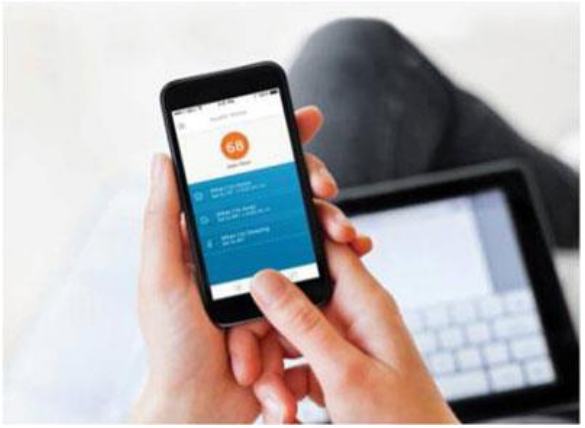


Ercan ÖRMEN
24.04.2019

Teknoloji sağlayıcı firmaların IEC 61511-2016 Uyarınca Farklı Sözleşme Yapılarında Üstlenmeleri Gereken Sorumluluklar

Honeywell
THE POWER OF CONNECTED

Kişisel Özgeçmiş Özeti

Ercan ÖRMEN

Eğitim

2005: Kabataş Erkek Lisesi

2010: Lisans; İstanbul Teknik Üniversitesi / Kontrol ve Otomasyon Mühendisliği

2015 - .. : Yüksek Lisans; İstanbul Teknik Üniversitesi / Kontrol ve Otomasyon Mühendisliği

Görevler

2010 – 2016: Proje Mühendisi; Sertifikalı Fonksiyonel Güvenlik Mühendisi, Honeywell

2016 - ... : EPC Projelerinden Sorumlu Satış Yöneticisi, Honeywell

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

FONKSİYONEL GÜVENLİK

- **GÜVENLİK**

Genel Olarak Endüstriyel Bir Tesisin Güvenliği Demek;

Doğrudan ya da dolaylı olarak, insan sağlığına, mülke ya da çevreye zarar verebilecek potansiyeldeki risklerin önlenmesi veya azaltılmasıdır.

