BÜYÜK ENDÜSTRİYEL KAZALARI ÖNLEME ÇALIŞMALARINDA KRİTİK SİSTEMLERİN TESPİTİ VE RİSK DEĞERLENDİRME YAKLAŞIM VE YÖNTEMLERİ

Özlem ÖZKILIÇ
Kimya Yük. Müh.
İş Teftiş İstanbul Grup Başkanlığı
ÇSGB Emekli Baş İşmüfettişi

ÖZET

İş kazaları ve meslek hastalıkları, insan hayatına maddi ve manevi zararlar vermekte, bunun yanında hem çalışanlara hem de işletmelere ve dolayısıyla ulusal ekonomiye önemli ölçüde maddi zarar ve yük getirmektedir.

İş kazaları ve meslek hastalıklarının oluşmasında teknolojideki hızlı gelişim, makineleşme, işyerlerindeki fiziksel ve kimyasal etmenler ile üretimde kullanılan ham ve yardımcı maddelerin yanında ekonomik, sosyolojik, psikolojik, fizyolojik ve ergonomik bir çok etken rol oynamaktadır. Özellikle sanayi devrimi sonrasında teknolojik gelişmeler sonucunda üretimin yapısı oldukça karmaşıklaşmış, hızlı ve kontrolsüz sanayileşme süreci ve üretimin giderek yoğunlaşması iş kazaları ve meslek hastalıkları ile çevre kirliliği gibi sorunların önemli boyutlara ulaşmasına neden olmuştur.

İşyerlerinde yapılacak risk değerlendirme çalışmalarında özellikle büyük endüstriyel kazalara sebebiyet verebilecek kritik sistemlerin de irdelenmesi ve bu sistemlerde oluşabilecek, tehlikeli olarak tanımlanan sapmaların giderilmesi ile sistemin güvenilirliğinin arttırılması gerekmektedir.

Anahtar Kelimeler: Büyük endüstriyel kazalar, risk değerlendirme, kritik sistemler, güvenilirlik.

Büyük Endüstriyel Kazalar ve Risk Değerlendirme

Uluslararası kuruluşlarca yapılan araştırmalar iş güvenliği ile iş gücü verimliliği arasında karşılıklı etkileşim olduğunu, sağlıklı ve güvenli işyerlerinde verimliliğin arttığını ortaya koymuştur. İş kazaları ve meslek hastalıklarının önlenmesi sonucu iş güvenliğinin sağlanması; yan etki olarak işyerinde verimlilik ve üretim artışına da yol açmaktadır. Özellikle iş kazaları işin akışını durdurarak üretimi kesintiye uğramakta ve maddi kayba neden olmaktadır. Uluslararası Çalışma Örgütü (ILO) araştırmalarında üretimde kullanılan makine ve tezgâhlarda koruma sistemlerinin geliştirilmesi ile iş güvenliğinin sağlanması sonucunda önemli ölçüde üretim artışının sağlandığını saptamıştır.

Risk değerlendirmesi kavramı mevzuatımıza yeni girmiş olmakla birlikte içeriği ve kullanılan yöntemler yeni değildir. Risk Değerlendirmesi kavramı 20. yüzyılın başlarında güvenilirlik teoreminin oluşturulması ve kullanılmaya başlanması sonrasında telaffuz edilmeye başlanmıştır. İlk defa NASA tarafından geliştirilen MIL-STD-882 nolu standart bu alandaki gelişmelerin önünü açan ilk sistemli belge olmuştur. Ünlü analist Peter F. Drucker yöneticilere vermiş olduğu bir konferansta 18., 19. ve 20. Yüzyıllarında Batı ekonomisinin ilerlemesinde teşebbüs, girişim ve çabuk ve doğru karar verme yeteneği kadar risk değerlendirme yönetiminin de önemli bir yere sahip olduğunu vurgulamıştır. Drucker'a göre riskleri yönetme ve önlem alma çalışmaları gelişmiş ülkeler ve gelişmekte olan ülkeler arasındaki en önemli farktır. (Özkılıç, 2005: 60)

Özellikle 20. yüzyıl başlarından itibaren tehlikeli maddelerin artan üretimi, kullanımı ve depolanması yüzünden büyük endüstriyel kaza olasılığı büyük oranlarda artmıştır. Dolayısıyla

da tüm halkın, çalışan kesimin ve çevrenin korunması gereği doğmuş, büyük endüstriyel kazaların önlenmesi için sistematik yaklaşım ihtiyacı belirmiştir. Üç Mil Adası'ndaki ve Çernobil' deki nükleer kazalardan sonra otoriteler nükleer tesislerin güvenli işletilmesi için birçok çalışmalar yürütmüştür. Ancak klasik endüstriye ilişkin risk değerlendirme çalışmalarının hızla başlamasında İtalya Sevesso'daki büyük endüstriyel kaza dönüm noktası olmuştur. (Özkılıç, 2007: 44)

Tablo1. 1959-2004 Yılları Arasında Meydana Gelen Kaza ve Felaketler (Özkılıç, 2007: 34)

Yıl	**Yer**	**Olay**	**Hasar**
1959	Minamata, Japonya	Su yollarına cıva deşarj edilmesi	400 ölü, 2,000 yaralı
1973	Fort Wayne, A.B.D.	Demiryolu kazası ile vinil klorür dökülmesi.	4500 tahliye
1974	Flixborough, İngiltere.	Patlamada siklohekzan açığa çıkması	23 ölü, 104 yaralı, 3,000 tahliye
1976	**Seveso, İtalya**	**Dioksin sızıntısı**	**193 yaralı, 730 tahliye**
1978	Los Alfaquez, İspanya	Ulaşım kazasında propilen dökülmesi.	216 ölü, 200 yaralı
	Xilatopec, Meksika	Karayolu kazasında gaz tankeri patlaması.	100 ölü, 150 yaralı
	Manfredonia, İtalya	Fabrikadan amonyak sızıntısı	10,000 tahliye
1979	Threemile Adası, A.B.D.	Nükleer reaktör kazası	200000 tahliye
	Novosbirsk, Rusya	Kimya fabrikasında patlama	300 ölü
	Mississagua, Kanada	Demiryolu kazası ile klor ve bütanın çevreye yayılması.	200000 tahliye
1980	**Summerville, A.B.D**	Demiryolu kazası ile fosfortriklorür dökülmesi	300 yaralı, pek çok tahliye
	Tacoa, Venezüella	Petrol yangını ve patlaması	145 ölü, 1,000 tahliye
1982	**Taft, A.B.D.**	Patlamada kimyasallardan akrolein açığa çıkması	17,000 tahliye

