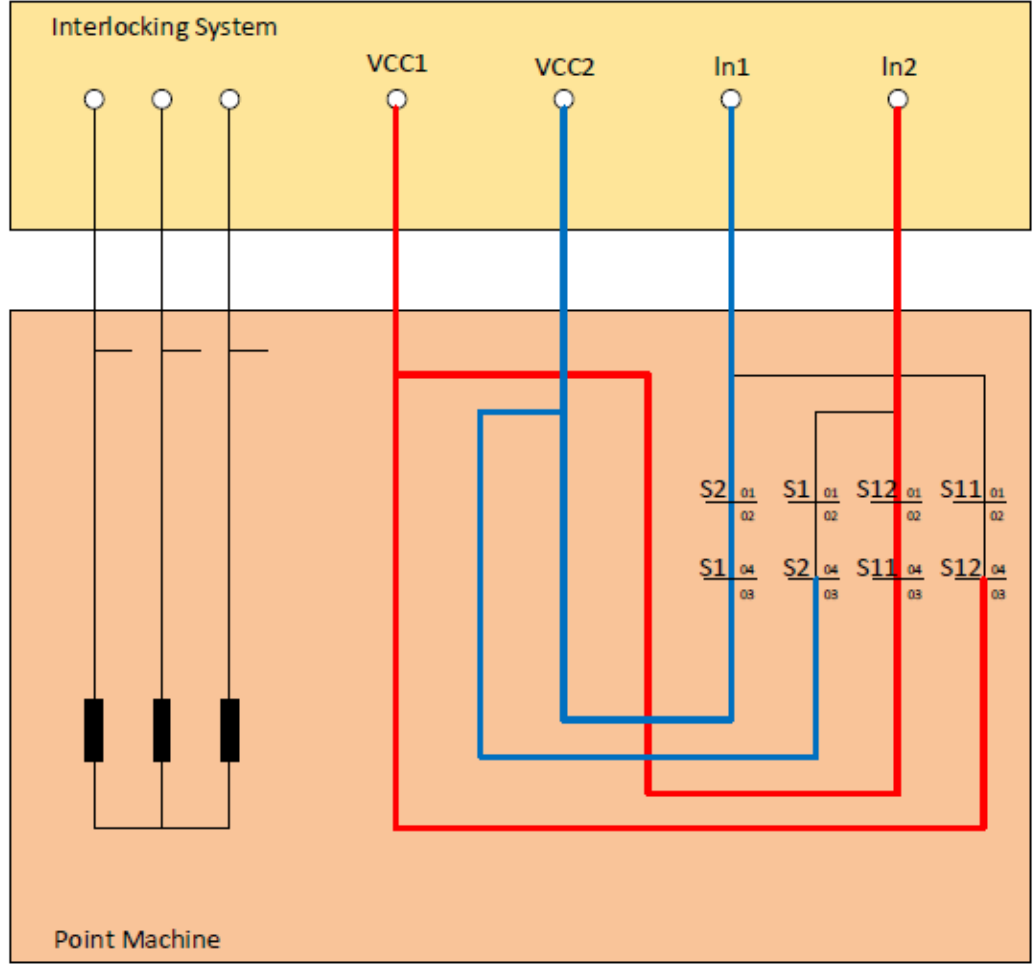
Şekil 2.6 : Sağ Son Pozisyon Konumu için Kurulmuş 7 –Kablo Tekniği

Makas konum değiştireceği zaman makasa güç devresi tekrar bağlanılır. Motorun 3 fazına giden enerji kablolarının bağlantısı kurulur ve makas motoruna gerilim iletmeye başlar. Şekil 2.7’de görülebileceği gibi makas motoru üzerindeki kontaklar pozisyon değiştirdiği için kontrol devresi makas üzerine iletmeye devam ettiği VCC1 ve VCC2 gerilimleri üzerinden herhangi bir geri dönüş alamaz. Motor son pozisyona ulaşıncaya kadar sürülür.



Şekil 2.7 : *Motorun Hareket Halindeki Devre Şeması*

Makas son konuma vardığında makas motoru üzerindeki kontaklar pozisyon değiştirir. Kontrol devresinde beslenmeye devam eden VCC1 ve VCC2 gerilimlerinden geri dönüş alınmaya başlanır. Makas sol son pozisyonda iken uygulanan gerilimlerden VCC1 makasın son pozisyon kontaklarından geçerek IN2 bağlantısı üzerinden geri dönüş sağlanmış olmalı ve aynı zamanda uygulanan VCC2 gerilimi ise IN1 girişinden geri dönüş sağlamalıdır. Şekil 2.8’de gösterildiği gibi bu iki bilginin elde edilmesi makasın sol pozisyona oturduğunun kanıtıdır.



Şekil 2.8 : *Sol Son Pozisyon Konumu için Kurulmuş 7 –Kablo Tekniği*

3. ÜÇ FAZ DÖRT KABLO TEKNİĞİ İLE SÜRÜLEN MAKAS MOTORU ARAYÜZ DEVRESİNİN TASARIMI

3.1 Giriş

Bu bitirme projesi kapsamında üç faz dört kablo tekniği ile sürülen makas motorunun arayüz devresinin tasarımı iteratif olarak gerçekleştirilecektir. Bu bölümde motorun tipi ve özellikleri, demiryolu projelerindeki standartlar ile uyumluluk, problemin tanımı, dizayn ve gerçekleştirme olarak devam edilecektir.

Proje kapsamında Voestalpine HYTRONICS firmasının ürettiği Ecostar 4 makas motoru üzerinde çalışılacaktır. Bu makas motoru firmanın açık hat konvansiyonel uygulamalarda en çok kullandığı motordur. Voestalpine firması dünyadaki en büyük demir-çelik imalatçılarından biridir. Demiryolundaki en büyük uzmanlık alanları makas üretimidir. Yani trenlerin manevra yapmasını sağlayan rayları üretmektedir. Bunun dışında demir-çelik, mekanik ve elektrik sistemlerindeki bilgilerini de kullanarak makasların sürülmesi için her türlü demiryolu uygulamasına uygun makas motorları geliştirmektedirler. Kullanılan makas motorunda elektrik motorunun sürdüğü mekanik kollar ile makas dilinin hareketi sağlanır. Makas son pozisyon ulaştığında makas motoru üzerinde mekanik parçalar konum değiştirir. Bu konum değişikliği ile makas motorunun üzerinde yer alan rölelerin kontakları pozisyon değiştirir.

Makas motoru içerisindeki AC motor JOMO isimli motor üreticisinden tedarik edilmiş olup. Çizelge 3.1’de motor ile ilgili bilgiler verilmiştir.

Çizelge 3.1 : Ecostar 4 Makas Motoru Elektriksel Parametreler

Bilgiler	Değerler
Motor Üreticisi	JOMO
Motor Kodu	Dr 80-2-17
Motor Gerilimi	400 VAC
Motor Akımı	2.9 A
Motor Devri	2470 min ⁻¹
Motor Gücü	1.1 KW
Motor Frekansı	50 Hz

3.2 Standartlar

Dizayn ve mühendislik faaliyetlerine geçmeden önce demiryolu projelerinde kullanılan 3 temel standart bu bölümde belirtilecektir.

- EN 50126: Demiryolu Uygulamaları – Güvenilirlik, Ulaşılabilirlik, Bakım Yapılabilirlik ve Güvenlik (RAMS) Şartnamesi ve Gösterimi:

Bu standart genel olarak demiryolu kullanımı için geliştirilen ürünlerin projelendirme aşamasından, geliştirme, test ve nihai ürüne dönüşürken atlatması gereken prosedürleri açıklayan standarttır. Standartın içerisinde Güvenilirlik, Ulaşılabilirlik, Bakım Yapılabilirlik ve Güvenlik kavramlarının neler olduğu bu kavramların bir uygulama esnasında nelere karşılık düştüğünün anlaşılması açısından en temel standarttır.

Bitirme tezinde özellikle ihtiyaç duyulan sistemin risk analizi için demiryolu projelerinde RAMS kıstaslarının tutturulması için demiryolu projelerinde sistem hayat döngüsü için izlenen yollar ele alınacaktır.

- EN 50128: Demiryolu Uygulamaları – Haberleşme, Sinyalizasyon ve İşleme Sistemleri – Demiryolu Kontrol ve Koruma Sistemleri için Yazılım:

Bu standart demiryolunda kullanılmak üzere geliştirilecek yazılımlar için gerekli olan standarttır. Standartın içeriği oldukça detaylıdır. Yazılım geliştirme hayat döngüsü, yazılım mimarisi, yazılım geliştirme teknikleri, yazılım test ve doğrulama gibi per çok farklı aşama detaylı olarak paylaşılmıştır. Güvenlik analizi sonucu geliştirilen yazılımın hangi güvenlik seviyesine karşılık düştüğü ve bu seviyeye karşılık söz edilen geliştirme aşamalarında hangi tekniklerin kullanılabileceği net bir şekilde belirtilmiştir.

Bitirme tezinde öncelikli olarak arayüz devresi röleler ve kontaktörler ile gerçekleştirilmiştir. İlerleyen süreçte arayüzün elektronik bir kontrol ünitesi ile kontrol edilmesi planlanmıştır. Ancak burası için geliştirilen yazılım EN 50128’de istenen tekniklere uyumluluğu ele alınmayacaktır.

- EN 50129: Demiryolu Uygulamaları – Haberleşme, Sinyalizasyon ve İşleme Sistemleri – Sinyalizasyon için Güvenlikle İlgili Elektronik Sistemler:

Bu standart demiryolu uygulamalarındaki temel 4 kavramdan olan güvenlik kavramını detaylıca analiz etmektedir. EN 50126'da daha yüzeysel olarak söz edilen risk analizi ve güvenlik değerlendirmesi EN 50129'da detaylıca işlenilmektedir. Sistemlerin güvenlik isteleri, güvenlik ve kalite yönetimi, sistemsel ve fonksiyonel güvenlik ve güvenlik ile ilgili sistemlerin kabulü gibi kavramlar bu standartta kendine yer bulmaktadır.

Bitirme tezinde risk analizi ve risk belirleme ile ilgili uygulanan teknikler için EN 50129 standardı referans alınacaktır. Ayrıca yapılan tasarımın oluşabilecek muhtemel hatalar karşısında nasıl tepki gösterdiği standartta belirtilen hata analiz yöntemlerinden olan Fault Tree Analysis kullanılarak açıklanacaktır.

- IEC 61508: Genel Fonksiyonel Güvenlik Standartı Elektriksel, Elektronik veya Programlanabilir Elektronik Sistemler için:

Bu standart fonksiyonel güvenlik için şemsiye standarttır. Bir başka deyişle EN 50126-50128-50129 için tepe standarttır. Ancak EN standartları ile IEC 61508 arasında bazı temel konularda ciddi farklar vardır. Bu sebeple demiryolu projelerinde öncelikli olarak EN standardı ele alınmaktadır. EN standardında net olarak atıfta bulunulmayan yerlerde IEC 61508'den yararlanılabilir.

- PD CLC TR 50451: Demiryolu Uygulamalarında Güvenlik Bütünlük İsterlerinin Sistematik Dağıtımı:

Bu teknik rapor, Risk Yönetimi ve İndirgenebilir ve Kabul Edilebilir Risk değerlendirilmesi açısından izlenecek yola yönelik sistematik bir yaklaşım ortaya koymaktadır.

- EN 50506: Demiryolu Uygulamaları – Haberleşme, Sinyalizasyon ve İşleme Sistemleri – EN 50129 için Uygulama Rehberi: Güvenlik Güvencesi

EN 50129 standardının nasıl uygulanacağına dair örnekler içeren rehberdir. Projelerde güvenlik ile ilgili uygulama kavramlarının detaylandırılması ve farklı standartlara göre sertifikalandırılmış ürünlerin kabul edilebilirliği incelenmektedir.

- EN 60947-4-1 Alçak Gerilim Anahtarlama Düzeni ve Kontrol Düzeni - Bölüm 4-1: Kontaktörler ve Motor Yol Vericileri - Elektromekanik Kontaktörler ve Motor Yol Vericileri ve EN 60947-5-1 Alçak Gerilim Anahtarlama Düzeni Ve Kontrol

Düzeni Bölüm 5-1: Devre Kontrol Cihazları Ve Anahtarlama Elemanları- Elektromekanik Devre Kontrol Cihazları

Makas motorunu sürmek için kullanılacak kontaktörün seçimi için refererans alınan ürün standartlardır.

3.3 Problemin Tanımlanması

Makas motorunun 3 faz 4 kablo tekniği ile sürülebilmesi için öncelikle motor karakteristiğinin ortaya çıkarılması gerekmektedir. Makas motorunu elektrik enerjisi ile sürmeden önce manevra kolu yardımı ile makas normal ve sapan konumlar (buradan sonra sağ son pozisyonu ve sol son pozisyonu olarak isimlendirilecektir) için son pozisyona getirilmiştir. Manevra kolu makas motoruna enerji veya kontrol indikasyonu için iletilen gerilimi S101 ana klemensini açarak keser. Bu sayede manevra kolu ile herhangi bir işlem yapılırken motora enerji iletilmesinin önüne geçilmiş olur.

Manevra kolu ile yapılan testler sonucunda sağ ve sol son pozisyon konumları için bağlantı kurulacak 4 noktanın yapısı ortaya çıkarılmıştır. Sağ son pozisyon için 1-4 ve 2-3 kontaklarının kısa devre olduğu, sol son pozisyon için ise 1-3 ve 2-4 kontaklarının kısa devre olduğu görülmüştür.

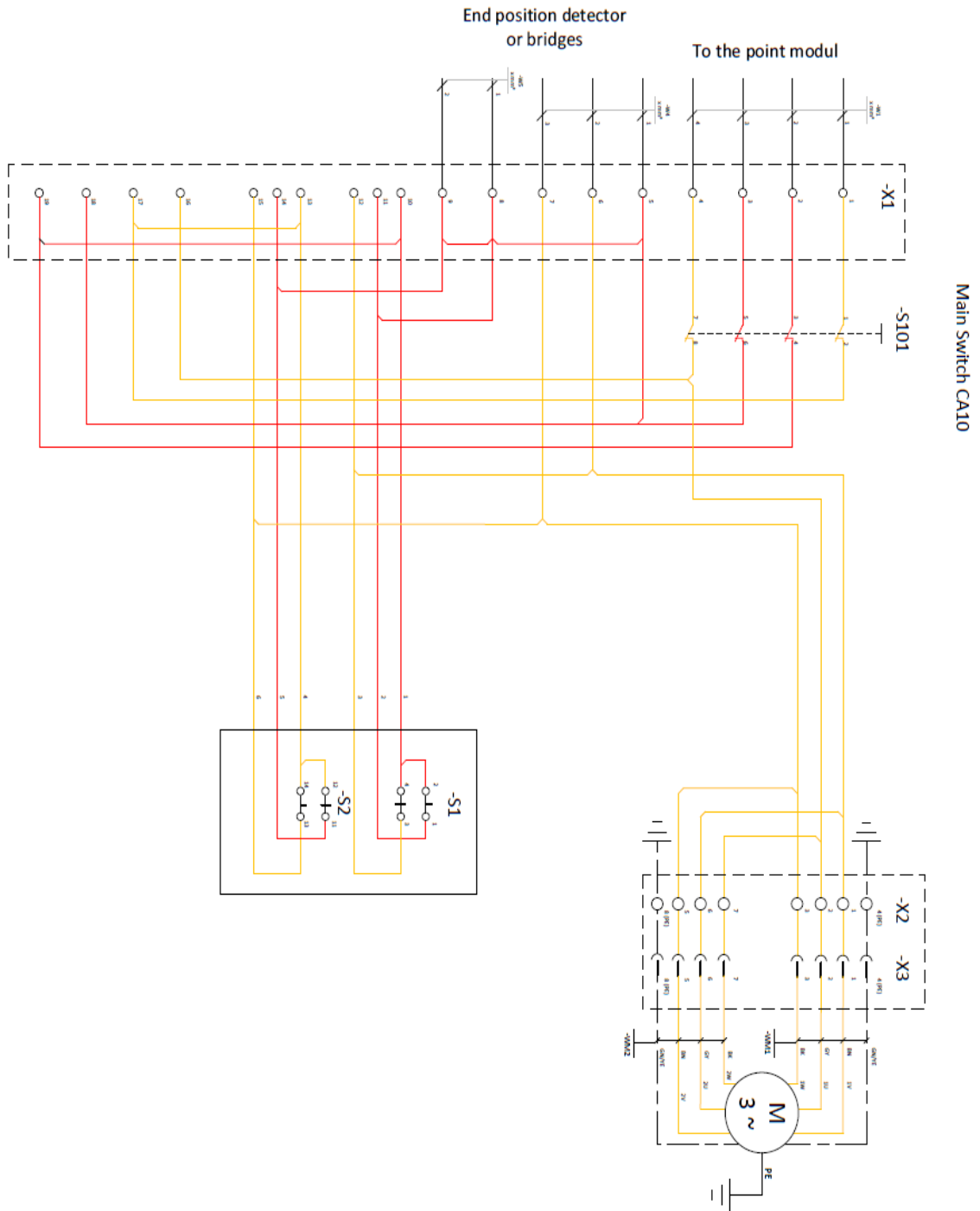
Bu noktadan sonra motorun içerisindeki S1 ve S2 kontaklarının pozisyonları motorun iç kablolama çizimlerinden yararlanarak çıkarılmıştır. Şekil 3.1’de görülebileceği gibi sağ son pozisyon konumunda S1 kontağının 1-2 uçları kısa devre, 3-4 uçları ise açık devredir. Aynı pozisyon için S2 kontağının 11-12 uçları açık devre, 13-14 uçları ise kısa devredir. Şekil 3.5’de ise sol son pozisyon için gösterim bulunmaktadır. Burada S1 kontağının 1-2 uçları açık devre, 3-4 uçları ise kısa devredir. Yine sol son pozisyon için S2 kontağının 11-12 uçları kısa devre, 13-14 uçları ise açık devredir. Bu bilgiler ışığında motor üzerinde son konum bilgisinin nasıl elde edileceği konusunda yol belirlenmiştir.

