ÇSGB

T.C. ÇALIŞMA VE SOSYAL GÜVENLİK BAKANLIĞI

İş Teftiş Kurulu Başkanlığı

KİMYA SANAYİ SEKTÖRÜNDE SEVESO II DİREKTİFİ KAPSAMINDAKİ ENDÜSTRİLERDE KAZA RİSKİ DEĞERLENDİRME METODOLOJİSİ

Yayın No.55

ÇSGB

T.C. ÇALIŞMA VE SOSYAL GÜVENLİK BAKANLIĞI

İş Teftiş Kurulu Başkanlığı

ARAMIS

SEVESO II DİREKTİFİ KAPSAMINDAKİ ENDÜSTRİLERDE KAZA RİSKİ DEĞERLENDİRME METODOLOJİSİ: ARAMIS (Accidental Risk Assessment Methodology For IndustrieS) KULLANICI REHBERİ

2012 / Kasım

Ankara

ÖNSÖZ

Avrupa Birliğinde, SEVESO II Direktifi kapsamında yer alan kuruluşların yapacakları risk değerlendirmelerinde "Olası Kaza Senaryolarının Tanımlanması" önemli bir unsur teşkil etmektedir. Bu kuruluşların risk değerlendirme çalışmalarına nereden ve nasıl başlamaları gerektiği ile olası kaza senaryolarını nasıl belirleyecekleri hususlarına ilişkin bir takım belirsizliklerin bulunması sebebiyle hem bu belirsizlikleri gidermek hem de ilgili taraflara yol gösterici olmak amacıyla Avrupa Birliği'ne üye ülkeler tarafından ortaklaşa olarak ARAMIS metodolojisi geliştirilmiştir.

Ülkemizde 18.08.2010 tarihli ve 27676 sayılı Resmi Gazetede yayınlanan Büyük Endüstriyel Kazaların Kontrolü Hakkında Yönetmelik kapsamında yer alan kuruluşların, büyük kaza önleme politika belgesi veya güvenlik raporu hazırlaması sırasında tehlike ve risklerin nasıl değerlendirileceği, olası kaza senaryolarının nasıl belirleneceği gibi yönetmelikten kaynaklanan yükümlülüklerini yerine getirirken karşılaşacakları bir takım belirsizlikler bulunmaktadır. Ayrıca, söz konusu belgelerin yetkili otoriteler tarafından kabul edilen bir metodoloji çerçevesinde hazırlanması gerekmektedir. Kullanılan metodolojiler, risklerin belirlenmesi bununla birlikte bu riskleri azaltmada kullanılan yöntem ve araçların etkinliği ve bu risklerin sürdürülebilir bir şekilde yönetilebilmesi ile ilgili geçerli, uygun ve kullanışlı bilgiler içermelidir. Yetkili otoritelerce belirlenen risklere ilişkin sonuç-etki modellemelerinde kaza senaryolarının nasıl seçildiği bilgisinin de sunulması gerekmektedir.

Tüm bu sebeplerle ARAMIS Metodolojisi Kullanıcı Rehberinin esas olarak sanayi kuruluşlarına, yetkili denetim birimlerine ve ilgili tüm otoritelere referans kaza senaryoları ile büyük kazalara ait risklerin tanımlanmasında, bunlara ilişkin güvenlik önlemlerinin belirlenmesinde ve bu güvenlik önlemlerinin performansların tayininde ayıca kaza sonuç-etki modellemeleri ile risklere ilişkin tesis çevresinde risk maruziyetinin sonuçlarının değerlendirilip gerekli planlamanın yapılabilmesinde yol gösterici olması amacıyla İş Teftiş Kurulu Başkanlığımız tarafından tercüme edilerek bir kitap haline getirilmesi kararlaştırılmıştır.

Bu kitabın hazırlanmasında emeği geçen; İş Teftiş Kurulu Başkan Yardımcısı Halil İbrahim ÇEVİK'e, İş Baş Müfettişi Özlem ÖZKILIÇ'a ve İş Müfettişi Yardımcıları Faruk SEVEN, Neslihan BABAARSLAN, Oğuz AYDIN, Z.Burcu MERCAN, Anıl HASDEMİR, Hamza SAYAN, Hüseyin Baran AKINBİNGÖL, Fatma Betül BAKKAL, Pelin TEMEL, Emrah GÖKALP, Altuğ CEYLAN, Serhenk ÇELİK, Önder EMNECAR ve Hilal YÜRÜK'e teşekkür eder, hazırlanan bu rehber kitabın tüm sanayi kuruluşları ile yetkili denetim birimleri ve makamlara faydalı olmasını dilerim.

Mehmet TEZEL
İş Teftiş Kurulu Başkanı

“Çalýþmadan, öðrenmeden, yorulmadan, rahat yaþamanýn yollarýný alýþkanlýk haline getirmiþ milletler; önce onurlarýný, sonra özgürlüklerini, daha sonra da geleceklerini kaybetmeye mahkumdurlar.”

M. Atatürk

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİL LİSTESİ

KISALTMALAR

ARAMIS: Accidental Risk Assessment Methodology For Industries

ASSURANCE: ASSessment of the Uncertainties in Risk Analysis of Chemical Establishment

ALARP: As Low As Reasonably Practicable

ALARA: As Low As Reasonably Achievable

EC-JRC: European Commission's Joint Research Centre

EU: European Union

GIS: Geographical İnformation System.

INERIS: Institut National de l'Environnement Industriel et des Risques (French National Instiute for Industrial Environment and Risks)

IPSC: The Institute for the Protection and Security of the Citizen

MAHB: The Major Accident Hazards Bureau

FPMs-MRRC: Faculté Polytechnique de Mons Major Risk Research Center.

UPC: Polytechnic University of Catalonia

CERTEC: Universitat Politecnica de Catalunya

RISOE: Risoe National Laboratory

VSB: Technicka Univerzita Ostrava

CMI: Central Mining Institute

IChemE: Institution of Chemical Engineers

EFCE: European Federation of Chemical Engineering

EPSC: The European Process Safety Centre

SMS: Safety Management System

RAS: Reference Accident Scenarios

STAT: The Substance State

HAZOP: Hazard and Operability Study

LC: Level of Confidence

SIL: Safety Integrity Level

IEC: International Electrotechnical Commission

SFF: Safe failure fraction

PFD: Probability of Failure on Demand

SCQPI: Safety Culture Questionnaire for Process Industries

VCE: Vapour Cloud Explosion

TEEL: Temporary Emergency Exposure Limits

INSEE: French National Institute for Statistics and Economic Studies

ISTAT: The National Institute for Statistics

APAT: Agency for Environmental Protection and Technical Services

ZNIEFF: Natural zone of faunistic and floristic interest in France

LFL: Lower flammability limit

LOC: Loss of Containment

ÖZET

Aramis Projesi 2001 yılının şubat ayında, Avrupa Komisyonu tarafından desteklenen, "Enerji, Çevre ve Sürdürülebilir Gelişme" alanındaki "Araştırma ve Teknolojik Gelişim için V. Çerçeve Programı" kapsamında, "Büyük Doğal ve Teknolojik Tehlikelerle Mücadele" başlıklı bölümü ile ilgili kabul edilmiştir. 3 yıl sürecek bu projeye, 2002 yılının Ocak ayında başlanmıştır. Bu proje, Avrupa Birliği tarafından desteklenen ve dördüncü çerçeve programı kapsamında düzenlenen ASSURANCE ve I-RISK projelerinin sonuçları üzerine kurulmuştur.

ASSURANCE kelimesi, "Kimya Kuruluşlarına ait Risk Analizinin Tutarsızlıklarının Değerlendirilmesi" anlamına gelen ingilizce proje başlığının baş harfleri kullanılarak oluşturulmuştur. Bu proje, bir kıyaslama çalışması olarak, risk analizi ile ilgili tutarsızlıkların kaynağının ve tipinin anlaşılmasında gelişme sağlamak amacını taşımaktadır. Proje sonuçlarına göre, istenmeyen sonuçların değerlendirilmesinde ve meydana gelme olasılıklarının tayininde çelişkiler görülmektedir. Bu çelişkiler ile ilgili risk temelli kararların değerlendirilmesinin, arazi kullanım planlanmasının, acil durum planlamasının ve risklerin kabul edilebilirliğinin gerekliliği (ALARP veya ALARA) de açıkça görülmektedir.

I-RISK projesi fikri, kantitatif risk değerlendirmesi ile güvenlik denetiminin, büyük kazaların kontrolünde iki ayrı değerli araç olduğu düşüncesinden ortaya çıkmıştır. Bu nedenle ana hedef, risklerin kontrolü ve izlenmesi için bir yönetim modeli geliştirmek ve daha sonra bu modeli dinamik yapıda olan kantitatif risk değerlendirmesi yöntemine dahil etmektir. Projenin sonucunda tümleşik teknik ve yönetime dayalı bu modelin çok sağlam olduğu ve denetim kurumlarına yeni bir yol gösterdiği açıkça görülmüştür.

Bu iki proje ve katılımcı ülkelerde gerçekleşen olaylardan edinilen tecrübelerle birlikte, her bir tesis işleticisine özgü büyük kaza senaryolarının tespiti ile bunları hem engelleme hem de hafifletme önlemlerini dikkate alan ve tutarlı kurallara dayanan bir yöntemin gerekliliği ortaya çıkmıştır. Ayrıca bu yöntem ile güvenlik önlemleri bir güvenlik yönetim sistemi içinde kontrol edilebilir hale gelecektir. Hem yetkili kuruluşların risk uzmanları hem de endüstri kökenli risk uzmanları arasında uzlaşma oluşmasını sağlayacak, risk tabanlı kararların verilmesinde tutarsızlıkları azaltacak bir risk değerlendirme metoduna olan gereksinim de böylece ortaya çıkmıştır. ARAMIS projesi de, bu gereksinime çözüm yolu sunmak amacıyla başlamıştır.

Bu doküman, öncelikle Avrupa Birliğinde büyük kazaların meydana gelmesine sebep olacak tehlikelerin önlenmesi konusuna değinecek, daha sonra, ARAMIS'in genel olarak hedefleri ve uygulanması için gerekli olan bilgileri detaylıca sunacaktır.

SEVESO II DİREKTİFİNİN İÇERİĞİ

Avrupa Çevre Ajansının 1999 yılında yayımlanan raporunda, dikkat çeken en önemli nokta büyük kazalardaki eğilimin son yirmi yıldır aynı olduğudur. Bu ifade bile, tek başına, çoğunlukla görünüşte basit ve "gerekli derslerin alındığı" kazaların, endüstriyel standartlara etki etmediğini ortaya koymaktadır. Şüphesiz ki, Avrupa Birliği ülkelerinde felaketler yine gerçekleşmeye devam edecektir. Bu felaketlerin bazıları teknolojik sebepler, bazıları da doğal afetler sebebiyle meydana gelmektedir. Risk değerlendirmesi anlamında, düşük olasılıklı ancak yüksek etkili kazalar konusu hala ana sorun olarak görülmektedir. Buna rağmen tehlikeler doğru yönetilmeli ve böylece risk azaltılabilmelidir.

SEVESO II direktifi, insanları ve çevreyi büyük kazalardan korumak için yayımlanan en önemli AB direktifidir. Bu direktif, endüstride "önemli miktarda tehlikeli madde" kullanan kuruluşlara uygulanmaktadır. Kuruluşların yönetim mercileri özellikle, büyük kaza önleme politikasını uyguladıklarını ve bir güvenlik yönetim sistemi içinde, kontrol edilen ve izlenen uygun önleme ve azaltma önlemlerini gerçekleştirdiklerini göstermelidirler.

SEVESO II direktifi, büyük kaza tehlikelerin yönetimine ilişkin net amaçlar ortaya koymaktadır. Fakat bu noktada "bu amaçlara nasıl ulaşılacak ve ulaşıldığı nasıl kontrol edilecek?" gibi bir soruyla karşılaşılmaktadır. Örneğin, risk değerlendirmesinde kullanılmak üzere, kaza senaryolarının uyumlaştırılmış halini tanımlayan bir ifade yoktur. Bu bağlamda, ASSURANCE projesi, seçilmiş senaryoların uzmanların değerlendirmesine, tecrübesine ve direktifi uygulayan üye ülkenin deterministik ya da risk odaklı yaklaşımına göre farklılık gösterdiğini ortaya koymaktadır. Dahası, arazi kullanım planlamasındaki kısıtlar, kimi zaman operatörleri "gerçekçi" senaryoları seçerek ve ilgili güvenlik araçlarının etkinliğini düşünerek, güvenlik bölgelerin azaltılmasını düşünmeye sevk etmektedir. Aslında, senaryoların belirlenmesi ve risk analizinin gerçekleştirilmesi ile ilgili kuralların eksikliği uzmanların işini genellikle karmaşıklaştırmakta ve şeffaf risk odaklı kararlara dayanmayacak kadar çok öznel hale getirmektedir.

Risk analizindeki belirsizliklere ek olarak, üye ülkeler arasındaki kültürel farklılıklar, yaklaşım ve yöntemlerde çeşitliliğe neden olmaktadır. Yakın zamanda gerçekleştirilen uluslararası bir çalıştayda katılımcıların bir çoğu, uyumlaştırılmış prosedürlerle beraber karşılaştırmalı risk değerlendirmesinin karar mekanizmalarının anlaşılmasına önemli ölçüde yardım edeceği hususunda uzlaşmışlardır. Böylece uyumlaştırılmış bir risk değerlendirme metodolojisi, risk temelli karar almanın gerekli şeffaflığı ve bilimsel anlayış ile önlem ilkesi arasında doğru bir denge sağlamasını mümkün kılmaktadır..

Risk değerlendirmesi için bir uyumlaştırılmış bir metodoloji tasarlamak oldukça zor ve karmaşık bir görevdir. Bununla birlikte deterministik ve olasılıksal yaklaşımlar da çoğunlukla bütünleyici oldukları için birbirinin karşıtı olarak görülmemelidir. Tarihsel bir bakış açısından deterministik metotlar öncelikle tesisin güvenli tasarlandığını kontrol etme imkanı sağlar. Olasılıksal metotlar ise tesisin kurulum sonrasında kalan risklerinin değerlendirilmesine yardımcı olur. Her iki yaklaşımın da güçlü ve zayıf noktaları bulunmaktadır. ARAMIS projesinin temel fikri, bu iki yaklaşımın güçlü taraflarını alarak, tesise özgü güvenlik bariyerlerinin -savunma hattının- değerlendirilmesine dayanan alternatif bir yarı kantitatif yöntem geliştirmektir.

HEDEFLER

ARAMIS projesinin ana hedefi, Avrupa Birliği ülkelerinde hâlihazırda kullanılan risk değerlendirme yöntemlerinin güçlü yanlarını birleştirerek, yeni bir bütünleşik risk değerlendirme metodu oluşturmaktır. Bu nedenle meydana gelecek metodun, tüm Avrupa Birliğinde, risk odaklı karar verenler tarafından desteklenen ve risk uzmanları tarafından kullanılan ve tavsiye edilen bir araç olması için deterministik veya risk temelli yaklaşımın benimsendiği farklı ulusal kültürlerde de kabul görmesi amacıyla olabildiğince esnek ve geçerli bir yöntem olması hedeflenmiştir.

ARAMIS projesi ile önerilen metot, üç ayrı ve bağımsız indeksten oluşan, bütünleşik bir risk indeksi tanımlanmasını olanak sağlamalıdır. İndeks 1, ilk kez tanımlanmış referans senaryolarının

sonuç şiddetini ve etkisini değerlendirmektedir. İndeks 2, yarı kantitatif bir bakış açısıyla referans senaryonun gerçekleşme olasılığını dikkate alınmasına olanak sağlayan önleme yönetim etkinliğini değerlendirmektedir. İndeks 3, SEVESO kuruluşunun çevresinde yer alan potansiyel hedeflerin duyarlılığını değerlendirerek çevresel hassasiyeti tahmin etmektir.

Proje, risk indeksinin mantıksal kurulumunu yansıtmak amacıyla kurulmuş ve aşağıdaki gibi maddeler halinde çalışma paketlerine bölünmüştür;

- İlk hedef, "referans" kaza senaryolarını tanımlamak için bir yöntem geliştirmektir. Bu senaryolar, SEVESO II güvenlik raporunda kullanılacak, üzerinde anlaşmaya varılmış "gerçekçi" senaryolardır. Bu senaryolar etkinliklerine göre tesisin önleme ve hafifletme önlemlerini de dikkate alırlar.
- İkinci hedef, üç ayrı indeksten oluşan bütünleşik bir risk indeksi kurmaktır. Bu üç indeks;
- Kaza sonuç şiddetinin değerlendirilmesi,
- Önleme yönetim etkinliği,
- Çevresel hassasiyetin tahmin edilmesi.

ÇALIŞMANIN AÇIKLAMASI

Bu projenin çalışma planı, son hali verilmiş risk indekslerinin mantıksal kurulumuna göre oluşturulmuş olup, doküman boyunca da aynı şekilde sunulmuştur.

Projeye biçilen sürenin yarısına gelindiğinde, yeni oluşturulan yöntem, Avrupa'da kurulu SEVESO kapsamındaki üç farklı endüstriyel tesis üzerinde test edilmiştir. Bu aşamada, Doğu Avrupa'dan iki ülkenin konsorsiyuma katılması ve her biri bir ülkenin kuruluşlarından olacak şekilde tarafsız işletmeler üzerinde tüm yöntemin testinin yapılması sağlanmıştır.

ARAMIS'in uyumlaştırılmış risk değerlendirme metodolojisinin Avrupa'da tümüyle kullanılması amacıyla destekleyici bir araç olarak sunulması ve proje başlangıcından itibaren yöntemin birbirinden farklı birçok nihai kullanıcı tarafından uygulanmış olması nedeniyle, metodoloji başlangıçtaki haline göre büyük oranda değişikliğe uğramıştır. Belirlenmiş nihai kullanıcılar, hem endüstriyel firmalar hem de SEVESO II direktifini uygulamaktan sorumlu yetkili kuruluşlardır. Bu yüzden, projenin ilerleyişinin ve sonuçlarının değerlendirilmesi, özel bir çalışma paketi vasıtasıyla yapılmaktadır. Endüstriyel katılımcılar, doğrudan konsorsiyuma dahil edilmiş ve bir araya gelen olası son kullanıcılardan paralel bir gözden geçirme ekibi oluşturulmuştur.

BÜYÜK KAZA TEHLİKELERİ KONTROL VE ÖNLEME İÇERİĞİ

AB direktifleri arasında, insanları ve çevreyi büyük kazalardan korumaya en çok yardım eden direktif; SEVESO II direktifidir. Bu direktif önemli miktarda tehlikeli madde kullanan endüstriler için geçerlidir. Bu endüstrilerdeki yöneticiler büyük kazaların önlenmesinde, "donanımsal" ve "yazılımsal" ölçümleri de dahil eden bir güvenlik yönetim sistemi politikalarının olduğunu göstermelidirler. Bu durum, doğal olarak tanımlanması zor olmasına rağmen sadece yüksek olasılıklı ve düşük etkili sonuçlara sahip kazaları değil aynı zamanda düşük olasılıklı ve yüksek etkili sonuçlara sahip kazalardaki risk seviyelerini de düşürmeye eğimli olmalıdır.

Seveso II direktifinde, risk yönetimi açısından amaçlar çok açıktır, ancak asıl soru şudur: Amaçlara nasıl ulaşılır? Örneğin; risk değerlendirmesi için kullanılan senaryoların düzenlenmiş bir tanımı yoktur.

Genellikle seçilen senaryolar, (BLEVE, önlemdeki toplam kayıp, en büyük tankta yangın, büyük kütle halindeki patlayıcı maddenin patlaması, vb.) direktifi uygulayan ülkelerdeki risk analistlerine göre, seçilen risk bazlı yaklaşımlara göre farklılık gösterebilir. Bu durum Avrupa Komisyonu projesi olan ASSURANCE kapsamında altı tane Avrupa ülkesinin belirli bir tesis üzerindeki karşılaştırmalı olarak yaptıkları çalışma sonuçlarında doğrulanmıştır. Bu partner ülkeler tehlike analizi ve çeşitli teknikler kullanmış ve güvenlik yönetimine konu olan esas senaryo için farklı sonuçlara ulaşmışlardır. Dahası arazi kullanım planlama kısıtları, yöneticilerin güvenlik mesafelerini düşürmesine yönelik baskı yapmaktadır. Aslında güvenlik ölçüm etkinliğini içeren senaryoları belirlemede kural eksikliklerinin olması sebebiyle, uzmanın işi zordur ve genellikle kişiye göre değişen öğeler içerir.

Sadece riski değerlendirme uzmanları değil, aynı zamanda karar mekanizmaları da çeşitli yaklaşımların değerlendirmesi ve endüstriyel risk yönetimi ile karşı karşıya kalmaktadır. Üye ülkelerin farklı kültürlerde olması büyük kaza tehlikelerinin değerlendirmesinde metot çokluğuna neden olmaktadır. Bu, farklı analistlerin yaptıkları risk çalışmalarının karşılaştırılmasını ve karar verme amacı için kullanılacak yaygın risk değerlendirmesini belirlemeyi güçleştirir. Mayıs 2000'de İtalya'da düzenlenen son Uluslararası Çalıştayının Teknik Uyumlu Tabanlı Karar Verme Tanıtımı'nda (ECJRC), katılımcıların çoğu, prosedürlerle uyumlaştırılmış karşılaştırmalı risk değerlendirmeleri kullanılmasının karar vermeyi anlamada yardımcı olacağı konusunda görüş birliğine varmışlardır. Uyumlaştırılmış bir risk değerlendirme metodolojisi risk bazlı karar verme sürecinde gerekli şeffaflığı sağlar ve bilimsel anlayış ile tedbir arasındaki doğru dengeyi vurgular.

Risk değerlendirmesi ile uyumlu hale getirilmiş bir metodoloji tanımlamak zordur. Ancak, büyük kazaların meydana gelme olasılığı ile ilgili senaryo tanımlanması, şiddet değerlendirilmesi ve güvenlik yönetiminin entegre edilmesi gibi farklı yaklaşımlar ortak sayılabilir.

PROJE ÇALIŞMA PLANI

ARAMIS'in amacı, girdilerin risk seviyelerini değerlendirmek için işletmeler tarafından uygulanan koruma tedbirlerini dikkate alarak risk değerlendirme metodolojisi geliştirmektir.
Projenin çalışma planı, Referans Kaza Senaryoları ve etkenlerinin tespitine dayanan risk düzeyi tanımlama sonuçlarına göre yapılır:

- Senaryolar sonucu şiddet (etki) değerlendirilmesi,
- Koruma yönetim etkinliği,
- Çevre güvenlik açığı (hasar görebilirliği) tahmini.

Hem sanayi kuruluşları hem de yetkili kuruluşlar metodolojinin nihai kullanıcıları olarak SEVESO II direktifini uygulamadan sorumludurlar.

PROJENİN TANIMLANMASI

Projenin üç ana aşaması şu şekilde açıklanabilir:

1. Metodolojinin geliştirilmesi,
2. Metodolojinin tamamlanması ve test edilmesi,
3. Planın değerlendirilmesi ve yaygınlaştırılması.

METODOLOJİNİN GELİŞTİRİLMESİ

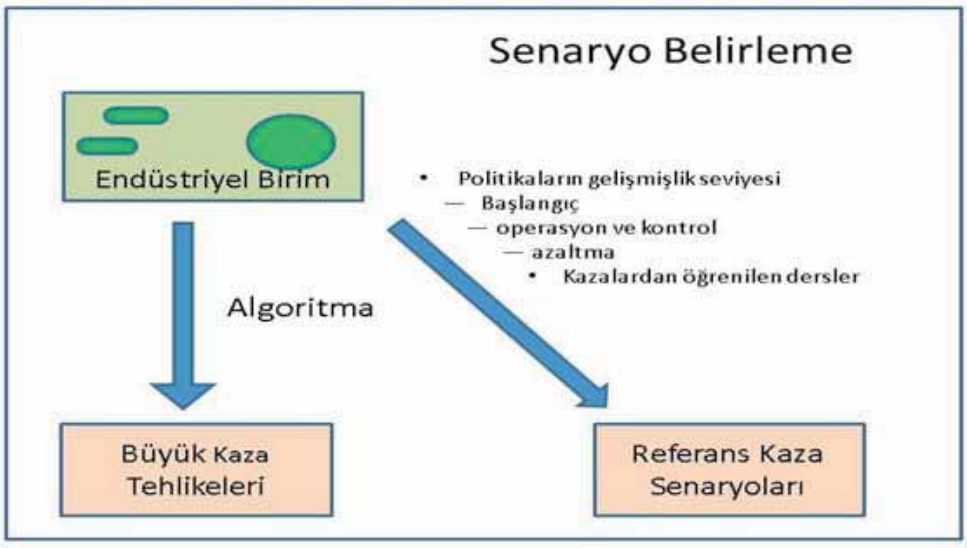
Metodolojinin geliştirilmesi önceden değerlendirilmiş referans senaryolarının tanımlanması ile başlar. Daha sonra önleme yönetim etkinliği ve tesisin çevresel hassasiyeti karakterize edilir. Tüm bu

sonuçlar tesisin risk seviyesini değerlendirmek için bir araya getirilir. Metodolojinin çeşitli aşamaları aşağıda detaylı olarak açıklanmıştır.

SENARYONUN TANIMLANMASI

Bu aşamanın amacı, Kaza Senaryolarının tanımlanması için metot önermektir. Endüstriyel tesisler için, Büyük Kaza Riskleri ilk olarak, maddelerin etiketlenmesine (Direktif 67/548/EEC) ve kullanım durumlarına (sıcaklık, basınç, akış vb.) dayanan algoritma ile tanımlanacaktır. Daha sonra, Referans Kaza Senaryolarından, Büyük Kaza Riskleri geliştirilecek ve benzer işletmelerde meydana gelen kazalar incelenecektir. Referans Kaza Senaryoları tasarım, kullanım, kontrol ve hafifletme aşamalarında yasal gerekliliklerde belirtilen ve mevcut uygulamaları da (en gelişmiş) dikkate alarak belirlenecektir.

Bu nedenle Referans Kaza Senaryoları, Şekil 1'de tanımlanan önleme yönetim etkinliği çalışmalarının sonuçlarını kullanacaktır. Referans Kaza Senaryoları, bugün yerleşik olan tesisleri de göz önünde bulundurarak gerçekçi senaryolar tanımlar. Bunlar büyük kazaların etkilerini (şiddetini) değerlendirmek ve tehlike potansiyelini tanımlamak için kullanılacaktır.



Şekil 1: Senaryo belirleme prosedürü

• SENARYOLARIN SONUÇ ŞİDDETİNİN DEĞERLENDİRİLMESİ

Bu aşamanın amacı, sadece fiziksel parametrelere bağlı olan bir şiddet indeksi S'yi tanımlamaktır. Burada amaçlanan, kazalarda meydana gelen olayların (yayılım, patlama, yangın) fiziksel özelliklerini incelemek ve senaryoların sonuç şiddet değerlendirmelerinde bu olguları da hesaba katmaktır. Dikkate alınan parametreler şunlardır:

- **Olayın etki alanı, A:** örneğin patlamada oluşan basınç halkası, gaz yayılmasında oluşan duman bulutunun yönünü öngörme
- **Olay kinetikleri, K:** patlamalar için hızlı, yayılma ve yangınlar için daha yavaş;
- **Felaketi hafifletmek için müdahale yeteneği, I:** yangın ve gaz yayılımı için mümkün olabilir, fakat patlama için sadece dizayn aşamasında mümkün
- **Domino etkisi potansiyeli, D:** parça emisyonu, geciken olayların birbirlerine etkisi

Bu nedenle şiddet indeksi olan "S" sadece fiziksel olayla ilgili parametredir. Daha sonra tanımlanan tüm senaryolar değerlendirilebilir ve şiddet indeksi, büyük kaza tehlikeleri için S_o ve referans kaza senaryoları için S_{ref} hesaplanamasına göre derecelendirilebilir.