1984	**Sao Poulo, Brezilya**	Petrol boru hattında patlama	508 ölü
	St. J.Ixhuatepec, Meksika	Gaz tankı patlaması	452 ölü, 4,248 yaralı, 300,000 tahliye
	Bhopal, Hindistan	Pestisit fabrikasından sızıntı siyan gazı	72,500 ölü, binlerce yaralı, 200,000 tahliye
1986	**Çernobil, Rusya**	Nükleer reaktör kazası	725 ölü, 300 yaralı, 90,000 tahliye, Avrupa ülkelerine yayılma
	Basel, İsviçre	Pestisit fabrikasında yangın	Ren nehrinde kirlilik
1987	**Kotka, Finlandiya**	Limanda monoklorobenzen dökülmesi	Deniz tabanı kirliliği
1991	**Körfez Savaşı, Basra Körfezi**	Petrol dökülmesi	Deniz kirliliği
1992	**Alaska**	Petrol dökülmesi	Deniz kirliliği
2000	**Enschede, Hollanda**	Havai fişek fabrikasında patlamada	21 kişi hayatını kaybetti. 800 kişi yaralandı ve1 km2 çaplı alanda 5300 kişi patlamadan ve sonuçlarından etkilendi.
2000	**Baia Mare, Romanya**	Yüksek konsantrasyonda siyanür içeren atık havuzunun aşırı yağışlarla yıkılması sonucu arıtılmamış siyanür atık Tuna Nehri'ne karıştı.	Nehir kirliliği
2001	**Toulouse**	Gübre tesisi patlaması sonucu standart dışı amonyum nitrat yayılımı	Geniş alanda etkilenme

Kasım, 1989'da ILO Yönetim Kurulu'nun 244. toplantısında alınan karar uyarınca, Cenevre'de 8-17 Ekim 1990 tarihlerinde büyük endüstriyel tehlikelerin önlenmesine ilişkin uygulama kodu hazırlanması maksadıyla bir uzmanlar toplantısı düzenlenmiştir. Bu uzmanlar toplantısında Büro tarafından hazırlanan taslağa dayalı uygulama kodu gözden geçirilmiş ve son şeklini almıştır. Toplantıda bu koda "Büyük Endüstriyel Kazaların Önlenmesi" adı verilmesi kararlaştırılmıştır. Ancak hazırlanan bu kod büyük endüstriyel kazaların önlenmesi için tüm ilgililere sadece pratik tavsiyeler niteliğinde kalmıştır.

İtalya'nın Seveso kasabasında 1976'da gerçekleşen ciddi endüstriyel kazayı takiben, endüstriyel donanımlarda kaza önleme üzerine bir Direktif olan Seveso Direktifi (82/501/EEC) kabul edilmiştir. Daha sonra Hindistan, Bhopal'de 1984 yılında ve İsviçre, Basel'de 1986 yılında gerçekleşen iki büyük kaza ve Mexico City'de doğal gaz patlaması sonucunun 500 ölü, 4.000 yaralı ile sonuçlanması bu direktifin tekrar gözden geçirilmesi gereğini doğurmuştur.

Son olarak yeni ve gözden geçirilmiş II. Direktif (96/82/EEC), 1996 yılında kabul edilmiştir ve 82/501/EEC sayılı Direktif'in yerini almıştır. Enschede ve Toulouse kazalarına tepki olarak AB, amonyum nitratla birlikte, patlayıcı ve yanıcı maddelerle ilgili Seveso II yönetmeliğindeki kuralları tekrar gözden geçirmiş ve daha da sertleştirmiştir. AB, Enschede, Baia Mare ve Toulouse'daki kazalardan sonra SEVESO II'nin kapsamını genişletmiş ve SEVESO II'de görülen bazı aksaklıkların da çözümü için bazı ek çalışmalar yaparak direktifin son hali olan 2003/105/EEC sayılı direktifi 16 Aralık 2003 tarihinde yayınlamıştır. Seveso II Direktifi adını alan veya diğer bir adıyla COMAH Direktifi; tehlikeli maddeler içeren büyük endüstriyel kazaların önlenmesine yönelik çeşitli kontrol yükümlülükleri getirmiştir. (Özkılıç, 2007: 46)

Kritik Sistemler ve Güvenilirlik Kavramı

İş ortamında "hata", genelde uygun görülen, tasarlanan ve beklenen davranış standardından sapma olarak tanımlanmaktadır.(Özgüven,2003:22) Hatalı davranışlar sistem güvenliği ve sistem performansını azaltan ya da azaltma potansiyeli olan, istenmeyen veya uygun bulunmayan davranış biçimleridir. Hatalı davranışların hem insan faktörü hem de iş sistemi üzerinde neden olduğu sonuçlar iki açıdan önemlidir. Birincisi can kaybı, yaralanmalar, çalışanlar üzerindeki psikolojik etkiler gibi insan öğesine yönelik istenmeyen sonuçlardır. İkincisi ise üretim kaybı, üretim kesintisi, verimlilik azalması gibi iş sisteminde maliyet boyutu taşıyan durumlardır. (Sabancı,1999:36)

Bir tesis veya proses de meydana gelebilecek hatanın önem derecesini belirlemek ve bu önem derecesine göre önlemleri planlamak gerekmektedir, ancak bu hataları belirleyebilmek için öncelikle sistem kavramı ve tanımına göz atmamız ve "Kritik Sistem" tanımını yapmamız gerekmektedir.