Motora enerji bağlanarak sürülmeden önce kullanılacak 4 kablodan hangilerinin fazlara bağlanılacağı ve hangi hattın nötr hattı olarak belirleneceğinin çıkarılması gerekmektedir. Bunun için makas motoru manevra kolu yardımı son pozisyon konumu dışında bir noktaya getirilir ve S101 ana klemensinde bağlantı kurulacak 4 nokta ile motor sargılarına X2-X3 klemensi arasındaki bağlantılar incelenmiştir. Sonuç olarak

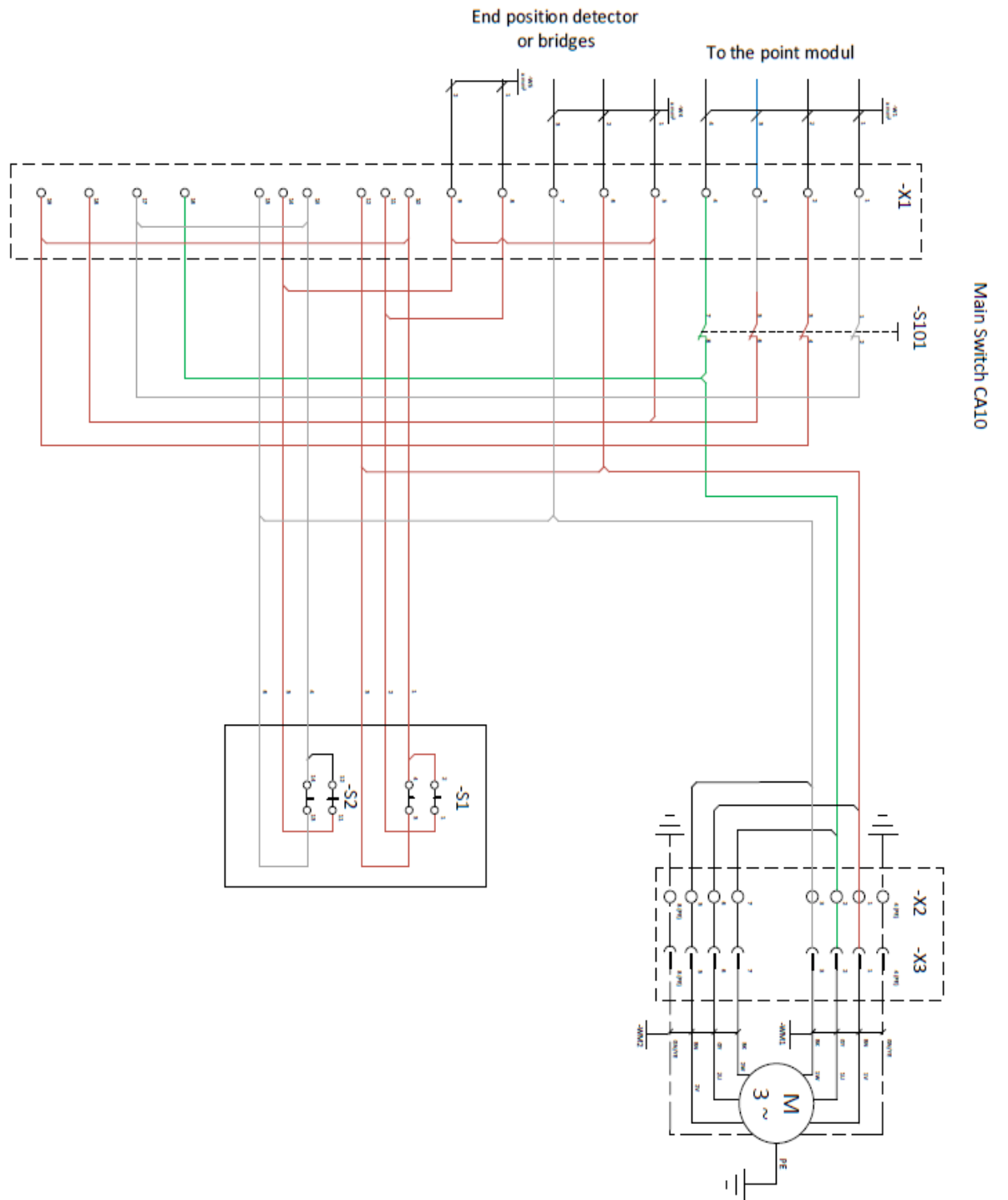
Şekil 3.3.'de görülebileceği gibi fazların 1-2-4 numaralı bağlantı noktalarına bağlanması gerektiği görülmüştür. 3 numaralı bağlantı noktası ise nötr hattı olarak kullanılacaktır. Motorun sürülme anında S1 ve S2 kontaklarının pozisyonları da incelenmiştir. Motor sürülme anında sağ konumdan sol konuma ilerleme yapılırken veya sol konumdan sağ konuma ilerleme yapılırken S1 ve S2 kontaklarının aynı pozisyonda bulundukları görülmüştür. Sürülme anında S1 kontağının 1-2 uçları açık devre, 3-4 uçları ise kısa devredir. Aynı pozisyon için S2 kontağının 11-12 uçları açık devre, 13-14 uçları ise kısa devredir. Şekil 3.2 ve Şekil 3.4'te motorun sürülme anı ile son pozisyon konumları arasındaki geçiş anındaki durumu göstermiştir. Çizelge 3.2'de yukarıda detaylandırılan S1 ve S2 kontaklarının pozisyonlara göre durumu özetlenmiştir.

Çizelge 3.2 : Pozisyonlara Göre S1 ve S2 Kontaklarının Durumu

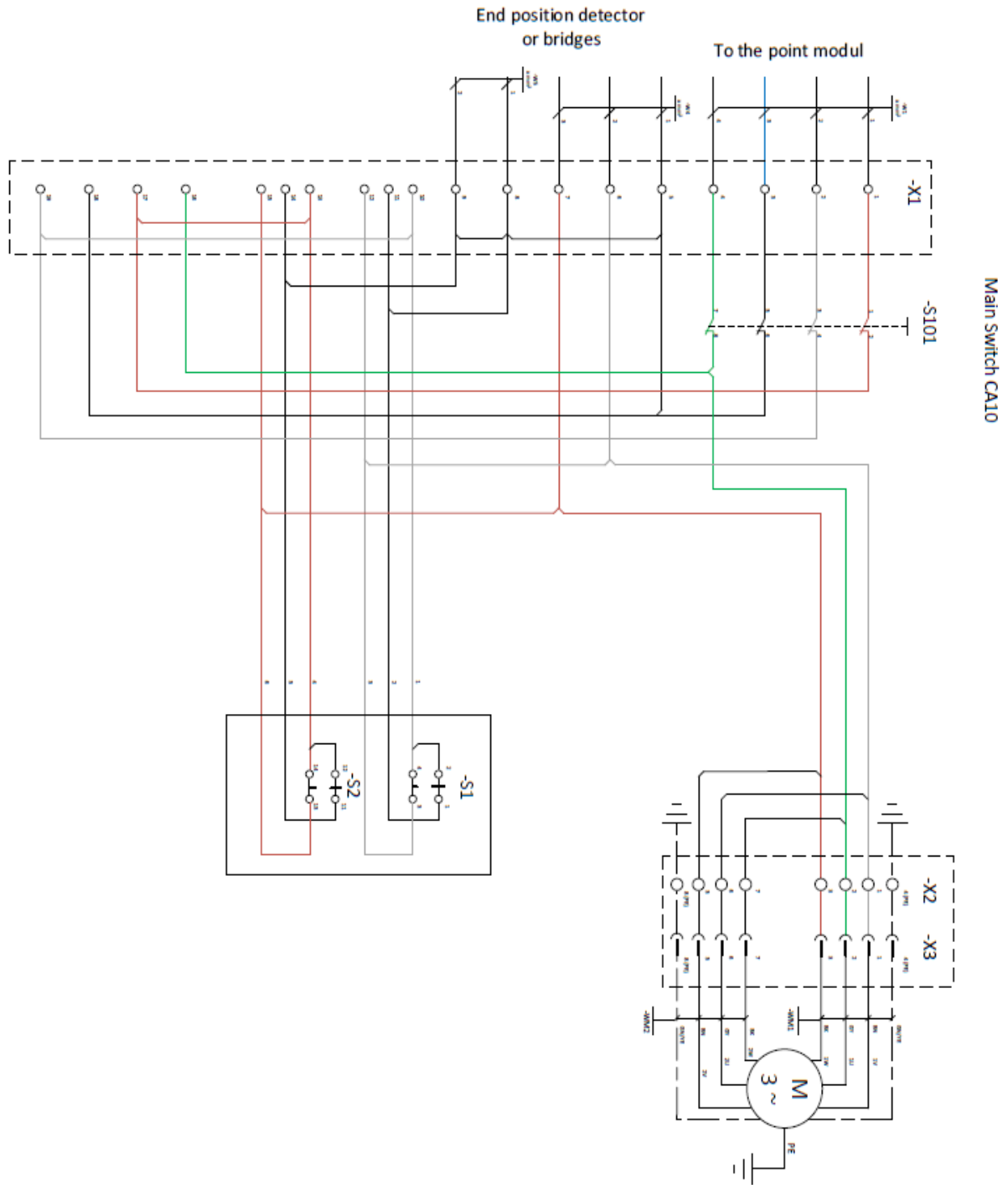
Pozisyon Durumu	S1 Konağı Kısa Devre	S2 Konağı Kısa Devre
Sağ Son Pozisyon	1-2	13-14
Hareket Hali	3-4	13-14
Sol Son Pozisyon	3-4	11-12



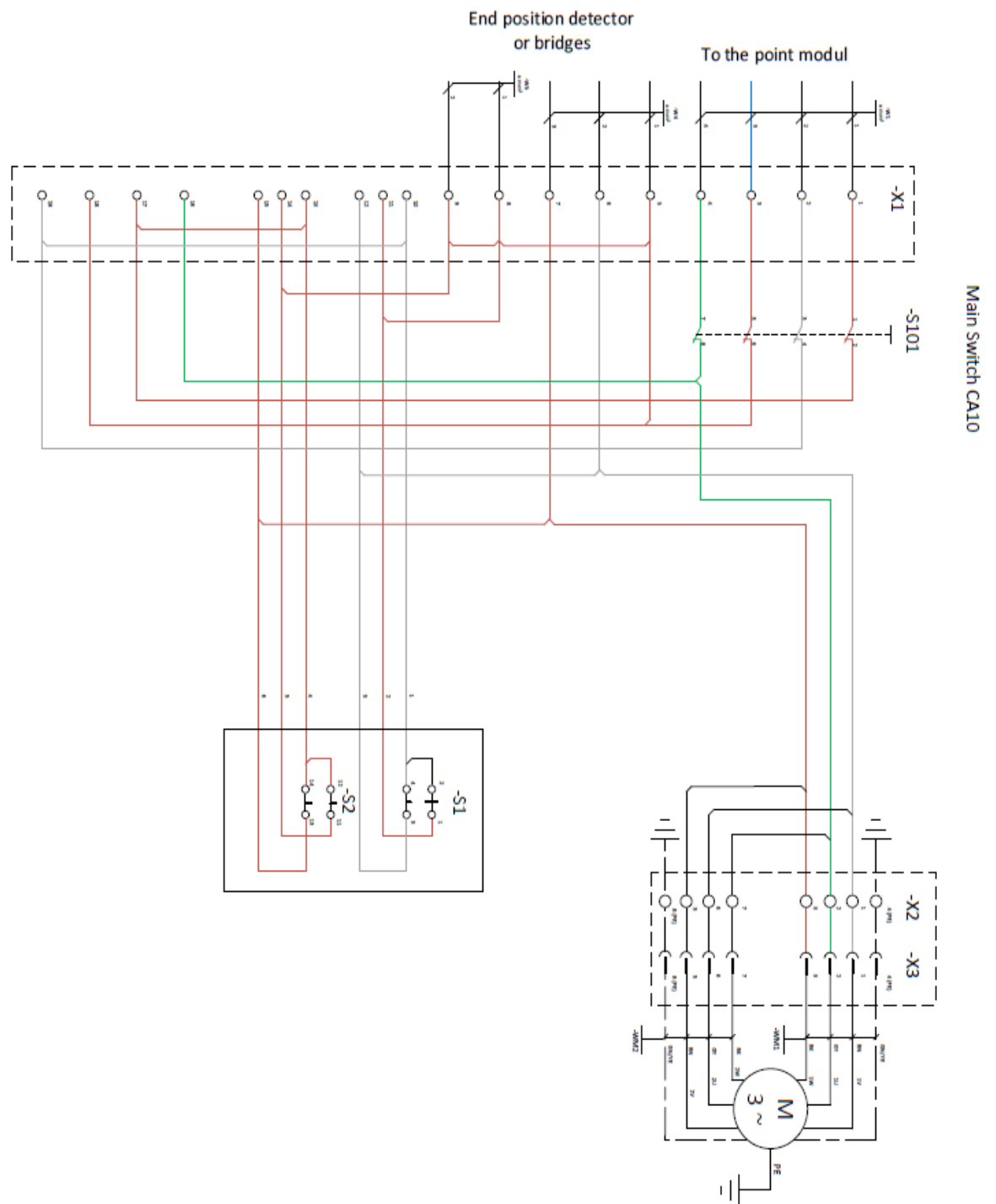
Şekil 3.1 : Motorun Sağ Son Pozisyonda İken



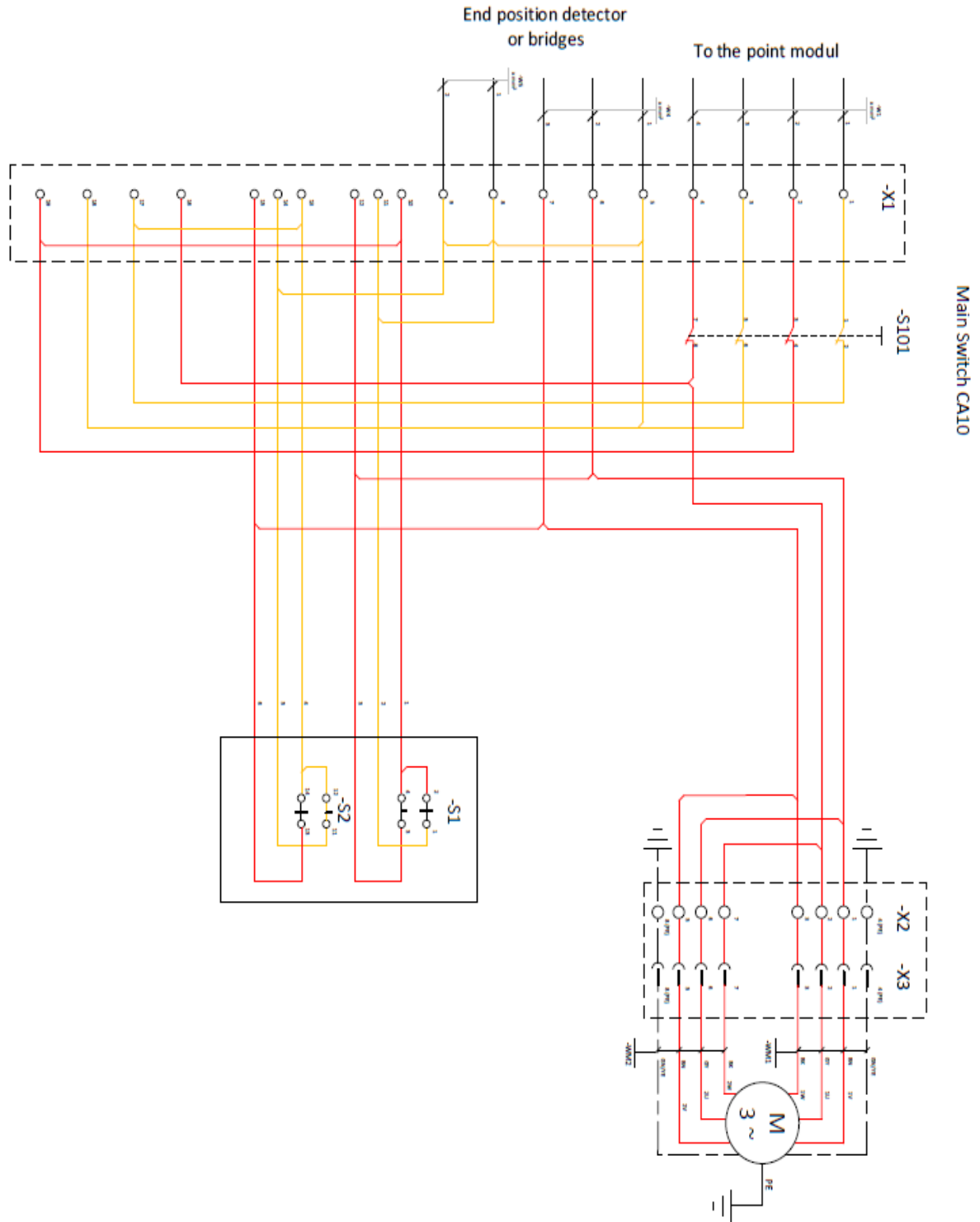
Şekil 3.2 : Motor İlk Enerji Aldığı An



Şekil 3.3 : Motor Sağ Pozisyonndan ve Sol Pozisyona Hareket Ederken



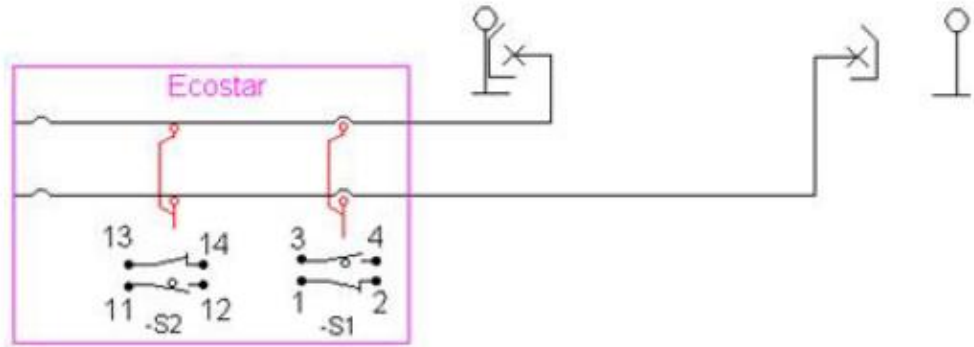
Şekil 3.4 : Motor Sol Son Pozisyona Ulaştığı An



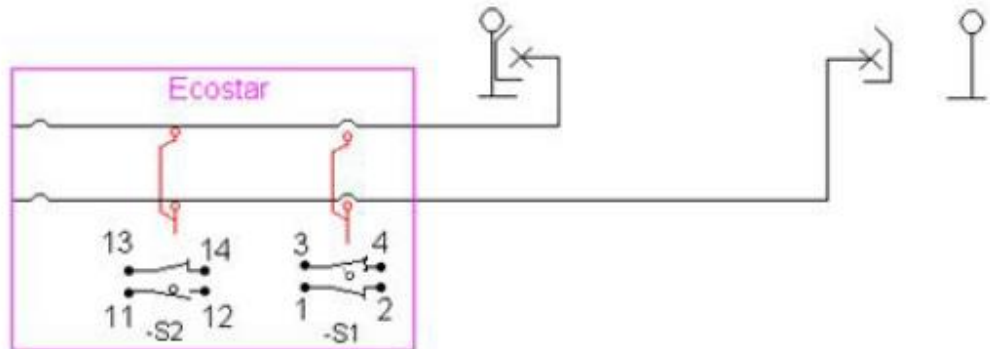
Şekil 3.5 : Motor Sol Son Pozisyonda İken

Buradan sonra makas motoruna enerji verilerek sürülmesi gerçekleştirilmiştir. Motorun enerji ile sürülürken S1 ve S2 kontaklarının son pozisyon konumlarından motorun sürülme pozisyonuna geçerken ve motor sürülürken son pozisyona ulaştığındaki karakteristiği incelenmiştir. Çizelge 3.2’den görülebileceği gibi, herhangi bir son pozisyondan sürüş pozisyonuna geçişte veya tam tersi harekette S1 ve S2 kontaklarından sadece bir tanesi pozisyonunu değiştirmektedir.

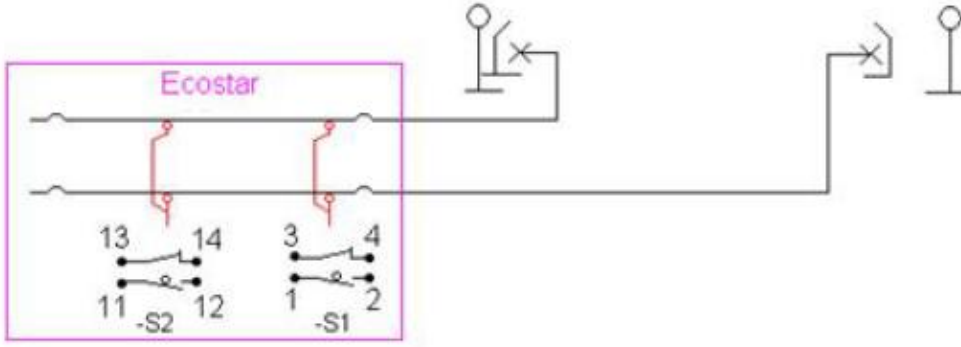
Yapılan inceleme doğrultusunda S1 ve S2 kontaklarının pozisyon değişimi esnasında önce her iki kontağını da kısa devre ettiği daha sonra ise önceden kısa devre ettiği kontağı açtığı görülmüştür. Şekil 3.7 ve Şekil 3.9’da her iki kontağında kısa devre olma durumu gösterilmiştir. Bu durum sağ son pozisyondan sol son pozisyona ilerleyen motor için aşağıda verilen görsellerde açıklanmıştır. Şekil 3.6 ve Şekil 3.10’da sırası ile motorun sağ son pozisyon ve sol son pozisyonundaki durumları gösterilmiştir. Şekil 3.8’de ise motorun hareket halinde iken kontaklarının gösterimi bulunmaktadır.