• ÖNLEME YÖNETİM ETKİNLİĞİ

Bu aşamanın amacı, önleme yönetim etkinliğini karakterize eden M indeksini tanımlamaktır. Teknik ve organizasyonel faktörler büyük kazayı önlemede ana unsurlar oldukları için bu aşama yönetim etkinliğini değerlendirmede bir metodoloji geliştirmeyi içermektedir. Büyük Kaza Önleme Politikasında uygulanan güvenlik yönetimi teknik, organizasyonel ve insan faktörlerini yönetmek için eylemlerin tanımlanmasını içermektedir.. Güvenlik yönetimin işletimsel amacı, bariyerleri ve kazalara karşı savunma hattını güçlendirmektir (güvenli ekipman veya insan etkinliği). Güvenlik yönetimi, çözülmesi zor olan fazla sayıda sorumluluklar, görevler ve fonksiyonlar içerir. Güvenlik yönetiminde farklı seviyeleri ayırt etmenin yolu şu şekilde verilmiştir:

- **Politika:** Tesis güvenliği, güvenlik yönetimi hedefleri ve amaçlarına ilişkin şirketin planlarının kapalı veya açık ifadesidir. Güvenlik yöntemi şirketin günlük yönetiminde önceliklendirilir ve bünyesine katılır.
- **Organizasyon:** Güvenlik yönetiminin organizasyonu, kaynakların tahsisi, görev tanımlanması ve faaliyetlerin programlanmasını gerektirir.
- **İşletme ve bakım:** Güvenlik yönetiminin en önemli parçası güvenlik açısından kritik olan teknik, organizasyonel ve insan bileşenlerinin güvenirliliğini sürdürmektir. Bu faaliyet/sorumluluk şunları içerir:
  - Eğitim, pratik ve personelin yeterliliği,
  - Teknik sistemlerin bakımı ve yeni güvenlik cihazlarının tanınması,
  - Prosedürlerin bakımı ve devamlılığı,
  - Örneğin risk değerlendirmelerini güncelleyerek tehlike farkındalığını devam ettirilmesi.
- **Liderlik:** Güvenlik yönetimi uygulaması liderlik gerektirir ve belirlenen politikalar, amaçlar, hedefler ve günlük tesisi yönetimi, örnek oluşturma, ortak değerler ve davranışlar meydana getirme arasında bir tutarlılık göstermelidir. Liderlik, güvenlik kültüründe, güvenlik farkındalığında ve "emniyetsiz davranışlardan" kaçınma üzerinde önemli etkiye sahiptir.

Değerlendirme metodolojisi bir kaç araştırma yönteminin kullanımı üzerine oluşturulacaktır:

- Niteliklerine göre fiziksel güvenlik bariyerleri ve savunma hattı sağlayan güvenlik cihazlarının etkinliklerinin analizi.. (doğası, kullanılabilirliği, güvenirliliği, sürdürülebilirliği ve test edilebilirliği vb.) Bu analizler IEC 61508 normları ve IEC 61511 standartlarındaki prensipler doğrultusunda yapılır,
- Özel güvenlik yönetim sistemlerinin analizi ve karşılaştırılması (örneğin standartların uygulanması) ve güvenlik politikalarının şirketin tüm yönetim sistemi içine katılması (güvenliğin performans göstergesi olarak hesaba katılmasını sağlayan modern yönetim modelleri),
- Yapısal Analiz ve Tasarım Teknikleri (SADT) veya fonksiyona dayalı modelleme ile yönetim görevlerinin teorik modellemelerinin geliştirilmesi kullanılması. Bu, AB'nin I-RISK gibi organizasyonel etkileri de içine alan farklı şekillerde yapılmış teknik risk analizlerini içeren bir çalışma ile yapılacaktır,
- Uzman kararlarına, değerlendirme amaçları için yönetim faktörlerini önceliklendirmek amacıyla yer verilmesi,
- Denetim teknikleri, anket tekniği ve kaza rapor analizi kullanan güvenlik performans göstergelerinin tanımlanması,

- Denetim tekniklerinin geliştirilmesi ve doğrulanması.

Güvenlik yönetimi, senaryoların meydana gelme olasılığını etkiler. Bu nedenle bu çalışmanın amacı şu şekilde belirlenmiştir:

- Kazaları önlemede, güvenlik yönetiminin değişik modellerinin ve bakış açılarının etkinliğinin, değerlendirilmesi,
- Bir tesisin güvenlik yönetiminin etkinliğininin iyi bir ölçümü olan güvenilir göstergelerin geliştirilmesi.

Bu bilgiler koruma yönetim etkinliğini karakterize eden, çok boyutlu bir M dizini tanımlanmasında kullanılacaktır.

• ÇEVRE HASSASİYETİNİN HESAPLANMASI

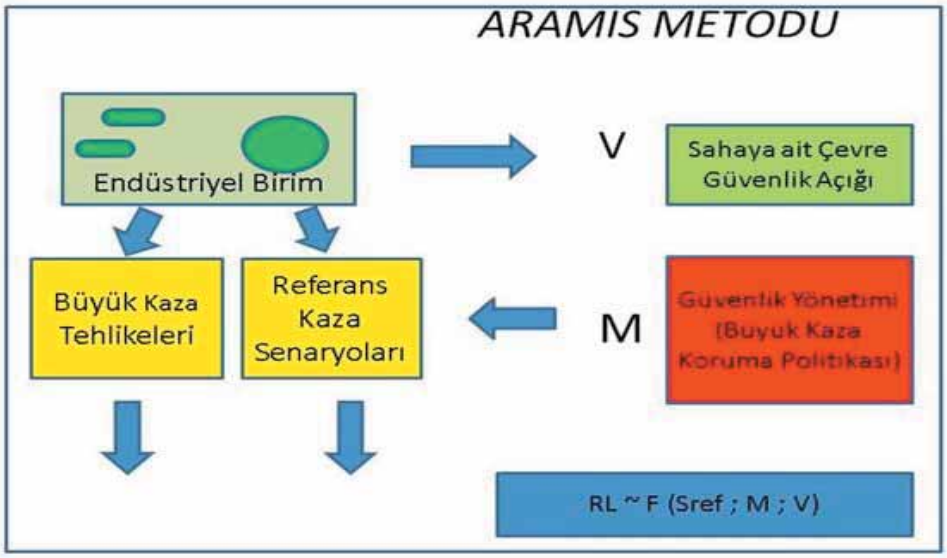
Bu aşama çevrenin konumsal hassasiyetini ve çevredeki potansiyel hedefleri (popülasyon, doğal ve insan yapımı çevre) karakterize etmek için bir V indeksi tanımlamayı ve bu hedeflerin duyarlılıklarını hesaplamayı amaçlamaktadır.

Bu amaca ulaşabilmek için, tesisin etrafındaki ilgili alan belirlenecek ve küçük karalere ayrılacaktır: Coğrafi Bilgi Sistemi (GIS)'nin desteğiyle de her bir sınıfa (popülasyon, doğal ve insan yapımı çevre) ait potansiyel hedefler tanımlanacak ve yerleri saptanacaktır. Olası hedeflerin hassasiyetleri ise (tesisin çalışanları, bölge sakinleri, yüzey ve yeraltı suları, kamu binaları…) çok kriterli bir sıralama metodu olan SAATY kullanılarak karakterize edilecek ve derecelendirilecek sonra hassasiyet seviyeleri skalası belirlenecektir. Hassasiyet haritaları incelenen alanın aynı karesine düşen olası hedeflerin hassasiyetlerinin hesaplanıp, toplanması ile elde edilecektir.

METODU SONUÇLANDIRMA VE TEST ETME

• RİSK SEVİYESİ (RL) KARAKTERİZASYONU

Bir tesisin çevresindeki risk seviyesini (RL) tanımlamak için, şiddet indeksi S, yönetim etkinliği indeksi M ve çevre hassasiyet indeksi V'nin bir araya getirilmesi ile yapılabilir. (bkz. şekil 2)



Şekil 2: ARAMIS metodunun gösterimi

Bu bölümde risk seviyesini (RL) karakterize etmek için bu üç indeks S, M, ve V arasındaki ilişki incelenecektir.. Bu üç indeks ile karakterize edilmiş risk seviyesinin kalmasının mı ya da üç indeksin çok boyutlu bir indeks oluşturmak için bir araya getirilmesinin mi daha iyi olacağı üzerinde çalışma yapılmıştır.

ARAMIS metodu, her bir senaryo için şiddet indeksi S'nin hesaplanması ile sadece şiddete göre tehlikelerin sıralanmasına olanak sağlamaktadır. Daha sonra çeşitli birimlerdeki belirlenmiş senaryolar karşılaştırılabilir. Aynı zamanda önleme güvenlik etkinliği M hesaplanması ile kuruluş tarafından yapılan çalışmaların (engelleyici önlemler) dikkate alınmasını sağlar.

Sonuçlar, güvenlik yatırım önceliklerinin belirlenmesi için bir endüstriyel grubun iki ya da daha fazla birimi arasındaki risk seviyelerinin karşılaştırılmasını mümkün kılar.

• ÖRNEK OLAY ÇALIŞMALARI

ARAMIS metodunu doğrulamak ve geliştirmek için Avrupadaki üç SEVESO kuruluşunda sanayicilerin ve yetkili kuruluşların işbirliği ile örnek olay çalışmaları yürütülmüştür. Test bölgelerinin seçiminde, sonuç-odaklı ve olasılığa dayanan yaklaşımların benimsendiği ülkelerin temsil edileceği garanti edilmiştir. Bu çalışmadan sonra prosedürün uygulanabilirliği ve doğruluğunu geliştirmek için indekslerin tanımları modüle edilmiştir.

• DEĞERLENDİRME VE YAYGINLAŞTIRMA

Değerlendirme ve yaygınlaştırma planındaki çalışmaların amacı, bu metodun nihai kullanıcıları olan risk değerlendirmesi uzmanlarına ve karar vericilere metodun aktarılması ve kullanımının yaygınlaştırılmasını sağlamaktır.

Sanayinin nihai kullanıcıları, konsorsiyumda Avrupa Sanayi Şirketleri adı altında bir birlik ile temsil edilmektedirler. Bu birlik konsorsiyuma proje ve projenin ilerlemesi hakkında bilgi aktarmış, örnek

olay çalışmaları için tesisler bulmuş ve projenin sonunda ise metodu yaygınlaştırmak üzere çalışmalar yapmıştır.

Yaygınlaştırma projesinden sorumlu çalışma grubu tarafından projenin sonuçlarını göstermek için bir web sitesi kurulmuştur. Geliştirme toplantılarından sonra web sitesinde proje yönetimi tarafından elektronik bir bülten yayınlanmıştır.

Ayrıca, nihai kullanıcıların projenin bazı kısmi sonuçlarını temin edebilmesi ve ileriki çalışmalar için yorumların toplanması için de bir ara dönem çalıştayı yapılmıştır.

Projenin sonunda konu ile ilgili tüm paydaşlara başlıca proje sonuçları yaymak amacı ile son bir çalıştay daha yapılmıştır. Bu iki çalıştay, konsorsiyumda bulunmayan üçüncül kişilere de açılmıştır. Çalıştayların bildirileri de web sitesinde ulaşılabilir konumdadır. Bunun yanında çalıştaylarla bağlantılı olarak, proje esnasında elde edilen sonuçların geniş bir şekilde yaygınlaştırılmasını sağlamak için katılımcılar makalelerini uluslararası bilimsel dergilerde ve konferanslarda yayınlanmıştır.

KONSORSİYUM TANIMI VE KATILIM

Konsorsiyum büyük kazaların risk analizinde yer alan 10 tane organizasyondan oluşmaktadır. Bunlar Tablo 1'de sunulmuştur:

Tablo 1: Ortak organizasyonlar

Organizasyon Adı	Kısa Adı	Ülke
1. Institut National de l'Environnement Industriel et des Risques Accidental Risk Division	INERIS	FRANSA
2. European Commission - Joint Research Centre - Institute for the Protection and Security of the Citizen-Major Accident Hazard Bureau	EC-JRC-IPSC-MAHB	İTALYA
3. Faculté Polytechnique de Mons Major Risk Research Center	FPMs-MRRC	BELÇİKA
4. Universitat Politecnica de Catalunya Centre for Studies on Technological Risk (CERTEC)	UPC	İSPANYA
5. Association pour la Recherche et le Développement des Méthodes et Processus Industriels	ARMINES	FRANSA
6. Risø National Laboratory System Analysis Department	RISOE	DANİMARKA
7. Universita di Roma Dipartimento Ingegneria Chimica	UROM	İTALYA
8. Central Mining Institute Safety Management and Technical Hazards	CMI	POLANYA
9. Delft University of Technology Safety Science Group	TUD	HOLLANDA
10. Institution of Chemical Engineers European Process Safety Centre	IChemEEPSC	İNGİLTERE

INERIS, projenin koordinatörüdür, büyük kaza önlemede uluslararası deneyime sahiptir. SEVESO II direktifinin uygulanmasında, ulusal yetkili kuruluşlara teknik olarak destek vermiştir. INERIS risk seviye indeksini oluşturmada ve onaylamada, idari komite ile birlikte öncü olarak çalışmaktadır. INERIS aynı zamanda değerlendirme, yaygınlaştırma ve paralel inceleme için destek sağlamıştır.

EC-JRC-IPSC ve özellikle MAHB büyük kaza önlenmesinde uluslararası tanınan bir tecrübeye sahiptir. MAHB, SEVESO I ve II Direktiflerinin uygulanması ile ilgili AB Çalışma Gruplarında canlandırma özelliğine sahiptir ve aynı zamanda Avrupa düzeyinde GIS araçları ile kaza veri tabanlarının geliştirilmesi ve kullanımı konusunda deneyimlidir. MAHB paralel inceleme ekibinin lideri olmasının yanı sıra, değerlendirme ve yaygınlaştırma aktiviteleri sonuçlarının da lideridir.

FPMs-MRRC, SEVESO II direktifinin uygulanmasında oldukça tecrübelidir ve domino etkilerinin kaza senaryolarının seçilmesinde birçok metodoloji geliştirmiştir. Senaryo belirlenmesi çalışmasında liderdir. Buna ek olarak, MRRC aynı zamanda domino etkilerindeki tecrübelerini ve şiddet (önem) değerlendirmesinde bulunan kaza sonuç modellemesindeki tecrübelerini aktarmıştır.

UPC (CERTEC aracılığı ile) SEVESO kuruluşlarındaki kaza sonuçlarının değerlendirilmesi ile ilgili tanınan bir deneyime sahiptir (yayılım, patlama, yangın modelleme). UPC bu görevin lideri olarak Şiddet(önem) değerlendirmesi için araştırma geliştirmiştir.

ARMINES'in "The Pole Cindyniques" bölümü, raporların, oturumların ve söyleşilerin analizlerinden topladığı bilgiler ile "deneyimin parçacıkları" olarak adlandırdığı, kazaların gelişimini şekillendiren bir metodoloji kurmuştur. Bu metodolojinin kullanılması, senaryo tanımlama ve koruma yönetim etkinliği çalışmalarına katkı sağlamıştır.

ARMINES'in SITE departmanı çevre yönetim sistemi karakterizasyonunda geniş bir deneyime sahiptir. Bu departman çevre koruma etkinliğine ve çevre güvenlik açığı tanımlanmasına odaklanmıştır.

ARMINES'in LGEI bölümü ise çok kriterli karar verme metotları olan SAATY ve GIS metodlarında yetkinliğe sahiptir. Tehlikeli maddelerin taşınmasındaki riskler konusunda bu iki metota dayalı bir yöntem geliştirmiş ve tesis çevresinde, o sahaya ait hasar görülebilirliği karakterize eden bir hasar görebilirlik haritası elde etmek için hedeflerin (insan, çevre, ekipman) hassasiyetini sıraya koymuştur.

RISOE tehlikeli tesislerin güvenlik raporlarını hazırlamada ve değerlendirmede deneyimlidir. Organizasyonların güvenlik prosedürlerinin etkinliğini analiz etmek için fonksiyon-yönlü modellemede deneyimlidir ve güvenlik kültürünün değerlendirmesinde de anketler yapmaktadır. RISOE Çevre Koruma Etkinliği çalışmasına öncülük etmiştir.

UROM risk analizi ve riskli alanlar çalışmasında, GIS sistemlerini ve yazılım araçları da kullanan metodolojilerde deneyimlidir. Bu organizasyon potansiyel hedefleri ve onların hasar görebilirliğini belirlemek için bir metodoloji geliştirmiştir. GIS bilgisindeki indekse dayanan, çevre hasar görülebilirliğini belirleyen bir yazılım aracı hazırlayacaktır.

CMI, bir tarafta yangın, patlama diğer tarafta güvenlik yönetimi, risk değerlendirmesi deneyimlerine göre şiddet değerlendirmesi çalışmalarını ve yönetim standartları ile kılavuzlarının uygulanması sonucu yönetim etkinliğinin analizi araştırmalarını sürdürmüştür.

TUD, güvenlik yönetimi modellemesindeki ve risk değerlendirmesindeki uzmanlığını, TUD'da geliştirilen denetim araçları ve uzman değerlendirmeleri ile ARAMIS projesindeki koruma yönetiminin etkinliğinde üstün bir çaba ile göstermiştir.

IChemE-EPSC(Kimya mühendisleri enstitüsü Avrupa Proses Güvenlik Merkezi), EPSC'nin üyeleri arasında yer alan endüstriyel kuruluşlara sonuçların dağıtılmasında yer almıştır. Şunu fark etmek önemlidir ki EPSC'nin üyeleri ARAMIS metodunun nihai kullanıcılarıdır. Projede EPSC, proje ile ilgili bilgileri ve sonuçları için üyelerle bilgi paylaşımını sağlamış ve inceleme ekibi katılımı ile de ilgilenmiştir.

1. GİRİŞ

1.1. ARAMIS'IN İÇERİĞİ VE TARİHİ

ARAMIS projesinin başladığı zamanlarda, Enschede (2000), Toulouse (2001) veya Lagos (2002) gibi ileri teknolojiye sahip olan işyerlerinde yaşanan kazalar toplumda büyük bir merak uyandırmış hatta risk bazlı kararlarda hem endüstriye hem de yetkili kuruluşlara şüpheyle yaklaşılmasına neden olmuştur. Bu kazalar çok daha tutarlı ve şeffaf karar alma süreçlerine olan ihtiyacı gündeme getirmiştir.

Risk bazlı kararlar şüphesiz, risk analizlerinden elde edilen güvenilir bilimsel girdiler gerektirir. Ancak bir risk uzmanından diğerine aynı olaylara ilişkin alınan kararlarda bile dikkate değer farklılıklar bulunmaktadır. Bu ASSURANCE projesinde de ortaya konulmuştur. Bu nedenle kaza senaryolarını seçmek için tutarlı kuralları olan ve risk kontrolü gösterimi için güvenlik yönetim etkinliğini dikkate alan bir metodolojiye ihtiyaç olduğu ortaya çıkmıştır. Seveso II Direktifi kapsamında, Avrupa genelinde risk uzmanları arasında fikir birliği sağlayan böyle bir yönteme temel bir ihtiyaç vardır.

ARAMIS'in potansiyel son kullanıcıları oldukça fazladır. Ancak en ilgili olanlar sanayi, yetkili kuruluşlar ve yerel yönetimlerdir . Hepsi aynı risk yönetim süreciyle ilgili olsa bile, ihtiyaçları birbirinden farklıdır.

SEVESO direktifinin 9. Maddesinin gerektirdiği gibi işletmeci, işyerindeki riski tespit etmek, değerlendirmek ve azaltmak ve risk azaltımını göstermek için bir yönteme ihtiyaç duymaktadır. Bu yöntem ve ispatı yetkili makamlar tarafından kabul edilmelidir. Bu yaklaşım, riskleri azaltmak ve devamlı karşılaşılan riskleri yönetmek için yararlı bilgileri geliştirmek zorundadır.

Yetkili kuruluşlar, özellikle güvenlik raporu aracılığıyla, "tesisin güvenlik düzeyini değerlendirebilmeye ihtiyaç duyarlar. Aynı zamanda sonuçların modellenmesi için hangi senaryonun seçildiğini de bilmek isterler.

Hem yetkili kuruluşlar hem de yerel yönetimler güvenlik seviyesi üzerinde yönetimin etkisini değerlendirmeye ihtiyaç duyarlar. Endüstriyel riski azaltmak ve büyük etkileri olabilecek gerçek risk seviyelerini değerlendirmek için bir yönetim sistemi geliştirilmelidir. Meydana gelen büyük kazaların % 50'den fazlasının nedeni insan ve organizasyon faktörüdür. ARAMIS metodunun oluşturulabilmesi için özellikle bu faktörlerin belirlenmesi bile yeterli bir nedendir.

Yerel yönetimler (belediyeler) özellikle arazi kullanımı konuları ile ilgilidirler. Onlar halkın karşılaşacağı riskler hakkında net ve anlaşılır raporlara ihtiyaç duyarlar. Aynı zamanda karar vermek için kullanılabilecek bilgilerde isterler. Temelde yerel yönetimlerin rolü ya riske maruz hedeflerin (insan, altyapı, çevre) sayısını sınırlamak ya da kaynaklarla bu hedefler arasına engeller koymakla ilgilidirler. Kaza senaryolarına dayanan bir risk konturu önerdikleri zaman işletmecilere ve yetkili kuruluşlara güvenme ihtiyacı duyarlar.

ARAMIS'in amacı tüm bu ihtiyaçlara cevap vermektir:

- Yönetim sisteminin etkinliğini hesaba katarak, tehlikelerin tanımlandığını ve riskin doğru bir şekilde yönetildiğini gösterir,

- Arazi kullanım planı ve acil durum planlaması ile ilgili karar verme sürecine bilgi sağlar,
- Halk tarafından anlaşılabilir net bir yaklaşım sunar.

Bu metot, hem sanayinin hem de kamu kurumlarının beklentilerini karşılayan deterministik ve olasılıksal yaklaşım arasında yakınsama sağlar.

ARAMIS'in genel amacı deterministik ve risk tabanlı iki yaklaşımın gücünü birleştiren endüstri için yeni bir kaza riski değerlendirme metodolojisi oluşturmaktır. 5. AB Çerçeve Programı kapsamında, bu üç yıllık proje Ocak 2002'de başlamıştır. Bu temel metodoloji, üç yıl sonra Avrupa SEVESO II Direktifi uygulamasını hızlandırmak için destekleyici bir araç olmayı amaçlamaktadır. ARAMIS kullanıcı kılavuzu, metodolojinin önemli özelliklerini ortaya çıkarmak ve potansiyel kullanıcılar için metodolojinin daha etkin kullanımını sağlamayı amaçlamaktadır.

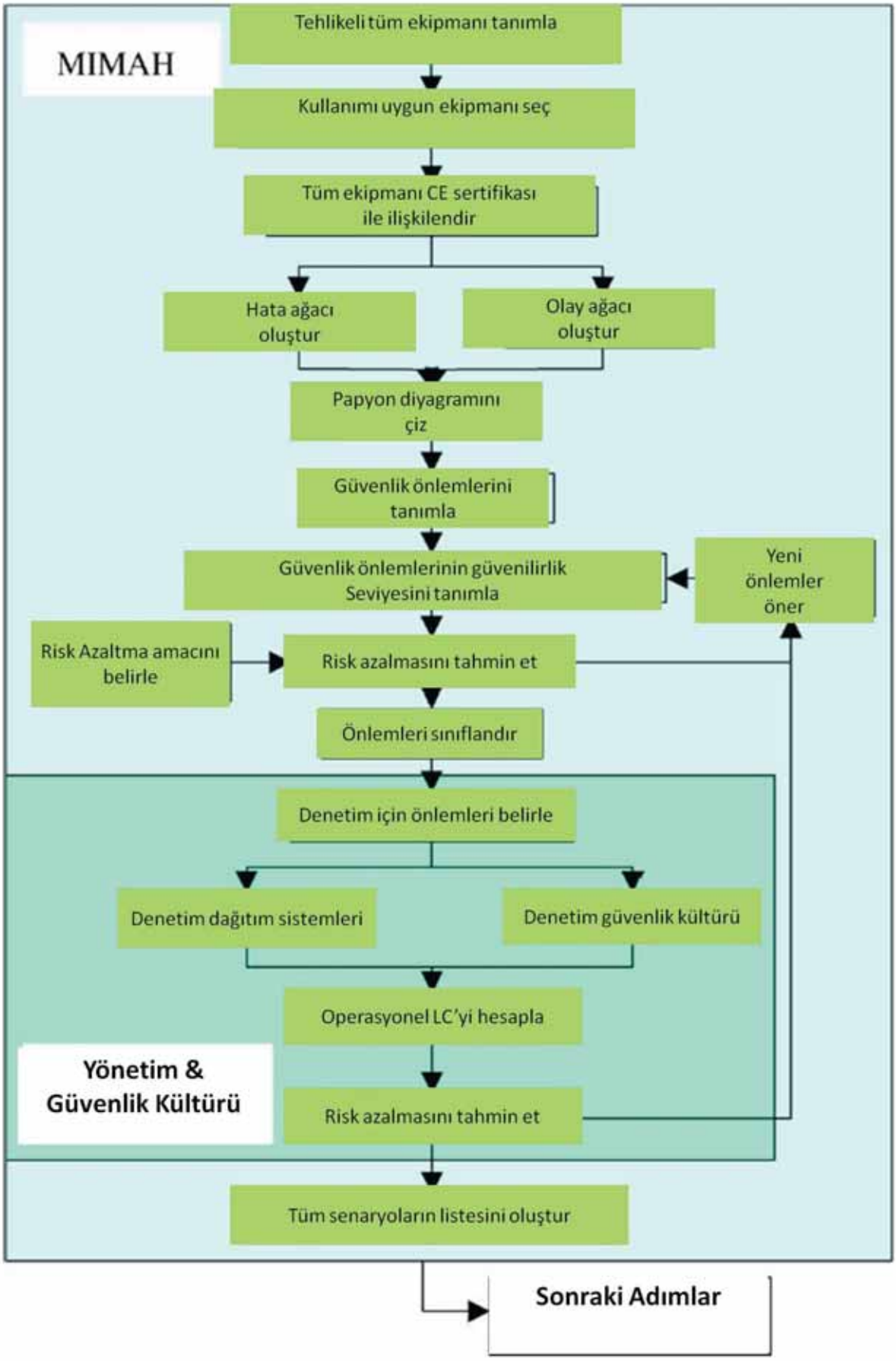
1.2. KULLANIM KILAVUZUNA GENEL BAKIŞ VE ANA HATLAR

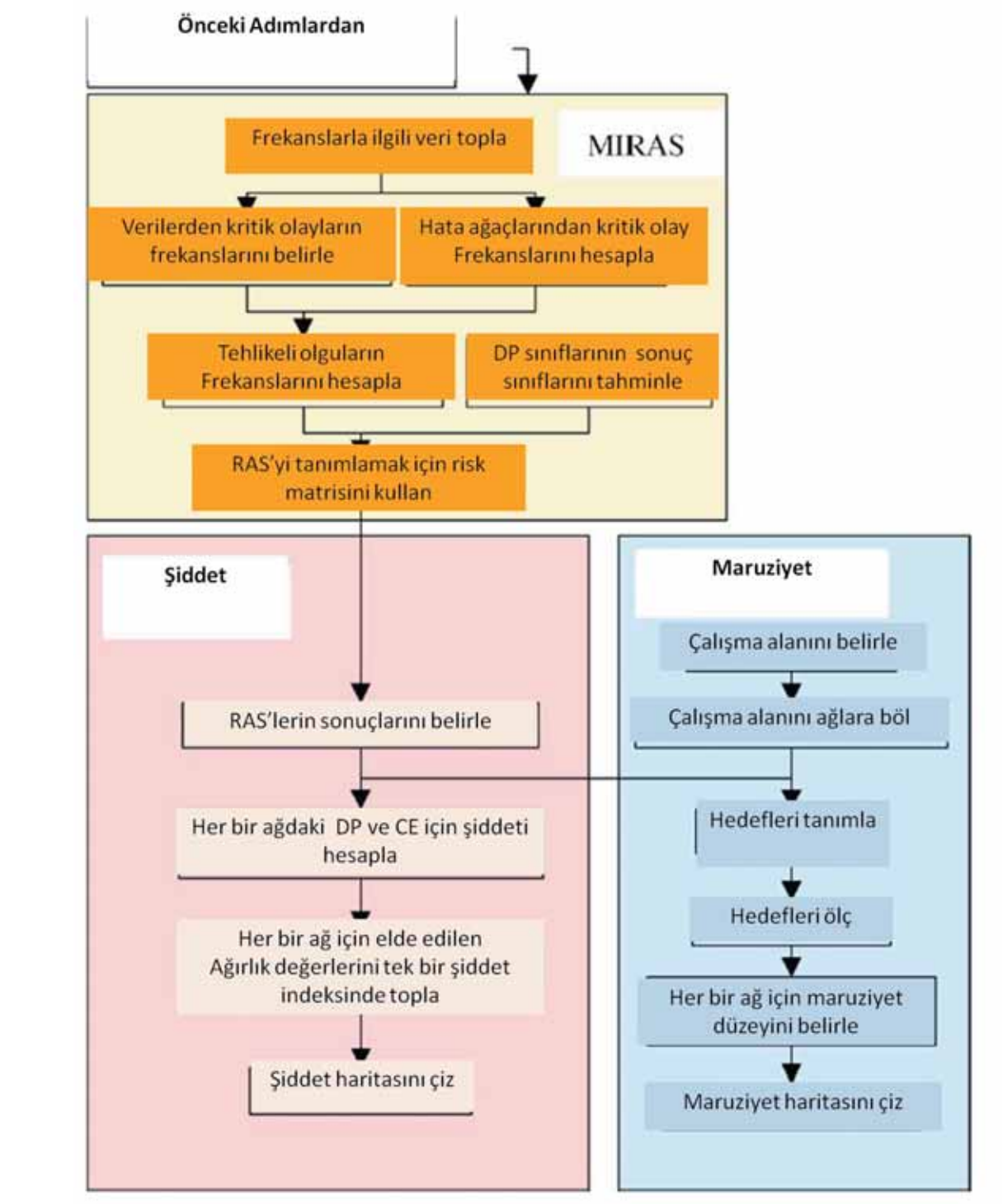
ARAMIS aşağıdaki başlıca aşamalara ayrılır:

- Büyük kaza tehlikelerinin belirlenmesi metodolojisi (MIMAH)
- Güvenlik bariyerlerin belirlenmesi ve performanslarının değerlendirilmesi
- Bariyer güvenilirliği için güvenlik yönetim etkinliğinin değerlendirilmesi
- Referans kaza senaryolarının belirlenmesi metodolojisi (MIRAS)
- Referans senaryolarının risk şiddetinin değerlendirilmesi ve haritalandırılması
- Tesis çevresinin hassasiyetinin değerlendirilmesi ve haritalandırılması

Son bölüm, daha ileri uygulamalar için ARAMIS'in potansiyel kullanımına ve araştırma alanlarına ayrılmıştır.