- **FONKSİYONEL GÜVENLİK**

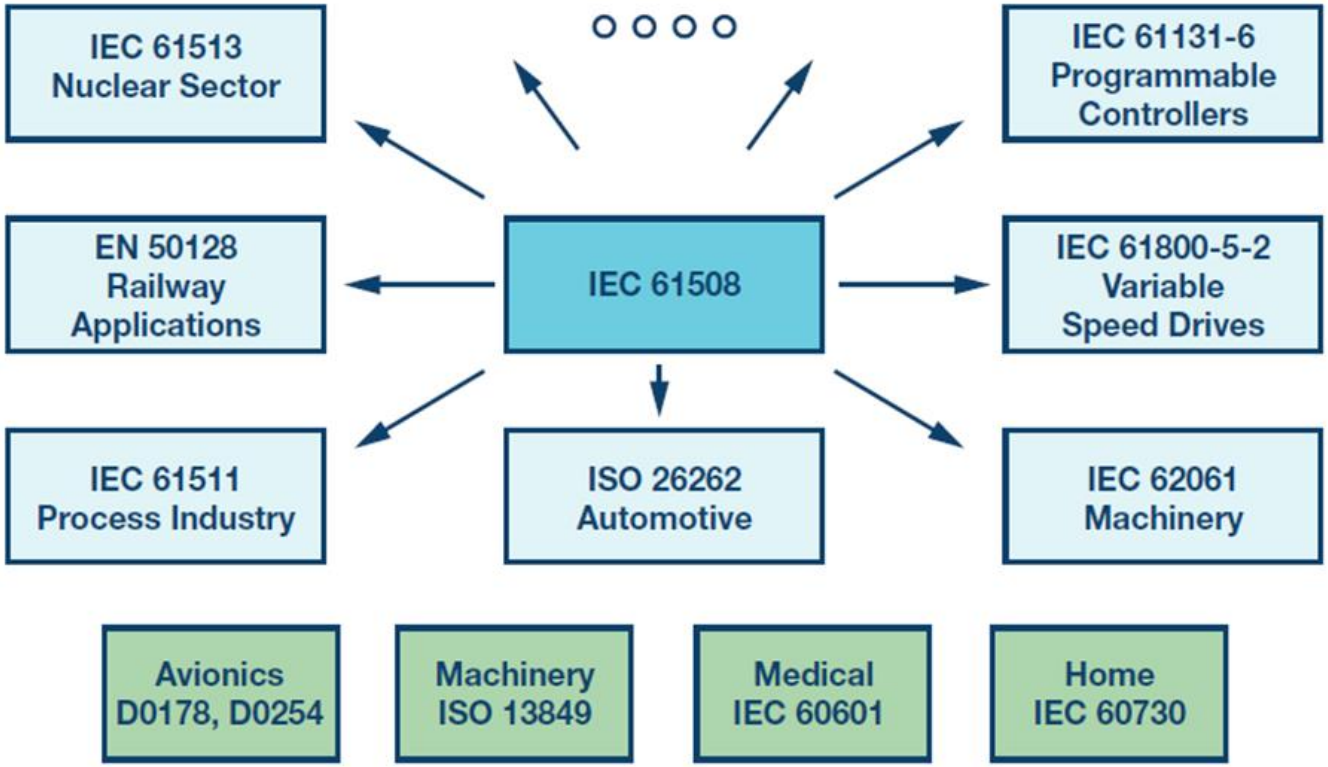
Fonksiyonel Güvenlik, genel güvenliğin bir alt kolunu oluşturur. Tehlike ve risklerin ortadan kaldırılması/azaltılmasına yönelik alınan tedbirlerin bir bölümünü oluşturur.
Okuduğu girişlere karşılık önceden belirlenmiş çıkışları otomatik olarak üreten cihaz ya da sistemler ile sağlanan güvenliktir.

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

STANDARTLAR

IEC 61508: E/E/PE (Elektriksel, elektronik ve programlanabilir elektronik) cihazların fonksiyonel güvenliği ile ilgili uluslararası standart. Bu cihazların üreticilerini hedef alır, daha çok onları ilgilendirir. Uygulamadan bağımsız, genel, şemsiye standarttır.