Uluslararası Sistem Mühendisliği Konseyi INCOSE (International Council on Systems Engineering), sistemi ortak bir hedefe doğru çalışan birbirleri ile ilişkili parçalar bütünü olarak tanımlamıştır. Sistemin özelliklerini ise aşağıdaki gibi vermiştir;

- Karmaşık bir bütün oluşturan, birbirlerini etkileyen, birbirine bağlı ve/veya birbirleriyle ilişkili parçalar (öğeler) grubudur,
- Parçaların her biri aynı süreç, işlem ve/veya yapı ile ilişkilidir,
- Parçalar birbirlerinden farklı biçim ve/veya işleve sahiptir,
- Parçaların kendilerine özgü nitelikleri(özellik ve işlevi) vardır,

- Sistem sınırlandırılabilir/sınırı çizilebilir bir yapıdadır,
- Parçalar birbirlerini ilişkiler ile etkiler,
- Parçalar da birer sistem olabilir.(Rostamzadeh ve diğ., 2004: 16)

Sistem bilimci olan Ian Sommerville (2004), sistemleri açıklarken aşağıdaki gibi bir ayrım vermiştir;

Emniyet -Kritik Sistemleri (Safety-critical systems); hatası yaralanma, ölüm veya büyük çevresel hasarlara yol açabilen sistemler olarak tanımlamıştır. Örneğin tren rotaları ve saatlerini düzenleyen sistemler.

Amacı Kritik Olan Sistemler (**Mission-critical systems)**; hatası sistemin amacını gerçekleştirememesine neden olan sistemler. Örneğin uzaya fırlatılan bir aracın rotasını belirleyen sistemler gibi.
İşi (Kullanıcısı) Kritik Olan Sistemler (Business-critical systems); hatası kullanan şirketin hata yapmasına yol açan sistemler. Örneğin bir bankanın müşteri hesap sistemi gibi.

MIL-HDBK-189 Military Handbook'da ise sistemler çökme bazlı ele alınarak tanımlama yapılmıştır;

Güvenliği-Kritik Sistemler (Safety-critical systems); çökmesi hayat kaybına, sakatlığa veya çevrenin zara görmesine neden sistemlerdir.

Görevi-Kritik Sistemler (Mission-critical systems); sistemin çökmesi belirlenmiş hedeflerin başarısızlığa uğramasına neden olur.

İşi-Kritik Sistemler (Business-critical systems); sistem çökmesi büyük ekonomik kayba neden olur. (Sommerville, 2004: 36)

Sistem tanımlarının genellikle aynı yaklaşımda verildiği görülmektedir. İki ayrı kaynaktaki en önemli fark; bir bakış açısının kritik hata bazlı bakarken, diğer bakış açısının sistemin çökmesi üzerine bakmasıdır. Ancak her iki tanımda da sonuç değişmemekte ve sistemin hata yapması veya çökmesi aynı sonucu doğurmaktadır.

Tüm sistemler, prosesler ve ekipmanlar için ise bir yaşam döngüsü söz konusudur. Yaşam döngüsü içerisinde güvenilirliği ne kadar yüksek bir sistem tasarlamaya çalışırsanız bu seferde karşınıza maliyet kavramı gelmektedir. %100 güvenilirlik sağlanmış bir sistemin maliyetinin çok yüksek olacağı aşikardır, işte bu aşamada gündeme yaşam döngüsü maliyeti (life-cycle cost concept of management) boyutlarından birkaçı olan dependability, reliability, avaliability ve security fonksiyonlarının analitik olarak tanımlanması gelmektedir.

Literatürde güvenilirlik analizi konusunda yapılmış birçok çalışma mevcuttur. Bunlardan, bir kısmı güvenilirlik analiz yöntemlerinin geliştirilmesine yönelik çalışmalar olup, diğerleri ise farklı sistemlerin güvenilirliklerinin belirlenmesine yönelik çalışmalardır. Yine literatür taraması yapıldığında güvenilirlik analizinde geçen terimlerin tanımlarında da bazı farklılıklar olmasına rağmen birbirine yakın ifadeler içerdikleri görülmektedir. Bu terimlerden bazılarını inceleyecek olursak;

Dependability ve reliability kelimeleri İngilizcede eş anlamlıdır ve Türkçe karşılıkları güvenilirlik olarak verilmektedir, bu nedenle de bu iki İngilizce kelimenin anlamı büyük kafa karışıklıklarına neden olabilmektedir. Özellikle de yeni sistemlerin veya makinelerin güvenilirlik hesaplamaları yapılırken eskiden reliability hesaplanmasının önemi vurgulanırken artık dependability'in bilinmesinin daha önemli olduğu otoritelerce kabul edilmektedir.

Bu nedenle de özellikle bu iki kelimenin arasındaki farkı iyi ayırt etmek gerekmektedir.

ASHRAE Aplications Handbook'ta verilen tanımlara göz attığımızda; Dependability için bir sistemin durumunun ölçüsü olarak tanım yapıldığı görülmektedir. Sistemin, hizmet ömrünün başlangıcında çalışır durumda olduğunu kabul ederek, dependability hizmet ömrünün içindeki herhangi bir anda çalışabilir durumda olma olasılığıdır. Tüm bu tanımlar ışığında Dependability'i, Türkçede teknik terim olarak dayanaklılık olarak karşılık vermek daha doğru olacaktır.

ASHRAE Aplications Handbook'ta Reliability; tanımlanmış bir zaman periyodunun öngörülen bir dilimi içerisinde sistemin çalışacağının göstergesi olarak verilmiştir. Yine Reliability için makine emniyeti ile ilgili EN standartlarına bakıldığında EN ISO 292'de, bir makine veya elemanın veya donanımın belirli şartlar altında ve verilen bir zaman süresi içerisinde arızalanmaksızın istenen bir fonksiyonu yerine getirebilme kabiliyeti şeklinde tanımlandığını görürüz. ISO/IEC 27001-27002'de ise sistemin herhangi bir zaman dilimi içinde gerekli hizmetleri doğru bir biçimde verebilmesi olasılığı olarak verilmiştir. Söz konusu bu tanımlar ışığında Reliability'in Türkçede teknik terim olarak güvenilirlik olarak karşılık bulduğunu söylemek doğru olacaktır.