ARAMIS metodolojisinin başlıca adımlarının her biri aşağıdaki şekilde özetlenmiştir:


MIMAH
Tehlikeli tüm ekipmanı tanımla
Kullanımı uygun ekipmanı seç
Tüm ekipmanı CE sertifikası ile ilişkilendir
Hata ağacı oluştur
Olay ağacı oluştur
Papyon diyagramını çiz
Güvenlik önlemlerini tanımla
Güvenlik önlemlerinin güvenilirlik Seviyesini tanımla
Yeni önlemler öner
Risk Azaltma amacını belirle
Risk azalmasını tahmin et
Önlemleri sınıflandır
Denetim için önlemleri belirle
Denetim dağıtım sistemleri
Denetim güvenlik kültürü
Operasyonel LC'yi hesapla
Yönetim & Güvenlik Kültürü
Risk azalmasını tahmin et
Tüm senaryoların listesini oluştur
Sonraki Adımlar



Şekil 3: ARAMIS metodolojisine genel bakış

1.2.1. Büyük Kaza Tehlikelerinin Belirlenmesi Metodolojisi – MIMAH

MIMAH yöntemi, büyük kaza tehlikelerinin belirlenmesi için geliştirilmiş bir metodolojidir. Esasen merkezinde kritik olay, solunda hata ağacı ve sağında olay ağacının bulunduğu papyon yönteminin (bow-tie) kullanımına dayanır.

MIMAH, tesisteki potansiyel tehlikeli ekipmanları belirlemek ve büyük kazalar meydana getirmeye müsait uygun tehlikeli ekipmanları seçmek için gerekli bilgileri toplayan kapsamlı bir metodoloji sağlar. İkinci adımda, her bir ekipman ile ilişkili olması muhtemel kritik olayların listesi oluşturulur. Metodoloji tarafından önerilen genelleştirilmiş ağaçlara dayanan hata ve olay ağaçları oluşturulur. Hata ve olay ağacı papyonu oluşturur. Bu aşamada hata ağacı ve olay ağacında herhangi bir güvenlik bariyeri olmadığı kabul edilir. Papyonların, risk analizi esnasında tesisin ilgili çalışanlarıyla oluşturulması gerekir.

Tehlike ve risk arasında açık bir ayrım yapmak bir avantaj sağlar. Bu metodun ilk adımında tehlikelerin tanımlanmasını sağlar. Sonraki adım ise tehlikeli kaza senaryolarından ve güvenlik bariyerlerinin arızalarından kaynaklanan risklerin belirlenmesini amaçlanmıştır.

1.2.2. Bariyerlerin Belirlenmesi ve Performanslarının Değerlendirilmesi

Metodolojinin ikinci adımı risk seviyesini tahmin etmek ve güvenlik sistemlerinin uygulanmasını desteklemeyi amaçlamaktadır. Bu adımda, güvenlik sistemlerinin etkileri hem kaza sıklığı açısından hem de sonuçlarının büyüklüğü açısından dikkate alınır ve papyonun analizinden elde edilen güvenlik fonksiyonlarının ve güvenlik bariyerlerinin belirlenmesini içerir.

Güvenlik bariyerlerinin etkisi, bariyerlerin performanslarının (senaryoya uygun güvenilirlik seviyesi, tepki süresi ve etkinliği gibi) değerlendirilmesiyle belirlenir.

Toplanmış güvenirlilik seviyelerine göre tanımlanan risk azaltma hedefi, risk analizi sırasında riskin kabul edilebilir seviyeye ulaşması amacıyla her bir senaryoya atanır.

1.2.3. Bariyer Güvenilirliği İçin Güvenlik Yönetim Etkinliğinin Değerlendirilmesi

İşletme yönetimi, risklerin kontrol kapasitesi üzerinde güçlü bir etkiye sahiptir. ARAMIS'in amacı güvenlik yönetim sistemini ve güvenlik kültürünü değerlendirmek için araçlar oluşturmak, yetkili kuruluşlar tarafından bunların dikkate alınmasını sağlamak ve bir de işletmecilerin güvenlik yönetim sisteminin amaçları ve özelliklerini tanımlamalarına yardım etmektir. ARAMIS'te benimsenen yaklaşım, risk analiz prosedürünün önceki adımlarından gelen güvenlik bariyerlerinin yaşam döngüsü üzerinde yönetim sisteminin gereksinimlerine odaklanmayı içerir. Bu yaşam döngüsü tasarım, kurulum, kullanım, bakım ve iyileştirme adımlarını içerir. Bunların her biri için; güvenlik yönetimi organizasyonun on önemli yapısal unsuru ve sekiz kültürel faktörü ile birlikte değerlendirilir.

1.2.4. Referans Kaza Senaryolarının Belirlenmesi Metodolojisi – MIRAS

Büyük kaza senaryoları değerlendirilip güvenlik bariyerleri belirlendikten (denetim ve güvenlik anketlerinin sonuçlarına göre değiştirildikten) sonra kaza sonuçları değerlendirilmelidir. MIRAS'ın amacı şiddet indeksi hesaplanması için gerekli olan referans kaza senaryolarını (RAS) belirlemektir. Bu ilke şiddet üzerinde gerçek etkileri olabilen frekans ve/veya sonuçlara göre tehlikeli olaya ilişkin senaryoları seçmektir. Senaryoların oluşma sıklığını ve tehlikeli olayların sonucunun sınıfını tahmin etmek için bir risk matrisi geliştirilmiştir.

1.2.5. Şiddetin Değerlendirilmesi ve Haritalanması

Referans kaza senaryoları seçildikten sonraki adımda, metodoloji bu senaryoların şiddetinin değerlendirilmesini gerektirir. Amaç şiddet haritaları oluşturabilmektir, böylece kazanın etkisi tesis çevresinin hassasiyeti eşleştirilebilir. Şiddet indeksi dört etki seviyesi hesaba katılarak geliştirilmiştir, öyleki değişik risk analizlerinin sonuçları karşılaştırılabilir. Tüm tesis için Risk Şiddet İndeksi (S), dikkate alınan her bir kritik olay ve sıklıklarıyla ilişkili olan spesifik risk şiddet indekslerinin bir kombinasyonudur. Spesifik risk şiddet indeksleri kritik olayların tüm olası sonuçları ve bunlarla ilişkili olasılıklar dikkate alınarak oluşturulmuştur.

1.2.6. Hassasiyetin Değerlendirilmesi

ARAMIS metodolojisinin son adımı hassasiyetin değerlendirilmesine ayrılmıştır. Hassasiyet indeksi insan, çevre ve maddi unusurları içeren faklı tipteki hedef sayısının lineer bir kombinasyonu olarak oluşturulur. Hedefin her bir kategorisine bağıl hassasiyetinin temsili fiziksel etkilerinin her biri için bir ağırlık katsayısı atanır. Hassasiyet haritalarının oluşturulması için GIS yazılımları geliştirilmiştir. Hassasiyet haritalarının şiddet haritalarıyla birleştirilmesi, arazi kullanım planlanması ve kaza sonucun baskılanmasını veya hedeflerin korunmasını içeren risk azaltım kararları için faydalı olacaktır.

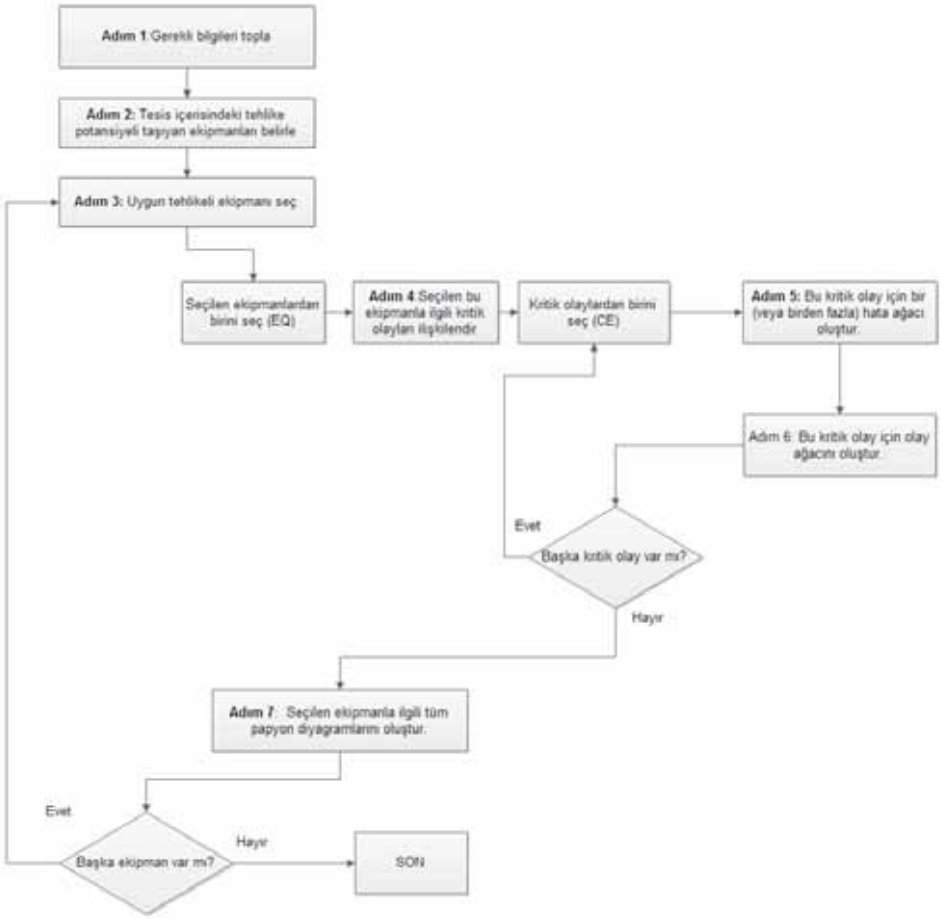
2. BÜYÜK ÇAPLI ENDÜSTRİYEL KAZALARA SEBEP OLAN TEHLİKELERİN TANIMLANMASINDA KULLANILAN BİR METODOLOJİ (MIMAH – GÜVENLİK BARİYERLERİ OLMAYAN PAPYON DİYAGRAMLARININ OLUŞTURULMASI)

Büyük Çaplı Kazalara Sebep Olan Tehlikelerin Tanımlanmasında Kullanılan Metodoloji (MIMAH) herhangi bir tesise ait maksimum tehlike potansiyelini tanımlamak için kullanılır. "Büyük Çaplı Kazalara Sebep Olan Tehlikeler" teriminden, ele alınan tesis üzerinde herhangi bir güvenlik sistemi olmaksızın (güvenlik yönetim sistemleri de dahil) veya kurulu olan güvenlik sistemlerinin etkin durumda olmadığı durumlarda meydana gelebilecek en kötü kazalar anlaşılmalıdır. Tanımlanmış olan Büyük Çaplı Kazalara Sebep Olan Tehlikeler sadece ele alınan ekipmanın cinsiyle, fiziksel durum şartlarıyla ve kullanılan kimyasalların tehlikeli özellikleri ile ilişkilendirilmiştir.

MIMAH yönteminde aşağıdaki 7 adım izlenmelidir:
Adım 1: Gerekli bilgilerin toplanması
Adım 2: Tesis içerisinde tehlike potansiyeli olan ekipmanları belirlenmesi
Adım 3: Uygun tehlikeli ekipmanın seçilmesi
Adım 4: Seçilen her ekipman ile kritik olayların ilişkilendirilmesi
Adım 5: Her bir kritik olay için hata ağaçlarının oluşturulması
Adım 6: Her bir kritik olay için olay ağaçlarının oluşturulması
Adım 7: Seçilen her ekipman için papyon ağaçlarının çizilmesi

MIMAH metodolojisinde takip edilen adımlar genel olarak Şekil-4'de gösterilmiştir.

ARAMIS'in ve özellikle MIMAH'ın uygulanmasına hazırlık yapabilmek, ARAMIS'in amaçlarını açıklayabilmek ve MIMAH metodolojisine başlayabilmek için gerekli verilerin toplanabilmesi amacıyla, tesis yönetimi ile ilk temasın kurulabileceği ön ziyaretlerin gerçekleştirilmesi gerekmektedir.



Şekil 4: MMAH adımlarının genel görünümü

2.1. GEREKLİ BİLGİLERİN TOPLANMASI

Büyük Çaplı Kazalara Yönelik Tehlikelerin Belirlenmesi Metodolojisinin uygulanabilmesi için gerekli olan minimum bilgi listesi aşağıdaki gibidir:

- Tesis hakkında genel bilgiler (tesis ve bu tesisteki prosesler hakkında genel bir fikre sahip olabilmek için),
- Tesis yerleşimi,
- Proseslerin kısaca açıklanması,
- Kullanılan ekipmanların ve boru hatlarının kısaca açıklanması,
- Tesisteki ilgili ekipman listesiyle ilişkili işlenen ve depolanan maddelerin listesi.
- Bu maddelerin tehlikeli özellikleri (risk ibareleri, tehlike sınıflaması).

Tehlike potansiyeli olan her bir ekipman için:

- Ekipmanın adı,
- Büyüklüğü (hacim, boyutları),
- Çalışma basıncı ve sıcaklığı,
- İşlenen maddeler,
- Bu maddelerin fiziksel hali,
- Ekipman "içerisindeki" madde miktarı (madde içerik miktarı için kg veya akış halinde olanlar için kg/sn),
- Bu maddelerin kaynama noktaları.

2.2. UYGUN TEHLİKELİ EKİPMANIN SEÇİLMESİ

2.2.1. Amaç

Uygun tehlikeli ekipmanın seçiminde kullanılan yöntemin amacı, üzerinde büyük çaplı kaza senaryolarının tanımlanabileceği ekipmanın seçilmesidir. Bu metodun uygulanmasından önce, tehlike potansiyeli olan maddeleri içeren ekipman listesinin oluşturulması gerektiği bir kez daha hatırlanmalıdır (bkz. paragraf 2.2.2).

2.2.2. Tesis İçerisinde Tehlike Potansiyeli Olan Ekipmanları Belirle (MIMAH - Adım 2)

Toplanan bilgiler temel alınarak (bkz. paragraf 2), tehlikeli maddelerin sınıflandırılmasında bahsedilen bir veya birkaç risk ifadesine sahip tehlikeli maddeler listesi (bkz. tablo 2) oluşturulmalıdır.

Tablo 2: Tehlikeli maddelerin sınıflandırılması (D.1.C.'deki Tablo 2 (MIMAH Adım 2 (J)

Kategori	Risk İfadeleri
Çok toksik	R26, R100
Toksik	R23, R101
Oksitleyici	R7, R8, R9
Patlayıcı	R1, R2, R3, R4, R5, R6, R16, R19, R44, R102(*)
Alevlenebilir	R10, R18
Kolay alevlenebilir	R10, R11, R17, R30
Çok kolay alevlenebilir	R10, R11, R12
Suyla şiddetli reaksiyona giren	R14, R15, R29, R14/15, R15/29
Başka bir maddeyle şiddetli reaksiyona giren	R103, R104, R105, R106
Çevre için tehlikeli (su ortamları için)	R 50, R51
Çevre için tehlikeli (su ortamları dışındaki ortamlar için)	R54, R55, R56, R57, R59

Ele alınan maddelere ait risk ifadeleri olay ağaçlarının oluşturulmasında dikkate alınacaktır.
İkinci bir adım olarak, bu maddeleri içeren ekipman listesi ve tehlikeli maddenin bu ekipman içerisindeki fiziksel halinin (iki fazlı, sıvı, gaz/buhar veya katı) yer aldığı bir listenin oluşturulması gerekmektedir.

Daha sonra ekipmanlar, ekipman tipine göre sınıflandırılmalıdır. 16 tip ekipman tanımlanmıştır:

Tablo 3: Ekipmanların tipolojisi (D.1.C.'deki Tablo 3 (MIMAH Adım 2))

#	Ekipman Tipi
EQ1	Yığın olarak katı halde depolama
EQ2	Küçük paketler halinde katı olarak depolama
EQ3	Küçük paketler halinde sıvı olarak depolama
EQ4	Basınç altında depolama
EQ5	Yalıtılmış halde depolama
EQ6	Atmosferik basınçta depolama
EQ7	Kriyojenik olarak depolama
EQ8	Basınçlı Taşıma (iletim) Ekipmanı/Aracı
EQ9	Atmosferik Taşıma (iletim) Ekipmanı/Aracı
EQ10	Boru İletim Ağı
EQ11	Prosese dâhil edilmiş ara depolama ekipmanı
EQ12	Maddelerin fiziksel veya kimyasal olarak ayrışması için kullanılan ekipmanlar
EQ13	Kimyasal reaksiyonlar içeren ekipmanlar
EQ14	Enerji üretimi ve ısı değişiminde kullanılan ekipmanlar
EQ15	Paketleme ekipmanları
EQ16	Diğer ekipmanlar

Bu seçim sonucunda aşağıdaki sütunlardan oluşan bir tablo elde edilecektir:

- Maddenin adı
- Maddenin tehlikeli özellikleri (risk ifadeleri)
- Maddenin içerisinde bulunabileceği ekipmanların adı
- İlgili ekipmanların tipleri
- İlgili ekipman içerisindeki maddenin fiziksel hali

2.2.3. Uygun Tehlikeli Ekipmanların Seçimi (MIMAH - Adım 3)

Eğer bir ekipman içerisindeki tehlikeli madde miktarı kütlesel eşik değere eşit veya bu değerden büyükse, bu tehlikeli maddeyi içeren her bir ekipman uygun tehlikeli ekipman olarak seçilecektir. Bu eşik değer maddenin tehlikeli özelliklerine, fiziksel haline, buharlaşma olasılığına ve olası domino etkilerini meydana getirebilecek diğer tehlikeli maddelere göre konumuna bağlıdır.

Uygun tehlikeli ekipmanın seçilmesinde kullanılan yöntem D.1.C. paragraf 2'deki (http://aramis.jrc.it adresinden ulaşılabilir) Ek-2'de tamamıyla açıklanmıştır. Bu metot, Belçika'daki Walloon Bölgesinde kullanılan "VADE MECUM" metodolojisi temel alınarak oluşturulmuştur (DGRNE, 2000).

Bu metodu kullanabilmek için, MIMAH Adım 2'de elde edilen ve potansiyel tehlikeli olarak tanımlanan her bir ekipman için (bkz. paragraf 2.2.2) ekipmanlara ait şu bilgiler gereklidir:

✓ Ekipmanın adı	✓ Çalışma sıcaklığı (^{0}C olarak)
✓ Ekipmanın tipi	✓ Risk ibareleri
✓ Kullanılan tehlikeli madde	✓ Tehlike sınıflandırılması
✓ Maddenin fiziksel hali	✓ Ekipman içindeki maddenin kütlesi (kg olarak) veya içinde akış olan ekipman için (borular gibi) 10 dakikada geçen tehlikeli madde kütlesi
✓ Kaynama sıcaklığı (^{0}C olarak)	

Bu bölümde tanımlanan adımlar tehlikeli ekipmanların seçimi için kütlesel eşik değerlerinin hesaplanmasında takip edilmelidir.

1. Maddenin özelliklerine göre referans olarak alınabilecek kütle Ma (kg)'yı belirle

Tablo 4: Referans Kütleler

	Referans Alınan Kütle Ma (kg)		
Maddenin Özellikleri	**Katı**	**Sıvı**	**Gaz**
1 Çok toksik	10000	1000	100
2 Toksik	100000	10000	1000
3 Oksitleyici	10000	10000	10000
4 Patlayıcı (Seveso II Direktifi Ek 1 Tanım 2a)	10000	10000	---
5 Patlayıcı (Seveso II Direktifi Ek 1 Tanım 2b)	1000	1000	---
6 Alevlenebilir	---	10000	---
7 Kolay alevlenebilir	---	10000	---
8 Çok kolay alevlenebilir	---	10000	1000
9 Çevre için zararlı	100000	10000	1000
10 R14, R14/15, R29 risk ibareleri kombinasyonlarında yukarıda verilen özellikler tarafından kapsanmayan sınıflandırma	10000	10000	---

2. Buharlaşma olasılığına göre sıvının referans kütlesinin ayarlanması

Sıvılar için, yukardaki tabloda verilen Ma değeri bir S katsayısına bölünmelidir. Böylece yeni elde edilen Mb referans kütlesi bulunur:

$$Mb = \frac{Ma}{S}$$

Eğer bir ekipmanın içerdiği M kütlesi, referans kütle Mb'den daha fazla ise ekipman tehlikeli ekipman olarak seçilecektir.

- S katsayısı, S_1 ve S_2 katsayılarının toplamıdır.
  S katsayısı 0,1 ile 10 aralığında olmalıdır.

$$0{,}1 \leq S \leq 10$$
$$Eğer\ S < 0{,}1\ ise\ S = 0{,}1;$$
$$Eğer\ S > 10\ ise\ S = 10\ \ olarak\ alınır.$$

- S_1 katsayısı, çalışma sıcaklığı T_p (^{0}C) ile atmosfer basıncı altındaki kaynama noktası T_{eb} arasındaki farkın bir fonksiyonu olup: $S_1 = 10^{T_p - T_{eb}/100}$ dür.
- S_2 katsayısı yalnızca 0^{0}C'den daha düşük olan sıcaklıklarda gerçekleşen prosesler için şu eşitliğe göre uygulanır: $S_2 = \frac{T_{eb}}{-50}$

Diğer durumlar için (pozitif proses sıcaklıkları) S_2=0 olarak alınır. Burada sıcaklıklar ^{0}C cinsinden ifade edilmiştir.

3. Domino etkisi tehlikesi durumunda referans kütle değerinin ayarlanması

İkinci adımda tehlikeli ekipman olarak seçilmeyen ($M<M_b$) ekipmanlar için şu mantık uygulanabilir: Patlayıcı ve yanıcı madde içeren ekipmanlar aynı zamanda riskli ekipmanlar olarak seçilmelidir:

- Eğer bu ekipman, birinci ve ikinci paragrafta anlatılan kurallara göre riskli olarak seçilen başka bir ekipmandan 50 m veya daha az bir uzaklıkta konumlandırılmışsa
- Ve eğer ekipmanın içerdiği tehlikeli madde kütlesi referans M_c kütlesinden büyükse:

$M_c = S_3 . M_b$

- $0{,}1 \leq S_3 \leq 1 \; ve$
- $S_3 = (0{,}02 . D)^3$

Burada D (metre) iki ekipman arasındaki uzaklığı ifade etmektedir. S_3 katsayısı 0,1-1 aralığında değerler almakta olup:

$0{,}1 \leq S_3 \leq 1$

$Eğer \; S_3 < 0{,}1 \; ise \; S_3 = 0{,}1;$

$Eğer \; S_3 > 1 \; ise \; S_3 = 1$ olarak alınır.

Bu metodun sonucunda içerdiği tehlikeli madde miktarı eşik değere eşit veya bu değerden daha büyük olan uygun tehlikeli ekipmanlar seçilmektedir. Seçilen ekipmanlar MIMAH metodolojisine göre değerlendirilir.

2.2.4. Değerlendirme

Ekipman seçim metodunu açıklamak, eksik verileri toplamak ve öncelikli olarak seçilen ekipmanlar hakkında tesis yönetimiyle görüşmek için tesise ön bir ziyaret gerçekleştirilmelidir.

Ekipmanın seçiminde kullanılan metot körü körüne uygulanmamalıdır. Eğer bir ekipman, içindeki tehlikeli maddenin varlığından ve/veya ekipman içerisindeki çalışma koşullarından dolayı tehlikeli olarak nitelendiriliyorsa, bu ekipman, içerdiği tehlikeli madde kütlesi eşik değerden küçük olsa bile uygun tehlikeli ekipman olarak seçilebilir ve MIMAH'a göre incelenebilir. Ayrıca, tesis sınırları yakınındaki bazı ekipmanlar da kendilerine yakın hedeflere olan etkileri nedeniyle uygun tehlikeli ekipman olarak seçilebilir.

2.3. PAPYON DİYAGRAMLARININ OLUŞTURULMASI

2.3.1. Amaç

MIMAH yönteminin amacı, bir proses endüstrisinde meydana gelebilecek tüm olası büyük kaza senaryolarını tanımlamaktır.

MIMAH yönteminin dayandığı temel araç papyon diyagramıdır (Şekil 3). Papyon diyagramının merkezinde kritik olay yer alır. Papyon diyagramının sol tarafında yer alan ve hata ağacı adı verilen bölümde kritik olaya ait olası sebepler tanımlanır. Olay ağacı olarak adlandırılan sağ bölümde ise, kritik olayın olası sonuçları açıklanır.