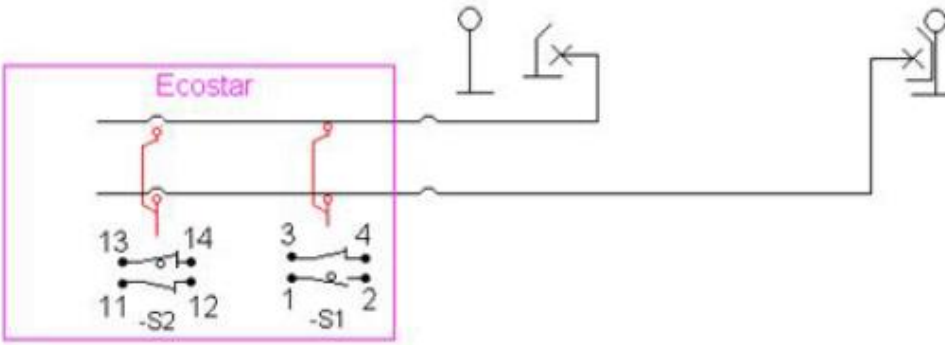
Şekil 3.6 : Motor Sağ Son Pozisyonda



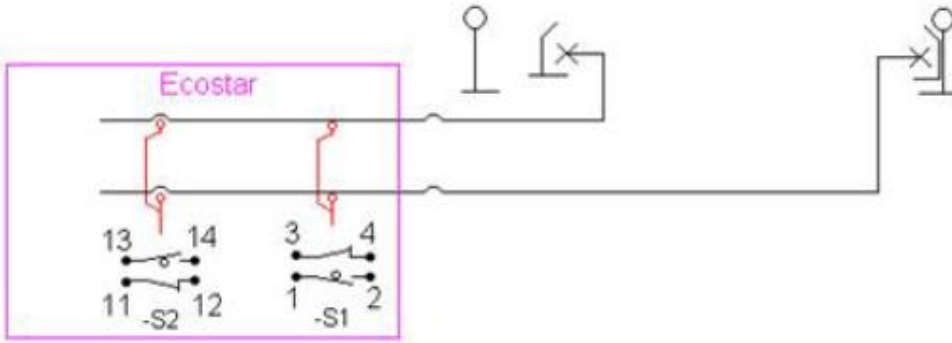
Şekil 3.7 : Motorun Harekete Başladığı İlk An



Şekil 3.8 : Motor Hareket Halinde



Şekil 3.9 : Motor Sol Son Pozisyona Ulaştığı An



Şekil 3.10 : Motor Sol Son Pozisyonda

Yukarıda belirtilen görsellerde belirtilen durum motorun özel karakteristiğini ortaya koymaktadır. Motora uygulanan kontrol gerilimi kesilip motorun harekete geçirilmesi için fazlar iletmeye başlanıldığında motor iki fazda kalkış yapmaktadır. Anlık olarak gerçekleşen bu hareket sol son pozisyona ilerlerken S1 kontak pozisyonlarını değiştirmesini tamamlaması ile sağ son pozisyona ilerlerken ise S2 kontak pozisyonlarını değiştirmesini tamamlaması ile beraber son bulmaktadır. Kontaklar pozisyon değiştirdiği andan itibaren makas 3 faz ile sürülmektedir. Tersi durumda ise motor sürüş pozisyonunda son konuma ulaştığında kontaklar pozisyon değiştirdiği için

motor yine iki faza düşmektedir. Bu durumda nötr hattından akım akmaya başlar. Bu bilgi makas motoru arayüzündeki en önemli problem olan güç devresi ile kontrol devresi arasındaki geçişin ne zaman sağlanacağı sorusunun cevaplarından biridir. Nötr hattında akım akmaya başladığı an makas motoru son konuma ulaşmış demektir ve iletilen güç kesilmelidir.

3.4 Arayüz Devresinin İsterlerinin Çıkarılması

Makas motorunun karakteristiği ortaya çıkarıldıktan sonra arayüz devresinin tasarımına başlanmadan önce arayüz devresi ile isterlerin çıkarılması amaçlanmaktadır. Makas motoru arayüzü temelde anlaşılan sistemi ile makas motoru arasında yer alan bir ünedir. Bu sebeple tasarıma başlanmadan önce her iki tarafta da yer alacak sistemlerin incelenmesi gerekmektedir.

Bir önceki bölümde makas motorunun karakteristiği ve yapısı incelenmiştir. Arayüzün diğer tarafında yer alan anlaşılan sistemi ise bu bölümde detaylandırılacaktır. Arayüz devresi, anlaşılan sisteminden iki giriş alır ve anlaşılan sistemine iki çıkış iletir. Girişler sağa ve solu git komutlarıdır. Anlaşılan sistemi makasın çevrilmesi ile ilgili güvenlik fonksiyonlarını kendi içerisinde denetlemektedir. Dolayısı ile arayüz devresi makasın çevrilmesi için diğer çevresel faktörlere bakmaz. Anlaşılan sistemi çevirme komutunu makas üzerinden indikasyon bilgisini okuyuncaya kadar sürekli olarak arayüz devresine iletir. Arayüz devresinin, anlaşılan sistemine iletteği çıkışlar ise makas sağ pozisyonda veya makas sol pozisyonda bilgisidir.

Anlaşılan sistemi belli bir süre boyunca makas arayüzünde pozisyon bilgisini okuyamaz ise bu durumda ürettiği komut bilgisini keser. Bu duruma makas dilinin arasına taş sıkışması veya soğuk havalarda makas dillerinin birbirine yapışması gibi özel durumlardan ötürü makasın son konuma ulaşamadığı zamanlarda karşılaşılabılır. Söz konusu durumlarda komut bilgisi kesilmeyecek olsaydı makas motoru hareket edemediği halde kendini zorlamaya devam ettiği için makas motoruna zarar verilebilirdi. Makasın son pozisyona ulaşamadığı durumlarda makasa iletilen gücün kesilmesi için arayüz devresi anlaşılmadan gelen komutun kesilmesini kullanabilir.

Ayrıca arayüz devresi hali hazırda makasın bulunduğu pozisyonda iken o pozisyona gidilmesine dair bir komut alınması durumunda bu komutu işletmemelidir. Bunu

gerçekleştirirken makasın o yöne doğru sürülmeye çalışılması veya makasın pozisyon indikasyonun anlık olarak kesilmesine de izin vermemelidir.

Makas motorunun sürülmesi güç devresi olmak üzere ve indikasyon için kontrol devresi olmak üzere iki ayrı devre kullanılacaktır. Bu devrelerde güç devresi 3 faz 400VAC gerilim anahtarlarken, kontrol devresi ise 24VDC gerilim göndererek makasın pozisyonunu okuyacaktır. Burada en önemli ve kritik konu güç devresinin ve kontrol devresinin kesinlikle motora aynı anda bağlanmamasıdır. Ayrıca güç devresi için bir başka ister motorun farklı pozisyonlara gidişi için farklı faz sırası ile anahtarlanacak 3 fazın bu farklı kombinasyonlarının kısa devre halinde olmamasıdır. Aynı şekilde kontrol devresinde de motora beslenecek DC gerilim farklı röleler üzerinden doğru sıra ile farklı zamanlarda verilmelidir.

Bir başka konu makasın son konuma ulaştığında nötr hattında oluşan akımın tespiti. Güç devresinin hatta bağlanması ile beraber akım sensörü de nötr hattına bağlanmalıdır. Hattan akım aktığı tespit edildiğinde üzerindeki normalde açık kontaklı röle üzerinden bu bilgi kullanılmalıdır.

Yukarıda belirtilen isterler doğrultusunda arayüz devresinin ana komponentleri belirlenmiştir. Motoru iki ayrı yöne sürebilmek için iki adet kontaktöre ihtiyaç vardır. Ayrıca iki ayrı konum sorgusu yapılabilmesi için iki röle üzerinden DC gerilim motora beslenecektir. Anlaşman sisteminden gelen komutların okunması için ayrı röle ve anlaşmana pozisyon bilgilerini iletmek için ise iki ayrı röleye daha ihtiyaç duyulacaktır. Son durumda toplamda iki kontaktör ve 7 röleden oluşan bir sistem oluşturulacaktır. Çizelge 3.3'te kullanılacak röle ve kontaktörlerin isimlendirmesi verilmiştir.

Çizelge 3.3 : Arayüz Devresindeki Röle ve Kontaktörlerin İsimlendirmesi

İsimlendirme	Tanım
CA	Akım bilgisinin okunacağı röle
DCL	Sol pozisyon konum tespiti için DC gerilim besleme rölesi
DCR	Sağ pozisyon konum tespiti için DC gerilim besleme rölesi
KML	Sol son pozisyona ulaşmak için motoru süren kontaktör
KMR	Sağ son pozisyona ulaşmak için motoru süren kontaktör
LC	Anlaşmandan gelen sola git komut rölesi
LP	Makas sol pozisyonda bilgisini aktaran röle
RC	Anlaşmandan gelen sağa git komut rölesi
RP	Makas sağ pozisyonda bilgisini aktaran röle

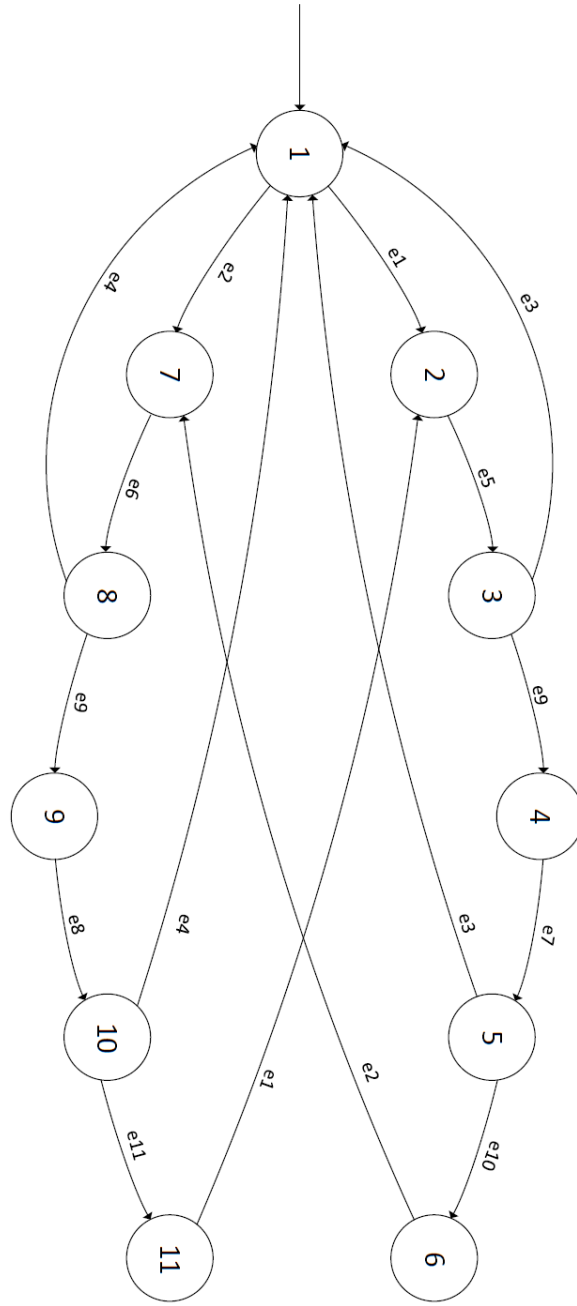
Arayüzden beklenen fonksiyonlar aşağıda sıralanmıştır:

1. Makas ilgili son pozisyonda iken indikasyon okunması için doğru uçtan DC gerilim besleme
2. Makasın komut gelmesi ile beraber DC gerilimi kesip doğru fazları ilgili uçlara besleyerek motoru sürme
3. Nötr hattında akım akması ile beraber akım rölesi üzerinden bu bilgi alınması
4. Akım rölesi üzerinden alınan bilgi veya anlaşılmadan iletilen komut bilgisinin kesilmesi ile AC gerilimin kesilmesi
5. Makasa AC ve DC gerilimlerin aynı anda iletilmemesi
6. Makasın bulunduğu konumun dışındaki pozisyonu anlaşılmaya iletmesi
7. Makasın ortada kalması durumunda herhangi bir pozisyon bilgisinin üretilmemesi
8. Farklı yönlere motorun sürülmesini sağlayan AC gerilimlerin aynı anda beslenmemesi
9. Farklı yönlerde konum sorgulaması yapacak DC gerilimlerin aynı anda beslenmemesi

3.5 Makas Motoru Arayüz Devresinin Röle-Kontaktörlerle Gerçeklenmesi

3.5.1 Otomat tasarımı

Arayüz devresinin tasarımı için sezgisel yaklaşım kullanılarak röleler üzerinden gerçekleştirilecektir. Sezgisel tasarıma geçmeden önce problemin basitleştirilmiş hali bir otomat modeli üzerinden ele alınmıştır. Şekil 3.11’de problemi DCL-KMR-DCR-KML arasındaki geçişleri düzenli halde sağlayan model aşağıda verilmiştir.



Şekil 3.11 : Arayüz Devresi Otomat Modeli

Olaylar Listesi:

e1 = RC rölesinin Lojik 1 konumuna geçmesi

e2 = LC rölesinin Lojik 1 konumuna geçmesi

e3 = RC rölesinin Lojik 0 konumuna geçmesi

e4 = LC rölesinin Lojik 0 konumuna geçmesi

e5 = DCR rölesinin Lojik 0 konumuna geçmesi

e6 = DCL rölesinin Lojik 0 konumuna geçmesi

e7 = DCR rölesinin Lojik 1 konumuna geçmesi

e8 = DCL rölesinin Lojik 1 konumuna geçmesi

e9 = RCA rölesinin Lojik 1 konumuna geçmesi

e10 = RP rölesinin Lojik 1 konumuna geçmesi

e11= LP rölesinin Lojik 1 konumuna geçmesi

Otomat devresine ilişkin devreler aşağıda verilmiştir.

$$Q1 = q2' * q3' * q4' * q5' * q6' * q7' * q8' * q9' * q10' * q11'$$

$$Q2 = q1 * e1 + q11 * e1 + q2 * e5'$$

$$Q3 = q2 * e5 + q3 * e3' + q3 * e9'$$

$$Q4 = q3 * e9 + q4 * e7'$$

$$Q5 = q4 * e7 + q5 * e3' + q5 * e10'$$

$$Q6 = q5 * e10 + q6 * e2'$$

$$Q7 = q1 * e2 + q6 * e2 + q7 * e6'$$

$$Q8 = q7 * e5 + q8 * e4' + q8 * e9'$$

$$Q9 = q9 * e9 + q9 * e8'$$

$$Q10 = q10 * e8 + q10 * e4' + q5 * e11'$$

$$Q11 = q10 * e11 + q11 * e1'$$

Modelin çalışma prensibi şu şekildedir. Başlangıç durumunda makas herhangi bir konum sorgusu yapmamaktadır. Anklaşmandan gelen sağa veya sola konum talebi ile beraber durum 2 veya durum 7'ye geçiş yapılır. Bu durumlarda bilgiyi iletecek olan komut röleleri lojik 1 konumun setlenir. Bu durumundan çıkış koşulu DC gerilim beslemesi ile konum sorgusu yapan rölelerin lojik 0 konumuna çekilmesidir. DCL veya DCR rölelerinin lojik 0'a çekilmesinin ardından durum 3'te KMR kontaktörü motoru sürmesi için enerjilendirilir, durum 8'de ise KML kontaktörü aynı şekilde enerjilendirilir.

Bu durumlardan çıkış için iki koşul vardır. Makas motoru istenilen sürede son pozisyona ulaşamaz ve anklaşman sistemi sağa git veya sola git komutunu keser. Bu

durumda model başlangıç durumuna geri dönmüş olur. Diğer durum ise makasın son duruma ulaşması sonucunda nötr hattında akım akmaya başlar ve akım rölesi üzerinden bu bilgi okunur. Bu olay üzerinden durum 4 veya durum 9'a geçiş yapılır. Bu durumlarda motoru süren kontaktörlerin enerjisi kesilir. KML ve KMR röleleri lojik 0 olduktan sonra ilgili DC gerilim besleme rölesinin çekmesi beklenir. DCR veya DCL rölesinin çekmesi ile beraber durum 5 ve durum 10'a ulaşılır.

Burada artık konum sorgusu için DC gerilim motora iletilmiş ve pozisyon rölelerinin durumu gözlenmektedir. Eğer pozisyon bilgisini üreten RP veya LP röleleri çekmez ise anlaşılan sistemi istenilen sürede son konum bilgisini alamayacağı için sağa git veya sola git komutunu keser bu durumda sistem başlangıç durumuna geri dönüş yapar. Eğer RP veya LP rölesi çekerse bu durumda son konum bilgisi başarı ile okunur ve durum 6 veya durum 11'e geçiş sağlanır. Makas son pozisyon bilgisi üretirken bu durumlardan tek çıkış koşulu makasın bulunduğu pozisyonun tersine anlaşılmadan komut iletilmesidir. Bu olaylar ile birlikte durum 2 veya durum 7'ye geri dönüş sağlanır.

Otomat modelinde bazı korumalar küçük program blokları ile gerçekleştirilmelidir. Bunlar için en bariz olanı KML-KMR-DCL-DCR rölelerinin hiçbir zaman aynı anda devreye girmemesi için iç kilitlerin program tarafından sağlanmasıdır.

Otomat modelinde görülen durum her bir durumun bir röle ile gerçekleştirilmesi durumunda toplam 11 adet rölenin kullanılacağıdır. Sezgisel tasarım için yapılan ilk yaklaşımda ise kullanılması planlanan röle sayısı 7 adetti. Ayrıca otomat modelinin elektronik bir kontrolörde koşturulmasında güç devresi ile elektronik kontrolörün arasındaki izolasyon için ekstra rölelerin de kullanılacağı göz önünde tutularak, bu aşamadan sonra problemin isterleri doğrultusunda sezgisel bir tasarıma geçiş yapılmıştır.