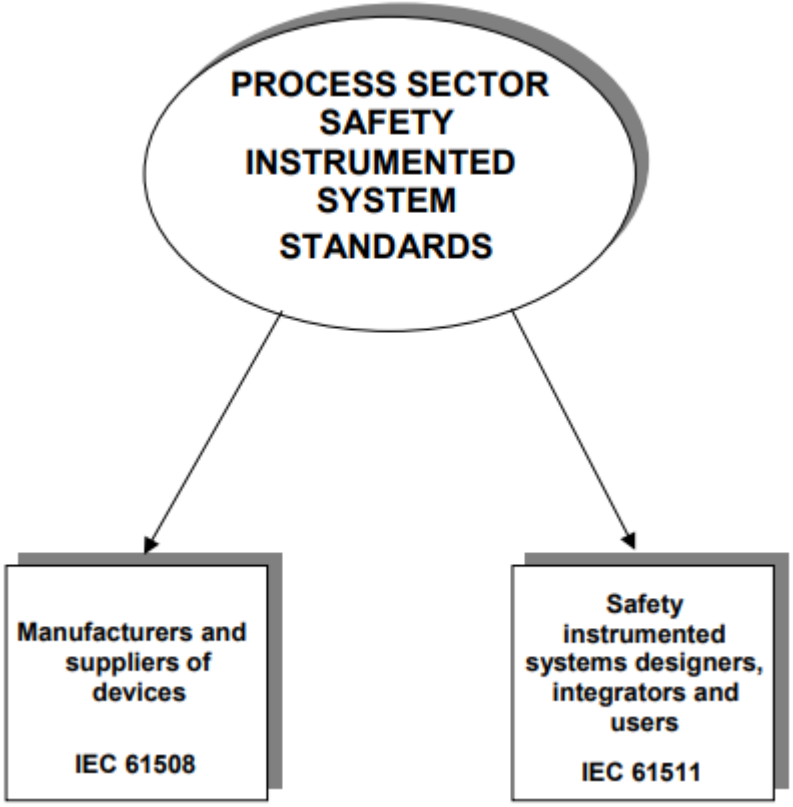


Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

STANDARTLAR

IEC 61511: Proses endüstrisi özelinde, kullanıcıyı, tasarımcıları ve integratörleri hedef alan standarttır. Sonuç odaklı ve sonuçları ölçmede kullanılacak metrikleri belirler. Beşikten mezara kadar, güvenlik donanımlı sistemlerin tasarım ve yönetim gereksinimlerini kapsar.



Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

GÜVENLİK YAŞAM DÖNGÜSÜ (SAFETY LIFECYCLE)

IEC 61511 içerisinde, Güvenlik Donanımlı Sistemlerin (SIS) Yaşam Döngüsü (Safety Lifecycle) tanımlanır.

Bu döngüde yer alan temel aktiviteler şu şekilde sıralanabilir:

- Tehlike ve risk değerlendirmeleri
- Güvenlik Gereksinimlerinin belirlenmesi ve şartname hazırlanması – SIL derecesi seçimi
- SIS tasarım kavramlarının belirlenmesi
- SIS doğrulamalarının yapılması
- SIS işletme, bakım ve test prosedürlerinin geliştirilmesi ve yürütülmesi
- Güvenlik Yaşam Döngüsü Yönetimi
- Güvenlik doğrulama, doğrulama, denetimler ve değerlendirmeler

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

GÜVENLİK YAŞAM DÖNGÜSÜ (SAFETY LIFECYCLE)