2.3.2. Kritik olayların ilgili tehlikeli ekipmanlarla ilişkilendirilmesi (MIMAH - Adım 4)

D.1.C.'nin Ek-3 bölümünde kritik olaylarla ilgili tehlikeli ekipmanların ilişkilendirilmesine yönelik bir yöntem açıklanmıştır. Bu yöntemde kısaca iki adet matrisin kullanıldığı görülmektedir:

1. Ekipman tipi ile MIMAH'ta ele alınan olası 12 kritik olayı eşleştiren matris aşağıda verilmiştir:

Tablo 5: Ekipman Tipi (EQ) - Kritik olay (CE) matrisi

	CE1 Bozunma	CE2 Patlama	CE3 Materyallerin yer değiştirmesi (hava hareketiyle)	CE4 Materyallerin yer değiştirmesi (sıvı hareketiyle)	CE5 Yangın başlangıcı (LPI)	CE6 Ekipmanın cidarında buhar fazında yırtılma meydana gelmesi	CE7 Ekipmanın cidarında sıvı fazında yırtılma meydana gelmesi	CE8 İçeriğinde sıvı fazda kimyasal bulunan borusunda sızıntı	CE9 İçeriğinde gaz fazda kimyasal bulunan borusunda sızıntı	CE10 Ani Yırtılma (Felakete neden olan çatlak)	CE11 Ekipmanın parçalanması – Kanal çökmesi	CE12 Prosesin bir bölümünün veya çatının Çökmesi
EQ1 Katı halde depolama	X	X	X	X	X							
EQ2 Katının küçük paketler halinde depolanması					X					X		
EQ3 Sıvının küçük paketler halinde depolanması					X	X	X			X		
EQ4 Basınç altında depolama					X	X	X	X	X	X		
EQ5 Yalıtılmış halde depolama					X		X	X		X	X	
EQ6 Atmosferik basınçta depolama					X		X	X		X	X	X
EQ7 Kriyojenik depolama					X	X	X	X	X	X	X	
EQ8 Basınçlı Taşıma (iletim) Ekipmanı/Aracı					X	X	X	X	X	X		
EQ9 Atmosferik Taşıma (iletim) Ekipmanı/Aracı					X		X	X		X	X	
EQ10 Boru İletim Ağı					X			X	X			
EQ11 Prosese dahil edilmiş ara depolama ekipmanı	X	X	X	X	X	X	X	X	X	X	X	X
EQ12 Maddelerin fiziksel veya kimyasal olarak ayrışmasını sağlayan ekipmanlar					X	X	X	X	X	X		
EQ13 Kimyasal reaksiyon içeren ekipmanlar					X	X	X	X	X	X		
EQ14 Enerji üretimi ve ısı değişiminde kullanılan ekipmanlar					X	X	X	X	X	X		
EQ15 Paketleme ekipmanları			X	X	X			X	X			
EQ16 Diğer ekipmanlar					X	X	X	X	X	X		

2. Ele alınan maddenin fiziksel hali ile olası 12 kritik olayı eşleştiren matris aşağıda gösterilmiştir:

Tablo 6: Maddenin fiziksel hali (STAT) - Kritik olay (CE) matrisi

	CE1 Bozunma	CE2 Patlama	CE3 Materyallerin yer değiştirmesi (hava hareketiyle)	CE4 Materyallerin yer değiştirmesi (sıvı hareketiyle)	CE5 Yangın başlangıcı (LPI)	CE6 Ekipmanın cidarında buhar fazında yırtılma meydana gelmesi	CE7 Ekipmanın cidarında sıvı fazında yırtılma meydana gelmesi	CE8 İçeriğinde sıvı fazda kimyasal bulunan borusunda sızıntı	CE9 İçeriğinde gaz fazda kimyasal bulunan borusunda sızıntı	CE10 Ani Yırtılma (Felakete neden olan çatlak)	CE11 Ekipmanın parçalanması – Kanal çökmesi	CE12 Prosesin bir bölümünün veya çatının Çökmesi
Katı STAT1	X	X	X	X	X	X			X	X		
Sıvı STAT2					X		X	X		X	X	X
Çift Fazlı STAT3					X	X	X	X	X	X		
Gaz/Buhar STAT4					X	X			X	X		

Bu iki matris bir arada kullanılarak, her bir tehlikeli ekipman için içerdiği tehlikeli maddenin fiziksel haline bağlı olarak meydana gelebilecek kritik olayların bir listesinin oluşturulması mümkündür.

2.3.3 Her bir kritik olay için hata ağaçlarının oluşturulması (MIMAH - Adım 5)

MIMAH, D.1.C.. [1]'in Ek-4'ünde yayınlanan 14 genel hata ağacını önermektedir. Hata ağaçlarının yapısı ve bu ağaçların oluşturulmasına yönelik metotlar D.1.C.. (MIMAH 5.Adım) [1] bölümünde verilmiştir.

Tablo 7: Her bir kritik olay için kapsamlı hata ağaçlarının listesi

CE Numarası	**Kritik Olay**	**Kapsamlı Hata Ağacı (FT)**
CE1	Bozunma	FT Kimyasal Bozunma FT Noktasal Tutuşma Kaynağına Bağlı Bozunma FT Termal Bozunma

CE2	Patlama	FT Patlayıcı bir maddenin patlaması FT Patlama (ani reaksiyon)
CE3	Materyallerin yer değiştirmesi (hava hareketi ile)	FT Hava hareketiyle materyallerin yer değiştirmesi
CE4	Materyallerin yer değiştirmesi (sıvı hareketi ile)	FT Sıvı hareketiyle materyallerin yer değiştirmesi
CE5	Yangın başlangıcı (LPI)	Yangın başlangıcı (fiziksel bütünlüğün kaybedilmesi)
CE6	Ekipmanın cidarında buhar fazında yırtılma meydana gelmesi	FT Kapta büyük çatlak ya da boruda sızma FT Kapta orta derecede çatlak ya da borudan sızma FT Kapta küçük derecede çatlak ya da borudan sızma
CE7	Ekipmanın cidarında sıvı fazında yırtılma meydana gelmesi	FT Kapta büyük çatlak ya da boruda sızma FT Kapta orta derecede çatlak ya da borudan sızma FT Kapta küçük derecede çatlak ya da borudan sızma
CE8	İçeriğinde sıvı fazda kimyasal bulunan borusunda sızıntı	FT Kapta büyük çatlak ya da boruda sızma FT Kapta orta derecede çatlak ya da borudan sızma FT Kapta küçük derecede çatlak ya da borudan sızma
CE9	İçeriğinde gaz fazda kimyasal bulunan borusunda sızıntı	FT Kapta büyük çatlak ya da boruda sızma FT Kapta orta derecede çatlak ya da borudan sızma FT Kapta küçük derecede çatlak ya da borudan sızma
CE10	Ani Yırtılma (Felakete neden olan çatlak)	FT Katastropik Yırtılma
CE11	Ekipmanın parçalanması –Kanal çökmesi	FT Tank Çökmesi
CE12	Prosesin bir bölümünün veya çatının Çökmesi	FT Çatının Çökmesi

Her bir kritik olay için tanımlanmış olan genel hata ağaçları, olası sebeplerin oluşturduğu bir kontrol listesi olarak düşünülmeli ve kullanılan ekipmanın karakteristik özelliklerine göre değiştirilebilmelidir

(başka olası sebepler eklenerek veya çıkartılarak). Dahası, başka risk değerlendirme metotları bu sebeplere ek olabilecek başka sebepler öngörüyorsa bu sebepler de hata ağacına dahil edilmelidir.

2.3.4 Her bir kritik olay için olay ağaçlarını oluşturulması (MIMAH Adım 6)

İncelenen her bir kritik olay için, matrislere dayalı olarak yürütülen otomatik bir metotla hata ağacı oluşturulmuştur. Bunun için gerekli olan veriler; dikkate alınan kritik olay, maddenin fiziksel hali ve tehlikeli özellikleridir (risk ibaresi).

Olay ağaçlarının oluşturulmasında kullanılan metot D.1.C..'in Ek-5 bölümünde tamamıyla açıklanmıştır. Burada bu metodoloji, temel prensipleri esas alınarak açıklanacaktır.

İlk olarak, seçilen ekipmanla ilişkilendirilen bir kritik olay için (bkz. paragraf 2.3.2) bu olaydan sonra ikincil kritik olay veya olayların da meydana gelebileceğinin bilinmesinde yarar vardır. Bu ikincil kritik olay veya olaylar tehlikeli maddenin fiziksel haliyle yakından ilişkilidir. Bir kritik olayda yer alan maddenin farklı fiziksel hallere sahip olması, birbirinden farklı ikincil kritik olay veya olayların oluşmasına sebep olabilir. Bu yüzden kritik olaylar (CE) ve maddenin fiziksel hali (STAT) ile ikincil kritik olayları (SCE) ilişkilendiren bir matris oluşturulur.

Aynı şekilde, ikincil kritik olaylarla (SCE) üçüncül kritik olayları (TCE) daha sonra ise üçüncül kritik olaylarla (TCE) tehlikeli olayları (DP) eşleştiren matrisler tanımlanır. Bu eşleştirmeler, tehlikeli maddenin fiziksel halinden bağımsızdır.

Tehlikeli olayların listesi aşağıdaki tabloda verilmiştir:

DP1: Birikinti (havuz) yangını	DP8: Şarapnel fırlaması/Yerinden fırlama
DP2: Tank Yangını	DP9: Aşırı basınç artışı
DP3: Jet yangını (jetfire)	DP10: Ateş topu
DP4: Buhar bulutu patlaması-VCE	DP11:Çevresel zarar
DP5: Ani Yangın (flashfire)	DP12: Toz patlaması
DP6: Toksik bulut	DP13: Kaynama taşması ve oluşan birikinti yangını
DP7: Yangın	

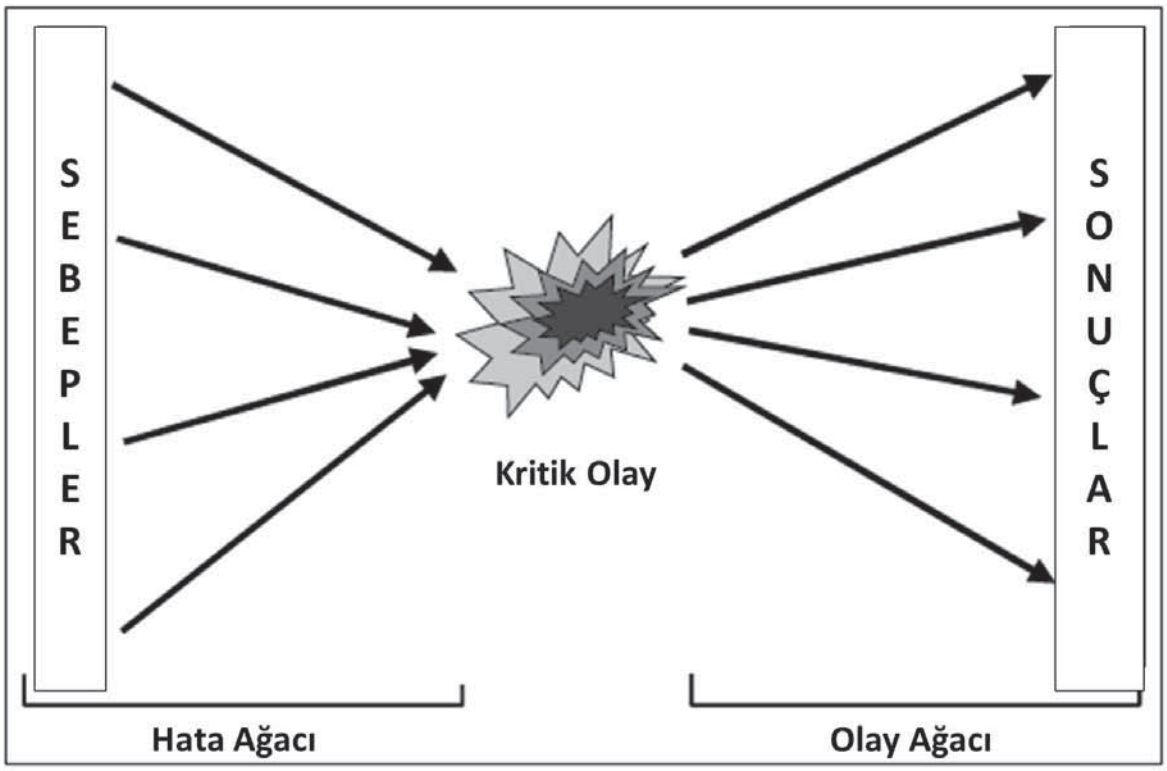
Son olarak, kullanılan maddenin tehlikeli özellikleri (risk ibareleri) "uygun tehlikeli olay"ın seçiminde dikkate alınmalıdır. Bu seçim, olay ağacının bazı dallarının silinmesine sebep olur. Bu seçimin yapılmasında ek olarak bazı kısıtlar kullanılmalıdır (bkz. D.1.C. Ek-5, paragraf 4 [1]). Eğer belirli bir ekipman ve iç veya dış koşullar için bazı olaylar mümkün değilse olay ağaçları üzerinde değişiklik yapılabilir.

Böylece MIMAH, seçilen her bir ekipman için papyon diyagramlarının oluşturulması ile sona erer. Her bir papyon diyagramı, bir kritik olayla, solunda bu kritik olaya karşılık gelen hata ağacı ve sağında bu olaya ait olay ağacının yer almasıyla, papyon şemasına göre elde edilir (MIMAH Adım 7). Her bir papyon diyagramı, seçilen ekipman için meydana gelebilecek büyük çaplı kazayı gösterir. Şekil 4'te merkezinde "Sıvı fazda kapta meydana gelen çatlak" kritik olayının yer aldığı örnek olarak verilen bir papyon diyagramı görülmektedir.

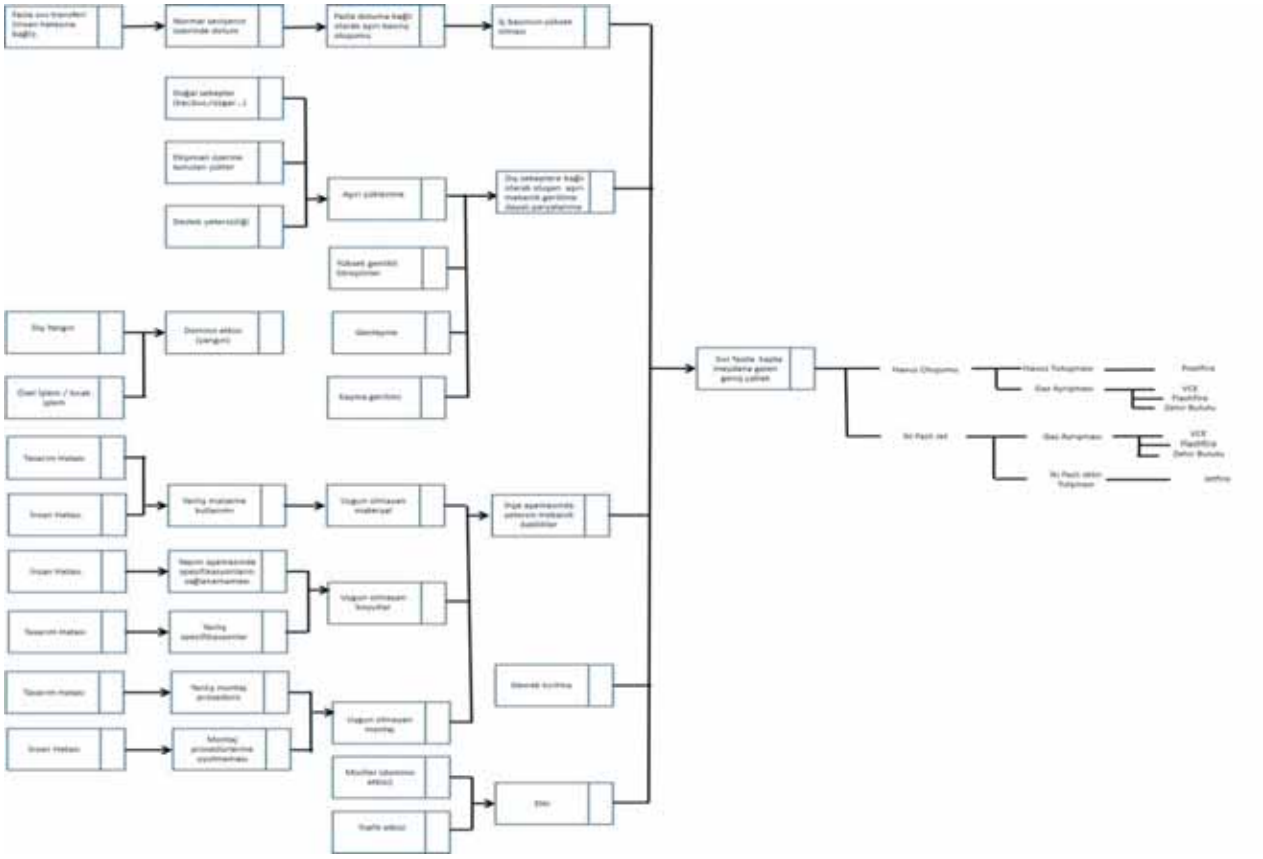
2.3.5. Değerlendirme

Her bir uygun tehlikeli ekipman ile ilişkilendirilmiş olan papyon diyagramları, herhangi bir güvenlik sisteminin olmadığı (güvenlik yönetim sistemleri dahil) veya bu sistemlerin etkin durumda olmadıkları varsayılarak meydana gelebilecek büyük çaplı kazalara ait riskleri göstermektedir. Bu diyagramlar, Referans Kaza Senaryolarının Tanımlanması Metodolojisi (MIRAS) için temel oluşturmaktadır.

Papyon diyagramlarının oluşturulması sürecinde, tesis yönetimiyle MIMAH yöntemiyle oluşturulan, olayların daha geniş kapsamlı olarak incelenmesinde birer araç ve kontrol listeleri olarak kullanılan geniş kapsamlı papyon diyagramları hakkında tartışabilmek için tesise ikinci bir ziyaretin gerçekleştirilmesi önerilmektedir. Kazaların gerçek sebepleri ve sonuçları üzerine yapılan araştırmalar geniş kapsamlı papyon diyagramları ile ve aynı zamanda diğer risk analizi araçlarının (HAZOP veya bir kazanın olası sebeplerini ortaya koyan diğer sistematik risk analizi metotları) yardımıyla yapılabilir. HAZOP yöntemi, özellikle proses ekipmanları için bazı olası sebeplerin tanımlanması amacıyla oluşturulan kapsamlı hata ağaçlarının oluşturulmasında tamamlayıcı bir yöntem olarak kabul edilmektedir. Burada aynı zamanda tesis içerisinde yapılan diğer risk analizlerinin kullanılması da mümkündür.



Şekil 5: Papyon diyagramının genel şeması



Şekil 6: Papyon diyagramı örneği

3. GÜVENLİK BARİYERLERİNİN TANIMLANMASI VE PERFORMANSLARININ DEĞERLENDİRİLMESİ

3.1. AMAÇ

Sadece büyük kaza senaryolarını hesaba katmak risk seviyesinin değerinden fazla hesaplanmasına neden olabilir ve güvenlik sistemlerinin uygulanmasını teşvik etmez. Bu problemle yüzleşebilmek için güvenlik sistemlerinin etkisine ve kaza senaryolarının tanımlanmasındaki güvenlik yönetimine odaklanmak gereklidir. Bu yaklaşımla risk seviyesinin daha kesin bir şekilde hesaplanması ve güvenlik sistemlerinin uygulanmasının teşvik edilmesi amaçlanmaktadır.

Bu bölümün amacı, kritik olayların oluşma olasılığı ve kazaların sonuçları üzerinde etkisi olan güvenlik sistemlerini tanımlamak ve güvenlik bariyerlerinin sağ tarafında bulunduğu bir papyon (bow-tie) diyagramı elde etmektir. Güvenlik bariyerleri tanımlanıp, papyon üzerinde yerleştirildiğinde, performanslarının (güvenirlilik seviyesi, etkinlik ve tepki süresi) değerlendirilmesi ve güvenlik bariyerlerinin kabul edilebilir bir risk seviyesi elde etmek için güvenlik gereksinimlerini karşılayıp karşılamadıklarının doğrulanması gerekir.

3.2. GÜVENLİK FONKSİYONLARINI VE BARİYERLERİNİN TANIMLANMASI

Bu adım, güvenlik fonksiyonu ve güvenlik bariyerleri kavramları sayesinde yerine getirilmektedir. Güvenlik fonksiyonları teknik veya organizasyonel fonksiyonlardır ama nesne değildirler. Başarılması gereken eylemelere göre ifade edilirler. Eylemler dört temel işlev ile tanımlanır: kaçınmak, önlemek, kontrol etmek ve sınırlamak. Bu eylemler güvenlik bariyerleri sayesinde gerçekleştirilmelidir. Güvenlik bariyerleri fiziksel ve mühendislik sistemleridir veya insan eylemleridir. Güvenlik fonksiyonu güvenliği sağlamak, artırmak ve/veya desteklemek için neye ihtiyaç duyulduğu ile ilişkiliyken, güvenlik bariyeri ise güvenlik fonksiyonlarının nasıl yerine getirileceği ile ilişkilidir.

Güvenlik fonksiyonları ve bariyerlerini tanımlamak için, papyonun her bir olayı dal dal incelenmeli ve sonra şu soru cevaplanmalıdır: "bu olaydan kaçınmayı, olayı engellemeyi, kontrol etmeyi veya sınırlamayı sağlayan bir güvenlik bariyeri var mı?" Eğer cevap evet ise bariyer dal üzerine yerleştirilir. Bariyer, bu olaydan kaçınmayı veya bu olayı önlemeyi sağlıyorsa kritik olayın sol tarafına, eğer olayı kontrol ediyor veya sınırlandırıyorsa kritik olayın sağ tarafına yerleştirilir.

3.3. GÜVENLİK BARİYERİNİN GÜVENİRLİLİK SEVİYESİ

Bir güvenlik bariyerinin güvenirlilik seviyesi (Level of Confidence, LC), belirli bir zaman periyodu içinde ve belirli koşullar altında belirli bir etkinlik (E) ve tepki süresine (RT) göre gereken bir güvenlik fonksiyonunu düzgün bir şekilde yerine getirmesi istendiği andaki hata olasılığıdır. Gerçekte bu kavramda güvenlik donanımlı sistemler için IEC 61511 [3] standardında tanımlanan SIL (Güvenlik Bütünlük Seviyesi) kavramından esinlenilmiştir ve güvenlik bariyerlerinin tüm çeşitlerini kapsayacak şekilde genişletilmiştir.

Güvenirlilik seviyesi, gerekirse bariyerden (detektör, arıtma sistemi, eylem) oluşan farklı alt sistemleri de içerecek şekilde tüm güvenlik bariyerleri (tek bir cihaz için değil) için hesaplanacaktır. Her bir

alt sistem için güvenlik seviyesi, etkinlik ve tepki süresi hesaplanacak ve bariyerin genel güvenlik seviyesi değerinin hesaplanması için toplanacaktır.

Bir alt sistem A tipi veya B tipinden herhangi birisi olabilir. Her bir tipin tanımı aşağıda verilmiştir:
A tipi alt sistemde:

- Tüm bileşenlerinin arıza biçimleri iyi bir şekilde tanımlanmıştır ve
- Hata koşulları altında alt sistemin davranışı tamamıyla belirlenmiştir ve
- Alt sistem için saha deneyiminden elde edilmiş güvenilir arıza verileri mevcuttur ve bu veri gereken hedef arıza ölçütünü karşıladığını göstermek için yeterlidir.

(Örnek: valf gibi mekanik cihazlar)

B tipi alt sistemde:

- En az bir bileşeninin arıza biçimi iyi tanımlanmamıştır veya
- Hata koşulları altında alt sistemin davranışı tamamıyla belirlenmemiştir veya
- Alt sistem için saha deneyiminden elde edilmiş güvenilir arıza verileri yoktur ve gereken hedef arıza ölçütünü karşıladığını göstermek için yeterli değildir.

(Örnek: işlemciler ve alt sistem donanımları gibi karmaşık sistemler)

Bir güvenirlilik seviyesine ulaşmak için, güvenlik bariyeri iki kritere uygun olmalıdır; ilki kalitatif (mimari kısıtlamalar) ve ikincisi kantitatif (tehlikeli arızanın olasılığı) kriterdir.

Alt sistemler için mimari kısıtlara ilişkin kalitatif kriter (A tipi ve B tipi) Tablo 8 ve Tablo 9'da tanımlanmıştır. Bu tablolar IEC 61508 [4] standardından alınmıştır.

A tipi için: tüm arıza biçimleri iyi bilinmektedir.

Tablo 8: A tipi için mimari kısıtlamalar

SFF: **Güvenli Arıza Kesri**	**Hata Toleransı**		
	0	**1**	**2**
< %60	LC 1	LC 2	LC 3
%60 - < %90	LC 2	LC 3	LC 4
%90 - <% 99	LC 3	LC 4	LC 4
≥ %99	LC 4	LC 4	LC 4

B tipi için: tüm arıza biçimleri bilinmemektedir.

Tablo 9: B tipi için mimari kısıtlamalar

SFF: **Güvenli Arıza Kesri**	**Hata Toleransı**		
	0	**1**	**2**
< %60	Mümkün değil	LC 1	LC 2
%60 - < %90	LC 1	LC 2	LC 3
%90 - < %99	LC 2	LC 3	LC 4
≥ %99	LC 3	LC 4	LC 4

Alt sistemler için (A tipi ve B Tipi) talep moduna bağlı olarak ve arıza olasılığına ilişkin kantitatif kriter Tablo 10 ve Tablo 11'da tanımlanmıştır.

Tablo 10: Güvenirlilik Seviyesi: Düşük talep modunda çalışan bir güvenlik bariyerine ait güvenlik fonksiyonu için arıza oranları (IEC 61508 standardından)

Güvenirlilik Seviyesi	**Düşük talep modlu çalışma** (Tasarım fonksiyonunu talep üzerine yerine getirirken karşılaşılacak arızanın ortalama olasılığı)
LC 4	$\geq 10^{-5} - < 10^{-4}$
LC 3	$\geq 10^{-4} - < 10^{-3}$
LC 2	$\geq 10^{-3} - < 10^{-2}$
LC 1	$\geq 10^{-2} - < 10^{-1}$

Tablo 11: Güvenirlilik Seviyesi: Yüksek talep veya sürekli modda çalışan bir güvenlik bariyerinde güvenlik fonksiyonu için arıza oranları (IEC 61508 standardından)

Güvenirlilik Seviyesi	**Yüksek talep veya sürekli modlu çalışma** (Saat başına tehlikeli arıza olasılığı)
LC 4	$\geq 10^{-9} - < 10^{-8}$
LC 3	$\geq 10^{-8} - < 10^{-7}$
LC 2	$\geq 10^{-7} - < 10^{-6}$
LC 1	$\geq 10^{-6} - < 10^{-5}$

Tüm bariyerin genel güvenirlilik seviyesi bariyeri oluşturan alt sistemlere ait en küçük güvenirlilik seviyesine eşittir.

Etkinlik(E), teknik güvenlik bariyerinin belirli koşullarda performansında azalma olmaksızın bir süre için bir güvenlik fonksiyonunu yerine getirebilme yeteneğidir.

Tepki süresi (RT), güvenlik bariyerinin çalışmaya başlaması ile güvenlik bariyeri tarafından gerçekleştirilen güvenlik fonksiyonunun tam olarak başarılması (etkinliğe eşit) arasında geçen süredir. Etkililik ve tepki süresi genel bir şekilde bilinemez. Tedarikçilerden, tecrübelerden, normlardan, teknik kılavuzlardan ve veri sayfalarından elde edilen bilgilerle belirlenebilir.