Yine özellikle sistem, proses, makine ve ekipmanların güvenilirlik çalışmalarında sıklıkla duyduğumuz avaliability, safety ve security kelimelerini de inceleyecek olursak;

EN ISO 292 'de avaliability için, amaçlanan kullanma şartları altında fonksiyonunu yerine getirebilmeye muktedir tutulabilme veya belirli uygulamalara göre ve belirli vasıtalar kullanarak yürütülen gerekli işlemlerle yeniden eski durumuna getirilebilme kabiliyeti şeklinde tanım verilmiştir. EN ISO 12100'de ise; bir makinenin diğerleri ile birlikte fonksiyonunun/fonksiyonlarının kolayca anlaşılabilir olmasını sağlayan özellikleri veya karakteristiği sayesinde kolayca kullanılabilme özelliği olarak verildiği görülmektedir. Yine sistem güvenilirliği ile ilgili bir standart olan ISO/IEC 27001-27002'de avaliability için, herhangi bir zamanda sistemin çalışır durumda olması ve istenilen hizmetleri verebilmesi olasılığı şeklinde tanım yapılmaktadır. Standartlardaki tanımlamalar incelendiğinde avaliability için Türkçede teknik terim olarak kullanılabilirlik şeklinde karşılık vermek yerinde olacaktır.

Yine aynı Dependability ve reliability kelimeleri gibi safety ve security kelimeleri de İngilizcede eş anlamlıdır ve Türkçe karşılıkları güvenlik olarak verilmektedir. Ancak yine standartlar araştırıldığında bu iki kelimenin anlamlarının birbirinden tamamen farklı anlamlar içerdiği görülür. EN ISO 12100- EN ISO 13849 –EN ISO 13850 standartlarında safety için makine dâhilinde veya çevresinde bulunan herhangi bir alan çerçevesinde bulunanlara zarar verebilme ölçüsü şeklinde tanımlama yapıldığı, ISO/IEC 27001-27002 standardında ise sistemin insanlara veya çevresine zarar verme ölçüsü olarak verildiği görülmektedir. Bu tanımlamalar çerçevesinde safety için Türkçe teknik terim olarak hatasızlık olarak karşılık vermek daha doğru olacaktır.

EN ISO 12100- EN ISO 13849 –EN ISO 13850 standartlarında security için makine dahilinde veya çevresinde bulunan fonksiyonların kasti ya da kazara yapılan etkilere dayanabilme ölçüsü olarak verilmişken, ISO/IEC 27001-27002 standardında otomasyon sisteminin kötü niyetli müdahalelere karşı kendini koruyabilme kabiliyeti şeklinde tanımlanma yapılmıştır. Bu tanımlar çerçevesinde security için Türkçe teknik terim olarak güvenlik kelimesini kullanmak yerinde olacaktır.

Tablo 2. Sistem Çalışma ve Arıza Çevrimi (Özkılıç, 2007: 98)

	Çalışma Süresi (MTTF)	← Arıza Süresi (MTTR) →				
Sistemin	Sistemin	Arıza ve	Arıza	Yedek	Arızanın	Sistemin

Test Edilmesi	Normal Çalışması	Bakımcının Çağrılması	Araştırması	Parçanın Temini	Giderilmesi	Test Edilmesi
	← İki Arıza Arasında Geçen Süre (MTBF) →					

Bir başka deyişle günümüzde bu değerler niteliksel değil sayısal olarak ifade edilmekte, sistemlerin, makinelerin ve ekipmanların değerlendirmeleri de bu sayısal değerlere bakılarak yapılmaktadır. Ekonomik sistemlerin kurulması, maliyetleri minimize eden optimum işletme koşullarının (doğru yapılmış tasarım değerlerinde) sağlanması veya işletme sürecinde yaratılması, etkin ve sürekli hizmet verebilmek için bu değerlerin bilinmesi gerekmektedir.

Modern işletme ve bakım mühendisliği sistemlerinin önemli unsurlarından biri olmakla birlikte, söz konusu uygulamaların yapılabilmesi için gerekli olan, sistem ve ekipmanların durumlarının gözlenmesini gerektirmektedir. Gözlem (monitoring), hem ilgili sistem şartlarının (sıcaklık, debi, basınç vs) ve ekipmanlarının şartlarının (titreşim, yük, ses vs) gözlenmesini ve kayıt edilmesini (test raporları) hem de değerlendirilmesi süreçlerini içermektedir. Bu süreçlerin sonunda, işletme ve bakım planları gerçekleştirilebilmektedir. Aynı zamanda yine aynı sistemlerin veya makine ekipmanlarının risk değerlendirmelerini veya makine emniyeti ile ilgili mevzuat hükümleri ile standartlarına uygunluğunun sağlanabilmesi için de yine aynı değerlerin sayısal olarak ifade edilmesine ihtiyaç bulunmaktadır.