3.5.2 Sezgisel tasarım

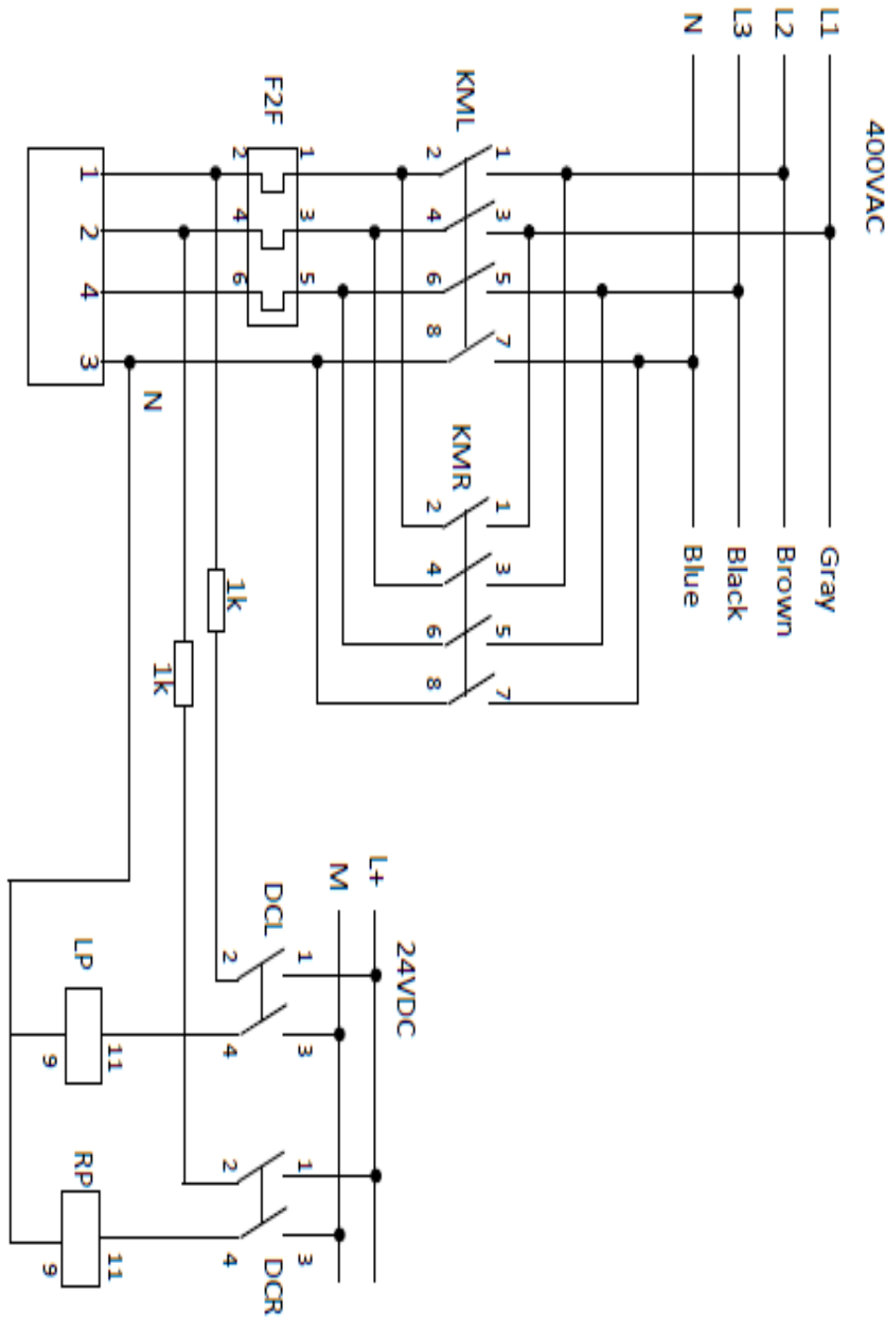
Sezgisel tasarıma başlandıktan sonra iki yeni ister fark daha ortaya çıkmıştır. Bunlar akım bilgisinin doğru zamanda kullanılması ve motora indikasyon beslemesi verilirken oluşturulan akımın limitlenmesidir.

Motorun özel yapısına daha önce değinildiği üzere, motor son pozisyona ulaştığında konum değiştiren rölenin kontaklarının hepsi kapalı kontak konumuna geçtiği durumda nötr hattından akım akmaya başlar. Ancak CA rölesinin aktardığı bilgiyi

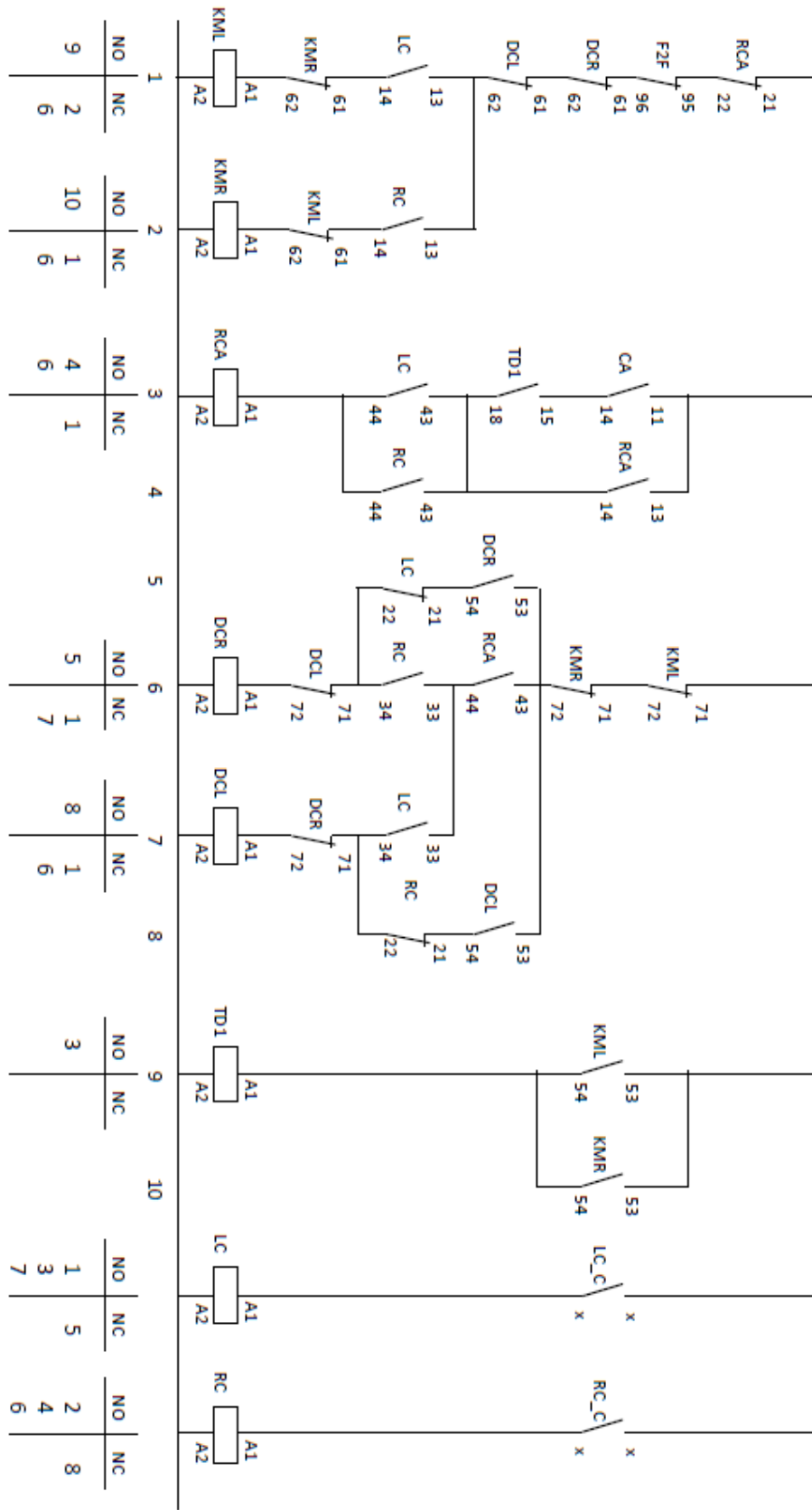
doğrudan kullanmak mümkün değildir. Çünkü bu özel durum motorun kalkış anında da geçerlidir. Motor kalkış anında aynı karakteristiği göstermektedir. Motor kalkışa başlangıç anında anlık olarak iki faz olarak harekete başlar. Bu sebeple nötr hattında akım akar ve CA rölesi üzerinden bu bilgi okunur. Oluşturulan röleli lojik devrede CA rölesinden okunan bilginin motorun kalkış anında mı yoksa motorun yavaşlama anında mı olduğunu röle sayısını fazlaca arttırmadan mümkün değildir. Bunu en basit şekilde ayırt etmenin yolu motoru harekete sokan kontaktörlerden elde edilen bilgi ile sürülen bir zaman rölesi kullanmaktır. Böylece zaman rölesi TD1 normalde açık kontağını kapatmadan CA rölesinden okunan bilgi anlamlandırılmaz. Yani motorun kalkış anında nötr hattından akan akım göz ardı edilir. Ana lojik içerisine bu durum için yeni bir RCA rölesi eklenmiştir. RCA rölesi motorun son konuma ulaştığında nötr hattında akan akım ile çekmektedir.

Motorun nominal akım değeri 2.9 amperdir. Makasın son konum sorgusu için 24VDC iletilecektir. Motorun üzerinden nominal akım değerinin üzerinde bir akım akmaması için kontrol devresine 1000 Ω 'luk dirençler eklenmiştir.

3.4. Bölümdeki belirtilen isterlerle beraber şekil 3.12'deki güç ve şekil 3.13'deki kontrol devresi tasarlanmıştır.



Şekil 3.12 : 3 Faz 4 Kablo Arayüz Güç Devresi



Şekil 3.13 : 3 Faz 4 Kablo Arayüz Güç Devresi

Arayüz devresi tasarımı yapılırken, devrenin gerçekleştirilebilir olmasına özen gösterilmiştir. Kontrol devresinde kullanılan rölelerin hiçbirinde 3 adet normalde açık 2 adet normalde kapalı kontak dışına çıkılmamıştır. Bu sayede yapılan tasarım tedarik edilebilen ürünler ile gerçekleştirilmiştir. Testlere geçilmeden önce 3.4. Arayüz Devresinin İsterleri bölümünde listelenen isterler karşılandığı bir kez daha kontrol edilmiştir.

1. Makas ilgili son pozisyonda iken indikasyon okunması için doğru uçtan DC gerilim besleme

Tasarım: DCL rölesi ile yapılan sorguda iletilen DC gerilim 1 numaralı motor kontak noktasından, DCR rölesi ile yapılan sorguda iletilen DC gerilim 2 numaralı motor kontak noktasından beslenmektedir.

2. Makasın komut gelmesi ile beraber DC gerilimi kesip doğru fazları ilgili uçlara besleyerek motoru sürme

Tasarım: Kontrol devresinde KML ve KMR'nin devreye girmesi için DCL ve DCR rölelerinin devrede olmadığı kontrol edilmektedir. Güç devresinde ise KML ve KMR 3 fazı farklı sıralar ile anahtarlayarak motora güç sağlamaktadırlar.

3. Nötr hattında akım akması ile beraber akım rölesi üzerinden bu bilgi alınması

Tasarım: CA rölesi ile beraber bu bilgi takip edilmektedir. Motorun kalkış ve son konuma ulaştığındaki ayrımın yapılması için TD1 rölesi ile oluşturulan lojik sonucu RCA rölesi kullanılmaktadır.

4. Akım rölesi üzerinden alınan bilgi veya anlaşılmadan iletilen komut bilgisinin kesilmesi ile AC gerilimin kesilmesi

Tasarım: RCA rölesi KML ve KMR rölelerini devre dışı bırakmada kullanılır. LC rölesi aktif olmadan KML, RC rölesi aktif olmadan ise KMR devreye giremez.

5. Makasa AC ve DC gerilimlerin aynı anda iletilmemesi

Tasarım: KMR ve KML rölelerinin çekmesi için DCL ve DCR rölelerinin çekmemiş durumda olması gerekir. Benzer şekilde DCR ve DCL rölelerinin çekmesi için de KML ve KMR rölelerinin çekmemiş durumda olması gerekir.

6. Makasın bulunduğu konumun dışındaki pozisyonu anlaşılmaya iletmesi

Tasarım: LP ve RP rölelerinin hatalı bir şekilde çekmemesi için iki aşamalı bir yapı kullanılmıştır. DCL veya DCR ile beslenen gerilim dönüşünde LP veya RP rölesinin bobinin enerjilenmesi için bobinin diğer ucu toprağa sorgulanması istenen pozisyon için çektirilen DC röle üzerinde ulaşmaktadır. Bu sayede lojikte DCL veya DCR arasında sıra karışması durumunda veya kısa devre gibi bir sebepten LP veya RP rölesinin çekmesinin önüne geçilmiş olur.

7. Makasın ortada kalması durumunda herhangi bir pozisyon bilgisinin üretilmemesi

Tasarım: Makastan son pozisyon bilgisi DC kontrol gerilimin doğru uçtan beslenmesi sonucu makas motoru içerisindeki kontakların kontrol edilmesi ile beraber pozisyon röleleri çektirilmektedir. Makasın son konuma ulaşamaması durumunda KML veya KMR röleleri anlaşılanın sürme komutunu ilettiği LC veya RC rölesinin düşmesi ile devre dışı kalacaktır. Bu durumda DCL veya DCR rölesi çekemeyeceği için ayrıca da bir koruma alınmıştır.

8. Farklı yönlerde motorun sürülmesini sağlayan AC gerilimlerin aynı anda beslenmemesi

Tasarım: KML ve KMR'nin çekmesi için birbirlerinin devrede olmadığı durum için garantiye alınmıştır.

9. Farklı yönlerde konum sorgulaması yapacak DC gerilimlerin aynı anda beslenmemesi

Tasarım: DCL ve DCR'nin çekmesi için birbirlerinin devrede olmadığı durum için garantiye alınmıştır.

Yukarıda belirtilen isteklerin doğrultusunda gerçekleştirilen tasarım Voestalpine Ecostar 4 motoru üzerinde denenmiştir. Yapılan testler sonucunda kontrol devresi ve güç devresi beklendiği makası sorunsuz şekilde sürüp, makas üzerinden konum bilgisini her seferinde doğru bir şekilde okumayı başarmıştır.

3.6 Fonksiyonel Güvenlik Kavramı ve Risk Analizi

Elektromekanik ve elektronik bileşenlerin güvenlik açısından kritik uygulamalarda kullanımı geçtiğimiz yüzyıl içerisinde gerçekleşen teknolojik gelişmeler ışığında hızla artmaktadır. Üstelik bilgisayarların hayatımızın her alanına girmesi sonucu bu öğelere

programlanabilir sistemler de eklenmiştir. Bütün bu gelişmeler ise beraberinde bilinmezlikleri ve yeni risk potansiyellerini getirmektedir.

Güvenlik açısından önemli uygulamalardaki yeni metotlar ve ekipmanlar yeni bir güvenlik anlayışını da gerektirmekteydi. Bu durum ise fonksiyonel güvenlik kavramının ortaya çıkmasına neden olmuştur.

“Kontrol altındaki ekipman ve bu ekipmanı kontrol eden sistemin bünyesindeki elektromekanik, elektronik ve programlanabilir bileşenlerin doğru işlevi yerine getirmesi esasına dayanan, genel güvenlik sisteminin parçası olan güvenlik yaklaşımı ve risk azaltma metotları” [2] olarak tanımlanan fonksiyonel güvenlik günümüzde ulaşımdan endüstriyel faaliyetlere, sağlık sektöründen enerji sektörüne pek çok alanda artan bir öneme sahiptir ve genel güvenlik yaklaşımının kritik bir parçasıdır.

Fonksiyonel güvenlik ile ilgili temel kavram ve metotlar uluslararası ve ulusal standartlar ile belirlenmeye çalışılmakta, bu sırada ise yeni araştırma ve gelişmelere göre güncellenmektedir. Bu bağlamda Avrupa ve çoğu Asya ülkesinde IEC ve ISO, Amerika kıtasında ise ISA’nın hazırladığı standartlar temel alınmaktadır. Her ne kadar bu kuruluşlar arasında ortak değerler ve hedefler etrafında bir harmonizasyon çalışması yürütülse de henüz bu hedefe ulaşmak tam anlamıyla mümkün olmamıştır.

Bu tezin içerisinde, temel olarak, Türkiye’nin de bir uygulayıcısı ve sorumlusu olduğu Avrupa Standartları onlara kaynaklık eden IEC standartları üzerinden bir anlatıma yer verilecektir.

IEC 61508 serisi standartlar 2000’li yıllardan itibaren fonksiyonel güvenlik uygulamaları için IEC’nin temel standartları işlevini üstlenmiştir ve EN 61508 serisi olarak, ciddi bir değişiklik geçirmeden, Avrupa Standartları olarak da kabul görmüşlerdir. Demiryolu uygulamaları ise EN 50129 isimli, EN 61508 baz alınarak oluşturulmuş sektör spesifik olarak hazırlanmış fonksiyonel güvenlik standardı ile uyumlu olmak durumundadır. Ayrıca EN 50126 (Demiryolu Uygulamaları – Güvenilirlik, Ulaşılabilirlik, Bakım Yapılabilirlik ve Güvenlik (RAMS) Şartnamesi ve Gösterimi) standardı da hem EN 50129 hem EN 61508 ile yapısal olarak bütünlük içerisindedir. [3]

Avrupa Birliği’nin demiryolu sektörüne yönelik hazırladığı Güvenlik Performansı raporlarına göre Demiryolu Taşımacılığı dört büyük taşımacılık sektörü (Hava, Demiryolu, Kara ve Deniz) içerisinde Havayolu taşımacılığından sonra mevcut en

güvenli sektör olsa dahi [4] yaşanabilecek kazalara yönelik güvenlik önlemlerinin artırılması ve bu önlemlerin sistematik bir biçimde standardize hale getirilmesi önemini korumaktadır.

Fonksiyonel güvenlik uygulamaları ve bunlar ile ilgili çalışmalar hem nitel kavramlar üzerinden hem de sayısal değerler aracılığı ile nicel olarak gerçekleştirilebilmektedir. Aslında her iki yaklaşım da özünde daha iyi ve güvenli mühendislik uygulamaları gerçekleştirmek için bir temel oluşturmayı hedef alsa da sayısal değerlerin ve bu alan için geliştirilen formüllerin kullanılabilir hale gelmesini sağlayan nicel yaklaşımlar sistem güvenliği, güvenilirliği, riskin boyutu gibi kavramların daha kolay takip edilebilir, kıyaslanabilir ve ön görülebilir olmasını sağlamıştır. Günümüzde bu konuda çalışmalar devam etmekte ve her daim yeni metotlar geliştirilmektedir.

Risk kavramı, nicel olarak bakıldığında zararın gerçekleşme ihtimali ile bu zararın boyutunun kombinasyonu [5] olarak tanımlanabilir. Her ne kadar bütün güvenlik uygulamalarının temel amacı riski sıfıra indirmek olsa da bu gerçekçi bir hedef değildir.

Bütün çaba ve çalışmalara rağmen her sistem ve ürünün bir miktar artık risk taşımaya devam ettiği kabul edilir. Getirilen her yeni önlem ve ortaya konulan her yeni metot bu artık risk miktarını azaltacak olsa bile bu önlem ve metotlar için harcanan para, zaman ve iş gücü kimi durumlarda risk miktarındaki azalmaya kıyasla oldukça marjinal boyutlarda kalmaktadır. Bu ise kabul edilebilir bir durum değildir.

Risk kavramı ilgili bu sorular zamanla kabul edilebilir risk kavramının ortaya çıkmasına sebep olmuştur. Özellikle nükleer enerji reaktörleri gibi hem potansiyel riskin hem de potansiyel kazancın çok yüksek olduğu uygulamalar kabul edilebilir riskin ne olduğunu belirleyecek, istatistiksel dayanakları olan metotlara ihtiyacı doğurmuştur.

3.6.1 Kabul edilebilir risk'i değerlendirme metotları olarak ALARP, GAME (GAMAP) ve MEM

Kabul edilebilir risk kavramı son derece politik bir konu olduğu için zaman içerisinde bu risk miktarını belirlemeye yönelik ortaya atılan kavram ve metotlar da içinden çıktıkları toplumların bakış açısı ile şekillenerek farklı yollar izlemişlerdir.

Günümüzde en yaygın kabul gören metotlardan bazıları İngiltere kökenli ALARP (As Low As Reasonably Practicable), Almanya kökenli MEM (Minimum Endogenous Mortality) ve Fransa kökenli GAME (Globalement Au Moins Equivalent) olarak listelenebilir. [6]

Bu metotların detaylı incelemesi bu tezin bir parçası olarak yer almayacaktır ancak bilgi vermesi açısından kısa bir açıklamaya yer vermekte fayda görülmüştür.