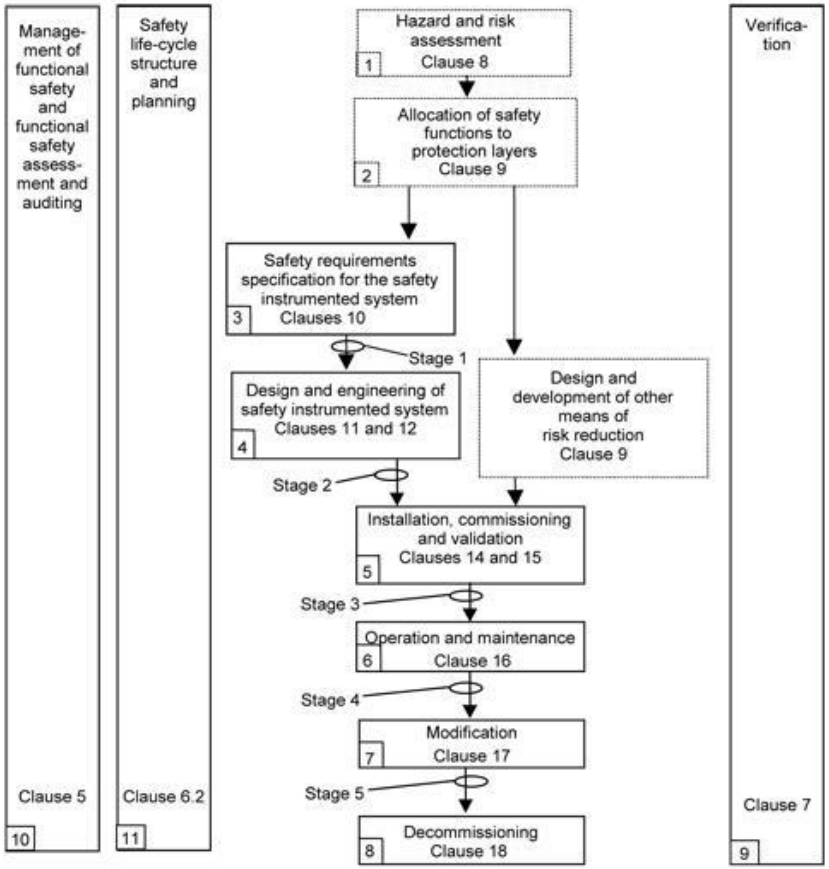


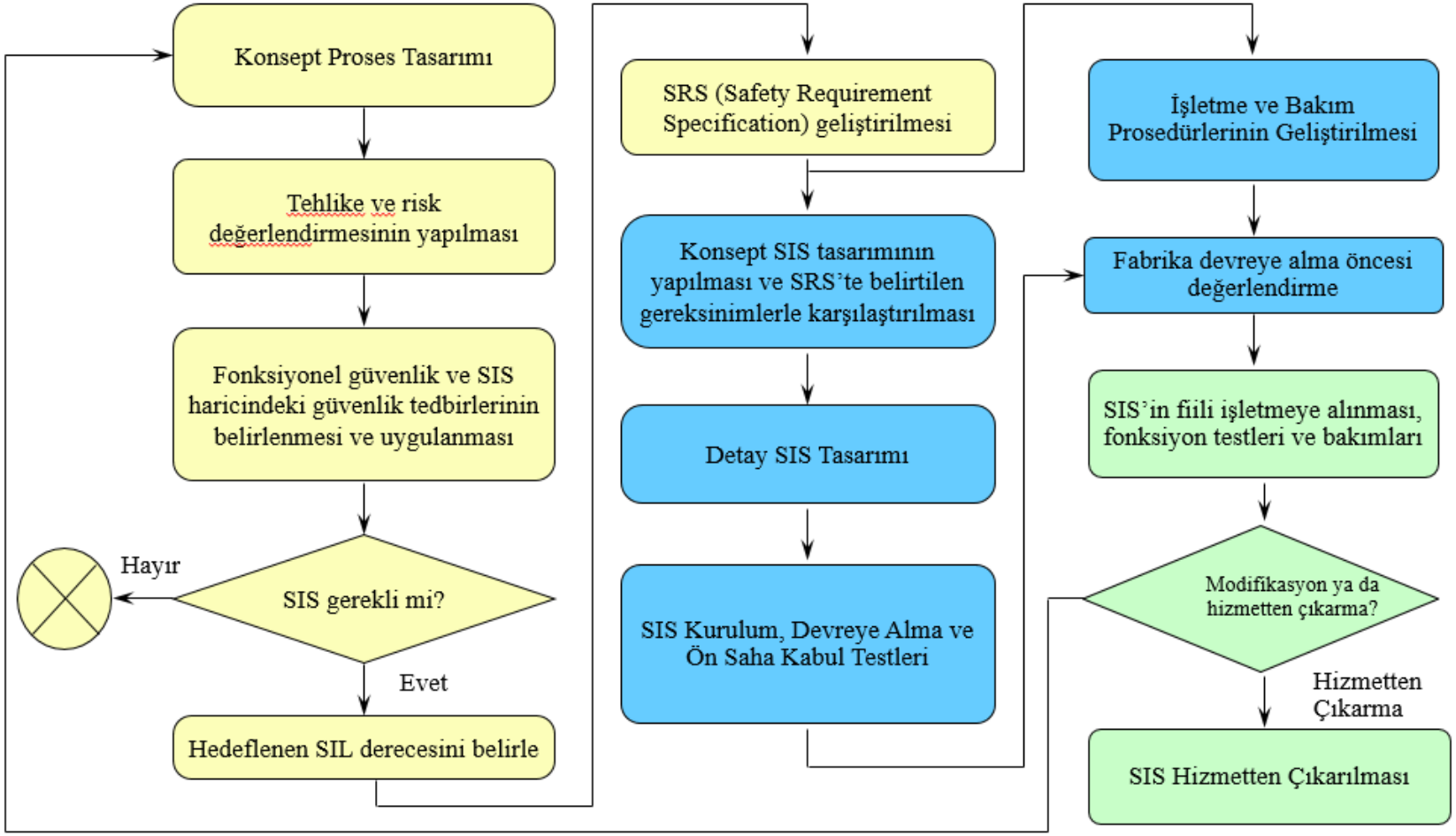
Figure 2 – ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) Safety Life Cycle

NOTE 1 Stages 1 through 5 inclusive are defined in clause 5.2.6.1.3.
NOTE 2 Phases 1 through 11 inclusive are shown: All references are to Part 1 unless otherwise noted.