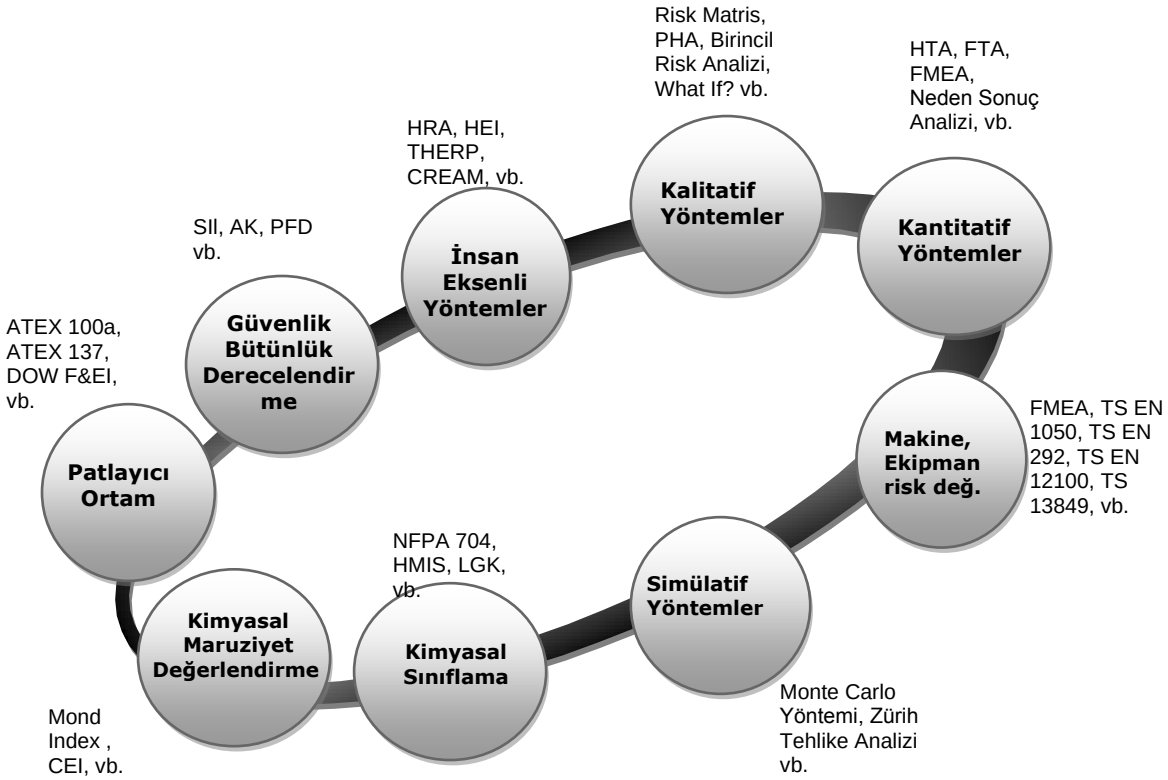
Kritik Sistemler ve Risk Değerlendirme

İnsanlar için fiziksel, ekonomik ve sosyal kayıplar doğuran, normal yaşamı ve insan faaliyetlerini durdurarak veya kesintiye uğratarak toplulukları etkileyen olayları afet veya felaket olarak tanımlayabiliriz.

Endüstriyel devrim öncesi meydana gelen felaketler, büyük ölçüde seller, taşkınlar, fırtınalar ve depremler gibi önlenemez doğa olayları ile sınırlı idi. Günümüzde halen doğal felaketler yaşanıyor ise de, endüstri devriminden sonra dünya çok farklı felaketlerle karşı karşıya gelmiş ve yeni bir felaket tanımının yapılmasına neden olmuştur, bu da "Endüstriyel Felaketler"dir.

Seveso II Direktifine göre, "Önemli Kaza" terimi Direktif kapsamındaki herhangi bir yerde çalışmanın sürdüğü anda kontrol dışında meydana gelen gelişmeler sonucunda oluşan ve insan hayatı ve/veya çevre üzerinde ani veya sonradan ortaya çıkan etkilere sahip, tesisin içinde veya dışında ve bir veya birkaç tehlikeli maddeyi içeren önemli bir sızıntı, yangın veya patlamayı belirtmektedir.

Tüm dünyadaki risk değerlendirme metodolojilerine yani yöntem bilimlerine ve standartlara baktığımızda ise 150'den fazla yöntem bulunduğunu görürüz. Bu yöntemlerin bir çoğu ihtiyaçtan doğmuştur, özellikle de sigorta şirketleri, üniversiteler, enstitüler ile NASA'nın bu yöntem bilimlerin çeşitlenmesinde büyük rolleri olmuştur. Endüstriyel fabrikaları sigortalayan şirketler bu fabrikalardaki iş sağlığı ve güvenliğini ilgilendiren tehlikeler, yangın, patlama, deprem, sel, çevre felaketi vb. konulardaki risklerinin net olarak tayin edilmesini istemiş ve bir çok yöntemin geliştirilmesinde öncülük yapmışlardır. Örneğin Zürih Sigortanın geliştirdiği Zürih Tehlike Analizi, DOW Chemical Co.'nun geliştirdiği DOW F&EI indeksi gibi. Risk değerlendirme metodolojilerini sınıflandırmaya çalışırken öncelikle hangi amaca hizmet ettikleri ve kullanıldıkları alanların dikkate alınması gereklidir, bu kriterlere göre risk değerlendirme metodolojilerini Şekil 1'deki şekilde sınıflandırabiliriz.



Şekil 1- Risk Değerlendirme Metodolojilerinin Sınıflandırılması (Özkılıç, 2008:14)

Bugün için dünyada kullanılan pekçok risk değerlendirme yönteminde riskin gerçekleşme olasılığı hakkında basit ve doğrusal dış değer biçme (linear extrapolation) mekanizmasıyla risk limitleri hakkında "Tahmin Yürütme" eğilimi mevcuttur. Ancak risk değerlendirme yöntemleri uygulanırken, bilinen olasılık dağılımları veya simülasyonları ile hareket etmediğimiz takdirde, riskin gerçekleşme olasılığına ilişkin tahminimiz, bu tahmine duyduğumuz güven ve risk öncelik katsayısına dair tahminimiz subjektif nitelikte olucaktır. Bu nedenlede işyerlerinde risk değerlendirme çalışmaları yapılırken mümkün olduğu kadar kalitatif yöntemler yerine kantitatif yada yarı kantitatif yöntemlerin olasılık ve güvenilirlik teoremleri ile birlikte kullanılması yerinde olucaktır. Bu şekilde yapılan çalışmalar sağlam temeller üzerine oturacak ve her nekadar tüm riskleri sıfırlamamız mümkün değilse de mümkün olduğu kadar sıfıra yakınsayacaktır.

Bir sistemde veya makinede ortaya çıkan arızalar, zamanında müdahale edilmezse, ikincil arızalara neden olur ve daha sonra sistemin katastrofik bir şekilde devre dışı kalmasıyla gelişir. Kritik sistemlerde hataların ne kadar ciddi boyutta insani ve ekonomik sonuçlar doğurabileceğini ancak güvenilirlik analizi yaparak anlayabiliriz. Güvenilirlik teorisi, olası sistem aksaklıkları hakkında genel bir teoridir. Araştırmacılara ve mühendislere, sistemlerinde ve sistemin elemanlarında meydana gelebilecek aksaklıkların, bu sistemin ömrünü ve belirlenmiş standartlara göre işletim kabiliyetini etkileyen faktörlerin tahmin edilmesini sağlar. Bir sitemin güvenilirliği ise, sistemin oluşturulması sırasındaki hatalardan kaçınmak, sistem kullanımda iken hataları belirleyip düzeltmek ve işlevsel hataların vereceği zararı kısıtlamak ile başarılabilir.