Fransa kökenli GAME prensibi bir sisteme yapılacak herhangi bir değişikliğin güvenlik seviyesindeki etkisinin kıyaslanabilir sistemler için uygulanan benzer yöntemler arasındaki en iyileri ile eşdeğer olması temeline dayanır. Bu prensibin güçlü yani matematiksel değerler ile fazla uğraşmadan, doğrudan, gerçekleştirilebilir en güvenli uygulamaları hedef noktası olarak gösterebilmesidir. Zayıf yanı olarak ise kıyaslanabilir sistem kavramının tanımlanmasındaki zorluklar ve elde bulundurulması gereken bilgi kümesinin genişliği gösterilebilir. Demiryolu sistemleri için GAME matematiksel bir tabana dökülmek istenirse kıyaslanabilir sistem kavramı yolcu sayısı ve sistemin çalışma süresi değerleri üzerinden incelenebilir.

Alman kökenli MEM prensibi 1980'lerin başında, Federal Almanya'da gerçekleştirilen istatistiki araştırmalara dayanmaktadır. Bu araştırmalar sonucu bir insanın ölüm olasılığının en düşük olduğu yaşların 5 ile 15 yaş arası olduğu ve bu yaş gurubundaki bir bireyin bir yıllık bir zaman dilimi içerisinde ölme olasılığının $2 \cdot 10^{-4}$ değerinde olduğu ortaya konmuştur. Yine bu sırada yapılan incelemeler yaklaşık 20 kadar tehlikeli sektörün olduğunu (ulaşım, petro kimya, enerji vb.) ortaya koymuş ve iki değer bir birine oranlanması sonucu olarak da herhangi bir güvenlik açısından kritik uygulamada 10^{-5} değerinden yüksek bir ölüm riski bulunmaması gerektiği sonucuna varılmıştır.

MEM prensibi zamanla kazalar sırasında ölen kişilerin sayısını, bu kazalarda ölen kişilerin kazalarda sorumluluk sahibi olup olmadığını ve bazı diğer faktörleri de göz önüne almaya başlamıştır. Hem bu nedenle hem de gelişen teknoloji ve değişen şartlar nedeniyle normal sebeplere dayalı ölüm oranlarının değişmesi nedeniyle MEM her daim güncelleme açık bir prensip olarak varlığını devam ettirmiştir.

Son olarak en yaygın kabul gören ve sistematik olarak incelenen İngiltere kökenli ALARP prensibi ise risk değerlendirmesinde azaltılacak riskin maddi yükünü azaltılan riskin boyutu ile kıyaslamaya dayanmaktadır. Bu bağlamda ALARP presibini

uygulayan ülkeler ve kurumlar belli miktardaki risk düşümleri için kabul edilebilecek maddi bedelelleri kendileri belirlemektedir. Bu miktarların nasıl belirlendiği bu tezin konusu olarak ele alınmamaktadır.

EN 50129 standardı kabul edilebilir risk miktarının belirlenmesini demiryolu otoritesinin sorumluluğuna bırakmaktadır. [7]

3.6.2 Mevcut risk boyutunun belirlenmesinde “risk matrisi” metodu

Kabul edilebilir risk konusunda hedefler, demiryolu sektöründe Tolere Edilebilir Kaza Oranı (THR) üzerinden değerlendirilir. [8] Bu risk hedefine ulaşmak için yapılması gereken ilk şey incelenen sistem veya ekipmanın taşıdığı mevcut riskin belirlenmesidir.

Mevcut risklerin belirlenmesinde çok sayıda nitel ve nicel metod kullanılmakla beraber bu tezin içeriğinde hem çok yaygın olarak kullanılması da hem de taşıdığı esneklik nedeniyle sadece risk matrisi metodu incelenmiş ve uygulanmıştır. Risk Matrisi hem nitel hem de nicel analiz için kullanılabilecek bir metottur.

PD CLC/TR 50451:2007 teknik raporu, nicel risk matrisinin uygulanmasında bir rehber olarak kullanılabilir. Bu teknik rapora uygun olarak oluşturulabilecek risk matrislerinden biri de frekans-sonuç matrisidir. [8]

Normalde ilgili fonksiyon veya komponent için hesaplanması gereken risk boyutu ve bunun sonucunda ortaya çıkacak güvenlik bütünlük seviyesi demiryolu otoritesinin sorumluluğundadır. Burada bir hesaplama yapılabilmesi makas motoru arayüzünden kaynaklanan bir hata sonucunda yaşanabilecek kaza olasılığının bilinmesine ihtiyaç duyulmaktadır. Örnek hesaplama yapabilmek için yıllık 0,5153 olay değeri üzerinden hesaplama yapılacaktır. Bu değerın saatlik karşılığı ise $5.88 \cdot 10^{-5}$ olarak ortaya çıkmaktadır.

Tehlikeye neden olabilecek kaza sıklığı 10^{-6} saatte bir olaya tekabül gelmektedir. Ancak tehlike sonucunun şiddet seviyesi olarak 10'dan fazla ölümlü sonuçlanma seçilecektir. Bu sebeple Çizelge 3.4 üzerinden elde edilen Toplam Güvenlik Risk Seviyesi 10^{-5} 'tir. Buradan sonra tehlike esnasında etkilenecek toplam insan sayısına karşılık Çizelge 3.5'de verilen doğrulama tablosundaki değer kullanılarak Bireysel Ölüm Riski /Saat (IRF/h) hesaplanacaktır.

Çizelge 3.4 : Risk Matrisi

Tehlikeye neden olabilecek bir olayın meydana gelme sıklığı	Toplam Güvenlik Risk Seviyeleri			
10 ⁻¹ saatte bir / Sık yaşanan	10 ⁻³	10 ⁻²	10 ⁻¹	1
10 ⁻² saatte bir / Mümkün	10 ⁻⁴	10 ⁻³	10 ⁻²	10 ⁻¹
10 ⁻³ saatte bir / Arada sırada	10 ⁻⁵	10 ⁻⁴	10 ⁻³	10 ⁻²
10 ⁻⁴ saatte bir / Düşük	10 ⁻⁶	10 ⁻⁵	10 ⁻⁴	10 ⁻³
10 ⁻⁵ saatte bir / Mümkün değil	10 ⁻⁷	10 ⁻⁶	10 ⁻⁵	10 ⁻⁴
10 ⁻⁶ saatte bir / İmkansız	10 ⁻⁸	10 ⁻⁷	10 ⁻⁶	10 ⁻⁵
	Hafif	Ciddi	Ölümlü	10'dan fazla
	Yaralanma	Yaralanma	Sonuçlanma	ölümlü sonuçlanma
Tehlike Sonucunun Şiddet Seviyeleri				

Çizelge 3.5 : Doğrulama Tablosu

Normalizasyon Faktörü	Etkilenecek İnsan Sayısı
1	1
10 ⁻¹	10
10 ⁻²	100
10 ⁻³	1000
10 ⁻⁴	10000

IRF kendi başına bir anlam içermemektedir. Çünkü normalizasyon faktörü her aynı tehlikeni farklı seferlerde meydana gelişinde aynı reaksiyonu göstermeyebilir. Bunun için bir tehlikenin risk değerinin, operatör tarafından kabul edilebilir limitinin belirtilmesi gerekmektedir. Operatör tarafından hedeflenen bağımsız risk değerinin (TIR/h) IRF/h'ye oranından ortalama değer çarpanı elde edilir. Bu değer Risk Matrisinde bulunan değeri ile çarpılması ile THR değeri ortaya çıkar.

$$IRF_h = 10^{-5} * 10^{-3} = 10^{-8} \quad (3.1)$$

$$S = (TIR/h) / (IRF/h) \quad (3.2)$$

$$THR = HR * S \quad (3.3)$$

Arayüz devresi için hesaplama yapmaya devam edersek kabul edilebilir risk değerinin demiryolu otoritesi tarafından 5000 seferde bir olarak belirlendiğini kabul ettiğimiz durumda, S değeri $2*10^{-4}$ olarak ortaya çıkacaktır. Bu durumda örneğimiz için THR;

$$THR = 10^{-5} * 2*10^{-4} = 2*10^{-9} \quad (3.4)$$

Bu değer üzerinden artık güvenlik bütünlük seviyesi (SIL) değerlendirmesi yapılabilir.

3.6.3 Güvenlik bütünlük seviyesi (SIL)

IEC 61508 serisi, güvenlik bütünselliğini elektromekanik /elektronik/programlanabilir elektronik, güvenlik ile ilgili sistemlerin belirlenen güvenlik fonksiyonunu tanımlanan bütün koşullar içerisinde tatmin edici bir biçimde gerçekleştirme olasılığı olarak tanımlamaktadır. [2]

Demiryolu sektöründe, ürünler ve sistemler 4 farklı güvenlik bütünlük seviyesine sahip olabilir. Bu seviyelerin her biri kendisinden daha düşük seviyelerin niteliklerini ve gerekliliklerini kapsamakta ve onlardan daha sıkı şartlar içermektedir.

Güvenlik bütünselliği, ürünlerin ve sistemlerin hem sistematik güvenliği içerisinde kalite, yazılım güvenliği gibi faktörler hem de rastgele gerçekleşen donanım arızalarına karşı güvenliği ile ilgili şartlar içermektedir.

Sistematik güvenlik şartları bu tezin içeriğinde değerlendirilmemektedir. THR değerleri ile nicel olarak ifade edilebilen, rastgele gerçekleşecek hatalara karşı tasarım önlemlerini içeren işlem ve metotlar ile bu metotların analizi ve onaylanması Hata Ağacı Analizi (FTA) metodu ile gösterilmektedir.

EN 50129 standardı bünyesinde, THR değerlerine karşılık SIL değer istekleri Çizelge 3.6’da verilmiştir. [6]

Çizelge 3.6 : SIL Değer Belirleme Tablosu

Tölere Edilebilir Risk Oranı (THR)	SIL Seviyesi
$10^{-9} \leq \text{THR} < 10^{-8}$	4
$10^{-8} \leq \text{THR} < 10^{-7}$	3
$10^{-7} \leq \text{THR} < 10^{-6}$	2
$10^{-6} \leq \text{THR} < 10^{-5}$	1

SIL Değer Belirleme Tablosuna göre, bir önceki bölümde elde edilen THR değeri SIL4’e karşılık düşmektedir. Buradan sonra arayüz tasarımın SIL4 seviyesini karşılaması için çalışma yapılacaktır.

3.7 Makas Motoru Arayüzünün SIL 4 Uyumluluğunun İncelenmesi

Tasarlanan ve test edilen arayüz devresinin yapılan risk analizi sonucu SIL4 seviyesine çıkartılması gerektiği görülmüştür. Kontrol devresindeki lojiğin başarı ile çalıştığı yeterince test edilerek kanıtlanmıştır. Bu noktadan sonra donanımsal açıdan sistemin SIL4 seviyesine uyumluluğu üzerinde çalışılacaktır.

Sistem temel olarak röle ve kontaktörlerden oluşmaktadır. Bu durumda elemanların SIL4 olarak seçilmesi en kolay çözüm olacaktır. Öncelikle röleler inceleme altına alınmıştır. Rölelerin IEC 61508 standardına göre hata oranı düşük ve SIL3 seviyesinde olan modelleri bulunmuştur. IEC 61508 standardı hiçbir elektriksel/elektronik veya programlanabilir elektronik cihazın SIL3'ten yukarı olamayacağını belirttiği için IEC 61508 SIL3 ve EN 50126/8/9 standartlarına göre SIL4 yapılacak bazı gösterimler ile eşit olarak kabul edilebilmektedir. Ancak IEC standardına uygun rölelerin hiçbirinin EN standardına göre demiryolunda kullanımı mümkün değildir.

Söz edilen farklar Çizelge 3.7'de özetlenmiştir.

Çizelge 3.7 : IEC – EN Röle İster Karşılaştırma Tablosu

İster Farkı No	IEC 61508	EN 50126-8-9
1	Rölelerin bobini 2.5 KV'a dayanım göstermek zorundalar	Rölelerin bobini 4.0 KV'a dayanım göstermek zorundalar
2	Hata durumuna geçen röle tekrar tetiklendiğinde pozisyon değiştirmeyeceğinin garantisini vermez	Hata durumuna geçen röle tekrar tetiklendiğinde pozisyon değiştirmeyeceğinin garantisini verir
3	Normalde kapalı kontaklar güvenlik temelli bir operasyonun içerisinde kullanılabilir	Sadece normalde açık kontaklar güvenlik temelli bir operasyonun içerisinde kullanılabilir

Rölenin dışına çıkıldığında kontaktör, zaman rölesi ve akım okuma rölesi için de benzer durumların geçerli olduğu görülmüştür. Bu elemanlar için IEC veya EN standardına uygun güvenli kullanıma yönelik bir ürün bulunmamaktadır. Bu noktadan itibaren yapılması gereken 3 faz 4 kablo arayüz devresinin tasarımının SIL4 olacak şekilde yeniden ele alınmasıdır.

Tasarımın revize edilmeye başlanmasından önce hangi fonksiyonların güvenlik fonksiyonları olduğu ve fonksiyonel güvenlik kıstasları içerisinde değerlendirileceği, hangilerinin ise dışarıda tutulması gerektiğinin kararına varılması gerekmektedir. Bunun için makas motoru arayüzünün yaptığı hangi işlemlerin, anklaşman sistemini tehlikeye soktuğuna bakılmalıdır. Arayüz devresinin makası olduğu bir pozisyonun dışında göstermesi veya ortada kalan bir makastan pozisyon bilgisi üretmesi, anklaşman sistemini hatalı bir karara sürükleyebilir. Bunun sonucu da birden fazla ölüm ile sonuçlanabilir. Dolayısı ile arayüz devresinde SIL4 seviyesini sağlayacak kısım motordan indikasyon okuyan kısımdır.

Bir başka deyiş ile motorun sürülmesi fonksiyonel güvenlik koşullarından biri değildir. Çünkü motorun sürülememesinden kaynaklı bir sorun, anlaşılan açısından hatalı bir karar vermeye neden olmayacaktır. Bu durum tabii ki istenen bir durum değildir ve demiryolunda temel aranan parametrelerden ulaşılabilirlik ve güvenilirlik talebine karşı düşmektedir. Ancak güvenlik açısından bir problem teşkil etmez.

Son durumda donanımsal olarak kontrol devresinin oluşturulacağı bir elektronik kontrolörün ve motor üzerinden pozisyon okumaya yarayacak olan RP, LP rölelerinin SIL4 olarak seçilmesi donanımsal açıdan SIL4 seviyesinin sağlanmasına olanak sağlayacaktır. Problemin bu şekilde ele alınması kontaktör, zaman rölesi ve akım rölesinin SIL olarak seçilmesinin zorunluluğunu ortadan kaldırmıştır.

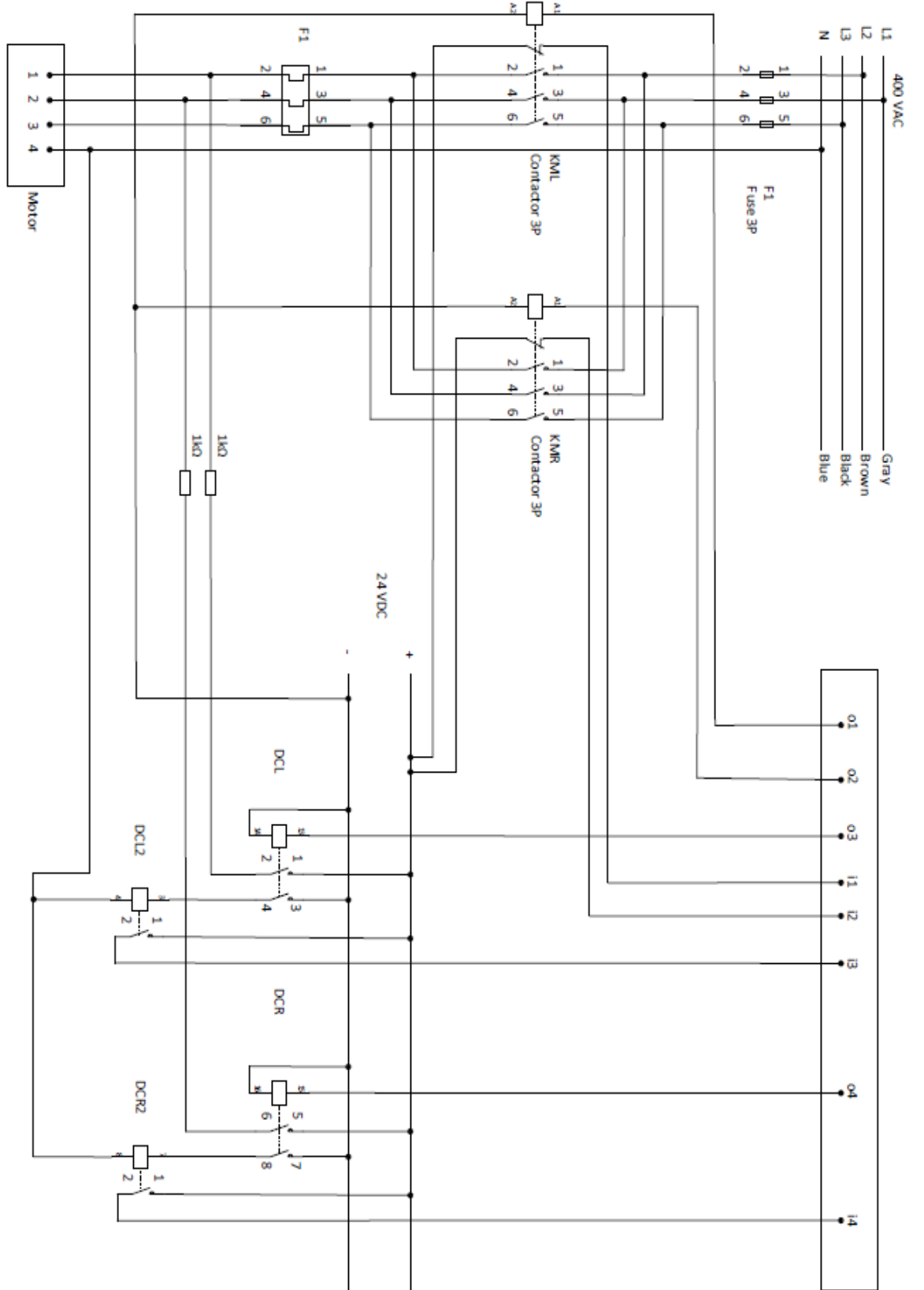
3.8 Arayüz Devresinin Elektronik Kontrolör ile Gerçeklenmesi

Tasarıma geçilmeden önce SIL4 seviyesinin sağlanabilmesi için dizayn parametrelerinin üzerinden bir kez daha geçilecektir. Daha önce kontrol devresi ile sağlanan lojik elektronik kontrolörün içerisine alınacaktır. Elektronik kontrolörün dışında DCL ve DCR güvenlik röleleri dışarıda bulunacaktır. Bu röleler AC gerilim altında motor sürülürken elektronik kontrolörün I/O'ları için izolasyon görevi görecektir. Bir önceki tasarıma benzer şekilde DCL ve DCR röleleri indikasyon okunması esnasında DC gerilimin motora beslenmesinde kullanılacaktır. Motordan gelen geri dönüş bilgisi aynı şekilde RP veya LP güvenlik rölelerini çektirecek ve bu röle üzerinden arayüz kontrolörüne bilgi iletilmiş olacaktır. Söz edilen dört röle EN 50126-8-9 standartlarında istenen koşullara göre SIL4 olacak şekilde seçilecektir. Arayüz kontrolörü de aynı şekilde IEC 61508 SIL3 veya EN 50126-8-9'a göre SIL4 bir kontrolör olarak seçilecektir.