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

GÜVENLİK YAŞAM DÖNGÜSÜ (SAFETY LIFECYCLE)



Analiz Fazı | **Uygulama Fazı** | **İşletme Fazı**

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

TEHLİKE VE RİSK DEĞERLENDİRMESİ

- Güvenlik Yaşam Döngüsü, mevcut tehlike ve risklerin tespit edilmesiyle başlar.
- Bu, döngünün ilk adımı olduğu gibi, aynı zamanda devamlı olarak yapılması gereken bir adımdır.
- Bu adımın sonunda, tüm tehlikeli durumlar, bu durumların sonuçları ve durumların olasılığı ortaya konur.
- Ortaya çıkan risk karşısında hedeflenen risk düşümü belirlenir.
- Son kullanıcı (Proses Sahibi), Mühendislik ya da Müteahhit firması ve teknoloji sağlayıcının yer aldığı temel bir kontratta, bu ilk adım son kullanıcının yani proses sahibinin sorumluluğu altındadır.
- Son kullanıcı, bu işi yaptırmak için bir danışmanlık firmasından destek alabilir ancak tesisin bizzat sahibi/işletmecisi olarak hedeflenen risk düşümünü son kullanıcının belirlemesi doğal zorunluluktur.

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

GÜVENLİK FONKSİYONLARININ BELİRLENMESİ

- SIL analizi ya da SIL belirlenmesi olarak da adlandırılabilecek bu adımda Güvenlik Enstrümanlı Fonksiyonlar (SIF) belirlenir.

- Analiz fazının önemli bir adımı olan SIF belirleme aşamasını son kullanıcı gözetiminde, proses tasarımından sorumlu firma ya da mühendislik/danışmanlık firması tarafından yapılabilir.

- Bir önceki Tehlike ve Risk Değerlendirmesi adımının sonucunda ortaya çıkan tehlike ve riskler güvenlik fonksiyonlarının belirlenmesinde önemli rol oynar.

- Her bir güvenlik katmanında eklenmesi gereken SIF'ler ve bu SIF'lerin hangi SIL derecesine sahip olacakları; son kullanıcı, proses teknoloji firması ve diğer mühendislik/danışmanlık firmaları tarafından ortaklaşa bir çalışma ile belirlenir.

- Bu çalışmanın sonucunda belirlenen SIF'ler, bunların hangi güvenlik katmanında olacağı ve SIL seviyeleri; son olarak son kullanıcının onayına tabi tutulur.

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

GÜVENLİK GEREKSİNİMİ ÖZELLİKLERİ (SAFETY REQUIREMENT SPECIFICATION – SRS)

- SRS dokumanı, detaylı mühendislik tasarımı ve proje uygulaması aşamalarında gerekli olacak tüm temel dayanakları ve prensipleri; SIS sistemlerinde olması gereken özellikleri içeren dokumandır.
- SRS dokumanının oluşturulması, Analiz Fazı olarak isimlendirdiğimiz Güvenlik Yaşam Döngüsünün ilk fazının, son adımıdır.
- Analiz fazında yapılan tüm çalışmaların nihai çıktısı olarak nitelendirebileceğimiz bu dokuman, yaşam döngüsünün diğer adımları için temel olma özelliğini oluşturur.
- Bu dokumanın hazırlanmasında, Tehlike ve Risk Değerlendirmesi ya da Güvenlik Fonksiyonlarının Belirlenmesi aşamasında görev almış mühendislik/danışmanlık ekibi görev alabilir. Hatta IEC61511 de bu yönde bir ifade içermektedir.
- Son kullanıcının işi anahtar teslim olarak bir müteahite verdiği durumlarda, müteahit firmanın da bu dokumanın hazırlanması rolü, sorumluluğu olacaktır.
- Teknoloji sağlayıcı firmalardan da bu aşamada destek alınabilir ancak nihai sorumluluk ya son kullancıda ya da müteahit firmadadır.