Bu üç parametrenin değerlendirilmesi yöntemi D.1.C.. [1] Ek 9'da detaylı olarak açıklanmıştır. Güvenlik bariyerlerinin performansını değerlendirmeden önce tanımlanan her bir güvenlik bariyeri, aşağıda ifade edilen minimum gereksinimleri karşılamalıdır (bkz. D.1.C.. ek 9, paragraf 2)

- Güvenlik bariyerinin bileşenleri, düzenleme sistemlerinden (temel proses kontrol sistemleri) bağımsız olmalıdır. (güvenlik ve düzenleme sisteminin ortak arızaları kabul edilemez). Bu kıstas aynı fonksiyonu yerine getiren farklı iki sisteme de uygulanabilir.

- Bariyerlerin tasarımı mevzuata (yönetmelikler, standartlar, normlar vb.) uygun bir şekilde yapılmalıdır. Tasarım ortamda var olan maddelerin ve çevrenin karakteristiklerine uyarlanmalıdır.
- Bariyerler etkinliği kanıtlanmış (tecrübe edilmiş) bir prensibe dayanmalıdır. Aksi halde, işyerinde bariyerin niteliğini test etmek için birçok test yapmak gerekebilir.
- Bariyerler belirlenmiş bir sıklıkta test edilmelidir. Testlerin sıklığı operatör deneyimine veya tedarikçiye bağlı olacaktır.
- Bariyerlerin önleyici bir bakım planı bulunmalıdır.

Sistem mimari analizini (bariyerler bağımsızsa, güvenli-arıza modlu ise…) ve periyodik testleri de içeren bariyerlerin önceki performans değerlendirmesi, güvenlik bariyerlerinin uygun olarak hesaba katılıp katılmayacağına, papyon (bow-tie) üzerine yerleştirilip yerleştirilemeyeceğine ve güvenlik seviyesinin değerlendirilip değerlendirilmeyeceğine karar vermek için önemlidir.

3.4. RİSK AZALTIM HEDEFİNİN BELİRLENMESİ

"Risk Graf" olarak adlandırılan ve IEC 61508/61511 standartlarının ilkelerine dayanan bir araç geliştirilmiştir. Papyondaki belirli bir neden için, onun oluşma sıklığı ve olası sonuçlarına (nedenin yol açabileceği en tehlikeli olay nedeniyle) bağlı olarak, kabul edilebilir bir risk seviyesi elde etmek için incelenen senaryoda güvenlik bariyerlerinin gereken güvenirlilik seviyesi belirlenir.

Risk Graf yöntemi D.1.C. [1] Ek 14 'te tam olarak tanımlanmış ve açıklanmıştır. Bu yöntem tasarım aşamasında konulmak zorunda olan güvenlik sistemlerinin önemini değerlendirmek için özellikle kullanışlıdır. Aynı yöntem güvenlik sistemlerinin olası senaryoları önlemek için yeterli olup olmadığını doğrulama amacıyla hali hazırda kullanılan ekipmanlar için de kullanılabilir.

Risk Graf'tan elde edilen sonuçlar Risk Matrisinden elde edilen sonuçlarla aynı olmayabilir. Risk Graf, papyonun her bir dalını ayrı olarak hesaba katar (bir nedenden tehlikeli olaya kadar). Risk Matrisi ise nedenlerin birleşiminden oluşan papyondaki tehlikeli olay dizisini dikkate alır.

3.5. ÖRNEK

Bu paragrafta bariyer çeşitlerine (pasif, aktif veya insan eylemleri) göre birkaç güvenlik bariyeri için güvenirlilik seviyesi örnekleri verilecektir.

3.5.1. Pasif Bariyerler

Pasif bariyerler, fonksiyonlarını gerçekleştirmek için herhangi bir insan eylemine, enerji ve bilgi kaynağına ihtiyaç duymaksızın sürekli bir şekilde çalışan ekipmanlardır. ARAMIS yönteminde, herhangi bir pasif bariyere genel bir "Talep Anındaki Arıza Olasılığı"(Probability of Failure on Demand, PFD) atanmasına karar verilmiştir. Bu değer, güvenirlilik Seviyesi (LC) ile karşılaştırılabilen, kaza veri tabanlarından ve kazalardan öğrenilen tecrübelerden elde edilen bir değerdir.

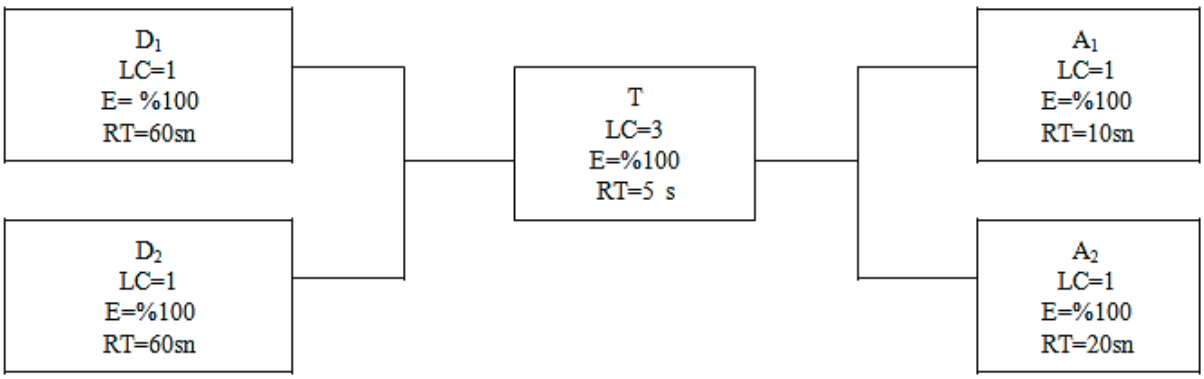
Tablo 12: Pasif bariyerler için güvenirlilik seviyesi örnekleri

Genel Pasif Güvenlik Bariyerleri	Literatürden ve endüstriden elde edilen PFD (boyutsuz)	Bariyerin Güvenirlilik Seviyesi
Bent (Etkili tutma kapasitesi ve sızdırmazlık)	10^{-2} - 10^{-3}	2
Yangın duvarı (etkili maksimum süre) / patlamalara karşı koruyucu duvar / sığınak	10^{-2} - 10^{-3}	2
Patlama riski (Etkili algılama basınç değeri ve bakım)		2
Tasarıma bağlı yapısal güvenlik yeteneği (Kalınlık, materyal kalitesi vb.)		4

Pasif bariyerler için güvenirlilik seviyeleri örnek olarak verilmiştir. Güvenlik yönetimine bağlı olan tamamlayıcı kriterler (bent boşaltma prosedürleri, bakım prosedürleri vb.) ile değiştirilebilir.

3.5.2. Aktif Bariyerler

Aktif bariyerler zincir halinde üç alt sistemden oluşur: Algılama sistemi (D), işleme sistemi (T) (lojik çözümleyici, röle, mekanik cihaz, güvenlik kilitleme sistemi (interlock, insan…) ve eylem (A) (aktüatör, mekanik, güvenlik donanımı, insan). Şekil 7 bir güvenlik bariyeri için genel bir güvenirlilik seviyesi kombinasyonunu göstermektedir.



Şekil 7: Güvenirlilik seviyesi kombinasyonu için genel konfigürasyon

Belli alt sistemler için güvenirlilik seviyesi, etkililik ve tepki süresinin değerleri Tablo 13'te verilmiştir. Etkililik ve tepki süresi her bir tesise göre uyarlanmalıdır.

Tablo 13: Alt sistemler için güvenirlilik seviyesi, tepki süresi ve etkililik örnekleri

Sistem	Güvenirlilik Seviyesi (LC)	Tepki Süresi (RT)	Etkililik (E)
Güvenlik amaçlı kapama valfi	1	10 ila 50 sn[1]	%100
Otomatik testli valf	2		
Basınç Emniyet Valfi[2]	1 (2)		
Basınç sivici	1	< 5sn	
Vantilatör	1	< 30sn	
Sınırlandırılmış alandaki gaz detektörü	/	15 sn ila 1,5 dk[3]	%100
Klasik röle	1	< 5sn	%100
Programlanabilir Lojik Kontrolör (güvenlik amaçlı tasarıma sahip) (Sertifikalı)	Sertifikasına bakınız	< 5sn	%100

[1] Değer, sistemin türüne ve işletme koşullarına bağlıdır.
[2] Güvenlik valfi için genellikle 2 değeri kabul edilir.
[3] Değer gazın türüne bağlıdır.

3.5.3. İnsan Eylemleri

Pasif bariyerlerde olduğu gibi, güvenirlilik seviyesinin değerlendirilmesinde IEC 61508/61511 standartlarının ilkeleri uygulanamaz. ARAMIS yönteminde, insan eylemlerinin, denk bir güvenirlilik seviyesinden türetilen genel bir "Talep Üzerine Arıza Olasılığı" (Probability of Failure on Demand, PFD) ile ilişkilendirilmesine karar verilmiştir.

Tablo 14: İnsan eylemleri için güvenirlilik seviyesi örnekleri

İnsan Bariyerleri	PFD (Literatür ve endüstriden)	Güvenirlilik Seviyesi (LC)
Önleme	10^{-2} (PFD)	LC 2
Normal işletme	10^{-2} (PFD)	LC 2
Müdahale	10^{-2} (PFD)	LC 1

İnsan bariyerleri için bu seviyeler örnek olarak verilmiştir. Diğer birkaç kriter (operatörün eyleme geçmek için ihtiyaç duyduğu zaman, müdahale anıda meydana gelen stres gibi davranışı etkileyen faktörler vb.) bu güvenirlilik seviyelerini değiştirebilir.

3.6. DEĞERLENDİRME

Papyon üzerine yerleştirilen güvenlik bariyerlerinin belirlenmesi "proses ve enstrümantasyon diyagramları" ve "akış diyagramları" veya diğer mevcut dokümanların yardımı ile tesis operatörleriyle birlikte yapılabilir/yapılmalıdır.

D.1.C.-Ek 8 dokümanındaki kontrol listesi, papyonlardaki fonksiyonların ve bariyerlerin tanımlanmasına yardımcı olacaktır. Kontrol listesi aynı zamanda yeni bir tesis üzerinde nelerin uygulanması gerektiğini belirlemek için veya "Risk Graf" yöntemine göre mevcut tesiste tatmin edici olmayan bir güvenlik seviyesini iyileştirmek için de kullanılabilir.

Ayrıca, ilk adımda D.1.C. Ek 9 verilen yönerge yardımıyla değerlendirilen güvenirlilik seviyesinin "tasarım" güvenirlilik seviyesi olduğunu vurgulamak gerekir. Bunun anlamı bariyerin kurulduğu zamandaki kadar etkin olduğu varsayımı anlamına gelmektedir. Ama güvenlik bariyerinin performansı güvenlik yönetim sisteminin niteliğine göre zaman geçtikçe azalabilir.

İkinci adımda, D.1.C. Tablo 10 (MIRAS - Adım 3.B) da gösterildiği şekilde belirlenen güvenlik bariyerlerinin sınıflandırılması gerekir. Bu sınıflandırma güvenlik bariyerlerinin performansları üzerinde güvenlik yönetim sisteminin etkisini değerlendirmek için kullanılır.

4. BARİYER GÜVENİRLİLİĞİ ÜZERİNDE GÜVENLİK YÖNETİM ETKİNLİĞİNİN DEĞERLENDİRİLMESİ

4.1. AMAÇ

Büyük Kaza Önleme Politikasında uygulanan güvenlik yönetimi, teknik, insan ve organizasyonel faktörlerle ilişkili eylemlerin tanımlanmasını sağlar. Güvenlik yönetiminin işletme için amacı, bariyerlerin (teknik veya davranışsal olarak) şartnamelerinde tanımlandığı gibi maksimum etkinlik seviyesinde olmasını sağlamak ve bunu sürdürmektir. Bariyerlerin etkinliği kazalara karşı organizasyonel ve yönetimsel bakış açısına (bakım, prosedürlerin yeterliliği, personelin güvenlik davranışları vs.) bağlıdır. Güvenlik yönetimi çok sayıda sorumluluk, görev ve fonksiyonlardan oluşur.

Güvenlik yönetimi, senaryoların oluşma olasılığını etkiler. Bu nedenle güvenlik yönetiminin değerlendirilmesinin amacı, kazaları önlemede güvenlik yönetiminin etkinliğini değerlendirmektir. Güvenlik yönetimi aşağıdaki unsurları içerir:

- Tehlike ve riskleri belirlemek için tehlike ve risk analizi,
- Riskleri azaltmak amacıyla güvenlik bariyerinin seçilmesi, uygulanması ve bakımı.

Genelleştirilmiş hata ve olay ağacına (papyonlara) dayanan MIRAS yöntemi (bkz. bölüm 5) SEVESO II kapsamındaki kuruluşlara risk analiz sürecinde yardım eder. Risk analiz faaliyetinin sonuçlarından biri mevcut güvenlik bariyerlerinin ve (eğer uygulanabiliyorsa) daha ileri güvenlik bariyerlerinin uygulama ihtiyacının tanımlanmasıdır.

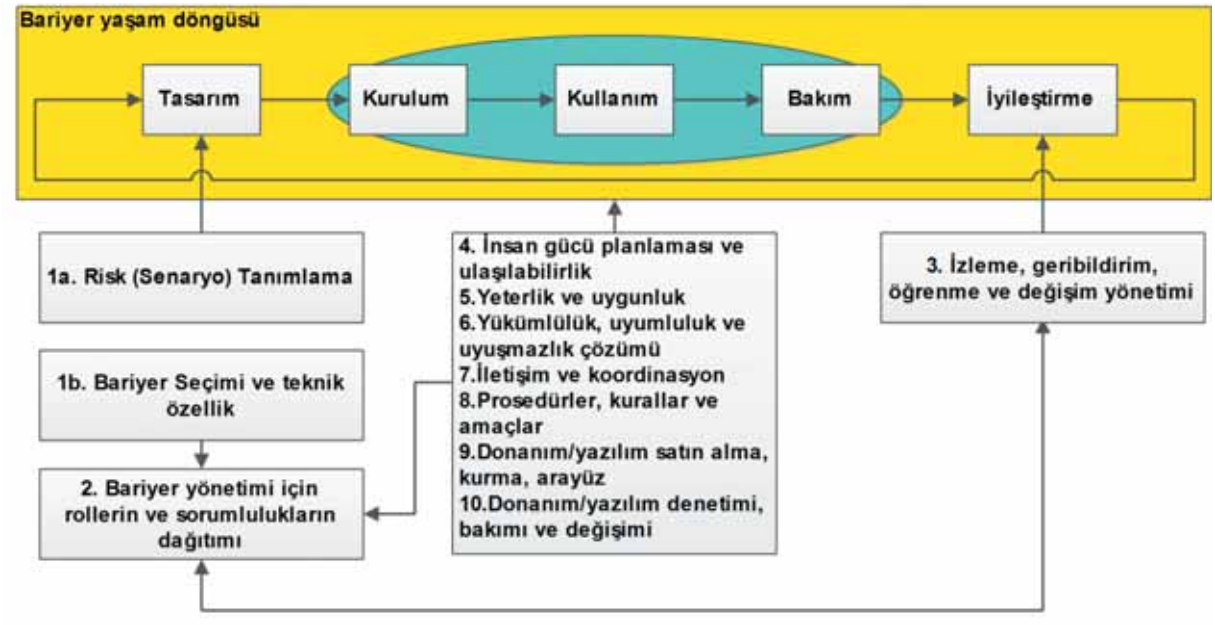
Tüm gerekli güvenlik bariyerleri tanımlanıp seçildiği zaman, güvenlik yönetiminin sonraki görevi ömürleri boyunca güvenlik bariyerlerinin etkinliğini sağlamaktır. Örneğin bariyerlerin yaşam döngüsünün yönetilmesi gerekir.

4.2. ARAMIS GÜVENLİK YÖNETİMİ DEĞERLENDİRME KAVRAMI

Güvenlik yönetiminin değerlendirilmesi için ARAMIS yöntemi, güvenlik yönetim sistemindeki birkaç yapısal elemana ve birkaç güvenlik kültür faktörünün etkisini tanımlayan kavramlara dayanır. Bu kavram "Güvenlik Yönetim Etkinlik İndeksini Belirleme Yöntemi D.3.B"nin 2. bölümünde anlatılmıştır.

Yapısal faktörler ve belirli bir bariyerin yaşam döngüsü ile ilişkisi Şekil 6'daki gibi görselleştirilebilir. Yapısal faktörlerin her birine ilişkin fonksiyonları yerine getirmek için güvenlik yönetim sisteminin her bir yapısal faktör için bir "dağıtım sistemi" içermesi gerekir. Yapısal faktörlerin değerlendirilmesi güvenlik denetimi vasıtasıyla gerçekleştirilir. Sorumlulukların (2. eleman) dağıtımını elde etmek için bir "eşleştirme" uygulaması gerçekleştirilirken, denetim Şekil 8'in 1. ve 3.-10. elemanlarını içerir. Bu eşleştirme, Şekil 8'de tanımlandığı gibi tesise bağlı uygulanan güvenlik yönetim sisteminin hangi bölümlerinin dağıtım sistemleriyle ilgili olduğunu tanımlar.

Güvenlik yönetiminin yapısal faktörlerine, "Güvenlik Yönetim Etkinlik İndeksini Belirleme Yöntemi D.3.B"nin 2. ve 3. bölümünde ve ARAMIS Denetim Kitapçığında (Ek-A) detaylı bir şekilde değinilmiştir. Ayrıca dağıtım sistemlerindeki adımlar veya "kutular" ARAMIS Denetim Kitapçığında anlatılmıştır.



Şekil 8: Güvenlik bariyerlerinin yaşam döngüsünün yönetilmesi görevine ilişkin güvenlik yönetim organizasyonunun yapısal elemanları.

Şekildeki elips, güvenlik bariyerlerinin etkinliğinin tanımlanması ile ilgili olarak değerlendirmenin odağını gösterir.

Güvenlik yönetim sistemi veya yapısı; ilkeleri (politikaları), planları, sorumlulukları vb. içerir. Güvenlik yönetimi için yukarıdan aşağıya resmi bir çerçeve sağlar. İyi bir güvenlik yönetim yapısı etkin güvenlik yönetimi için gerekli bir koşuldur ama etkin güvenlik yönetimi aynı zamanda resmi olmayan düşünceler, normlar ve pratiklere de dayanır (örneğin aşağıdan yukarı işgücünün güvenlik kültürü gibi). Güvenlik kültürü planlanmış görevlerin ve prosedürlerin ne kadar iyi uygulandığı ve bağlantılı olduğunu belirler.

Bu nedenle güvenlik kültürü, güvenlik yönetiminin değerlendirmesinde dikkate alınan diğer bir husustur. Güvenlik yönetim sisteminin yapısal elemanlarıyla bağlantılı olarak, güvenlik yönetim fonksiyonlarının ne kadar iyi uygulandığını etkileyen güvenlik kültürü faktörlerinin bir dizisi olduğu açıktır.

Aşağıda sekiz adet kültürel faktöre değinilmiştir:

Öğrenme ve raporlamaya isteklilik: Bu faktör, çalışanların kaza ve olayları raporlamaya istekliliklerini veya isteksizliklerini, raporlamadan itibaren geribildirim algılarını ve öğrenilen derslerin yayılmasını içeren geniş bir faktördür. Bu aynı zamanda sadece kültürel bakımdan üst yönetime olan güvenle örtüşen bir konudur.

Güvenlik önceliklendirme, kurallar ve uyumluluk: Bu kapsamlı faktör, birkaç unsur ile kurallar ve yönergelerin kullanımını ve bunlara yatkınlığı; güvenliğin önceliklendirilmesine karşı verimlilik ve işin kolaylaştırılması; güvenlik prosedürlerinin ihlal edilebildiği koşullara kadar genişletilebilen tekil birkaç göstergeden oluşur.

Üst yönetim müdahalesi ve yükümlülük: Bu faktör açık bir şekilde hem yönetim, hem yöneticinin hem de takım liderlerinin müdahalesi ve yükümlülükleri ile ilişkilidir. Ayrıca onların yükümlülük ve müdahalesinin çalışan tarafından algılanmasını da içerir.

Risk ve insan performans kısıtlama algısı: Çalışma alanının türüne göre değişebilen bir faktör olmakla birlikte tehlikelere, risklere ve olası insan hatalarına (yorgunluk, otomasyon vb.) karşı yönetim ve çalışanların bilinci ile ilişkilidir.

Hissedilen sorumluluk: Bu faktör, işyerinde güvenlikten sorumlu olan kişinin çalışan algısı ile ilişkilidir.

Güven ve tarafsızlık: Bu faktör yönetimin çalışanlara güveninnin yanısıra önemli bir biçimde de çalışanların üst yönetime ve amirlerine güveni ve işyerindeki çalışanların tarafsızlık algısı ile ilişkilidir.

Çalışma takımı ortamı ve desteği: Bu faktör, çalışanların takım çalışması algısı ve kendi takımlarındaki takım ruhuyla ilişkilidir. Takımın üyelerine destek verilmesi ve yardım edilmesi, tehlikelere karşı diğer çalışanlarla konuşma ve uyarmaya istekli olma şeklinde genişletilebilir.

Motivasyon, etki ve müdahale: Bu faktör, algılara ilişkin dört unsur içerir: (i) işin ne anlama geldiği; (ii) iş planlama ve yürütümü üzerindeki kendi etkisi; (iii) motivasyon ve müdahale; (iv) bilgilendirilmiş hissetme ve işi tahmin edilebilir bulma.

Kendine özgü tehlikeleri içeren bir tesiste güvenlik yönetiminin değerlendirilmesi aşağıdakilerin bir kombinasyonuyla gerçekleştirilir:

1. On adet yapısal unsur kavramını kullanan güvenlik yönetim sisteminin denetimi ve tesise bağlı güvenlik yönetim sisteminin seçilen temsili bariyer dizisini nasıl ele aldığına odaklanma (örneğin gerçek ve mevcut güvenlik bariyerlerine ilişkin somutlaştırma gibi),
2. Tesisteki çalışanlar arasında güvenlik kültürünün anket temelli incelenmesi.

Bir sonraki bölüm değerlendirmenin ve gerekli dokümantasyonun nasıl gerçekleştirilmesi gerektiğini adım adım tanımlamaktadır.

4.3. DEĞERLENDİRME SÜRECİNİN ADIM ADIM TANIMLANMASI

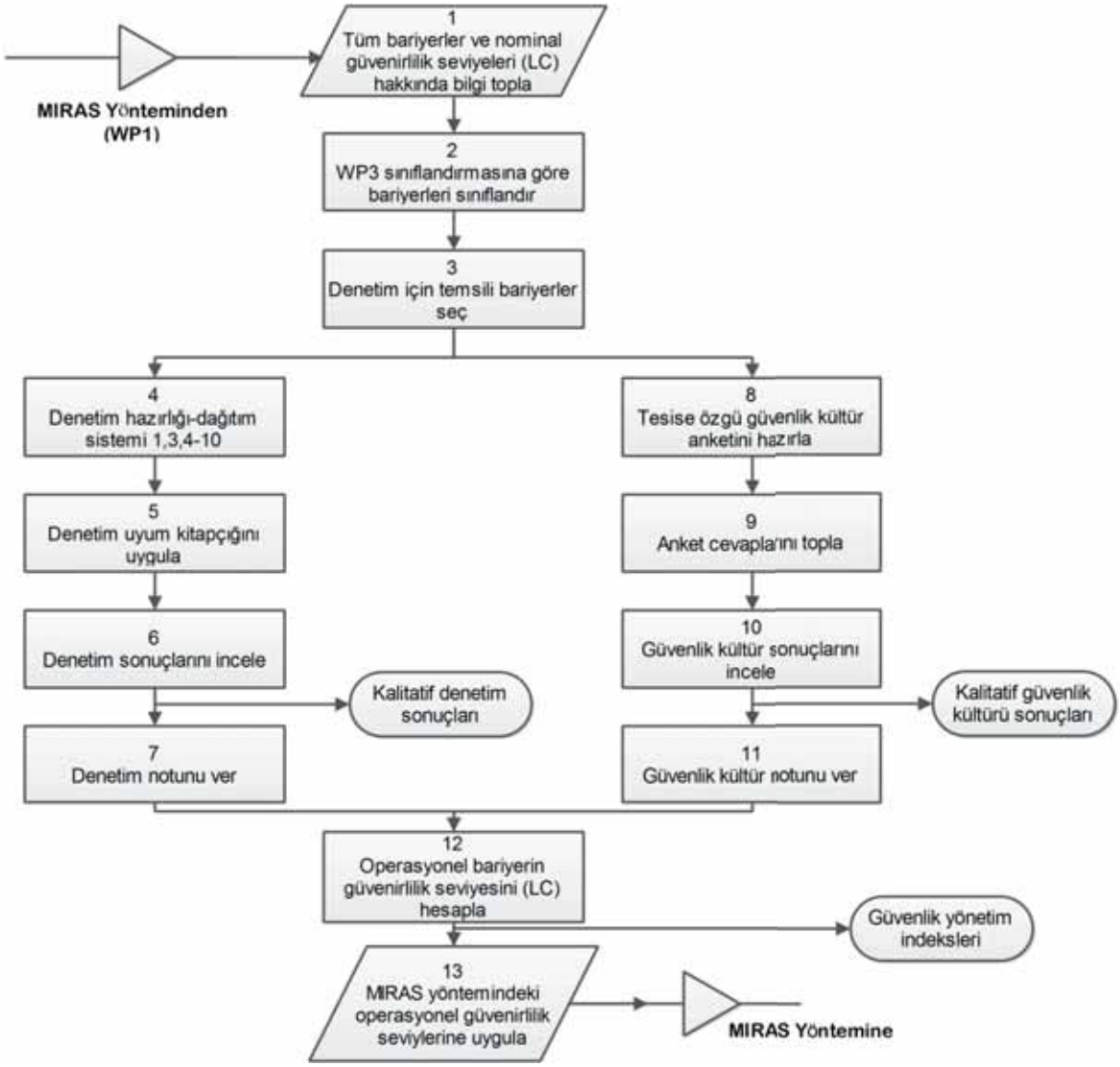
Şekil 9'daki akış diyagramında değerlendirme süreci görselleştirilmiştir. Bu adımlar takip eden bölümlerde anlatılacaktır.

4.3.1. Adım 1: Tüm bariyer ve nominal güvenirlilik seviyesi (LC) değerleri ile ilgili bilgi toplama

Güvenlik yönetim değerlendirmesi, MIRAS yöntemini kullanarak yapılan risk analizi aracılığı ile oluşturulur (bkz. bölüm 5). MIRAS kaza senaryolarının (papyon ile görselleştirilerek) bir listesi oluşturur ve güvenlik bariyerleri tanımlanır. Bu bariyerler için "tasarım" güvenirlilik seviyesi değerlendirilir (bkz. D.1.C. Ek 9). Bu bilgi güvenlik yönetim değerlendirme sürecindeki bir girdidir.

4.3.2. Adım 2: Bariyerleri sınıflandırma

Bariyerleri uygulamak ve sürdürmek için gerekli güvenlik yönetim eylemleri, bariyerlerin özelliklerine ve bariyerlerin (donanım, yazılım veya insan davranışı) hangi elemanlardan oluştuğuna bağlıdır. Sonuç olarak, güvenlik yönetiminin değerlendirilmesi bu bariyerlerin özelliklerini hesaba katmayı gerektirir. Bundan dolayı, güvenlik bariyerleri için bariyerleri birlikte gruplandıran bir sınıflandırma şeması oluşturulmuştur. Sınıflandırma şeması tablo 15'te gösterilmiştir. Bu şema MIRAS yöntemindeki tablo (D.1.C. Tablo 10) ve ARAMIS Denetim Kitapçığındaki tablolarla aynıdır. Testlerden elde edilen tecrübeler tabloda verilen sınıflandırmanın önemsiz bir şey olmadığını göstermiştir. Burada yer alan tablodaki tanımlamalar birkaç zorluğu aşmak için bir miktar genişletilmiştir.