Bir elemanın arızalanması, sistemi tamamen devre dışı bırakabileceği gibi sistemin davranışına hiçbir etkisi de olmayabilir veya sistemin kapasitesinde (performansında) bir düşüşe yol açabilir. Kritik sistemlerin en temel özelliği yüksek bir güvenilirliğe sahip olmaları gerekliliğidir. Bu nedenlede kritik sistemler, sistemin kullanış amacına göre kullanılabilirlik,

doğruluk, hatasızlık, güvenlik, güvenilirlik konularına daha fazla önem vermek zorundadır. Bir sistemde güvenilebilirlik ve kullanılabilirlik gerekli görülürken çalışabilirlik ve güvenlik için kesin şartlar yoktur.

Günümüzde özellikle kritik risklere sahip işletmeler için sadece acil eylem planları oluşturulmasının yeterli olmadığı görüşü hakim olmaktadır. Özellikle ülkemizde de Çevre ve Orman Bakanlığı tarafından taslağı hazırlanarak yönetmelik olarak yürürlüğe girecek olacak "Büyük Endüstriyel Kazaları Önleme Yönetmeliği" çerçevesinde acil eylem planlarının, felaket senaryoları oluşturularak olası felaket durumundan geri dönüş planları içermesi gerekecektir.

Bu değerlendirme çerçevesinde, işyeri veya organizasyon için müdahale gerektiren en önemli riskler ortaya çıkarılabilir ve öncelikle bu riskler üzerine odaklanılması sağlanarak, etkileri ve olasılıkları değerlendirilir. Bu çalışmalar sonucunda ortaya çıkacak risk haritası ilgili tüm taraflarla da paylaşılarak bilinçlendirme sağlanır.

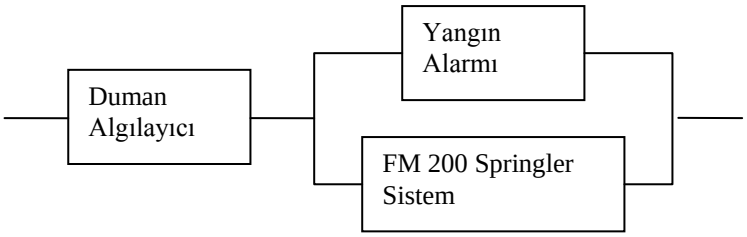
Kayıpların hangi noktalarda oluşabileceğinin belirlenmesi en önemli aşamadır. Bunun için işyeri birimleriyle görüşülmesi, mevcut olanakların, süreçlerin, proses ekipmanlarının, makina parkının, sistem tasarımlarının incelenmesi, açık noktaların ve tehditlerin araştırılması, simülasyon tekniklerinin kullanılması gerekebilecektir. Ancak değerlendirme yapılırken, kritik olmayan sistem ve süreçlerle vakit kaybedilmemesi gerekir. Örneğin, bir kimya fabrikasında kritik önem taşıyan proses koşulları veya kontrol odası yada yangın tesisatı dururken, atelye kısmına yada ofis kısmına veya yemekhaneye öncelik tanımak doğru bir yaklaşım olmayacaktır. Felaket senaryoları ile çalışmak zaman alıcı bir çalışma olabilir, ancak bu analizlerde, riskin gerçekleşme sıklığı, yaşanabilecek kaybın önem ve şiddeti, toplam kayıpların hesaplanması ve riskin gerçekleşme zamanı konuları üzerinde durulmalıdır. Bunlarla ilgili veri mevcutta tutulmuyor olabilir ama zaman içinde sağlıklı analiz için bu bilgilerin tutulmaya başlanması önemlidir.

Tüm bu çalışmalar yapıldıktan sonra olası tehditler dikkate alınarak, "Tehdit gerçekleşirse işyerindeki kritik sistemlerin kaybı ne olur? Bu kayıpları ve/veya olayın etkilerini en aza indirgeyebilmek için önceden ne tür tedbirlerin alınması gerekir?" şeklindeki soruların netleştirilmesi gerekir. Son aşamada ise alınan önlemler sonucunda kabul edilebilirlik derecelendirmesinin yapılması şarttır.

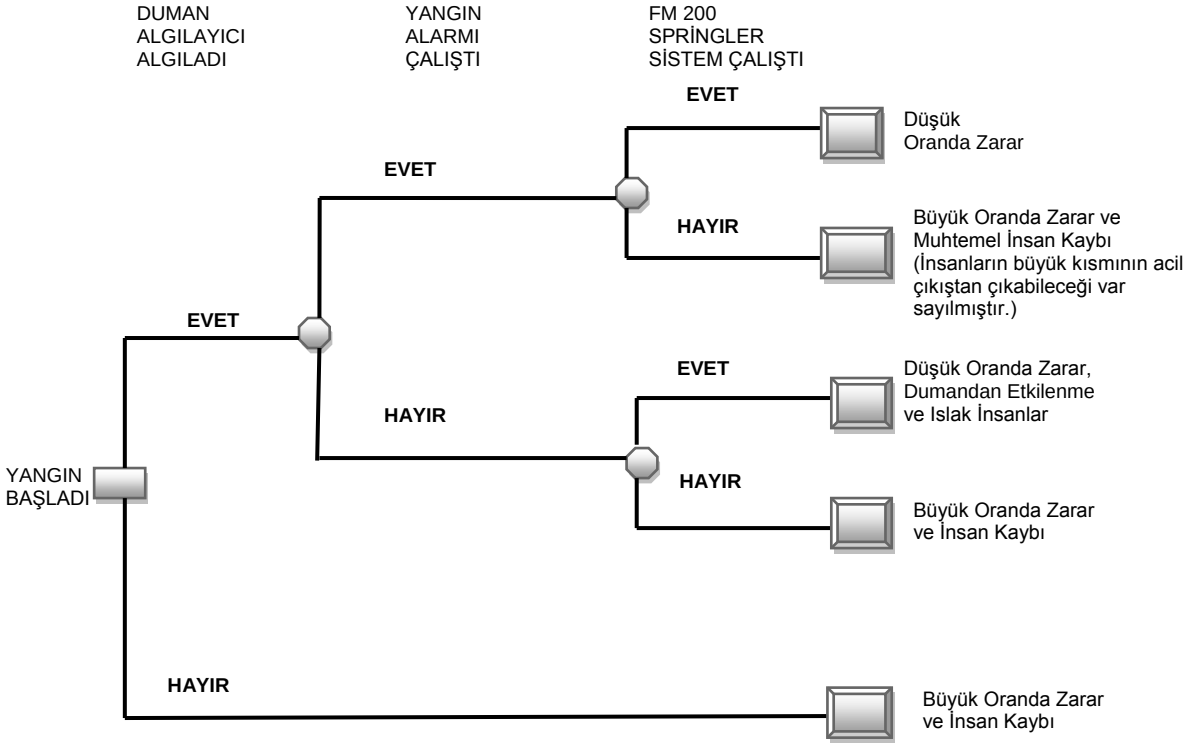
Kritik sistemlerde uygulanabilecek yöntemlere bir uygulama örneği olarak bu bildiride Olay Ağacı Analizi (Event Tree Analysis) seçilmiş ve örnek bir uygulama yapılmıştır. Olay Ağacı analizi, başlangıçta seçilmiş olan olayın meydana gelmesinden sonra ortaya çıkabilecek sonuçların akışını diyagram ile gösteren bir yöntemdir. Hata ağacı analizinden farklı olarak bu metodoloji tümevarımlı mantığı kullanır.