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

DETAYLI SIS SİSTEM MÜHENDİSLİĞİ

- Bu adımın temel amacı, SRS dokumanını baz alarak, SIS sistemlerinin, istenen güvenlik fonksiyonlarını (SIF), hedeflenen SIL seviyesinde sağlayacak şekilde tasarlanmasını sağlamaktır.

- Standart, Temel Proses Kontrol Sistemi (Basic Process Control System) olarak isimlendirdiği sistemin, güvenlikle ilgili olmayan fonksiyonlardan sorumlu olmasını ve bu sistemle SIS sistemin tamamen birbirinden bağımsız olması gerektiğini vurgular.

- Detaylı SIS sistem mühendisliğinde temel sorumluluk, SIS sistemlerini sağlayan teknoloji sağlayıcısı firmaların mühendislik ekiplerindedir.

- SRS dokumanının belirlediği temel tasarım unsurları göz önünde bulundurularak, sağlanan sistemlerin teknolojik altyapılarına ve karakteristiklerine özgü detaylı konfigurasyonları yapmak, ancak o sistemlere tam olarak hakim olan ve fonksiyonel güvenlik sertifikalı mühendislerin sorumluluğunda olmalıdır.

- SIS sistem mühendisleri temel sorumluluğa sahip olmakla birlikte, SRS dokumanının yanında bazı detaylı tasarım dokumanlarına da ihtiyaç duyarlar. Bu noktada onlara destek olması gereken mühendislik/danışmanlık firması ya da müteahit firmasıdır. Örneğin, birçok SIS projesinde vazgeçilmez bir dokuman olan Neden ve Etki Diyagramı (Cause and Effect Diagram)

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

FABRİKA KABUL TESTİ

- SIS sistemlerinin sahaya sevkinden önce, Fabrika Kabul Testi (Factory Acceptence Test – FAT) isteğe göre yapılabilir.

- Bir sonraki aşama olan kurulum ve devreye alma aşamasında tarafların üzerine düşen yükü azaltması ve bu aşamanın süresini kısaltması açısından Fabrika Kabul Testleri oldukça faydalıdır.

- Fabrika Kabul Testleri, teknoloji sağlayıcı firmanın organize ettiği, müteahit ve son kullanıcı firmaların temsilcilerinin dahil olduğu bir süreçtir.

- FAT prosedürleri, FAT'ın nasıl yapılacağı, hangi testlerin yapılacağı ve yöntemleri içerir. Bu prosedürler, teknoloji sağlayıcı firma tarafından hazırlanır ve son kullanıcının onayına sunulur.

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

KURULUM, DEVREYE ALMA, DOĞRULAMA

- Kurulum ve devreye alma aşaması, bilindiği üzere projelerin en kritik aşamasıdır. Bir yandan zaman baskısıyla mücadele edilirken, bir yandan eksiksiz ve detay tasarım dokumanlarına uygun şekilde ekipman ve sistemlerin faaliyete geçmesine çalışılır.

- Bir projenin devreye alma aşaması, kimisi birbiriyle ilişkili, çok farklı aktivitelerden oluşur. SIS sistemlerinin devreye alınması işi, belki de projenin devreye alma işinin çok küçük bir parçasını oluşturuyor olabilir.

- Her halükarda, devreye alma işleri, projenin bütünlüğüyle uyum ve koordinasyon içerisinde gerçekleştirilmelidir.

- Dolayısıyla, kurulum ve devreye alma işinde genel sorumluluk; ana yüklenici müteahitte; eğer bu yoksa, son kullanıcıdadır.