Şekil 9: Güvenlik yönetimi değerlendirmesi akış diyagramı

Tablo 15: ARAMIS güvenlik yönetimi sistemi değerlendirmesindeki bariyerlerin sınıflandırılması

	Bariyerler	**Örnekler**	**Algılama**	**Tanı/ Etkinleştirme**	**Eylem**
1	*Sürekli -pasif- Kontrol*[4]	Boru, hortum veya tank duvarı; korozyondan koruyan boya; tank mesneti, yüzer tavanlı tank kapağı; flanş bağlantısı; sızdırmazlık contaları salmastralar; tanktaki gözetleme delikleri	Yok	Yok	Donanım
2	*Sürekli -pasif- bariyer*	Tank seti, bent, drenaj, toplama çukuru, korkuluk, çit, patlamalara karşı koruyucu duvar, paratoner	Yok	Yok	Donanım
3	*Geçici -pasif* İnsanlar tarafından yerleştirilir (veya kaldırılır)	Tamir çalışması etrafındaki bariyerler, açık boru üzerindeki kör flanş, baret/eldiven/güvenlik ayakkabısı/gözlük, karışımdaki inhibitör	Yok	Yok (Çalışanlar tarafından yerleştirilmeli)	Donanım
4	*Sürekli - aktif*	Aktif korozyon koruma, ısıtma veya soğutma sistemi, havalandırma, ekipmanlara inert gaz sağlama sistemi	Yok	Yok (Belirli proses aşamaları için operatör tarafından aktifleştirilmesi gerebilir)	Donanım
5	Aktif bariyer veya kontrol -talep üzerine çalışan donanım-	Basınç emniyet valfi, lojik donanımlı kilitleme sistemi (interlok), yağmurlama (sprinkler) tesisatı, elektro-mekanik basınç, sıcaklık veya seviye kontrolü	Donanım	Donanım	Donanım
6	*Otomatikleştirilmiş- aktif*	Programlanabilir otomatik cihaz, kontrol sistemi veya kapatma sistemi	Donanım	Yazılım	Donanım
7	*Aktif - manuel* Aktif donanım algılaması tarafından tetiklenen insan eylemi	Enstrümanda okunan değere, alarma cevaben elle kapama veya ayarlama, tahliye, solunum cihazı takma, alarm üzerine itfaiyeyi arama, uzak kamera tarafından başlatılan eylem, tahliye valfi, valfi kapatıp/açma (doğrulama amaçlı)	Donanım	İnsan (Beceri, kural veya bilgiye dayalı)	İnsan/ uzaktan kontrol
8	*Aktif - ikaz* Pasif uyarıya dayalı insan eylemi	Tehlikeli alanda kişisel koruyucu ekipman kullanma, sigara içmekten kaçınma, beyaz çizgi içinde kalma, işaretlenmiş boruyu açma, tehlikeli alanlardan uzak durma	Donanım	İnsan (Kurala dayalı)	İnsan

9	*Aktif – yardım* Yazılım operatöre sistemle ilgili tanı verir	Uzman sistem kullanma	Donanım	Yazılım- İnsan (Kural veya bilgiye dayalı)	İnsan/ uzaktan kontrol
10	*Aktif – yöntemsel* Enstrüman kullanmadan lokal koşulların gözlemi	(Doğru olarak) çalıştırma/kapatma/yığın süreç prosedürünü izleme, donanım ayarlarını düzeltme, eylem veya tahliye için diğerlerini uyarma, hattı açmadan önce boşaltma/tahliye etme, tankeri sürme, su perdesini çalıştırma	İnsan	İnsan (Beceri veya kurala dayalı)	İnsan/ uzaktan kontrol
11	*Aktif - acil* Sapmanın anlık gözlemi + geçici önlem alma	Beklenmeyen acil duruma cevap verme, bakım esnasında geçici olarak uydurulmuş çözüm, yangınla mücadele	İnsan	İnsan (Bilgiye dayalı)	İnsan / uzaktan kontrol

[4] Kontrol ve bariyer arasındaki farklılık MORT (Management Oversight and Risk Tree) yöntemindeki terminolojiden kaynaklanır. Kontrol, (örneğin, seviye kontrolü gibi) temel prosesi gerçekleştirmek için gereken bir bileşendir. Ancak tehlikeleri kontrol etmeye de hizmet eder. Bariyer (tank etrafındaki set, basınç emniyet valfi) ise sadece tehlikeleri önlemek veya hafifletmek için kurulan bir bileşendir.

Tüm tanımlanmış bariyerler için Adım 12 çerçevesinde sınıflandırmanın yapılması gerekmektedir. Çünkü sınıflandırma operasyonel güvenirlilik seviyesinin hesaplanması için olup bu sınıflandırmanın biliniyor olması gerekmektedir.

Sınıflandırma dikkatli bir şekilde yapılmalıdır. Burada çeşitli problemlerle karşılaşılabilir. Patlama kapakları sıklıkla pasif bariyer olarak sınıflandırılır. Ancak, gerçekte güvenlik fonksiyonlarını gerçekleştirebilmeleri için aktifleştirilmeleri gerekir. Bu yüzden patlama kapakları sınıf 5 olarak sınıflandırılırlar. Alevlenebilir bir sıvı üzerinde yer alan inert gaz pasif bariyer olarak (sınıf 2) sınıflandırılır. Ancak, doldurma ve diğer işlemlerden sonra inert gazın tekrar yerine konulması ve bu asal gazı sağlayan, dağıtan ve tahliye eden bir sistem olması gerekir. Bu yüzden sınıflandırma sınıf 3 veya sınıf 4 olabilir. Herhangi bir tereddüt durumunda, bariyer sınıflandırılması, söz konusu olan bariyerin uygulanması ve bakımı için en önemli olan güvenlik yönetim yapısının (dağıtım sistemlerinin) elemanlarına bağlı olarak yapılır. Bariyerler ve güvenlik yönetim yapısının uygun elamanları arasındaki ilişki ve denetimin ilgili unsurları Şekil 10'da gösterilmiştir.

4.3.3. Adım 3: Denetim için temsili bariyerlerin seçimi

Genellikle uzun zaman aldığı için her bir senaryonun yönetimi ve her bir bariyer değerlendirilemez. Şiddet ve etkiye dayalı olarak makul bir seçim yapılmalıdır.

Bu adım sonucunda, denetime referans teşkil eden senaryo ve bariyerler dizisi elde edilmektedir. Bu bariyerlerin yönetim niteliği denetim sırasında değerlendirilecek ve tüm bariyer yönetim sistemine genellenecek daha sonrada sayısallaştırılacaktır.

Bu adıma ARAMIS denetim kitapçığında denetim sürecinin 1. adımı olarak detaylı bir şekilde değinilmiştir.

Tablo 15'teki sınıflandırma, bariyerlerin seçiminde temel olarak kullanılmalıdır ve her kategoriden en az bir bariyer, önem arz ettiği farklı dağıtım sistemleri için örnek olarak kullanılmalıdır. Bu konuda birkaç yol gösterici örnek aşağıda belirtilmiştir (Örneklerdeki sayılar, Tablo 15'teki bariyer tiplerini gösteren sayılar olup; '/' ayrılmış sayılar için ikisinden biri [veya birkaçından biri] tip olarak seçilebilir.)

- En az şu tipteki donanım yaşam çevrimi protokolleri: 1,2,3,4,5,6/9,7,8
- Prosedürler ve yükümlülük için:3/8, 7/10, 9, 11
- Yeterlilikler için: Beceri/kural/bilginin her bir seviyesi için en az bir tip
- İletişim için:3/7/9/10/11, birden daha fazla kişinin koordineli eylemini gerektirir
- Ulaşılabilirlik: 3,7/10,11

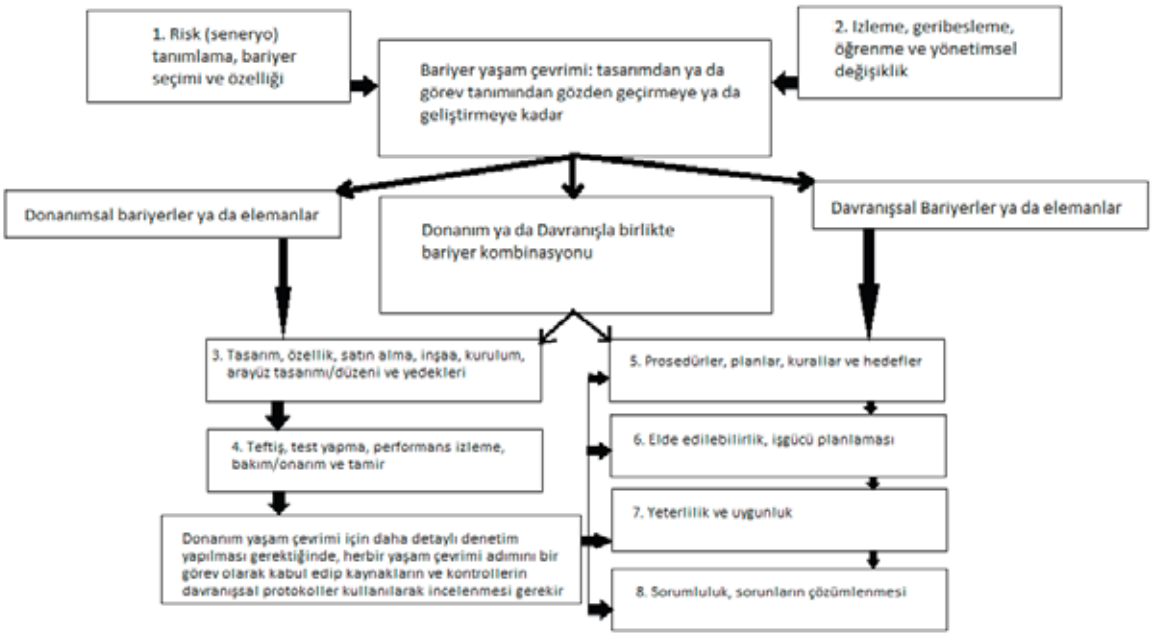
Şekil 10, hangi dağıtım sistemlerinin ve bununla birlikte hangi denetim eylemlerinin farklı tipte bariyerler için önemli olduğunu göstermektedir. Bariyerler çoğunlukla birkaç elemandan meydana gelmekte olup, seçilen her bir bariyer için denetim esnasında hangi elemanların ele alınacağının makul bir seçimi yapılmalıdır.

Bariyer aktif donanımdan oluşmuşsa, denetim, izleme ve adaptasyon önem arz etmektedir.

Eğer bariyer pasif donanım elemanlarından oluşmuşsa, denetim, özellikle pasif bariyerin değişikliklerle riske atılmadığını ve şartnamesine uygun işlediğini garanti etmek için yapım, kurulum ve birkaç bakım unsuruna odaklanmalıdır.

Bariyerler davranışsal elemanlardan oluşuyorsa, davranışsal dağıtım sistemleri kullanılarak denetlenebilir:

- Bariyere ilişkin gerekli davranışı tanımlayan prosedürler,
- Bariyer fonksiyonunu oluşturan gerekli davranışa sahip bireylere ulaşılabilirlik,
- Gerekli davranışı gerçekleştiren bireylerin yeterliliği,
- Riski kontrol etmek için, doğru zamanda, gerekli gözetim ve farkındalığa sahip bireylerin yükümlülükleri,
- Birden fazla bireyin bariyerin etkinliğinden sorumlu oldukları durumlarda gerekli koordinasyon ve iletişim.



Şekil 10: Bariyerler için bariyerlerin kurulduğu ve mevcut olduğu durumlarda bariyer tipleri arasındaki ilişki ve yönetim etkileri

4.3.4. Adım 4: Denetime hazırlık

Denetim hazırlığı için yapılabilecek en önemli aktivite, kuruluşun kendine özgü güvenlik sisteminin, ARAMIS güvenlik yönetimi yapısına göre eşleştirilmesidir. ARAMIS güvenlik yönetim yapısı, denetime tabi tutulan kuruluşun güvenlik yönetim sisteminin uygun parçalarıyla Şekil 8'de gösterilen ARAMIS denetiminin farklı bileşenleri arasındaki bağlantıları içerir.

Bu eşleştirme, kuruluşun dokümantasyonuyla birlikte ön denetim ziyareti esnasında gerçekleştirilen görüşmelere de dayanır. Görüşmelere ya denetim takımının ilk izlenimlerini doğrulamak için ya da eşleştirme uygulamasını yürütmek için yeterli bilgi sağlanamıyorsa, mevcut dökümanlardan edinilen bilgilere ilave edebilmek için ihtiyaç duyulur. Eşleştirme denetim esnasında kime neyin sorulduğunu netleştirmelidir.

Eşleştirme, ARAMIS Denetim Kitapçığında denetim sürecinin ikinci adımı olarak detaylı şekilde açıklanmıştır.

4.3.5. Adım 5: Denetimin Gerçekleştirilmesi

ARAMIS denetimi, ARAMIS bariyer yönetim sistem yapısında ayrılan dört alanı kapsar (Şekil 8 ve Şekil 10). ARAMIS denetimi, aynı zamanda farklı yerel güvenlik sistemleri tarafından yönetilen alanlara kadar değerlendirilen belirli kuruluşlara da bağlıdır. Önceki adımdan gerçekleştirilen eşleştirme, tesiste güvenlik yönetiminin bu alanlara dağıtımının net bir şekilde tanımlanmasını sağlamalıdır.

Değerlendirilen 4 konu aşağıda sıralanmıştır:

1. Bariyerlerin seçiminde karar alma sürecinin denetimi,

2. Güvenlik yaşam döngüsü adımlarını kullanan ve gerekli olduğunda onlarla ilişkili uygun dağıtım sistemlerini kapsayan bir şekilde donanım bariyerlerinin denetimi,
3. Uygun dağıtım sistemlerini kullanan davranışsal/prosedürel bariyerlerin denetimi,
4. Öğrenme ve değişim yönetim sisteminin denetimi.

Denetim gerçekleştirilirken özellikle, hem donanımsal hem de davranışsal elemanlı bariyerlerin çalışması incelenirken 2. ve 3. maddenin ayrılmaması kararlaştırılabilir.

Denetimi yapan kişi denetimi gerçekleştirirken (denetim sırasında) özellikle bariyerlerin donanımsal ve davranışsal elemanlarla birlikte gerçekleştirdiği işlemler sırasında olmak üzere 2 ve 3 nolu başlıkları ayırmama yönünde bir karar alabilir.

Bu adım ARAMİS Denetim Kitapçığındaki denetim prosesinin 3ncü adımında detaylı bir şekilde açıklanmıştır ve ARAMİS Denetim Kitapçığının Ek-2 ile Ek-10 arasında dağıtım sistemlerinin ve Ek 11'deki araçların tanımlamalarını kullanır.

4.3.6. Adım 6 : Denetim Sonuçlarının Analizi

Denetim sonuçlarının analizi, seçilen senaryolarda tanımlanan güvenlik fonksiyonlarının her birini yerine getirmek için kuruluşun yaptığı seçimlerin niteliğinin bir değerlendirmesini içerir. Başka bir deyişle, kuruluşa özgü tehlikeleri kontrol etmede en son tekniklerin kullanılıp kullanılmadığı değerlendirilir. Bu, bariyerin hata olasılığının mevcut teknolojiyi kullanan ve aşırı maliyetli olmayan, "olabildiği kadar düşük ve makul bir şekilde ulaşılabilir" (As Low As Reasonably Achievable - ALARA ilkesi) olduğu anlamına gelmektedir.

Denetim "kutuları" (ARAMIS Denetim Kitapçığının Ek 2 ile Ek 10 arasındaki dağıtım sistemlerinin tanımlamalarına bakınız) ve onlar arasındaki bağlantıları ele alır. Bu kutuların ve bağlantıların niteliği (tercihen) 5 puanlı derecelendirmeye göre ifade edilir. Sonuçlar dağıtım sistemlerini gösteren renk kodlu grafikler (yeşil= en iyi, kırmızı=en kötü, kitapçıkta 5 puanlı derecelendirmeyi üç renkli ölçeğe indirgemek için bir öneri sunulmuştur) kullanılarak görsel hale getirilir.

Bu renkli kodlama, denetim takımının özgün bulgularının bir listesiyle birlikte kuruluşa kalitatif bir geri bildirim sağlar. Kuruluşa dönen geri bildirimler ARAMIS Denetim Kitapçığının 7. Bölümünde, denetim raporu ise ARAMIS Denetim Kitapçığının 9. Bölümünde tanımlanmıştır.

Kalitatif sonuçların, iyileştirilebilir veya değiştirilmesi gereken özel güvenlik yönetimi sorunları hakkında anlık bilgi sağladığından, kuruluş için (ve diğer hissedarlar veya yetkili kuruluşlar gibi) kantitatif sonuçlardan çok daha uygun olabileceği vurgulanmalıdır.

4.3.7. Adım 7: Denetim Sonuçlarının Sayısallaştırılması

Sahadaki risk seviyesi üzerindeki güvenlik yönetiminin etkisinin değerlendirilmesi için denetim sonuçları sayısallaştırılır. Değerlendirme mevcut kurulu bariyerlere sahip mevcut bir tesisi ele alır; bu tesisin işletimsel güvenlik yönetimini etkileyen güvenlik yönetimi dağıtım sistemlerine odaklanılacağı anlamına gelir (bkz. şekil 8'deki elips). Bu, "risk analizini" ve "öğrenme ve değişim" unsurlarını kapsamaz ve güvenlik bariyerlerinin güvenirlilik seviyesi üzerinde doğrudan etkisi olan yedi unsura bakılır (bkz. şekil 10).

Denetim süreci dağıtım sistemleri içerisindeki her bir kutunun kalitatif 5-puan ölçeği üzerinden derecelendirilmesini sağlar. Bu ölçek en iyi derecenin %100 en kötü derecenin ise %20 olduğu, kalitatif dereceler arasında eşit uzaklıklara sahip olan sayısal bir derecelendirme sistemine dönüştürülür.

Bir bütün olarak dağıtım sisteminin derecesi, her bir kutunun derecelerinin toplanmasıyla elde edilir. Bu, şu şekilde yapılır: Dağıtım sistemleri bir veya iki "baskın" kutu içerir. Bu dağıtım sistemleri için derecelendirmesi aşağıdaki şekilde yapılır:

Bir bütün olarak dağıtım sisteminin derecesi= EN DÜŞÜK (baskın kutuların en düşük derecesi, tüm kutuların derecelerinin ortalaması)

Baskın kutuların tanımlanmadığı kutular için, derece tüm kutuların derecelerinin ortalamasıdır.

Dağıtım sistemlerinin başarısızlığına aşağıdaki tüm kutuların eşit katkı sağladığı varsayılan bir grup dağıtım sistemi vardır:
a. İşgücü planlaması,
b. İletişim,
c. Satın alma/kurulum.

Dağıtım sisteminin başarısızlığına baskın olarak aşağıdaki birkaç kutunun katkı sağladığı varsayılan bir grup dağıtım sistemi vardır:
d. Süreçler (kutu 5: iletişim, eğitim, kuralların uygulanması; kutu 8: kutuların etkinliğinin değerlendirilmesi),
e. Yetkinlik (kutu 2: uygunluk tanımlama ve davranış için gereken yetkinlik),
f. Yükümlülük (kutu 2: değerlendirme ve davranışsal geçmişin değişimi ve sonuçları),
g. Denetim ve bakım (kutu 2: bakım kavramlarının ve planlarının tanımlanması; ve kutu 7: bakım ve tamirin uygulanması).

Bu adımın sonucunda, güvenlik bariyerlerinin güvenirlilik seviyeleri üzerinde etkilere sahip olduğu varsayılan yedi elemanın tümü için %20 ile %100 arasında sayısal bir derece elde edilir. Bu yedi eleman aşağıda tekrar listelenmiştir:
1. İş gücü planlaması ve ulaşılabilirliği
2. Yetkinlik ve uygunluk
3. Yükümlülük, uyum ve çatışmanın çözümü
4. İletişim ve koordinasyon
5. Süreçler, kurallar ve amaçlar
6. Donanım/yazılım sayın alımı, kurulumu ve arayüzü
7. Donanım/yazılım incelemesi, bakımı ve değiştirilmesi

Sayısal dereceler sonraki referanslar için S_1 den S_7'ye kadar değişkenlerle gösterilmiştir.

4.3.8. Adım 8 : Kuruluşa Özgü Güvenlik Kültürü Anketinin Hazırlanması

D.3.B'nin "Güvenlik Yönetim Etkinliği İndeksi Belirleme Metodolojisi" Ek B dokümanı "proses endüstrileri için genel bir güvenlik kültür anketi (SCQPI)" içerir. Anketin, tesisteki işçilere dağıtılmasından önce birkaç küçük noktasının değiştirilmesi gerekir. Bu değişiklikler aşağıda sıralanmıştır:
- Tesiste bu anketten sorumlu kişinin adı, görevi, telefon numarası (anketin birinci sayfasında),
- Tesiste farklı olay türleri ve raporlamaya konu olan kazalar için kullanılan terminolojinin kontrol edilmesi gerekir (sayfa 2),

- Anketteki 7. ve 8. Bölümler altında tanımlanan: yönetici/üretim müdürü/güvenlik mühendisi ve memuru/çalışma grubu lideri/takım lideri ve çalışma grubu ve takım yer almalıdır (sayfa 4 ve 5),
- Ankete birkaç açık soru eklemek mümkündür bu ayrı bir analiz gerektirir,
- Demografik bölüm hedef tesise uyum sağlayacak biçimde değiştirilmeli ve cevapların anonimliğini bozacak düzeyde bilgi istenmemesine dikkat edilmelidir.

Anket araştırmasına katılacak olan işçiler seçilmelidir. Bir yandan seçilen grupların, örneğin bir grubun (çalışma ekipleri, vardiyalar veya benzer fonksiyonlara ve pozisyonlara sahip işçiler) 15 kişiden az olmayacak (aynı zamanda cevapların bireysel olarak tanımlanamayacağını garanti edecek şekilde) şekilde ve belirgin istatistiksel sonuçlar elde edilmesini sağlayacak kadar büyük olması isteniyorken diğer bir yandan kalabalık gruplar için gerekli kaynak ihtiyacı (örneğin analiz için gerekli olan süre yalnızca birbirleriyle karşılaştırılacak olan grupların sayısına bağlı olsa da çalışanların harcadıkları süre gibi) daha fazladır.

Prensip olarak, saha kontrol ve kumanda operatörleri, bakım ve temizlik personeli, mühendisler gibi tehlikeli ekipmanlarla çalışan veya tehlikeli ekipmanlarla direkt olarak ilişkili olan tüm işçiler bu araştırmaya dahil edilmelidir. Farklı gruplardan alınan cevapların, yönetimin etkin bir şekilde müdahalesinin sağlanması adına tanımlanması yararlı olabilir. Bu yüzden karşılaştırılacak olan gruplar demografik bölümde listelenmelidirler. Fakat, belirli bir tesis içerisinde yer alan gruplar arası farklılıklar ARAMIS güvenlik kültürü indeksinin hesaplanmasında dikkate alınmaz. Anketin doldurulması ve geri verilmesine ilişkin şartlar işçiler için gayet net bir şekilde ifade edilmelidir. Bu şartlar aşağıda listelenmiştir:

- Bütün cevaplar anonim (isimsiz) olmalıdır,
- Bireysel düzeyde hiçbir bilgi raporlanmamalıdır,
- İşçilere güvenlik kültürü anketinin sonuçlarıyla ilgili geri besleme yapılmalıdır.

İşçilerin ilgisini çekebilmek ve onlarla ortak çalışabilmek amacıyla sendika temsilcilerinin desteğinin sağlanması yararlı olabilir. Anketin birincil amacı, tesisin güvenlik performansının (çeşitli mesleklere sahip işçilerin hayatı ve sağlığı için yeterli korumanın sağlanması, sendikaların amaçlarından bir tanesidir.) artırılmasını sağlayacak olan bilgilerin toplanmasıdır.

4.3.9. Adım 9: Anket Cevaplarının Toplanması

Anket sonuçlarının toplanmasında kullanılabilecek en etkin yöntem, (değişik gruplarda yer alan) işçiler için, anketlere cevaplarını yazabilecekleri ve hemen geri verebilecekleri yaklaşık bir saat süren toplantıların düzenlenmesidir. Cevap verme oranı, anketlerin evde gönüllülük esasına dayalı olarak doldurulması ve cevapların (ön ödemeli) posta yoluyla gönderilmesi veya tesis içerisinde yer alan toplama kutularındaki zarflara konulması istendiğinde belirgin bir şekilde düşüş göstermektedir.

4.3.10. Adım 10: Güvenlik Kültürü Sonuçlarının Analizi

Tek bir soruya verilen cevaplar 5 puanlı derecelendirmeye göre ifade edilen hem fikirlik derecelerinin bir listesi şeklinde verilecektir. Sonuçlar, 5 puanlı derecelendirme üzerinden verilen cevapların dağılımını grafiksel olarak gösterecek şekilde raporlanır. Elde edilen sonuçların ARAMIS beş referans bölge örneğinde ortaya çıkan sonuçlarla karşılaştırılması önerilir (N=255).

Sonuçların referans grupla karşılaştırılması ile güvenlik kültürünün güçlü ve zayıf yönleri rölatif olarak tanımlanabilir ve kuruluş, bu bilgiyi benzer sorunlara ait şartların ve olası sebeplerinin belirlenmesinde ve bu sorunlara çare bulabilmek için müdahale yöntemlerinin geliştirilmesinde kullanabilir.

Kalitatif sonuçların, iyileştirilebilir veya değiştirilmesi gereken özel güvenlik yönetimi sorunları hakkında anlık bilgi sağladığından kuruluş için (ve diğer hissedarlar veya yetkili kuruluşlar için) kantitatif sonuçlardan çok daha uygun olabileceği vurgulanmalıdır.

4.3.11. Adım 11: Güvenlik Kültürü Değerlendirmesinin Sayısallaştırılması

Aşağıda verilen adımlar belirli bir k örneği için güvenlik kültürü indeksi'nin hesaplanmasını göstermektedir. Tablo 16'da Avrupa'da yer alan 5 referans tesisten elde edilen sonuçlara ait ortalama ve standart sapma değerleri yer almaktadır. Burada kullanılan kısaltmalar:

$$\mu_i^{REF} = Referans\ örneğin\ i.elemanının\ ortalaması\ (beş\ test\ alanı)$$

$$\sigma_i^{REF} = Referans\ örneğin\ i.elemanının\ standart\ sapması$$

$$\mu_i^{NEW} = Yeni\ hedef\ örneğin\ i.elemanının\ ortalaması$$

Adımlar:

1. Anketin her bir elemanına (sorusuna) 1, 3, 5, 6, 9, 10 ve 11 no'lu anket grupları tarafından verilen cevaplar 1, 2, …5 puan ölçüsüne göre şu şekilde kodlanmalıdır [2, 4, 7 ve 8. Gruplar güvenlik kültürü indeksinde dikkate alınmaz; benzer şekilde 3.14 elemanı kapsam dışında bırakılmalıdır]: tüm elemanlar için en fazla verilen, "güçlü bir şekilde hemfikir olunan" veya "çok yüksek bir dereceyi" gösteren 1 sayısı, ikinciye 2 ve son olarak sağda yer alan değere 5 sayısı atanır. 1.9, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 5.6, 5.7, 6.2, 9.1, 9.3, 9.8, 9.9, 9.10, 10.7 no'lu elemanlar için yapılan atama tersine çevrilmelidir. Böylece "güçlü bir şekilde hemfikir olunan" veya "çok yüksek bir dereceyi" ifade eden derece 1 sayısıyla bunu takip edenler de sırasıyla diğer sayılarla ifade edilmiş olur. Ters çevirme işlemi pozitif ve negatif cevap değerlerinin yönünün davranışlar ve algılar bakımından garanti edilmesini sağlar.

2. Her bir eleman için örneklem ortalaması μ_i^{NEW} hesaplanır.

3. Her bir eleman için ortalama ve standart sapma değerlerini içeren Ek A'daki referans örneklem verilerine bağlı kalarak hedef örnekleme ait y değeri şu şekilde hesaplanır: ilk olarak her bir i elemanı için y değeri hesaplanır.