Örnek olarak bir fabrikada kritik bir sisteme güç sağlayan elektrik dağıtım odası ve jeneratör dairesinde mevcut bulunan yangın sisteminin analizi yapılacaktır. Diyelim ki yangın sistemi şu şekilde çalışmaktadır; elektrik dağıtım odası ve jeneratör dairesinde içerisinde oluşabilecek muhtemel bir yangında duman algılıyıcılar algılama yapmakta ve FM 200 springler sistemi ve yangın alarmını çalıştırmaktadır. İşletmede yangın başlamasından sonra duman algılayıcının dumanı algılaması, yangın alarmının çalışması ve springler sisteminin devreye girerek yangını söndürmesi gerekmektedir. Yapılacak analizde bu üçlü sistemin açıklıkları görülmeye çalışılacaktır.

Güvenilirlik Blok diyagramını çıkarıcak olursak;



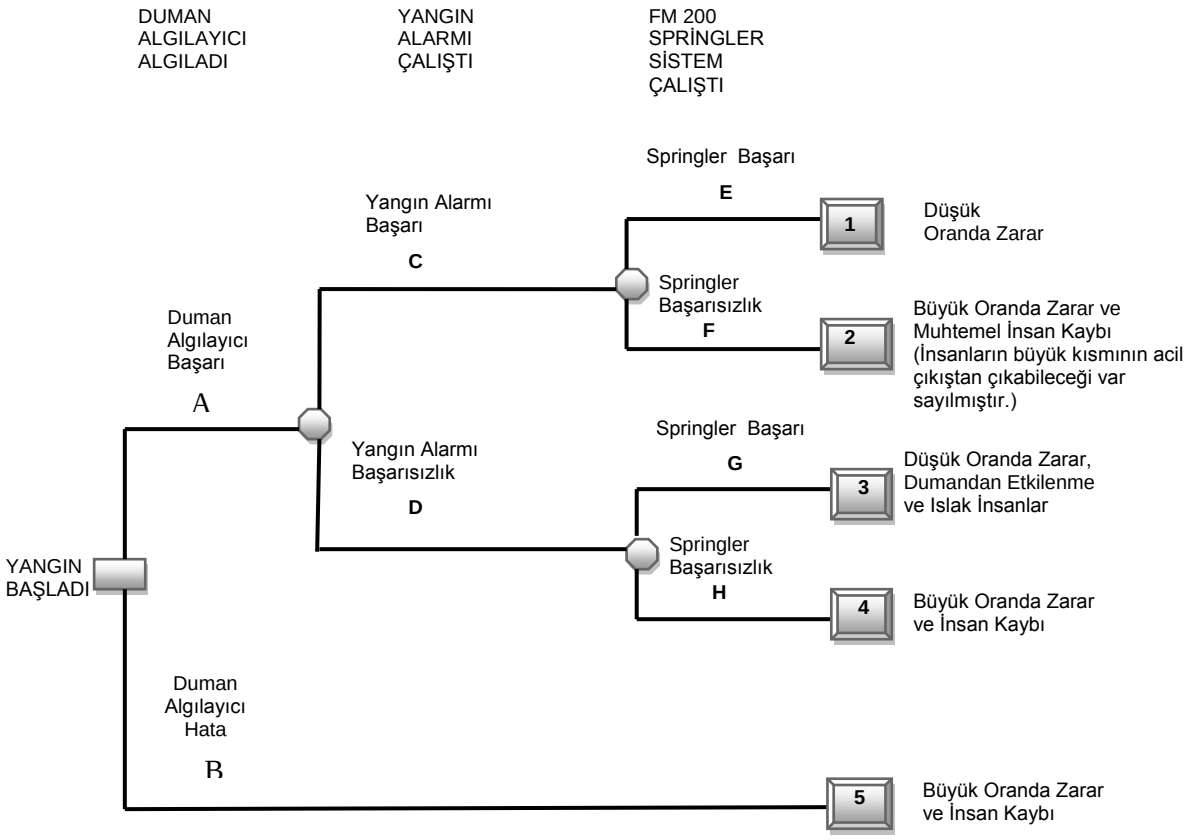
Şekil 2- Güvenilirlik Blok Diyagramı



Şekil 3- Sistemin Olay Ağacı Analizi

Olay Ağacı Analizinde sistem içindeki tüm güvenilir operasyonal değişimler tanımlanır. Her bir yol takip edildiğinde nihai başarı veya hataya götürür. Yapılan analiz sonucunda her bir dal için olasılık hesapları yapılır, özellikle büyük oranda can ve mal kaybına neden olabilecek durumlar için sistemin yedeklenmesi gerekmektedir.