- Genel devreye alma takvimi ve iş programı belirlendikten sonra, SIS devreye alınması kapsamında yapılacak işlerin planlamasını yapmak ise teknoloji sağlayıcı firmadadır.

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

KURULUM, DEVREYE ALMA, DOĞRULAMA

- Fabrika Kabul Testleri sonucu tüm eksiklikleri giderilmiş bir SIS sisteminin devreye alınması, önceden belirlenmiş prosedürlerlerin takip edilmesi ve gereken testlerin yapılmasını içerir.
- Sinyal testleri, ekipman fonksiyon testleri ve senaryo testleri gibi adımlar bu testlerden bazılarıdır.
- Bu testler, SIS sistemlerinin yanısıra, birçok saha ekipmanı ve işletme ile ilgili konularla da ilgili olduğu için, ana yüklenici müteahhit ve/veya son kullanıcı tarafından organize edilmeli ve yönetilmelidir.
- Doğrulama adımı da aynı devreye alma adımı gibi bir bütün olarak düşünülmeli ve ana müteahhit ve/veya son kullanıcı yönetiminde ve sorumluluğunda yürütülmelidir.
- Doğrulama adımının çoğu zaman tamamen SIS sağlayıcının sorumluluğundaymış kanısı hakimdir. Bunun nedeni, çoğu SIS şartnamesinde, “SIL Verification (SIL Doğrulama)” dokumanının talep edilmesidir.
- SIS sistem sağlayıcılar tarafından hazırlanan SIL Doğrulama dokumanı, temin edilen SIS sisteminin nihai mimarisiyle hedeflenen SIL seviyesini sağlayıp sağlamadığının hesaplama sonuçlarıyla kanıtlandığı bir dokumandır.

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

İŞLETME, BAKIM VE DEĞİŞİKLİKLER

- Proje bazlı kontratların çoğunda, İşletme, Bakım ve Değişikliklerde sorumluluk son kullanıcı olan işletme sahibine geçer.
- SIS sistem sağlayıcılarından bazıları, istenildiği taktirde, bu süreçte de son kullanıcılara destek vermeyi sürdürebilirler.
- Örneğin, Honeywell gibi SIS sağlayıcı firmaların bazılarında, işletme, bakım ve değişiklik süreçlerinin takip, kontrol ve kaydını tutacak yazılımlar mevcuttur.
- Bu yazılımlar temel olarak aşağıdaki fonksiyonları üstlenir:
  - Tesisteki varsa Bypass (Atlatma) uygulanmış alarmların takibi ve limitlenmesi
  - Kanıt testlerinin (Proof test) programlanması, yürütülmesi ve sonuçlarının kayıt altında tutulması
  - SIS sistemlerinin durumlarının takibi
  - Oluşan arıza ya da bypass durumlarının neticesinde anlık SIL değerlerinin takibi
  - Tüm sistemlerde, yazılımsal ya da donanımsal olarak yapılan işlem ve müdahalelerin takibi
  - Devreye alma sonrası ortaya çıkacak değişiklik ihtiyaçlarının takibi, dokumante edilmesi ve yapılacak değişikliklerin diğer kısımlarda yaratacağı olası etkiler

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.

SONUÇ / ÖZET

Görev	Son Kullanıcı	Otomasyon / SIS Sistem Sağlayıcı	Mühendislik / Müteahhit Firması
HAZOP yürütülmesi	D/O		S
Tolere edilebilir riskin belirlenmesi	S		
SIL Gereksiniminin belirlenmesi	D/O		S
Sistem Tasarım & Mühendisliği	O	S	D
Kurulum ve doğrulama (validation)	O	D	S
Devreye alma	S	D	D
İşletme	S		
Bakım ve modifikasyonlar	S	D	

S: Sorumlu, D: Destekleyici, O: Onaylayıcı

Honeywell
THE POWER OF CONNECTED

Honeywell Confidential © 2017 by Honeywell International Inc. All rights reserved.