Buradan tüm elemanlara ait ortalama y değeri Y^{NEW} şu şekilde elde edilir:

4. Son olarak k hedef örneklemine ait y değerinin Güvenlik Kültürü İndeksi S_0^k'ya dönüştürülmesi şu şekilde gerçekleştirilir:

$$Eğer\ Y^{NEW} \geq 1\ ise\ S_0^k = 1;$$

$$Eğer\ -3 < Y^{NEW} < 1\ ise\ S_0^k = 0{,}25.Y^{NEW} + 0{,}75;$$

$$Eğer\ Y^{NEW} \leq -3\ ise\ S_0^k = 0\text{'dır.}$$

(Burada referans alınan örneklem için Güvenlik Kültürü İndeksi S_0^{REF} = 0,75 olduğu vurgulanmalıdır.)

Tablo 16: ARAMIS güvenlik kültürü anketinde olay çalışmalarından elde edilen öğeler için ortalamalar ve standart sapmalar

Öğe no. *		Ortalama	Standard Sapma	Öğe no. *		Ortalama	Standard Sapma	Öğe no. *		Ortalama	Standard Sapma
Öğe	01.1	2.159	0,985	Öğe	05.1	1,836	0,74	Öğe	10.1	2,6	0,921
Öğe	01.2	1,659	0,676	Öğe	05.2	1,94	0,66	Öğe	10.2	2,756	0,929
Öğe	01.3	1,823	0,815	Öğe	05.3	2,06	0,778	Öğe	10.3	2,302	0,757
Öğe	01.4	1,74	0,689	Öğe	05.4	2,506	0,894	Öğe	10.4	2,3	0,78
Öğe	01.5	2,043	0,811	Öğe	05.5	2,72	0,787	Öğe	10.5	2,298	0,777
Öğe	01.6	2,097	0,852	Rev	05.6	2,39	0,966	Öğe	10.6	2,541	0,91
Öğe	01.7	2,664	0,913	Rev	05.7	2,308	0,988	Rev	10.07	2,808	0,919
Öğe	01.8	2,492	1,039	Öğe	06.1	2,52	0,902	Öğe	10.8	2,48	0,841
Rev	01.9	2,669	1,008	Rev	06.2	2,484	0,842	Öğe	11.1	2,622	0,998
Öğe	01.10	2,332	0,972	Öğe	06.3	2,344	0,777	Öğe	11.2	3,317	0,915
Öğe	01.11	2,068	0,869	Öğe	06.4	2,534	0,966	Öğe	11.3	3,162	0,91
Öğe	01.12	2,574	0,85	Öğe	06.5	2,404	0,756	Öğe	11.4	2,98	0,994
Öğe	03.1	1,853	0,617	Öğe	06.6	2,716	0,833	Öğe	11.5	2,177	0,715
Öğe	03.2	2,376	0,815	Rev	09.1	2,855	1,006	Öğe	11.6	2,045	0,621
Öğe	03.3	2,204	0,842	Öğe	09.2	2,414	0,834	Öğe	11.7	2,052	0,752
Öğe	03.4	2,321	0,886	Öğe	09.3	3,59	0,938	Öğe	11.8	2,967	0,927
Öğe	03.5	2,641	0,959	Öğe	09.4	2,258	0,886	Öğe	11.9	2,544	0,768
Rev	03.6	2,679	1,084	Öğe	09.5	2,265	0,784	Öğe	11.10	2,492	0,942
Rev	03.7	2,353	1,029	Öğe	09.6	2,602	0,842	Öğe	11.11	2,722	0,99
Rev	03.8	2,121	0,987	Öğe	09.7	2,237	0,765	Öğe	11.12	2,801	0,989
Rev	03.9	2,702	1,05	Rev	09.8	2,27	0,914	Öğe	11.13	2,269	0,845
Rev	03.10	2,438	1,043	Rev	09.9	2,258	0,798				
Rev	03.11	2,151	0,934	Rev	09.10	2,258	0,798				
Rev	03.12	2,81	1,05	Öğe	09.11	2,177	1,024				
Rev	03.13	2,737	0,981	Öğe	09.12	2,5	0,8				
				Rev	09.13	2,691	0,873				

4.3.12. Adım 12: Bariyerlerin Operasyonel Güvenirlilik Seviyesinin Hesaplanması

Donanım bariyerlerinin, Tasarım (aynı zamanda nominal veya optimal olarak da adlandırılır) Güvenirlilik Seviyesi veya SIL (Safety Integrity Level) veya davranışsal bariyerlerin bu değerlere eşdeğer genel performans derecesinin gerçekte uygulanan bariyerlere paylaştırılması gerekmektedir. Bu paylaştırma güvenlik yönetimi değerlendirmesinin sağlama alınmasını sağlayacaktır. Yapısal ve kültürel elemanların değerlendirilmesi, güvenlik yönetim sistemi elemanlarının gereksinimleri karşılamakta yetersiz kaldığı alanları da kapsayan bir derece elde edilmesini sağlar. Bu, güvenlik kültürü ve bilinen 7 dağıtım sisteminden herhangi birisi için performans değerlerinin optimum performans değerleri ile karşılaştıran bir dizi S_i (yönetim indeksleri) değerinin hesaplanması anlamına gelmektedir. k tipinde bir güvenlik bariyeri (veya güvenlik bariyeri bileşeni) işletimsel güvenirlilik seviyesinin basit bir modellemesi aşağıda verilmiştir.

$$LC_{işletimsel,k} = \left(1 - \sum_{i=0}^{7} (1 - S_i).B_{i,k}\right).LC_{tasarım,k}$$

Burada S_i , i yapısal elemanı için denetim ve güvenlik kültürü değerlendirmelerini de içeren şekilde i elemanına karşılık gelen dağıtıma ait son değeri, incelenen k bariyer tipi için i dağıtım sisteminin önemini bağdaştıran bir dizi ağırlıklandırma katsayısını göstermektedir. (Eğer B_i'lerin toplamı 1'den büyükse, o zaman sonuç 0'a maksimize edilmelidir.)

Bu sonuçla, LC değerinin olduğunu hatırlayarak, tüm ilgili kaza senaryolarının beklenen frekans değerleri, papyon diyagramlarında gösterilen bariyerlerin gerçek PFD değerleri kullanılarak gözden geçirilebilir. Bu beklenen frekans değerleri, güvenlik yönetimi sisteminin değerlendirmesini de içerir.

4.3.13. Adım 13: Risk Değerlendirmesi Metedolojisinde Operasyonel Güvenirlik Seviyesinin Uygulanması (MIRAS)

MIRAS tarafından kabul edilen senaryolarda yer alan tüm bariyerler için, adım 12 kullanılarak Tasarım Güvenirlilik Seviyesindeki azalmalar hesaplanmıştır. Sonuçta elde edilen İşletimsel Güvenirlilik Seviyesi değerleri kaza senaryolarının beklenen frekanslarının hesaplanmasında kullanılır. Son olarak elde edilen değer, güvenlik yönetiminin değerlendirmesini de kapsayan kuruluşun risk düzeyini ifade eder.

4.4. ÖRNEK

Örnek olarak, vaka analizlerinden elde edilen dereceleri gösteren tablolar aşağıda verilmiştir. Gri renkli hücreler, denetim takımının bulgularının da dahil edildiği hücrelerdir. Toplam değerler (en iyi performansın yüzdesi olarak ifade edilmiş olan) dağıtım sistemi başınadır ("risk analizi" ve "öğrenme" bariyer analizinde açıkça hesaba katılmamış ve sayısallaştırma burada verilmemiştir.)

Bir sonraki tablo, Tasarım Güvenirlilik Seviyesi 3 olan bir tahliye vanası (5 no'lu bariyer tipi) için "ARAMIS Güvenlik Yönetimi Etkinliği Hesaplaması"'ndan elde edilen değerleri göstermektedir. Denetim notunun sonuçları güvenirlilik seviyesinin azaltılması işlemlerine otomatik olarak dahil edilmiştir (Güvenlik Kültürü Araştırmasından elde edilen sonuç yeşil hücreye manuel olarak yazılmalıdır). Azaltma elbette B ile ifade edilen ağırlık faktörüne bağlı olup, bu örneğin yararına hem "satın alma ve kurulum", hem de "inceleme ve bakım" için %50 olarak alınmıştır. Ağırlık faktörlerinin son değerlerinin uzman görüşü alınarak belirlenmesi gerekir.

Tablo 17: Bir olay çalışması sonucunda elde edilen sonuçların değerlendirme cetveli

ARAMİS Dağıtım Sistemi	Adım No.:	Adımlar	Değerlendirme (1-5)
Bariyer Yönetimi için Rollerin ve Sorumlulukların Dağıtımı		*Sayısallaştırma Gerekli Değildir*	
	1	Birincil ve İkinci İş Prosesleri Envanter Çıkarma	4
	2	Kaza Senaryolarının Tanımlanması	4
	3	Senaryo başına risk önceliği vermek (sayısal)	4
	4	Gerekli güvenlik fonksiyonlarının tanımlanması	4
	5	Bariyer görevlerinin HF ve Verimlilik temelinde ayrılması	4
	6	Uygunluğun belirlenmesi - efektif bariyerler ve bunlar için performans kriterlerinin ve çalışma koşullarının (LCA) tanımlanması	4
	7	Bariyer çalışma ömrü etkinliği için kaynakların planlanması ve sağlanması	4
	8	Bariyer performansının izlenmesi ve değerlendirilmesi	4

ARAMİS Dağıtım Sistemi	Adım No.:	Adımlar	Değerlendirme (1-5)
1. İşgücü Planlaması ve Elde Edilebilirliği		*Toplam*	% 100
	1	Görevler için gerekli işgücünü değerlendirmek	5
	2	Uyum Tedarikini ve Talebini Tanımlamak	5
	3	Sözleşme yapanların tanımlanması	5
	4	Personel Havuzu	5
	5	Kiralama Sözleşmeleri	5
	6	Personel/Müteahhit Tatil günleri de dahil olmak üzere kapsama	5
	7	Acil Durum Planı ve Çağrısı	5
	8	İşgücü hesaplaması	4

ARAMİS Dağıtım Sistemi	Adım No.:	Adımlar	Değerlendirme (1-5)
İzleme, Geri besleme, öğrenme ve değişim yönetimi		*Sayısallaştırma Gerekli Değildir*	
	1	Bariyer tasarımı ve yönetiminde son teknolojiye ilişkin bilgileri hesaplanması	4
	2	Bariyer durumunun ve performansının kayıt altına alınması	5
	3	Olay ve kazaların, bariyer başarısızlıklarının ve yönetimin kayıt altına alınması	4
	4	Bariyer performansı ile ilişkili denetim yönetim sistemi	2
	5	Bariyer seçiminde, tasarımında ve yönetiminde veri ve amaç değerlendirilmesi	5
	6	Prosesteki değişiklikler için planlanan envanter	5
	7	Önerilen değişikliklerin risklerinin ve bariyer ihtiyacının (değişikliği) değerlendirilmesi	5
	8	Organizasyonel değişiklikler için planların envaterleştirilmesi	
	9	Bariyerlerin görevleri ile ilgili gerekli değişikliklerin risklerinin değerlendirilmesi	3
	10	Değişiklilerin, uygulanması ve hesaplanmasının kararı	4

ARAMİS Dağıtım Sistemi	Adım No.:	Adımlar	Değerlendirme (1-5)
2. Yeterlilik ve Uygunluk		*Toplam*	% 86
	1	Bariyerlerin davranışsal elemanlarının ya da yönetiminin görev analizi	4
	2	Uygunluğun ve davranış için yeterliliğin tanımlanması	5
	3	Sözleşme yapılan işletmelerin personeli ile kendi personelimizin tertiplenmesi	4
	4	Uygun personelin ve işletmelerin seçimi	5
	5	Eğitim programının hazırlanması ve gözden geçirilmesi	4
	6	Personelin ve sözleşme yapılan işletmelerin eğitilmesi	4
	7	Gerekli Yeterliliğin değerlendirilmesi	5
	8	Görev performansının izlenmesi	4
	9	Yeterliliğin hesaplanması	4
	10	Yenileyici Eğitim	4

ARAMİS Dağıtım Sistemi	Adım No.:	Adımlar	Değerlendirme (1-5)
İzleme, Geri besleme, öğrenme ve değişim yönetimi		*Sayısallaştırma Gerekli Değildir*	
	1	Bariyer tasarımı ve yönetiminde son teknolojiye ilişkin bilgileri hesaplanması	4
	2	Bariyer durumunun ve performansının kayıt altına alınması	5
	3	Olay ve kazaların, bariyer başarısızlıklarının ve yönetimin kayıt altına alınması	4
	4	Bariyer performansı ile ilişkili denetim yönetim sistemi	2
	5	Bariyer seçiminde, tasarımında ve yönetiminde veri ve amaç değerlendirilmesi	5
	6	Prosesteki değişiklikler için planlanan envanter	5
	7	Önerilen değişikliklerin risklerinin ve bariyer ihtiyacının (değişikliği) değerlendirilmesi	5
	8	Organizasyonel değişiklikler için planların envaterleştirilmesi	
	9	Bariyerlerin görevleri ile ilgili gerekli değişikliklerin risklerinin değerlendirilmesi	3
	10	Değişiklilerin, uygulanması ve hesaplanmasının kararı	4

ARAMİS Dağıtım Sistemi	Adım No.:	Adımlar	Değerlendirme (1-5)
2. Yeterlilik ve Uygunluk		*Toplam*	% 86
	1	Bariyerlerin davranışsal elemanlarının ya da yönetiminin görev analizi	4
	2	Uygunluğun ve davranış için yeterliliğin tanımlanması	5
	3	Sözleşme yapılan işletmelerin personeli ile kendi personelimizin tertiplenmesi	4
	4	Uygun personelin ve işletmelerin seçimi	5
	5	Eğitim programının hazırlanması ve gözden geçirilmesi	4
	6	Personelin ve sözleşme yapılan işletmelerin eğitilmesi	4
	7	Gerekli Yeterliliğin değerlendirilmesi	5
	8	Görev performansının izlenmesi	4
	9	Yeterliliğin hesaplanması	4
	10	Yenileyici Eğitim	4

ARAMİS Dağıtım Sistemi	Adım No.:	Adımlar	Değerlendirme (1-5)
İzleme, Geri besleme, öğrenme ve değişim yönetimi		*Sayısallaştırma Gerekli Değildir*	
	1	Bariyer tasarımı ve yönetiminde son teknolojiye ilişkin bilgileri hesaplanması	4
	2	Bariyer durumunun ve performansının kayıt altına alınması	5
	3	Olay ve kazaların, bariyer başarısızlıklarının ve yönetimin kayıt altına alınması	4
	4	Bariyer performansı ile ilişkili denetim yönetim sistemi	2
	5	Bariyer seçiminde, tasarımında ve yönetiminde veri ve amaç değerlendirilmesi	5
	6	Prosesteki değişiklikler için planlanan envanter	5
	7	Önerilen değişikliklerin risklerinin ve bariyer ihtiyacının (değişikliği) değerlendirilmesi	5
	8	Organizasyonel değişiklikler için planların envaterleştirilmesi	
	9	Bariyerlerin görevleri ile ilgili gerekli değişikliklerin risklerinin değerlendirilmesi	3
	10	Değişiklilerin, uygulanması ve hesaplanmasının kararı	4

ARAMİS Dağıtım Sistemi	Adım No.:	Adımlar	Değerlendirme (1-5)
2. Yeterlilik ve Uygunluk		*Toplam*	% 86
	1	Bariyerlerin davranışsal elemanlarının ya da yönetiminin görev analizi	4
	2	Uygunluğun ve davranış için yeterliliğin tanımlanması	5
	3	Sözleşme yapılan işletmelerin personeli ile kendi personelimizin tertiplenmesi	4
	4	Uygun personelin ve işletmelerin seçimi	5
	5	Eğitim programının hazırlanması ve gözden geçirilmesi	4
	6	Personelin ve sözleşme yapılan işletmelerin eğitilmesi	4
	7	Gerekli Yeterliliğin değerlendirilmesi	5
	8	Görev performansının izlenmesi	4
	9	Yeterliliğin hesaplanması	4
	10	Yenileyici Eğitim	4

Tablo 18: Güvenlik tahliye vanası için güvenlik yönetimi verimlilik hesabı

ARAMİS Güvenlik Yönetimi Verimlilik Hesabı								
Bariyer:		Güvenlik Tahliye Vanası						
Bariyer Tipi		5	Aktive edilmiş - talep edilmiş donanım - bariyer ya da kontrol					
	Bariyerin Tasarım Güveninirlik Seviyesi	3						
	Değerlendirmeler			İndirgeme Faktörleri				
0	Güvenlik Kültürü			0%				
1	İşgücü Planlaması ve Elde edilebilirlik	100%		0%				
2	Yeterlilik ve Uygunluk	86%		0%				
3	Sorumluluk, Uyumluluk ve Sorunların Çözümlenmesi	80%		0%				
4	İletişim ve koordinasyon	85%		0%				
5	Prosedürler, kararlar ve hedefler	80%		0%				
6	Donanım/yazılım satın alınması, inşaası, arabağlama (arayüz), kurma	100%		0%				
7	Donanım/yazılım teftişi, bakım onarımı ve değişimi	80%		0%				
	Bariyerin Operasyonel Güveninirlik Seviyesi:	2,7						

4.5. DEĞERLENDİRME

4.5.1. Denetimi ve SCQPI'ı kim yapabilir?

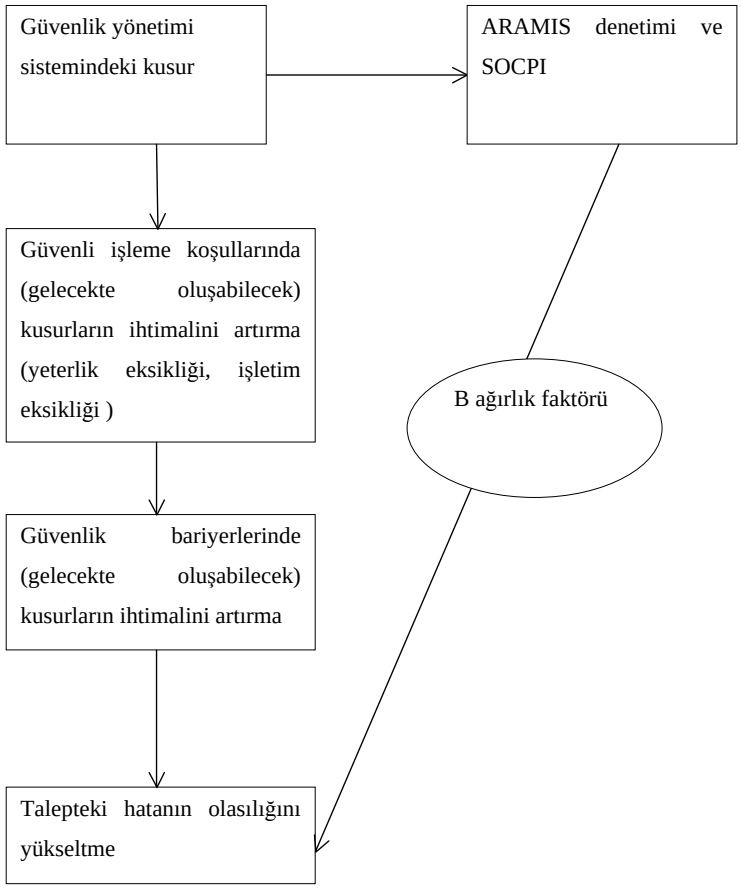
Aslında proje uzman yetkililerin yanında, dışarıdan bir denetim almadan, endüstrinin de kendi kendine kullanabileceği bir yöntem geliştirmek amaçlamıştır. Ancak ARAMIS inceleme grubunun endüstrinin bu denetimi kendi başlarına yapabileceğine dair şüphesi vardır. ARAMIS denetim manuelinin iç denetimde kullanılmasını engelleyecek teknik bir yasak yoktur ve iç denetim sonucu ortaya çıkan yönetim etkinlik raporunu esas almak yetkililerin inisiyatifindedir.

SCQPI sabit bir doküman olduğundan, denetime oranla az miktarda öznel yorum katarak, endüstri SCQPI'ı kullanabilir ve denetimini yapabilir.

4.5.2. Güvenilirlik seviyesi azaltma hesapları güvenlik yönetimi noksanları bakımından ne kadar sağlıklıdır?

Güvenlik bariyerlerinin Güvenilirlik Seviyesi tasarım değerlerinin azaltılmasının tahmin edilen etkileri herhangi bir tarafsız veri ile doğrulanmamıştır. Hollanda'nın "Pembe Kitab"ı konuya farklı içeriklerde değinmiştir. Güvenlik yönetimi verimliliğinin başarısızlık oranlarına etkisine kesin olmamasından dolayı değinilmemiştir, buna karşılık "gelişme seviyesi"ne kıyasla çok veya az (fiziksel?) güvenlik ölçümü olması basınçlı kapların beş kat az veya çok arıza vermesine yol açabilir.

Güvenlik yönetimi oranları ve güvenlik kültürünün, bariyerlerin güvenirlilik seviyesi ile tavsiye edildiği gibi direk eşleştirilmesi gerçeğin basitleştirilmiş hali olmasına rağmen uygulanmıştır, çünkü gerçek olayların kendi içinde kantitatifliğinin belirlenmesi daha da zordur. Aşağıdaki şekilde açıklama yapılmıştır.



Şekil 11: Yönetim sistemi ve güvenlikle ilgili verilen bileşenin hata olasılığı ve ARAMIS denetimi ile bağlantısı ve güvenlik kültürü anketi arasındaki ilişki

Şu anki metodolojide kabul edilen en önemli kısa yol güvenlik yönetimi sürecindeki eksikliğin doğrudan güvenlik bariyerindeki eksikliğe bağlı olmasıdır. Halbuki gerçek ilişkide güvenlik yönetimi çıktısındaki eksiklik, bariyerin hata olasılığına sebep olmuştur.

Öte yandan güvenlik yönetimi süreci, güvenlik bariyerlerinin ileride de aynı güvenlik seviyelerini koruyup koruyamayacağının belirtilerini verir. Diğer bir deyişle güvenlik yönetimi süreci, güvenlik bariyerlerinin gelecekteki durumu hakkında bir fikir verir.

Şüphesiz ki şu anki ağırlık faktörlerinin dizilimi güvenlik yönetiminden kaynaklı beklenen güvenirlilik seviyesi azalması hakkında çok yüzeysel bir bilgi verir ve gelecekte bu konuda çaba sarf edilmesi gerekir. Ancak problemin doğasından dolayı veri toplamak oldukça güçtür.

4.5.3. Güvenlik yönetimi verimliliği değerlendirmesi risk değerlendirmesine dâhil edilmeli midir?

ARAMIS inceleme grubu bazı yetkililerin kantitatif güvenlik yönetimi değerlendirmelerini risk değerlendirmesinin içinde kullanmaktan çekineceğini belirtmiştir. Gerekçeleri şudur ki güvenlik yönetimi hızlı değişen bir yapıdır ve buna göre - mesela arazi kullanım planlarına göre- verilen karar sağlıklı olmayacaktır.

Bu görüşe karşı çıkanların sebepleri ise:

1. Şu anki risk değerlendirmesi güvenlik bariyerlerinin güvenirlilik seviyesi için belirlenmiş optimum ve tasarım değerlerine dayanmaktadır. Güvenlik yönetimi değerlendirmesini dâhil etmek daha ölçülü risk tahminlerine sebep olacaktır, neticede de sonuçlar gelecek koşullar bakımından daha sağlıklı olacaktır. Güvenlik yönetimi verimliliğini yok saymak aslında güvenlik bariyerlerinin geçici güvenlik yönetimi koşulları altında olası bozulmalarını yok saymak demek olacaktır.

2. Daha önceki bölümde belirtildiği gibi güvenlik yönetimi süreci güvenlik bariyerlerinin gelecekteki durumları (mesela gelecekteki risk seviyesi) hakkında fikir sağlayan tek kaynaktır. Güvenlik yönetimi değerlendirmesi içeren bir risk değerlendirmesi yetkililere işletmelerin denetimi için daha açık bir referans sağlar ve yetkililerin güvenlik yönetiminin özel maddelerine açıklayıcı istekler koymasına engel olur.

5. REFERANS KAZA SENARYOLARININ BELİRLENME METODOLOJİSİ (MIRAS)

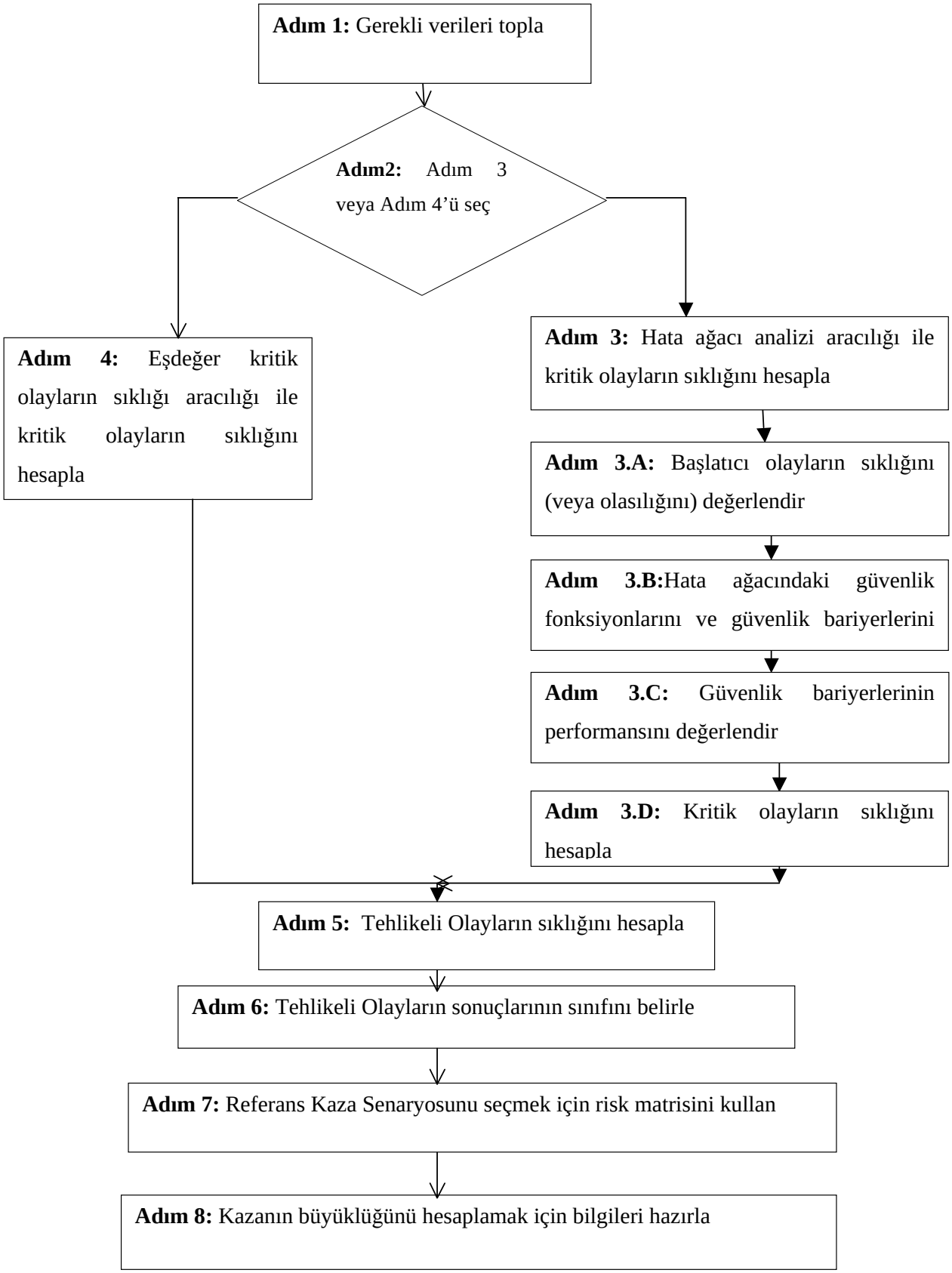
5.1. AMAÇ

Referans Kaza Senaryolarının Belirlenme Metodolojisinin amacı; Paragraf 2.3'te MIMAH (Büyük kaza tehlikelerinin belirlenmesi metodolojisi) ile anlatılan Ana Kaza Senaryoları arasından Referans Kaza Senaryosu (RAS) seçmektir. RAS, tesiste meydana gelebilecek kazanın büyüklüğünü hesaplayan bir modelde kullanılacaktır(bkz. paragraf 6).