Örneğimizde duman algılayıcının hatasına W1, yangın alarmının hatasına W2 ve springler hatasına da W3 diyecek olursak;



Sistemi incelediğimizde 2, 4 ve 5. Durumlarda sonucun büyük oranda zarar ve insan kaybı ile sonuçlandığını görmekteyiz. Öyleyse 2, 4 ve 5. sonuçların hata olasılıklarını olasılık teoremlerini kullanarak hesaplayacak olursak;

2. Sonuç için;

A dalının basarı olasılığı; (1-W1)

C dalının basarı olasılığı; (1-W1)(1-W2)

F dalının hata olasılığı; W3(1-W1-W2+W1W2)

4. Sonuç için;

A dalının basarı olasılığı; (1-W1)

D dalının hata olasılığı; (1-W1).W2

H dalının hata olasılığı; W3(W2-W1.W2) olarak buluruz.

5. Sonuç için;

B dalının hata olasılığı; W3 olarak bulunur.

Duman dedektörünün algılamadığı 5. sonucu ele aldığımızda duman algılayıcının çalışmaması durumunda diğer iki sistemin birden devre dışı kaldığı ve büyük oranda zarar ile insan kaybı ile karşılaşmanın mümkün olduğu görülmektedir ki bu durum kabul edilemez. Bu nedenle de duman algılayıcının ısı algılayıcı ile yedeklenmesi gibi çözüm üretilmesi uygun olacaktır.

SONUÇ:

Bir sistem, kendi başına bir bütün, ayrı ayrı alt sistemlerden oluşmuş bir kompleks ya da farklı yerlerde kurulmuş alt sistemleri birlikte içeren endüstriyel bir düzen olabilir. Kazaların nedenleri incelendiğinde çoğu zaman çok basit bir hata ile karşılaşılmakta ve bu denli küçük bir hatanın felaketleri doğurduğu görülmektedir.

Her teknolojik gelişmeyle birlikte yeni sorunlar ortaya çıktığı gibi bu yeni sistemlerinde ortaya çıkaracağı sorunlar bulunmaktadır. Tüm sistemlerin hatası kullanıcıyı zor durumda bırakır, ancak her hata çok ciddi ve uzun süreli hasarlara yol açmaz. Fakat bazı sistemlerin hatası ciddi ekonomik kayıplara, fiziksel hasarlara veya insan hayatını tehdit edebilecek sonuçlara neden olabilir. Güvenilirlik ise işte bu aşamada gündeme gelir ve güvenilirlik sorunları tek tek incelenmesi ve değerlendirilmesi gereken sorunlardır.

Literatür taraması yapıldığında kritik sistemlerin risklerinin değerlendirilmesi amacıyla kullanılabilecek bir çok yöntem ve analiz tekniğinin bulunduğu görülmektedir. Teknolojik gelişmeler sonucunda özellikle makineler, proses kontrol ekipmanları, yangın sistemleri, otomatik söndürme sistemleri ya da organizasyonel bir sistem vb. tüm ekipmanlar ve fonksiyonlar için yapılacak risk değerlendirmelerinde güvenilirlik değerlendirmesi yapılması mutlak suretle gereklidir. Özellikle de Hata Ağacı Analizi, Olay Ağacı Analizi, Neden Sonuç Analizi, Olası Hata Türleri ve Etki Analizi, Tehlike ve İşletilebilme Çalışması (HAZOP), Zürih Tehlike Analizi, Markov Simülasyonu vb. risk değerlendirme analizlerinde sistem analizi ve güvenilirlik değerlendirmelerinin büyük önem arz ettiği görülmektedir.

Yeni mevzuatımız işverenlere ve işletmelerde görev yapan işveren vekillerine kendi işyerlerindeki tehlikeleri belirleme ve bu tehlikelerin meydana gelme ihtimalini kabul edilebilir bir seviyeye indirme yükümlülüğü getirmiştir. Örneğin Alman hukukunu inceleyecek olursak, risk ile ihtiyatın tanımının yapılmış olduğunu ve seçim hakkının işverene verildiği görülür.

"Hukuk kesin bulgular beklenene kadar, hareketsiz kalmayı kabul edemez. "Tehlike" kavramı esas alınarak, önlemler alınmalıdır, "İhtiyat" ilkesinin özü de budur. Risk; tehlikeyi göze almak, ihtiyat ise riski dikkate alarak önlemleri düşünmektir. Risk ile ihtiyat arasındaki seçim işverene aittir." Bu aşamada yeni mevzuatımız da aynı Alman hukukunda olduğu gibi risk alma ile ihtiyat arasında seçim yapma şansını işveren veya işveren vekillerine tanımıştır.

KAYNAKÇA:

1. ASHRAE Applications Handbook (1984) "System", UK
2. MIL-HDBK-189 Military Handbook (1990) "Reliability Growth Management", USA
3. Özgüven, E., (2003) Endüstri Psikolojisi; PDREM Yayınları, Ankara
4. Özkılıç, Ö. (2005) İş Sağlığı ve Güvenliği Yönetim Sistemleri ve Risk Değerlendirme Metodolojileri; TISK, Ankara
5. Özkılıç, Ö. (2007) İş Sağlığı, Güvenliği ve Çevresel Etki Risk Değerlendirmesi; MESS, İstanbul
6. Özkılıç, Ö. (2008) "Yeni İş Sağlığı ve Güvenliği Mevzuatı Çerçevesinde Risk Değerlendirmesi", *İş Güvenliği Dergisi*, İSGİAD, 29 (3) 10-14
7. Rostamzadeh B., Lönn H., Snedsbøl R., Torin J., (1999) A Distributed Computer Architecture for Safety-Critical Control Applications, New York, DACAPO
8. Sabancı, A. (1999) Ergonomi; Baki Kitabevi, Adana

9. Sommerville I. (2004) Software Engeneering 7th Edition Capter 3, London, Addison Wesley Longman

10. TS ISO/IEC 27001 (2006) Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler, TSE, Ankara

11. TS EN ISO 12100-1 (2007) Makinalarda Güvenlik - Temel Kavramlar, Tasarım İçin Genel Prensipler - Bölüm 1: Temel Terminoloji, Metodoloji, TSE, Ankara

12. TS EN ISO 13849-1 (2004) Makinelerde Güvenlik- Kumanda Sistemlerinin Güvenlikle İlgili Kısımları- Bölüm 1: Tasarım İçin Genel Prensipler, TSE, Ankara