Kontrolörün anlaşılan sistemi ile daha önce ön görüldüğü gibi iki giriş ve iki çıkış olacak şekilde bir arayüzü olacaktır. Kontrolörün motor üzerindeki sürme ve indikasyon okuma işlemleri için ise 5 adet giriş 4 adet ise çıkış kullanması planlanmıştır. İki adet giriş kontaktörlerin üzerinde yer alacak ayna kontağın bilgisini okumak üzere kullanılacaktır. Ayna kontak, kontaktörün fazları anahtarlayan kontaklarına zıt olacak şekilde çalışacaktır. Bu kontak üzerinden okunan bilgi AC-DC gerilim arasındaki geçiş için kullanılacaktır. Diğer iki giriş ise RP ve LP pozisyon röleleri üzerinden alınan pozisyon bilgilerinin kontrolöre iletilmesidir. Son giriş ise makas motorunun son pozisyona dayandığını bildiren akım sinyalini ileten rölenin

okunması için kullanılacaktır. Kontrolörün çıkışları ise motoru sürmek için KMR ve KML kontaktörlerinin ve indikasyon okumak için ise DC gerilim beslenmesi için DCL ve DCR rölelerinin bobinlerini enerjilendirmek için kullanılacaktır.

Pozisyon bilgisinin okunma bilgisi bir önceki tasarımla hemen hemen aynıdır. Kontrolör konum sorgulaması yapmak istediğinde dijital çıkış üzerinden DCL veya DCR rölesinin bobini enerjilendirir. Bu röleler iki adet normalde açık kontağa sahiptir. Bobinin enerjilenmesi ile kapanan kontaklardan birinin üzerinden motora 24VDC gerilim iletilir. Motordan geri dönüş olması durumunda pozisyon bilgisini üretecek RP veya LP rölesinin çekmesi için ilgili DCL veya DCR rölesinin ikinci kontağının çekmiş olması gerekir. Çünkü röle bobinin nötr kısmı ikinci kontak üzerinden geçerek nötr hattına ulaşır ve devreyi tamamlar. Pozisyon rölesinin çektilmesi ile beraber son pozisyon indikasyon bilgisi kontrolöre iletilir. DCL ve DCR rölesinin üzerinden herhangi bir takip gerçekleştirilmez. Bu röleler SIL4 olarak seçildiği için rölelerin hata yapma ihtimali göz ardı edilmektedir. Ancak yine de çok düşük olan bu ihtimalin gerçekleşmesi durumunda kontaklar yapışık kalacağı için kontrolöre pozisyon bilgisi iletmeye devam eder. Bu durumda kontrolör kontaktörlere çıkış bilgisi iletmez. Şekil 3.14'te elektronik kontrolörlü arayüz güç devresi bulunmaktadır.



Şekil 3.14 : Elektronik Kontrolörlü Arayüz Güç Devresi

Kontrolör için PILZ firmasının ürettiği PnozMulti isimli model seçilmiştir. Kontrolörün IEC 61508 standardına göre SIL3 sertifikası bulunmaktadır. Ürünün yedekli yapıda kullanılması durumunda EN 50126-8-9 standardına göre SIL4 olarak kullanılması mümkündür.

Yazılım aşağıda verilen giriş-çıkış dağılımına göre geliştirilmiştir.

Girişler:

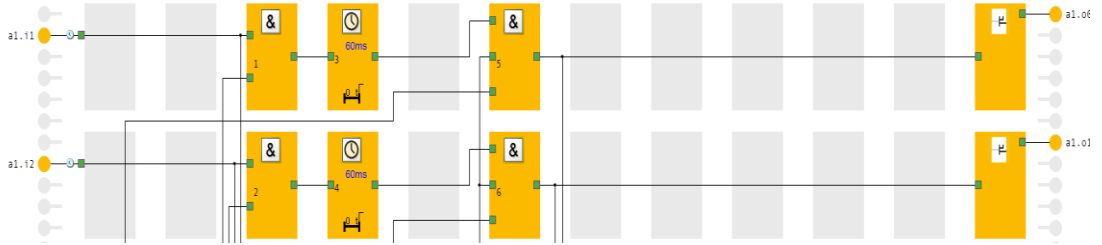
- Giriş 1: Anlaşman Sisteminden Gelen Sağa Git Komutu
- Giriş 2: Anlaşman Sisteminden Gelen Sola Git Komutu
- Giriş 3: KMR Kontaktörünün Ayna Kontakının Bilgisi
- Giriş 4: KML Kontaktörünün Ayna Kontakının Bilgisi
- Giriş 5: RP Rölesinden Gelen Pozisyon Bilgisi
- Giriş 6: LP Rölesinden Gelen Pozisyon Bilgisi
- Giriş 7: Akım Bilgisi

Çıkışlar:

- Çıkış 1: KMR Kontaktörünü Sürmek için Kullanılan Çıkış
- Çıkış 2: KML Kontaktörünü Sürmek için Kullanılan Çıkış
- Çıkış 3: DCR Rölesini Sürmek için Kullanılan Çıkış
- Çıkış 4: DCL Rölesini Sürmek için Kullanılan Çıkış
- Çıkış 5: Anlaşman Sistemin İletilen Motor Sağ Pozisyonda Bilgisi
- Çıkış 6: Anlaşman Sistemin İletilen Motor Sağ Pozisyonda Bilgisi

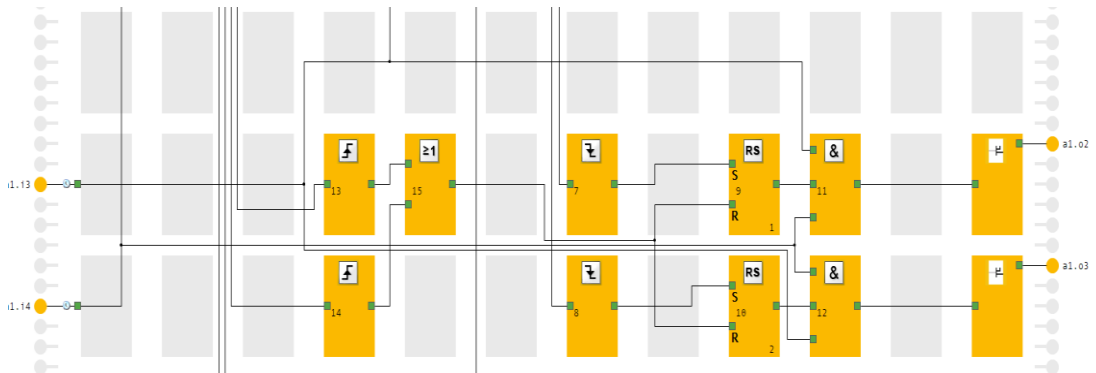
Yazılım detayları bu bölümü devamında açıklanmaktadır. RP, LP ve akım rölelerinden gelen bilgi program içersindeki lojikte ‘not’ kapısından geçirilerek kullanılmaktadır. Anlaşmandan gelen komut sinyali öncelikle makasın mevcut pozisyonu ile karşılaştırılır. Yazılım içersindeki Blok 1 ve Blok 2 bu işlem için kullanılır. Eğer makasın bulunduğu pozisyon için komut gelmiş ise buradaki ‘ve’ kapısından geçiş sağlanmaz. Eğer ilgili pozisyonda değil ise kontaktörlerin sürülmesi için blok çıkışı aktif olur. Buradan sonra motorun sürmeye yarayan kontrolör çıkışının aktif olması için bir kontrol daha yapılır. Blok 5 ve Blok6’da yer alan ‘ve’ kapıları akım rölesinin durumu ve diğer pozisyona giden kontaktörün ayna kontakının bilgisini gözler.

Buradaki amaç, motorun ters yöne gitmesini sağlayacak kontaktörün devrede olma ihtimaline karşın kontaktörün devreye girmesinin önüne geçilmesidir. Akım kontrolü ise makas son konuma ulaştığında kontaktörün enerjisinin kesilmesi için kullanılır. Şekil 3.15'te KML ve KMR kontaktörlerinin sürülmesi için hazırlanan yazılımın görseli bulunmaktadır.



Şekil 3.15 : KMR-KML Kontaktörlerinin Sürülmesi ile İlgili Yazılım Parçası

Blok 1-2'den Blok 5-6'ya geçiş yapılırken bir zaman gecikmesi uygulanır. Bunun sebebi DC gerilimden AC gerilime geçerken güvenli bir şekilde geçiş yapılması içindir. DC gerilim kontakları takip edilmediği için DCR ve DCL rölelerinin kontaklarının normalde kapalıdan, normalde açığa doğru geçişi sırasındaki süreden daha fazla bir süre gecikmesi burada kullanılır. Bu sayede DCL ve DCR röle kontaklarının açık devre pozisyonuna geçmesi garanti altına alındıktan sonra KML ve KMR kontaktörlerinin enerjilendirilmesi sağlanır. Şekil 3.16'da DCL ve DCR rölelerinin sürülmesi için hazırlanan yazılımın görseli bulunmaktadır.



Şekil 3.16 : DCR-DCL Rölelerinin Sürülmesi ile İlgili Yazılım Parçası

Motor hareketi sonlanması Blok 7 ve Blok 8'deki düşen kenar blokları ile anlık olarak çıkış üretilir. Bu bilgi Blok 9 ve Blok 10'da başka bir karşılaştırmada kullanılmak üzere set edilir. Blok 11 ve Blok 12'de yer alan 've' kapılarında ise DCL veya DCR rölesinin çektilmesi için gerekli koşullar kontrol edilir. Burada KMR ve KML kontaktörlerinin enerjili durumda olmaması ve ilgili yön için olan hareketin



3.9 Sistemin Güvenlik Bütünlük Seviyesi Analizi

Elektronik kontrolör ile gerçekleştirilen sistemin güvenlik bütünlük seviyesi analizi yapılmalıdır. Yeni tasarlanan sistemde elektronik kontrolör, röle ve kontaktörden oluşmaktadır. Elektronik kontrolör ve röle SIL4'ü karşılamaktadır. Ürün olarak doğrudan güvenlik bütünlük seviyesi sertifikasına sahip olmayan sadece kontaktör vardır. Bu sebeple kontaktörün SIL seviyesinin belirlenmesi gerekmektedir.

Bu değerlendirilmesinin yapılabilmesi için komponent ile ilgili belli parametrelere ihtiyaç duyulmaktadır.

Görev Döngüsü 'C': Bir saat içerisinde öngörülen operasyon sayısıdır.

B10: Ürünlerin %10'unun başarısız olacağı operasyon sayısı

λ : Arızaların Oranı

λ_E : Elektromekanik komponent için belirlenen arıza oranı

λ_D : Tehlikeye yol açacak arızaların oranı

λ_{DD} : Tehlikeye yol açacak arızaların içerisinde tespit edilebilenlerin oranı

β : Ortak sebepten ötürü hataya götüme faktörü

T1: Ürünün önerilen kullanım süresi

T2: Diagnostik sisteminin test aralığı

DC: λ_{DD} / λ_D

Yukarıdaki parametrelerin ışığında kontaktörün tehlikeye yol açacak arızaların oranı hesaplanır. C değeri makas motoru operasyonu için 2 olarak belirlenir ve bunun üzerinden işlemler yapılır.

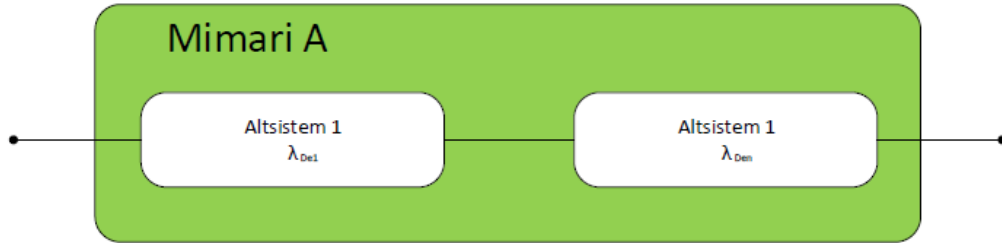
$$\begin{aligned}\lambda_{D_Cont} &= \lambda_D * (0.1 * C / B10) \\ &= 0.61 (0.1 * 1 / B10) \\ &= 6.1 * 10^{-8}\end{aligned}\tag{3.5}$$

$$\begin{aligned}PFH_{cont} &= \lambda_{D_Cont} * 1 \text{ saat} \\ &= 6.1 * 10^{-8}\end{aligned}\tag{3.6}$$

Yukarıdaki hesaplama sonucunda kontaktör ürünün kendisi SIL3 olarak hesaplanmıştır. SIL hesaplamaları yapılırken sadece komponentin kendisi değil aynı zamanda kullanıldığı mimari de ele alınmalıdır. Makine ekipmanları için fonksiyonel güvenlik standardı 62061'e göre kullanılabilecek mimari tipler aşağıda açıklanmıştır.

Mimari A:

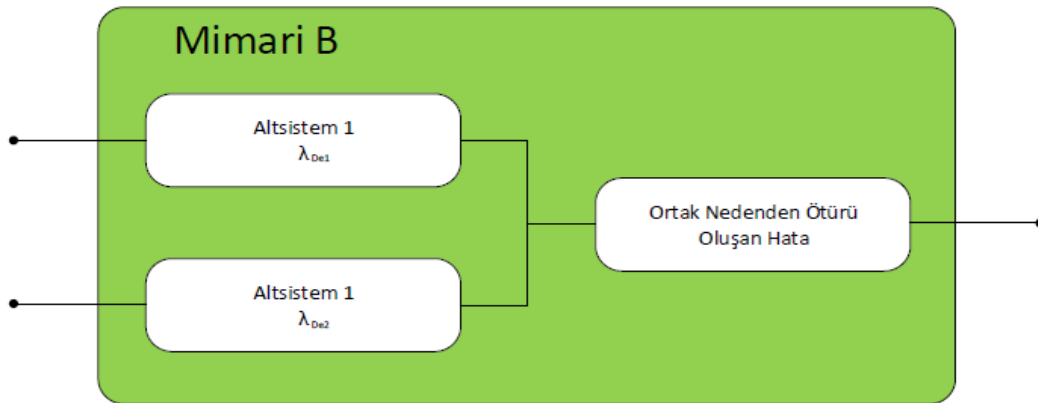
İki alt sistem fonksiyonel güvenlik açısından birbirlerine seri olarak bağlanır. Şekil 3.19'da bulunan görselde bu mimari tipini gösterilmiştir.



Şekil 3.19 : Mimari A Gösterimi

Mimari B:

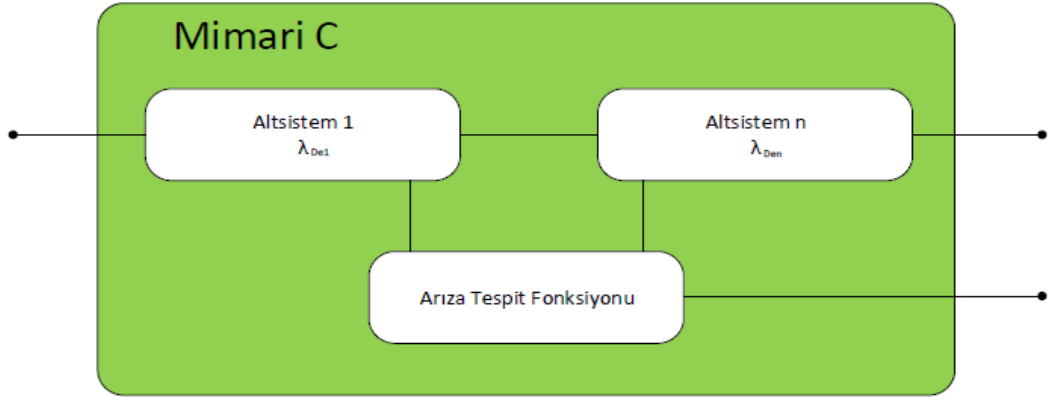
İki alt sistem fonksiyonel güvenlik açısından birbirlerine paralel olarak bağlanır. Şekil 3.20'de bulunan görselde bu mimari tipi gösterilmiştir.



Şekil 3.20 : Mimari B Gösterimi

Mimari C:

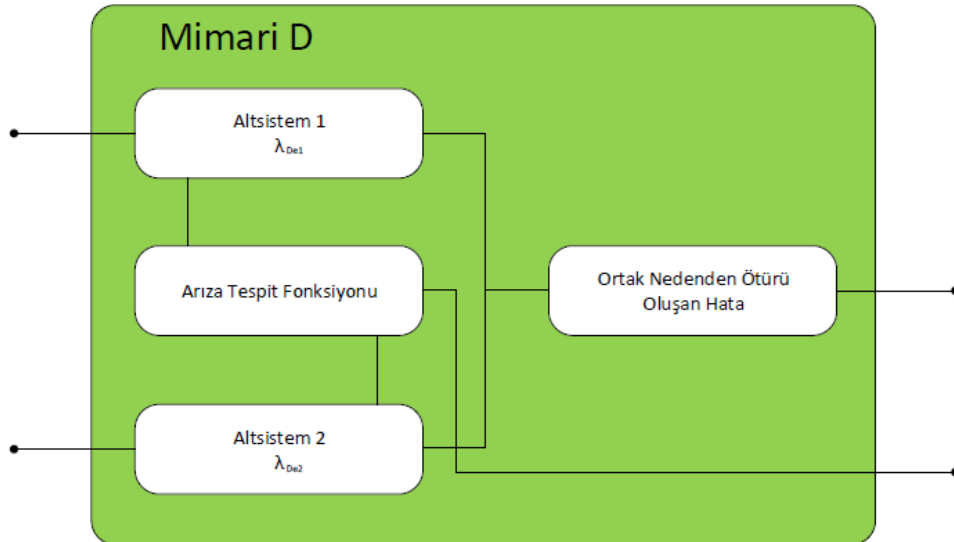
İki alt sistem fonksiyonel güvenlik açısından birbirine seri olarak bağlanır. Ekstra olarak her iki sistemi kontrol eden bir arıza tespit sistemi vardır. Arıza tespit sistemi, herhangi bir sistem arızaya geçmemiş olsa bile arıza yaratabilecek bir durum tespit ettiği zaman önceden tanımlanmış fonksiyonlar doğrultusunda sistemi hatada-güvenli duruma alabilir. Şekil 3.21'de bulunan görselde bu mimari tipi gösterilmiştir.



Şekil 3.21 : Mimari C Gösterimi

Mimari D:

İki alt sistem fonksiyonel güvenlik açısından birbirlerine paralel olarak bağlanır. Ekstra olarak her iki sistemi kontrol eden bir arıza tespit sistemi vardır. Normal şartlarda her iki sistemin de ortak karar vermesi beklenir ve bu ortak karar çıkış olarak uygulanır. Ancak arıza tespit sistemi iki sistemin verdiği karar arasında bir uyumsuzluk tespit ederse, önceden tanımlanmış fonksiyonlar doğrultusunda çoğunluğun verdiği kararı çıkışa uygulayabilir veya sadece bir tane farklı karar olsa bile o kararı çıkışa yansıtabilir. Şekil 3.22’de bulunan görselde bu mimari tipi gösterilmiştir.



Şekil 3.22 : Mimari D Gösterimi

Yukarıda açıklanan mimarilerden arayüz uygulamasında kullanılması en uygun olanı Mimari B'dir. Daha önce açıklandığı gibi makasın sürülmesi ile ilgili fonksiyonlar güvenlik açısından değerlendirilmezken, makasın konumunun okunması ilgili fonksiyonlar güvenlik çerçevesinden değerlendirilmesi gereken fonksiyonlarıdır. Bu yaklaşım sonucunda kontaktörler ile ilgili güvenlik fonksiyonu motor sürülmesi tamamlandığında kontaktör bobinine iletilen enerji iletimi kesildiğinde kontaktörün kontaklarını açarak AC gerilimin motora iletilmesinin engellenmesidir. Bu sayede motora DC gerilim beslemesi yapıldığında doğru bir şekilde pozisyon bilgisi okunabilir. Ancak kontaktörde yaşanacak bir hata durumunda motora halen AC gerilim iletiliyorken DC gerilimi ile konum sorgulaması yapılması tehlike oluşturan bir duruma yol açacaktır.

Bu fonksiyonun sağlanması için sağ ve sol yön için motorun sürülmesi fiziksel olarak iki seri kontaktör ile sağlanacaktır. Bu şekilde sağlanacak yapı fonksiyonel güvenlik açısından mimari B'ye karşılık düşmektedir. Çünkü kontaktörlerden birinin düzgün çalışması amaçlanan güvenlik fonksiyonu olan AC gerilimin kesilmesini sağlamaktadır. Bu yaklaşım altında $\beta=0.1$ seçilerek güvenlik bütünlük seviyesi için yeniden hesaplama yapılır.

$$\begin{aligned} T1 &= B10 / C \\ &= 1000000 / 1 \\ &= 1\ 000\ 000 \text{ saat} \end{aligned} \quad (3.7)$$

$$\begin{aligned} \lambda D_Cont &= (1 - \beta)^2 * \lambda D_Cont_1 * \lambda D_Cont_2 * T1 + \beta * \\ &\quad (\lambda D_Cont_1 + \lambda D_Cont_2) / 2 \\ &= (1 - 0.1)^2 * 6.1 * 10^{-8} * 6.1 * 10^{-8} * 1000000 + 0.1 * (6.1 * 10^{-8} + \\ &\quad 6.1 * 10^{-8}) / 2 \\ &= 0.81 * 6.1 * 10^{-8} * 6.1 * 10^{-8} * 1000000 + 0.1 * 6.1 * 10^{-8} \\ &= 0.81 * 2.1316 * 10^{-14} * 1000000 + 0.1 * 6.1 * 10^{-8} \\ &= 3.01401 * 10^{-9} + 6.1 * 10^{-9} \\ &= 9.11401 * 10^{-9} \end{aligned} \quad (3.8)$$

$$\begin{aligned} PFH_cont &= \lambda D_Cont * 1 \text{ saat} \\ &= 9.11401 * 10^{-9} \end{aligned} \quad (3.9)$$

Yapılan hesaplama doğrultusunda oluşturulan yapı SIL4 seviyesine ulaştırılmıştır. SIL4 röleler ve SIL4 kontrolör ile beraber 3 faz 4 kablo makas motoru arayüzü bütün bir sistem olark SIL4 seviyesine sahip hale gelmiştir.

3.10 Hata Ağacı Analizi

Çıkarılan isterler doğrultusunda, risk analizi sonucu sistemin olması gereken güvenlik bütünlük seviyesi 4'e uygun olarak dizaynı yapılan makas motoru arayüz devresi için Hata Ağacı Analizi gerçekleştirilecektir.

FTA, güvenlik fonksiyonları barındıran bir sistemin hataların doğrudan sebeplerini aşama aşama listelemeye ve bu sebepler arasında Boolean mantığına dayanan “mantık kapıları” aracılığı ile ilişki kurmaya dayanan, yukarıdan aşağıya doğru işleyen bir hata ve risk analiz metodudur. Dizayn ile paralel yürütülmesi daha etkili bir kullanımı ortaya çıkarır. FTA sonucu bazı isterlerin karşılanamaması durumunda dizayn üzerinde değişiklikler yapılarak, iyileştirme sağlanır.

FTA, tekil arızaların doğrudan etkilerini ve ortak sebepten oluşabilecek arızaların gerçekleşmesi sonucu ortaya çıkan durumları incelerken sisteme dair istenmeyen sonucun gerçekleşmesine giden yolları belirleyerek bu sonuca karşı önlem alınmasını ve bu sonucun gerçekleşme ihtimalinin hesaplanabilir olmasını sağlar.

FTA, Avrupa Normları kapsamında standardize edilmiş bir hata analiz metodudur. Demiryolu için özelleştirilmiş standartlardan EN 50129'da SIL4 seviyesi aranan sistemler için uygulanması önerilen hata ve tehlike analiz metodlarından biridir. EN 61025 standardı FTA'nın kendi standardıdır. Burada metot ile ilgili detaylar ve uygulama örnekleri mevcuttur. Buradan sonraki aşamada standartların önerdiği şekilde analiz açıklanmış ve belgelemiştir.

3.10.1 Makas motoru arayüz devresi tasarımının tanımı

Makas ve makas motorunun tanımı daha önce yapıldığı için burada detaylandırılmayacaktır. Makas motoru arayüz devresinde yer alan komponentlerin ve standarda uygun olarak alt sistem tanımları yapılacaktır.

Hatada güvenli elektronik kontrolör tarafından gerçekleştirilen mantık işlemleri sonucu motor kontaktörleri aracılığı ile motorun çalışması ve makas manevrasının gerçekleşmesi sağlanırken yine elektronik kontrolör ve güvenlik röleleri aracılığı ile

motorun amaçlanan son konuma ulaşip ulaşmadığı kontrol edilir ve buna bağlı bir konum bilgisi oluşturulur.

Motor Hareketi (Güç Devresi) ile Motor Konum Bilgisi Sorgulaması ve Tespiti (Kontrol Devresi), “Makas Motoru Arayüzü” alt-sistemini oluşturan ve bir alt seviyede yer alan iki alt-sistemdir. Bu iki sistem bir biri ile sıralı olarak faaliyet göstermektedir.

Makas motoru kontaklarına ‘Motor Hareketi’ alt-sisteminin faaliyeti sırasında AC gerilim uygulanırken ‘Motor Konum Bilgisinin Sorgulanması ve Tespiti’ alt-sisteminin faaliyeti sırasında DC gerilim uygulanır.

3.10.2 Sistem sınırları ve işletimi

Makas Motoru Arayüzü, anlaşılan tarafından verilen ilk hareket komutu ile devreye girer. Hareket komutu makasın sağ yöne veya sol yöne ilerlemesi olmak üzere iki şekilde gerçekleşebilir.

Elektronik kontrolör ilgili yöne hareketi sağlayacak motor kontaktörlerini 24 VDC sinyal ile tetikleyerek bu kontaktörlerin motoru enerjilendirmesini sağlar ve ‘Motor Hareketi’ alt-sistemi faaliyetine başlar. Motor kontaktörlerinin normalde kapalı konumdaki yardımcı kontakları elektronik kontrolör tarafından gözlemlenmektedir. Gözlemeleme işlemi için kullanılacak kontaktların EN 60947-4-1 standardı ile tanımlanmış ayna kontak özelliğini sağlamaktadır. Ayna kontaklar, güç kontakları ile her zaman zıt konumda bulunur. Ayna kontaklar sayesinde kontaktörler kontak yapışması sonucu açılmama, kontak kapanmaması, kontak açma/kapama sürelerinde değişme gibi sebeplerden hatalı işlem gerçekleştirse bile güvenli olarak kontak konumları takip edilmektedir. Aynı şekilde ayna kontaklar normalde kapalı konumda oldukları için elektronik kontrolör ve bu kontaklar arasında elektriksel bağlantı herhangi bir sebeple kopması durumunda sinyal kesileceği için bu durum tespit edilebilecektir.

Anlaşımandan gelen hareket komutunun sonlanması veya motor güç devresi üzerinden takip edilen akım bilgisi ile makasın son konuma ulaştığı bilgisinin tespit edilmesi durumunda, motor hareketi için elektronik kontrolörden DCL veya DCR kontaktörlerine iletilen sürme sinyali sonlandırılır. DCL veya DCR kontaktörlerine iletilen sürme sinyali kesildikten sonra ayna kontaklar aracılığı ile kontaktörün güç kontaklarının güvenli bir biçimde açık konuma geçtiği anlaşılır. Kontaktörler motora

giden enerjiyi kestiğinde ‘Motor Hareketi’ alt-sistemi fonksiyonunu sonlandıracak ve ‘Motor Konum Bilgisi Sorgulaması’ alt-sistemi fonksiyonuna başlayacaktır.

Makas motoru son konuma oturduğunda, daha önceden tespit edilen, güç devresinde bir faz ve nötr hattı bağlantısının yapıldığı motor bağlantı noktaları üzerinde motor pozisyon kontaklarının kısa devre olduğu daha önce açıklanmıştı. Motorun son konumda olduğunu kontrol etmek için bu konumda kısa devre olması beklenen motor bağlantı uçlarından birinden 24 VDC sinyal uygulanarak, geri dönüş kontrol etmektedir.

Elektronik kontrolör, ‘Motor Hareketi’ alt-sisteminin faaliyeti esnasında motor hangi yöne sürülmüşse bu yöne ait son konum için kontrol gerçekleştirecektir. Eğer ‘Motor Konum Bilgisi Sorgulaması’ alt-sistemi işletimi sonucunda herhangi bir son konu bilgisi elde edilmişse, tekrar o konuma için sürme komut üretilmeyecektir. Bu durum elektronik kontrolör yazılımı sayesinde garanti altına alınmıştır.

‘Motor Hareketi’ ve ‘Motor Konum Bilgisi Sorgulaması’ alt-sistemlerinin sınırları motor kontaktörlerinin motora giden enerjiyi kestiği bilgisine ve anlaşılmadan iletilen makas hareket komutuna dayanarak belirlenmiştir.

‘Makas Motoru Arayüzü’ alt-sisteminin sınırları, motor hareketinin tetiklenmesi ve motorun hareket edilen yönde son konuma ulaştığının teyit edilmesi olaylarının arasını kapsayacak şekilde belirlenmiştir.

Motoru sürmek için iletilen AC gerilim ve konum kontrol işleminde kullanılan DC gerilimin motora birlikte uygulanmaması, güvenlik açısından kritik ister olarak belirlenmiştir. ‘Motor Hareketi’ ve ‘Motor Konum Bilgisi Sorgulaması’ alt-sistemleri arasındaki geçiş bu kritik güvenlik isteri üzerinden tanımlanmıştır.

AC ve DC gerilimlerin motor kontaklarına aynı anda uygulanmasının elektronik kontrolörün zarar görmesine ve hatalı konum bilgisi oluşturulmasına sebep olabileceği ihtimali nedeniyle aşağıdaki ek önlemler alınmıştır:

- Motor güç devresinde, her iki yöne hareket için kullanılan bağlantılar üzerinde fiziksel olarak seri, fonksiyonel güvenlik açısından paralel şekilde bağlı 2 adet kontaktör kullanılarak, kontaktör güvenilirliği artırılmıştır.

- ‘Motor Konum Bilgisi Sorgulaması’ alt-sisteminin faaliyeti sırasında motor kontaklarına uygulanan DC gerilimi taşıyan hatlar, 1000 Ω ’luk direnç aracılığı ile yüksek akıma karşı korumaya alınmıştır.
- ‘Motor Hareketi’ alt-sisteminin faaliyeti sırasında motor kontaklarına uygulanan DC gerilimi taşıyan hatlar F2F yüksek akım rölesi ile olası bir kısa devre veya yüksek akım durumu yaşanması durumunda koruma altına alınmıştır.
- ‘Motor Hareketi’ alt-sisteminin faaliyeti sırasında motor kontaklarına uygulanan AC gerilim röleleri ‘Motor Konum Bilgisi Sorgulaması’ sırasında kullanılan indikasyon röleleri ile elektronik kontrolörün giriş çıkışlarından izole edilmiştir. Güvenlik röleleri EN 50129 standardının belirttiği yüksek akım değerini sınırlandırmak zorundadır.
- Motor hareketi sonrasında konum bilgisi sorgulanırken kısa devre olması beklenen kontaklar arasına uygulanacak DC gerilim güvenlik röleleri aracılığı ile DC çıkışlı bir güç kaynağı üzerinden elektronik kontrolörün denetiminde anahtarlanarak motora iletir.

Konum sorgulama işlemi sırasında gerilim uygulanan hattın iki ucu da aynı rölenin birlikte çalışan, normalde açık konumda bulunan iki kontağı üzerinden anahtarlanır ve çifte anahtarlama uygulanır. Her iki konuma ait sorgulama işleminde kullanılan fazlara giden bağlantılar arasında gerçekleşebilecek bir kısa devrenin etkisi böylelikle bertaraf edilmiş olur. Konum sorgulama işlemi sırasında gerilim uygulanan hattın üzerine yerleştirilen bir başka güvenlik rölesi ise bu hattın tamamlanması sonucu tetiklenecek ve elektronik kontrolöre izole bir gerilim sinyali gönderecektir. Böylelikle motorun sorgulanan son konuma ulaştığı teyit edilecektir.

Makasa son konum sorgusu yapılması için DC gerilim iletilmesi sonucu pozisyon bilgisi tespit edilip edilmemesine bağlı olmadan ‘Motor Konum Bilgisi Sorgulaması’ alt-sistemi’nin faaliyeti sona erir ve anlaşılmadan gelecek bir sonraki hareket komutu ile ‘Motor Hareketi’ alt-sistemi’nin faaliyete tekrar başlayacaktır.

‘Motor Hareketi’ alt-sistemi gelen hareket komutlarının her zaman ‘Motor Konum Bilgisi Sorgulaması’ alt-sisteminde kullanılan güvenlik rölelerinin kontak açma süreleri göz önüne alınarak gecikmeli başlatacak ve bu gecikme işlemi elektronik kontrolör yazılımı ile garanti altına alınacaktır.

3.10.3 Arayüz tasarımı ile ilgili varsayımlar

- Makas Motoru Arayüzü alt-sisteminin ve ‘Motor Konum Bilgisi Sorgulaması’ alt-sisteminin sadece motor sağ son konumda ve motor sol son konumda bilgilerini güvenilir biçimde ve SIL 4’e uygun olarak üretebileceği kabul edilmiştir.
- Motor sağ son konumda değil ve motor sol son konumda değil bilgilerinin bir üst sistem olan anlaşılan sistemi tarafından hata olarak belirlendiği kabul edilmiştir. Söz konusu hatanın ortaya çıkmasında motor sürme süresinin yetersiz olması, motorun zorlanması, motor kontaktörlerine giden tetikleme sinyalinin açık devre nedeniyle ulaşamaması, motor kontaktörlerine giden tetikleme sinyalinin kısa devre nedeniyle hatalı ulaşması, elektronik kontrolör arızası veya motor arızası gibi olası sebepler mümkündür.
- Motor sağ son konumda ve motor sol son konumda bilgilerinin aynı anda üretilmesinin bir üst sistem olan anlaşılan sistemi tarafından hata olarak belirlendiği kabul edilmiştir. Söz konusu hatanın ortaya çıkmasında pozisyon bilgisinin üretilmesinde kullanılan güvenli röleler ile elektronik kontrolör meydana gelebilecek kısa devre, pozisyon rölelerinden kaynaklı hatalar, elektronik kontrolör arızası ve motor arızası gibi olası sebepler mümkündür.

3.10.4 FTA için tepe olayın belirlenmesi

FTA tepeden aşağıya doğru yapılan bir analizdir. FTA için öncelikle sistem içerisindeki güvenlik kritikliği olan fonksiyonlar belirlenir. Bu fonksiyonun hatalı işletilmesi durumunda güvenliği ne boyutta tehdit ettiği analiz edilir. Seçilen tepe olayın ardından ilgili alt sistemler ve bu sistemlerin içerisinde hataya neden olabilecek olaylar detaylandırılır. [8]

Normal çalışma koşulları içerisinde makas motoru arayüzü alt-sisteminin güvenlik çerçevesi içerisinde sağlaması gereken bilgi makasın hareket komutu verilen yönde son konuma oturup oturmadığı bilgisidir. Makas, sağa hareket komutu sonrası üç farklı konumda bulunabilir; sağ son konum, ortada ve sol son konumda. Aynı şekilde sola hareket sonrası ise sol son konum, ortada ve sağ son konum olmak üzere üç farklı konumda bulunma ihtimali vardır. Motor Konum Bilgisi Sorgulaması alt-sistemi sadece makas motorunun hareket komutu verilen yönde son konumda olup olmadığını sorgulamaktadır. Bu durumda sorgu faaliyeti öncesi makasa hangi son konuma gitme

emri verildiyse alınacak sonuç makasın o son konumda olduğu veya makasın o son konumda olmadığı şeklinde olacaktır.

Çeşitli tasarım kısıtlamaları nedeniyle makasın ilerlediği yönün aksine bilgi iletmesi mümkün değildir ancak böyle bir durum olma ihtimaline karşın veya makas motorunun ulaştığı son konumun aksine sorgu yapılması sonucu üretilebilecek beklenmeyen yöndeki konum bilgisi veya hiçbir konumun üretilmemesi güvenlik açısından sorun teşkil etmemektedir. Böyle bir durumun meydana gelmesi durumunda bir üste seviyede yer alan anlaşılan sistemi bu durumu hata olarak tespit etmektedir ve bu durum ile ilgili tanımlanmış güvenlik fonksiyonlarını işletmektedir. Ancak makas sorgulanan son konuma ulaşmadığı halde bu konumda olduğuna dair alınacak hatalı bir konum bilgisi bir başka deyiş ile sahte son konum onayı kazaya sebep olabilecek güvenliğe etki eden bir tehlikedir.

Bu nedenle güvenlik açısından kritik olarak son konum bilgileri seçilmiştir. Makas Motoru Arayüzü'ne ait FTA'de tepe olayı olarak sahte son konum onayı olarak seçilmiştir.

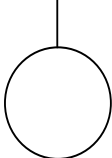
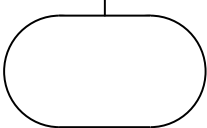
3.10.5 Arayüz devresi için hata ağacı analizi

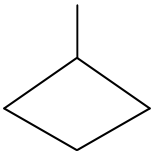
Hata ağacı analizi sırasında kullanılan sembol ve şekiller CENELEC EN 61025 satandardının Ek A bölümü referans alınarak seçilmiştir. Çizelge 3.8'de olayları belirten semboller yer almaktadır.

Hata ağacı analizi sırasında TopEvent FTA Express 2016 yazılımı kullanılmıştır.

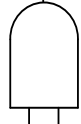
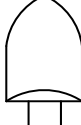
Hata ağacı analizi için öncelikle CENELEC EN 61025'e göre nitel yöntem olan Metot A ve daha sonra nicel CENELEC EN 61025'e göre Metot B olmak üzere iki biçimde gerçekleştirilmiştir. Çizelge 3.9'da FTA lojik kapı sembolleri verilmiştir.

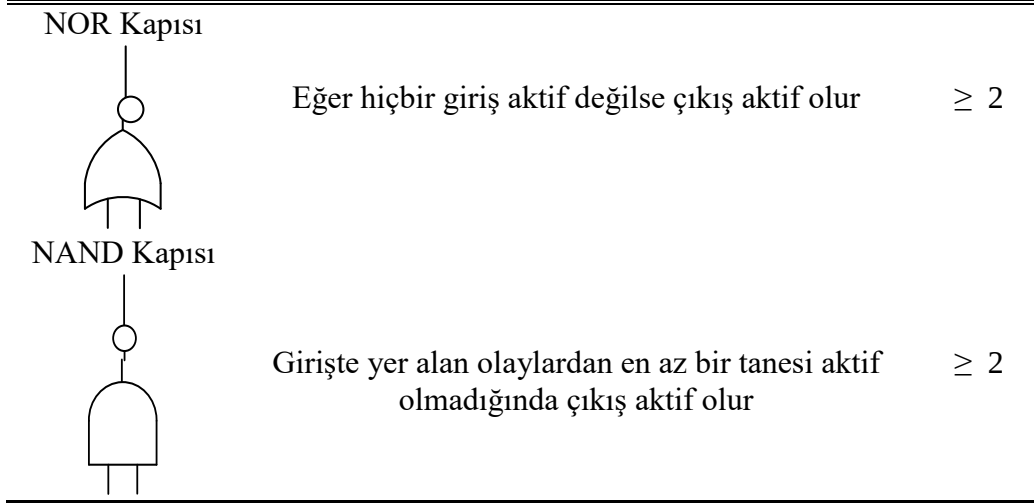
Çizelge 3.8 : FTA Sembol Tablosu

Olay Sembolü	Sembolün Adı	Tanım	Açıklama
	Basit Olay	En düşük seviyede tanımlanan hata oranı veya güvenilirliği konusunda tahmin yapılabilen olay	Bir komponentin hata modu veya bağımsız bir hata sebebi
	Koşullu Olay	Bir olayın meydana gelmesi başak bir olayın da meydana gelmesine bağlı olması, bir başka deyiş işe	Koşullu olay, çıkış üretebilmek için bir çıkış olayına ihtiyaç duyar

	Gelişmemiş Olay	iki olayda meydana geldiğinde çıkış aktif olur Bir sistemin henüz tam olarak tanımlanamayan bir parçası ile ilgili olay	Tepe olayın oluşmasına neden olabilecek bir olaydır ancak olayın oluşması ile ilgili durumlar tam olarak ortaya konamamaktadır
---	------------------------	---	---

Çizelge 3.9 : FTA Lojik Kapı Tablosu

Olay Sembolü	Sembolün Adı	Tanım
VEYA Kapısı 	Herhangi bir olayın meydana gelmesi çıkışın aktif olmasını sağlar	≥ 2
VE Kapısı 	Bütün girişlerin aktif olması durumunda çıkış aktif olur	≥ 2
ÇOĞUNLUK Kapısı 	Toplam n girişten belirlenen m veya daha fazla girişin aktif olması ile durumunda çıkış aktif olur	≥ 2
DEĞİL Kapısı 	Girişin aktif olmadığı durumda çıkış aktif olur	1
ÖZEL VEYA Kapısı 	Girişlerden sadece bir tanesi aktif olduğunda çıkış aktif olur	=2



Sistem demiryolu uygulamalarında kullanılmak üzere tasarlanmıştır. Bu sebeple EN 50129 standardına uygun olması amaçlanan donanımsal yapılardan ve EN 50128'e uygun olması amaçlanan yazılım uygulamaları göz önünde bulundurulmalıdır. Donanım ve yazılım sistem çıkışı üzerinde doğrudan etkili olduğu için tepe olayın doğrudan sebepleri arasında ikisine de yer verilmiştir.

Çevresel koşullar hem donanımsal hatalara sebep olabileceği hem de yazılımsal hatalara sebep olabileceği kabul edilmiştir. Yazılımsal hata iyi izole edilmemiş bir elektrik bağlantılarında yaşanacak gerilim dalgalanmalarının elektronik kontrolörün giriş çıkışlarını etkilemesi olarak nitelendirilebilir. Bu sebeple çevresel koşullar, onanım kaynaklı hatalar ve yazılım kaynaklı hatalar altında ortak kökenli hata olarak değerlendirilmiştir..

Kullanıcı programı kaynaklı hata ihtimali EN 50128 standardına uygun bir kullanıcı programı hazırlanması yolu ile en aza indirilmeye çalışılmıştır. Kullanıcı programı hata analizi bu rapor bünyesinde incelenmemektedir.

Güvenlik rölelerinden gelen konum bilgisi için kullanılan elektronik kontrolörün girişlerine sinyal taşıyan kabloların herhangi bir noktada kısa devre durumunda olmasının hatalı konum bilgisi oluşmasına sebep olabileceği göz önüne alınmıştır. Kablo kısa devreleri kablolar genellikle bir birini etkileyebilecek ve yangın gibi çevresel koşullardan ortak olarak etkilenebilecekleri için nitel hata ağacına dahil edilmiştir.

Güvenlik röleleri EN 50129 standardının belirtildiği gibi rölenin normalde açık kontaklarının konumlarını tetikleme sinyalinin olmadığı durumlarda koruyacak

şekilde dizayn edildiği için beklenmedik röle tetiklenmelerine dair bir ihtimal göz önüne alınmamıştır.

Motor kontaklarına AC ve DC gerilimin aynı anda uygulanması çeşitli arızalara sebep olabileceği için bu durumun sahte son konum onayı bilgisi üretebileceği göz önüne alınmış ve tasarım sırasında buna karşılık çeşitli önlemler alınmıştır.

Motor kontaklarında AC gerilim mevcutken DC gerilim uygulanmasını önlemek için motor kontaktörlerinin ayna kontak özellikli yardımcı kontakları izleme işlemi amaçlı kullanılmış ve bu bilgi elektronik kontrolör içerisinde koşan lojik içerisinde kullanılmıştır. Ayrıca ayna kontakların güvenliğini artırmak amacıyla seri halde bağlı birden fazla kontaktör kullanılmış kontaktörle oluşturulan yapının istenen güvenlik bütünlük seviyesine ulaşması sağlanmıştır.

Motor kontaklarında AC gerilim mevcutken DC gerilim uygulanması durumunda elektronik kontrolörün ve güç kaynağının zarar görmesini önlemek için konum bilgisi takibi amacıyla kullanılan elektronik kontrolörün girilşerine ve güç kaynağı girişine sigortalar konulmuştur. Ayrıca söz konusu komponentlerin zarar görmesini engellemek amacı ile izole güç kaynakları kullanılmıştır.

Motor kontaklarında DC gerilim mevcutken AC gerilim uygulanması durumunda elektronik kontrolör ve güç kaynağının zarar görmesine sebep olabilme ihtimali taşıdığı için güvenlik rölelerinin de hata olasılıkları göz önünde tutulmuştur.

Konum sorgulama işlemi sadece öncesinde hareket talimatı verilen yön için gerçekleştirileceğinden DCL ile DCR rölelerinin, LP ile ise RP rölelerinin aynı anda faaliyete geçmeyeceği göz önüne alınmıştır. Buna bağlı olarak, bütün güvenlik röleleri aynı marka ve model olduğu ve aynı hata oranlarına sahip olduğu için hata olasılığı değerlendirilmesi dört röle üzerinden değil iki röle üzerinden gerçekleştirilmiştir.

E1: Tepe olay; Sahte konum sinyali

E2: Donanım kaynaklı sahte konum sinyali

E3: Donanım kaynaklı sahte konum sinyali

E4: AC ve DC gerilim taşıyan kablolar arasında kısa devre

E5: Kontaktör kaynaklı hatalar

E6: Güvenlik röleleri ile ilgili hatalar

E7: AC ve DC gerilim taşıyan hat üzerinde kısa devre oluşması

E8: LP-RP rölelerinde meydana gelecek arızalar

E9: DCL-DCR rölelerinde meydana gelecek arızalar

E10: Kontaktörün ayna kontağında meydana gelecek arızalar

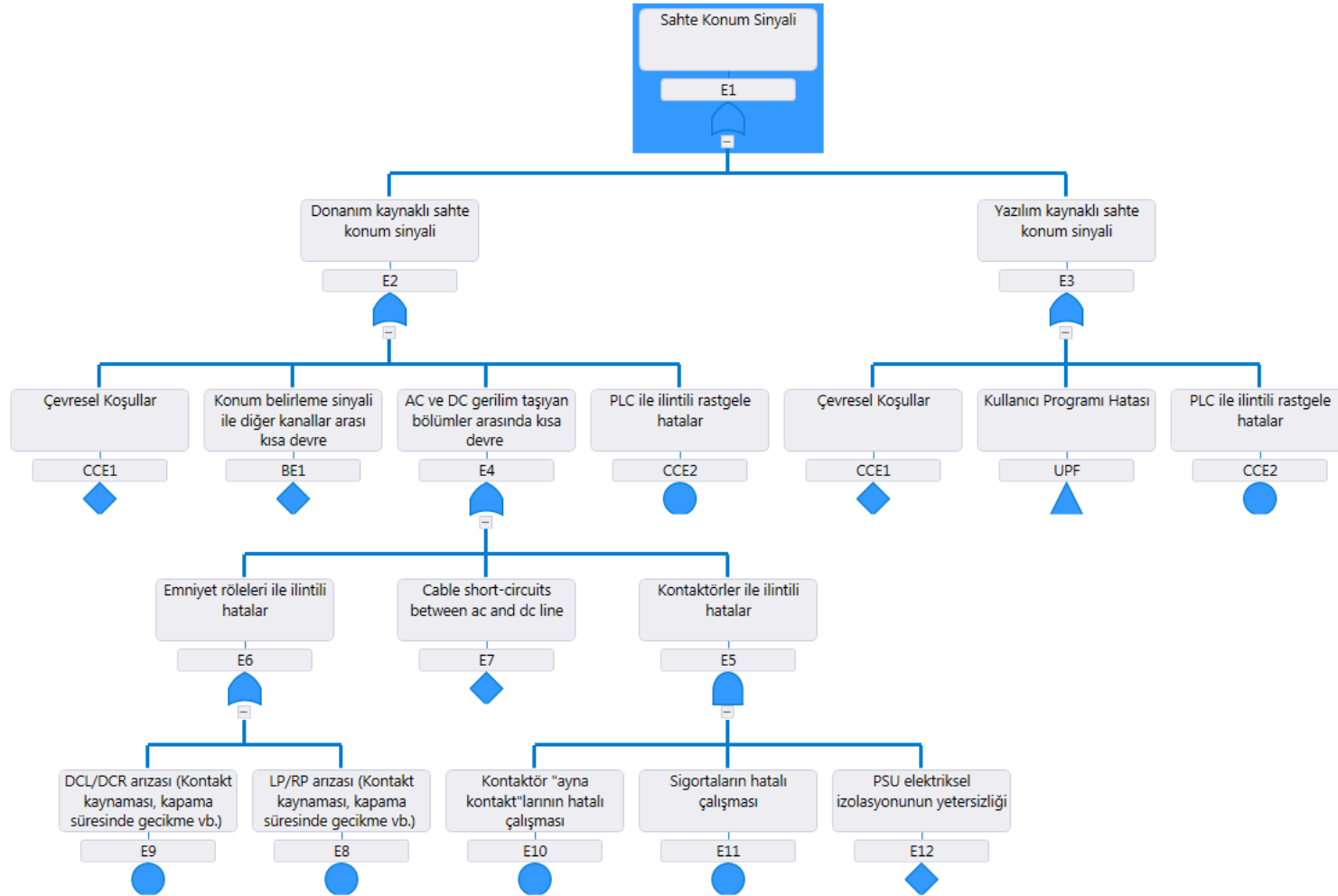
E11: Sigortaların çalışmaması

E12: Güç kayanığının elektriksel izolasyon açısından yetersiz olması

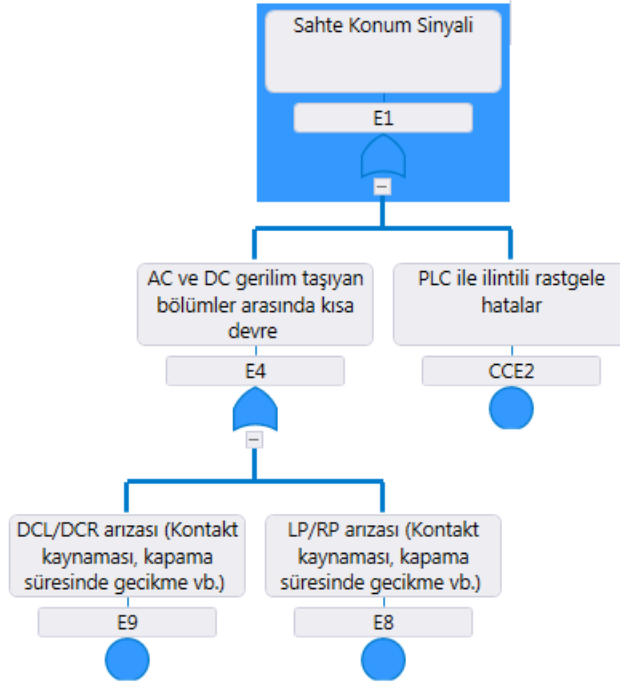
CCE1: Çevresel koşullar

CCE2: Elektronik kontrolör kaynaklı rastgele hatalar

Yukarıda belirtilen bilgiler ışığında hazırlanan Nitel Hata Ağacı Analizi Şekil 3.23'te, Nicel Hata Ağacı Analizi ise Şekil 3.24'te verilmiştir.



Şekil 3.23 : Nitel Hata Ağacı (Metot A)



Şekil 3.24 : Nicel Hata Ağacı (Metot B)

4. SONUÇ

Bu tezde Voestalpine Ecostar 4 makas motorunun 3 faz 4 kablo tekniği sürülmesi için iki ayrı tasarım yapılmıştır. Tasarıma başlanmadan önce makas motorunun içyapısı ve karakteristiği üzerinde çalışılmıştır. Motora AC gerilim ve DC gerilimin belli bir lojik içerisinde ardışıl olarak verilmesinden ötürü bu geçiş durumu sağlayan işaretler ve geçiş anlarındaki motorun karakteristiğini bilmek tasarım için kritik öneme sahiptir. Enerji verildiği anda ve motorun son konuma ulaştığında motorun iç kontaklarında olan değişim makas motoru üzerinde gerçekleştirilmesi amaçlanan motor sürme ve makasın pozisyonunu okuma bilgilerinin elde edilmesi için anlaşılması gereken konulardır. Makasın sağ son pozisyon ve sol son pozisyon için kontak durumları ve aynı zamanda motorun hareket halindeki kontak pozisyonları belirlendikten sonra motor arayüz tasarımı için isterler tamamlanmıştır. İlk tasarım röle ve kontaktör kullanılarak gerçekleştirilmiştir. Makasın kumandası ve kontrolü için geliştirilen lojik röleler kullanılarak sağlanmıştır. Lojik temel olarak motoru iki ayrı konuma götüren kontaktörleri sürmekte ve motora güç iletilmediği sırada makasın konum bilgilerin sorgulamaktadır. Yapılan testler sonucunda makas motoru başarı ile kumanda edilmekte ve makasın pozisyon bilgilerinin sorunsuz bir şekilde elde edildiği görülmüştür.

Makas motoru arayüzünden elde edilen bilgi güvenlik hassasiyeti yüksek bir bilgidir. Anlaşman sistemine iletilen pozisyon bilgisi doğrultusunda, anlaşman tren hareketini sağlayacak kararlar verir. Oturmamış bir makas üzerinden pozisyon bilgisi üretmek veya makasın bulunduğu pozisyonun aksine bir yön göstermek sonucu ciddi kazalar meydana getirebilir. Bu sebeple tasarlanan sistemin karşılaması gereken güvenlik bütünlük seviyesinin belirlenmesi gerekmektedir. Yapılan risk analizi sonucunda elde edilen değer göstermektedir ki arayüz devresi güvenlik bütünlük seviyesi 4 düzeyinde olmalıdır. Bu seviye, demiryolu ve birçok endüstride farklı şekillerde belirlenen en yüksek güvenlik seviyesidir.

Seviye 4 için kullanılabilecek komponentler incelenirken öncelikle standartlar açısından temel farklılıklar görülmüştür. Elektrik/Elektronik/Programlanabilir

Elektronik için kullanılan IEC 61508 standardı ile EN 50126-8-9 standartları arasında röle komponentini değerlendirme açısından farklılıklar mevcuttur. Bu nedenle çoğu rölenin sahip olduğu IEC standardına göre yapılan değerlendirmeler bir anlam taşımamaktadır. Ayrıca güvenlik uygulamalarında sadece normalde açık kontağın güvenli olarak kullanılabilmesi karşılaşılan bir başka zorluktur. Bu sebeplerden ötürü tasarımın baştan aşağı yeniden ele alınıp kontrol lojiğini gerçekleştirmek için elektronik kontrolöre geçilme kararı alınmıştır. Bu doğrultuda tasarım yeniden yapılarak, ikinci bir tasarım süreci başlamıştır. Sistem istekleri aynı şekilde kaldığı için bu süreçteki ana unsur elektronik kontrolörde koşturulmak üzere yazılım geliştirmesi yapılmasıdır. Yazılımın tamamlanmasının ardından gerçekleştirilen testler sonucunda sistem başarılı bir şekilde çalışmıştır.

Yeni tasarım elektronik kontrolör, güvenlik röleleri ve kontaktörlerden oluşmaktadır. Kontrolör ve röle EN standartlarına göre güvenlik bütünlük seviyesi 4'e uygun olarak tedarik edilebilmektedir. Ancak kontaktör kısmı için güvenlik analizi yapılması gerekmektedir. Yapılan analiz sonucu sistemin istenilen güvenlik seviyesini karşılamadığı görülmektedir. Standardın önerdiği çeşitli mimariler ile birlikte sistemin güvenlik seviyesinin yükseltilmesi amaçlanmıştır. Fiziksel olarak seri, fonksiyonel güvenlik açısından paralel bağlantı gerçekleştirilerek sistemin güvenlik seviyesi yükseltilmiştir.

Son olarak tasarlanan sistemin için tehlike analiz yöntemlerinde hata ağacı analizi uygulanmıştır. Buradaki amaç sistemin tasarımı ve hesaplamaları yapılmasına karşın belirlenen güvenliği etkileyen hatanın sebeplerini detaylandırarak incelemektir. Bu sayede dizaynın bir çeşit doğrulanması yapılacak ve gözden kaçan bir nokta var ise bunun tespiti mümkün olacaktır. FTA sonucunda da yapılan sistemin istenilen güvenlik seviyesine uyumluluğu garanti edilmiştir.

Bu bitime tezi ile beraber demiryolu sektöründe geliştirilecek bir projenin boyutuna bakmaksızın ne kadar detaylı olabileceği görülmüştür. Sinyalizasyon sistemi içerisinde küçük bir öge olan makas motoru arayüz devresi için bile problemin çözümü sadece tasarım gerçekleştirmek değil aynı zamanda standartlara uyumluluk ve çeşitli matematiksel gösterimler ile yapılan tasarımın doğrulanması gerektiğini ortaya konmuştur. Standartlar çoğu zaman aranan bilgiyi doğrudan sunmamakta ve aksine diğer benzer standartların bütünsellik içerisinde incelenmesi sonucu ortaya konan

tezler ile sonuca gidilebileceđi görölmüştür. Uygulanan risk ve güvenlik analizi yöntemlerinin daha kapsamlı projelere uygulanması mümkündür.

KAYNAKLAR

- Braband J. & Rüdiger vom Hove, and Hendrik Schöbe**, *Probability of failure on demand – the why and the how*, pp. 46–54, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
- EN 50129**, (2003). *Railway Applications. Communication, Signalling and Processing Systems. Safety Related Electronic Systems for Signalling*, Annex A, Sayfa 32,41
- Hermann K. & Thomas R. & Bernhard H. & Roland B. & Edin A. and Roman Popp**, (2016). *A Core Ontology of Safety Risk Concepts*, pp. 165–180, Springer International Publishing, Cham
- IEC 61508-4**, (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems - Part 4: Definitions and Abbreviations*, Sayfa 10-11, 19
- NASA Fault Tree Handbook with Aerospace Applications**, (2002). NASA Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC 20546
- PD CLC/TR 50451**, (2007). *Railway applications. Systematic allocation of safety integrity requirements*, Sayfa 32, Tablo 8.1
- Rail Safety and Standards Board**, *Safety Risk Model*, Version 8.1, Table A1 v8.1.0
- Railway Safety Performance in the European Union**, European Union Agency For Railways, 2016 (Final E), Sayfa 25
- The Game, Mem And Alarp Principles of Safety, Recherche - Transports – Sécurité**, (2000). Volume 68, Haziran–Eylül, Sayfa 63-65
- Ulaştırma Denizcilik ve Haberleşme Terimleri Sözlüğü**, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Yayınları, Sayfa 118

ÖZGEÇMİŞ



Ad-Soyad : Serhan SUBAŞI
Doğum Tarihi ve Yeri : 10.11.1990 / Şişli
E-posta : serhansubasii@gmail.com

ÖĞRENİM DURUMU:

- **Lisans** : 2013, İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Kontrol ve Otomasyon Mühendisliği

MESLEKİ DENEYİM VE ÖDÜLLER:

- 2013-2016 Yapı Merkezi İDİS Mühendislik San. A.Ş., Sistem Mühendisi
- 2016-Halen Yapı Merkezi İDİS Mühendislik San. A.Ş., Sistem Entegrasyon ve Teknoloji Transferi Yöneticisi