Referans Kaza Senaryolarının belirlenmesi yöntemi şunları göz önünde bulundurur:
- Ekipmanlara ve ekipmanların etrafına kurulan güvenlik sistemleri,
- Güvenlik yönetim sistemi,
- Kazanın oluşma sıklığı,
- Kazanın olası sonuçları.

MIRAS sekiz adımdan oluşur. Adımların tamamı MIMAH ile oluşturulan bütün "papyonlar" için uygulanmalıdır. Bütün adımlar ve birbirlerini izleyişleri Şekil 12'da gösterilmiştir:

- Adım 1: Gerekli verileri topla
- Adım 2: Adım 3 ve Adım 4 arasında seçim yap
- Adım 3: Hata ağacı analizi aracılığı ile kritik olayların sıklığını hesapla
- Adım 3.A: Başlatıcı olayların sıklığını (veya olasılığını) değerlendir
- Adım 3.B: Hata ağacındaki güvenlik fonksiyonlarını ve güvenlik bariyerlerini belirle
- Adım 3.C: Güvenlik bariyerlerinin performansını değerlendir
- Adım 3.D: Kritik olayların sıklığını hesapla
- veya Adım 4: Eşdeğer kritik olayların sıklığı aracılığı ile kritik olayların sıklığını hesapla
- Adım 5: Tehlikeli Olayların sıklığını hesapla
- Adım 6: Tehlikeli Olayların sonuçlarının sınıfını belirle
- Adım 7: Referans Kaza Senaryosunu seçmek için risk matrisini kullan
- Adım 8: Kazanın büyüklüğünü hesaplamak için bilgileri hazırla



Şekil 12: MIRAS adımlarının genel görünümü

5.2. GEREKLİ VERİLERİN TOPLANMASI (MIRAS - ADIM 1)

Tüm MIRAS adımları boyunca ilave verilere ihtiyaç olacaktır. Gerekli bilgi listesi D.1.C. kısmında bulunan Tablo 7'de verilmiştir.

5.3. KRİTİK OLAYLARIN SIKLIĞININ HESAPLANMASI (MIRAS - ADIM 2 VE ADIM 3 VEYA 4)

Adım 3 ve Adım 4 aynı amacı taşır: düşünülen papyon için her yıl başına düşen kritik olayların sıklığını belirlemek. Adım 2'de analizi yapan, Adım 3 ve Adım 4 arasında seçim yapmak zorundadır.

MIRAS'ın 3. basamağında öncelikle başlatıcı olayların sıklığı (veya olasılığı) değerlendirilmek zorundadır. D.1.C.'nin Ek 7 kısmında başlatıcı olayların sıklığına (veya olasılığına) ait verilerin uygunluğu hakkında genel bir fikir verilmiştir. Eğer Tablo 19'da (D.1.C. kısmında bulunan Tablo 8, MIRAS Adım 3) verilen kalitatif frekanslar yardımıyla işletme çalışanları tarafından olasılıklar belirlenebiliyorsa veya zaten mevcutsa, işletmeye özel veriler kullanılması tavsiye edilir.

Tablo 19: Başlatıcı olay frekanslarının kalitatif tanımları

YILLIK GERÇEKLEŞME FREKANSLARI		**SINIF**
Kalitatif Tanım	**Kantitatif Tanım**	**Sıralama**
Çok düşük sıklık(gerçekleşmesi zor)	$F \leq 10^{-4}$ /yıl	F_4
Düşük sıklık(1000 yılda bir)	10^{-4} /yıl < $F \leq 10^{-3}$ /yıl	F_3
Düşük sıklık (100 yılda bir)	10^{-3} /yıl < $F \leq 10^{-2}$ /yıl	F_2
Mümkün-yüksek sıklık(10 yılda bir)	10^{-2} /yıl < $F \leq 10^{-1}$ /yıl	F_1
Oluşması muhtemel- çok yüksek sıklık (sahada birçok kez yaşanmış)	$F \geq 10^{-1}$/yıl	F_0

Daha sonra hata ağacındaki güvenlik bariyerlerinin belirlenmesi (MIRAS Adım 3. B) ve güvenlik bariyerlerinin performansının değerlendirilmesi (MIRAS Adım 3. C) yapılmalıdır.

Bu işlemlerin sonunda elde edilen verilerle kritik olayların frekansını hesaplamak için hata ağacı analizi yapmak mümkündür. Analiz yapılırken "kapıdan kapıya" (gate-to-gate) yöntemi kullanılacaktır ve hata ağacı içerisinde güvenlik bariyerleri de göz önünde bulundurulacaktır. Bu işlemler kullanıma hazır D.1.C. (MIRAS Adım 3.D) içerisinde anlatılmıştır.

Kısaca, "kapıdan kapıya" yöntemi hata ağacındaki başlatıcı olaylar ile başlar ve yukarı, kritik olaylara doğru ilerler. Kapı çıktısını (gate output) değerlendirmeden önce kapı girdileri (gate input) değerlendirilmek zorundadır. Bir üst seviyeye ilerlemeden önce en alttaki kapılar hesaplanmak zorundadır.

Buna paralel olarak, güvenlik bariyerlerinin kaza senaryolarına (papyona) etkisi göz önünde bulundurulur. "Önleme bariyeri" bir alt adımdaki olayın gerçekleşmesini imkânsız hale getirir. Yani ilgili dal artık kritik olay sıklığını etkilemiyordur. Engelleme ve kontrol bariyerleri hata ağacındaki iki olay arasındaki geçiş olasılığını düşürür ve kritik olay sıklığını etkiler. Şu kadar ki; bir bariyer dalının güvenirlilik seviyesi n ise, o daldaki olayın sıklığı 10-n'e düşürülür.

Eğer bir kritik olayın sıklığı hata ağacı üzerinden hesaplanamıyorsa, eşdeğer kritik olay sıklığı yoluyla hesaplamak bir diğer seçenek olabilir. Bu yöntem MIRAS Adım 4'te anlatılmıştır. D.1.C. Ek 10'da bu konunun yayınlanan verilerinin bibliyografik inceleme sonuçları verilmiştir.

5.4. TEHLİKELİ OLAYLARIN FREKANSINI HESAPLAMA (MIRAS - ADIM 5)

Bu kısımdaki amaç, olay ağacında adım adım ilerleyip, çıktı olarak her bir olayın frekansını hesaplamaktır.

Öncelikle, MIMAH ile eşdeğer olay ağacı hazırlanır, bu aşamada 'VE/VEYA' kapıları açık bir şekilde çizilmemiştir. Aslında, kapıların açıkça dâhil edilmesi olay ağacında yapılır. VE kapıları olaylar ile eşzamanlı sonuçlar arasına yerleştirilir. VEYA kapıları ise oluşabilecek sonuç olaylarından bir tanesinin alt basamağındaki olay olarak görülür. D.1.C. Ek 11'de kapılar hakkında detaylı bilgi verilmiştir.

VEYA kapıları olay ağacında göründüğünde, bu kapılara bağlı geçiş olasılıklarının değerlendirilmesi gerekir. Geçiş olasılıkları şunlardan biri olabilir; yağmurlama sistemiyle önleme olasılığı, anında tutuşma olasılığı, gecikmiş tutuşma olasılığı veya VCE olasılığı. D.1.C. Ek 12'de bazı geçiş olasılıkları verilmiştir.

Bunların ardından olay ağacı bölümüyle bağlantılı güvenlik bariyerleri hem sonuçlar bakımından hem de olayların frekansı bakımından hesaba katılabilir. Dağıtıma hazır D.1.C. (MIRAS Adım 5)'de ayrıntılı açıklama yapılmıştır. Kısaca denilebilir ki; önleme ve kontrol bariyerleri, güvenilirlik seviyeleri ve tehlikeli olayların etkileri aracılığıyla iki olay arasındaki geçiş olasılığını düşürür. Limit bariyerler kaynağı sınırlayarak veya etkilerini sınırlayarak tehlikeli olayların sonuçlarını azaltır. Olay ağacında bir limit bariyer ile karşılaşıldığında, iki dal çizilmelidir, biri talep hatası olasılığına eşit bir olasılıkla bariyerin başarısız olması, diğeri ise bariyerin (1-PFD)'ye eşit bir olasılıkla başarılı olmasıdır. Bir güvenlik bariyerinin PFD'si 10-n'e eşittir ve n, bariyerin güvenilirlik seviyesini ifade eder. Her iki dal da olay ağacında tutulmak zorundadır, çünkü ikisi farklı tehlikeli olaylara sebep olur. Birinin frekansı yüksek ancak sonuçları daha az etkilidir, diğerinin ise frekansı az ancak sonuçları oldukça şiddetlidir.

Bu basamağın çıktısı MIMAH tarafından her bir kritik olayla ilişkilendirilen tehlikeli olayların (DP) listesidir. Her bir tehlikeli olayın frekansı hesaplanır ve kaynağın sınırlayıcılığı veya limit güvenlik bariyerlerinin etkileri göz önünde bulundurulur.

5.5. TEHLİKELİ OLAYIN SONUCUNUN SINIFINI BELİRLEME (MIRAS - ADIM 6)

Referans Kaza Senaryolarının seçimi potansiyel sonuçları ile beraber, tehlikeli olayların frekansına dayanır. Dolayısıyla, her bir tehlikeli olayın sonucu kalitatif olarak belirlenmek zorundadır. Bu değerlendirme Tablo 20'de belirtilen dört sonuç sınıfına göre yapılır ve limit güvenlik bariyerlerini olay ağacında dikkate alır. (bkz. D.1.C. (MIRAS Adım 6))

Tablo 20: Sonuç sınıfları

SONUÇLAR			SINIF
Domino etkisi	**Canlı Hedefe Etki**	**Çevreye Etki**	**Sıralama**
Domino etkisini hesaba katmak için, üzerinde çalışılan tehlikeli olayın sonuç sınıfı, ilk olayın neden olduğu ikincil olayın sınıfına yükseltilir.	Hiç yaralanma yok veya alışmayı durdurmaya gerek kalmayacak kadar küçük yaralanma	Harekete geçmeye gerek yok, sadece izleme	C_1
	24 saatten fazla hastanede kalmayı gerektirecek yaralanma	Çevreye ciddi zararlar verilmiş, yerel müdahale gerekli	C_2
	Saha içerisinde telafisi olmayan yaralanmalar veya ölüm, Saha dışında telafisi olan yaralanma	Saha dışında da çevreye zarar verilmiş, ulusal müdahale gerekli	C_3
	Saha dışında telafisi olmayan yaralanma veya ölüm	Saha dışına telafisi olmayan zararlar verilmiş, ulusal müdahale gerekli	C_4

Tablo 21'de "tam gelişmiş" tehlikeli olayların kabaca sınıf sonuçları verilmiştir [*]. Bu tablo sadece alışma aşamasında kullanılmalıdır.

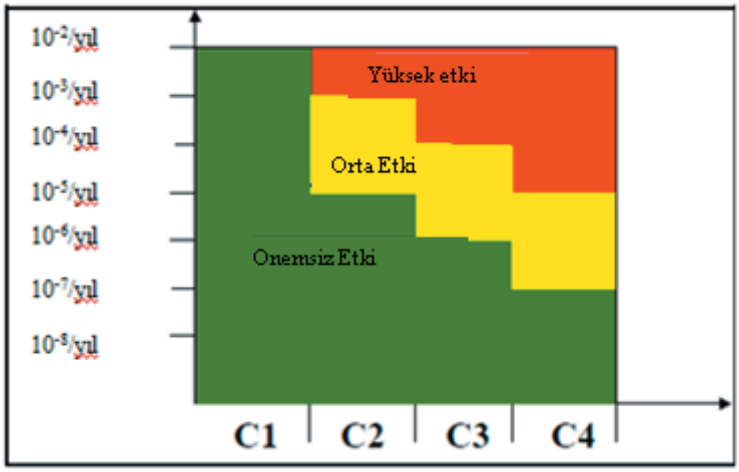
Tablo 21: "Tam Gelişmiş" kaza olayı sonuçlarının kabaca sınıfları

Tehlikeli Olay	***Sonuç Sınıfı***
Birikinti (Havuz) Yangını	C2
Tank Yangını	C1
Jet Yangını	C2
VCE	C3 veya C4 (salınan miktara göre)
Flash Yangını	C3
Toksik Bulut	C3 veya C4 (Risk tabirlerine göre- çok toksik maddeler için C4)
Yangın	C2
Şarapnel(Missiles) Şeklinde Fırlama	C3
Fazla Basınç Salımı	C3
Yangın Topu	C4
Çevresel Hasar	İşletmede karar vermek için

5.6. REFERANS KAZA SENARYOLARININ SEÇİMİ (MIRAS - ADIM 7)

Kaza senaryolarının seçimi "Risk Matrisi" denilen, frekans ve kazaların potansiyel sonuçlarını kesiştiren, yöntemle yapılır (bkz. şekil 13). Matristeki üç bölge şu şekilde tanımlanır: aşağıdaki yeşil bölge ("ihmal edilebilir etki bölgesi"), ortadaki sarı bölge ("orta şiddetli etki bölgesi") ve yukarıdaki kırmızı bölge ("yüksek etki bölgesi").

Papyondan gelen her bir tehlikeli olay tahmin edilen frekansına ve sonuç sınıfına göre risk matrisine yerleştirilmedir. **Kırmızı ve sarı bölgelerde bulunan Tehlikeli Olaylar Referans Kaza Senaryolarıdır ve şiddet hesaplamaları modellenmelidir.**



Şekil 13: Risk matrisi

5.7. ÖRNEK

Örnek olarak gösterilen papyon için (bkz. paragraf 2.3.4), hata ağacından CE7 "Ekipmanın cidarında sıvı fazında yırtılma meydana gelmesi" olayının frekansının hesaplanması, başlatıcı olayların frekans tahminlerinin göz önünde tutulması, güvenlik bariyerlerinin belirlenmesi ve performanslarının değerlendirilmesi Şekil 14'de gösterilmiştir.

Şekil 13'te, güvenlik bariyerleri ve olay ağacındaki geçiş olasılıkları da hesaba katılarak tehlikeli olayların frekansı hesaplanmış ve daha önce örnek olarak çalışılan olay ağacında gösterilmiştir (bkz. paragraf 2.3.4).

Tehlikeli olayların kalitatif olarak değerlendirilmiş sonuç sınıflarını elde ettikten sonra, bu veriler Risk Matrisine yerleştirilmiştir (bkz. şekil 16).

Dolayısıyla, burada düşünülen örnekte, altı Referans Kaza Senaryosu (tehlikeli olay ile ilgili, "sarı" ve "kırmızı" bölgelere yerleştirilmiş) şiddet hesabı için modellenecektir.

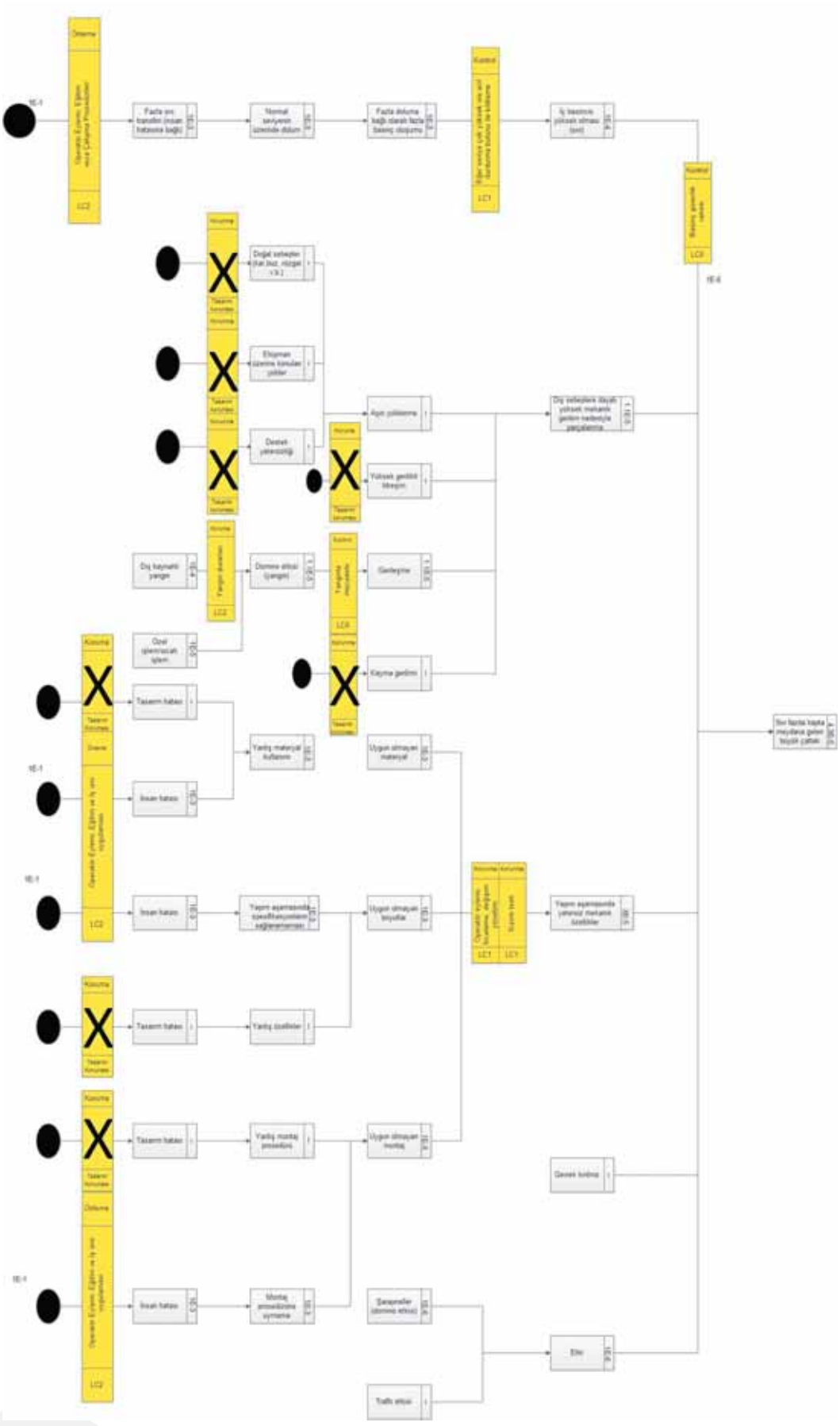
5.8. DEĞERLENDİRME

MIRAS uygulamasında, başlatıcı olayların frekans/olasılık hesapları, güvenlik bariyerlerinin belirlenmesi, güvenlik bariyerlerinin performanslarının değerlendirilmesi ve geçiş olasılıklarının belirlenmesi için gerekli veriler, sahaya yapılan ikinci ziyaret sırasında elde edilebilir ve tartışılabilir.

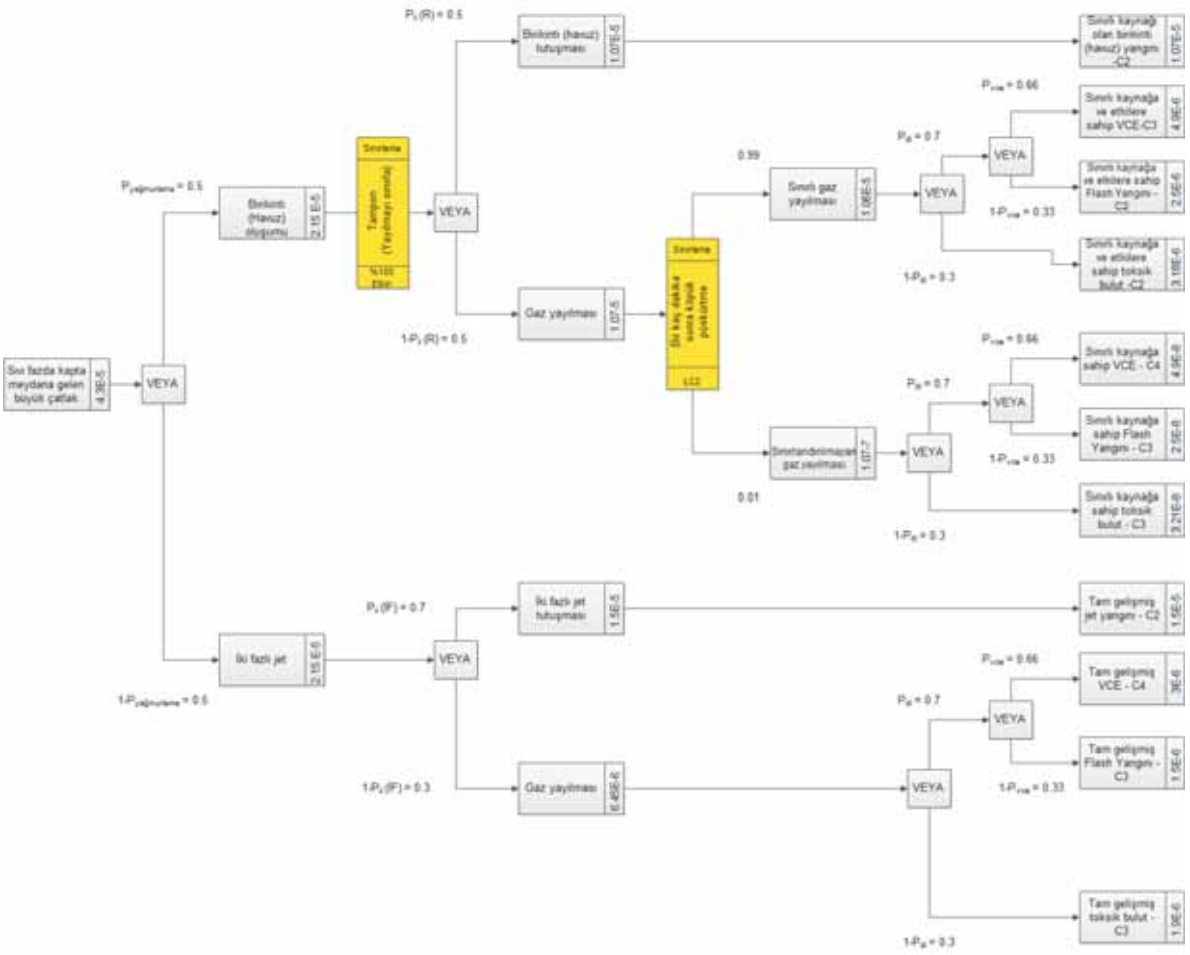
D.1.C. Ek 7, 10 ve 12'de verilen önbilgi amaçlı şekiller bilinçsizce kullanılmamalıdır çünkü bu bilgiler kendine özgü özellikler taşımaktadır. Bu verilerde birçok belirsizlik bulunmaktadır, kaynakları çok kesin değildir ve uygulama koşulları bilinmemektedir.

MIRAS'da, kazaların sebepleri hakkında derin bir çalışma yapılması, olasılık seviyeleri ve güvenlik sistemleri senaryoları büyük kaza tehlikelerinden daha gerçekçi senaryolar belirlenmesine olanak sağlamaktadır. Referans Kaza Senaryoları, güvenlik sistemlerini (ayrıca güvenlik yönetim sistemini) de hesaba katarak, ekipmanların gerçek tehlike potansiyellerini ortaya koymaktadır. Referans Kaza Senaryoları, modeli uygulamak için gerekli bilgiler ile kaza şiddet indeks (S) hesaplaması yapacak kişilere verilir (bkz. dağıtıma hazır D.1.C. (MIRAS Adım 8).

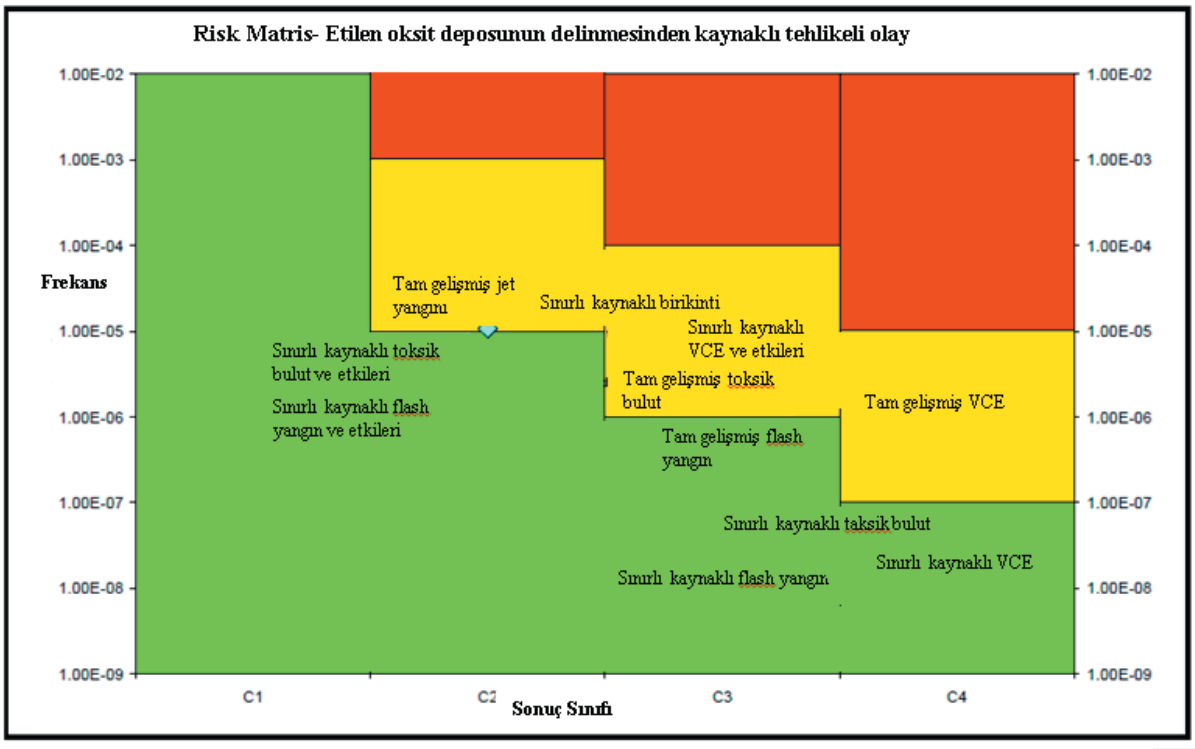
Unutulmamalıdır ki risk matrisi, riskin kabul edilebilirliği için değil, sadece referans kaza senaryoları seçmek için bir rehberdir. Referans Senaryolar şiddet hesabı yapılabilmesi için modellenen ve işletmenin çevresinin hassasiyeti ile kıyaslanacak olan senaryolardır.



Şekil 14: CE7 "Ekipmanın cidarında sıvı fazında yırtılma meydana gelmesi" olayının frekansı ile hata ağacı



Şekil 15: Tehlikeli olay frekansı ile olay ağacı



Şekil 16: CE7 "Ekipmanın cidarında sıvı fazında yırtılma meydana gelmesi" tehlikeli olayının risk matrisi

6. ÖRNEK SENARYOLARIN RİSK ŞİDDET HARİTASI

6.1. AMAÇ

ARAMIS metodolojisinin amaçlarından biri de; senaryoların şiddet ölçümleri ile ilgili bağımsız parametrelerden oluşan entegre risk indeksi vasıtasıyla risk seviyesinin belirlenmesidir. Ayrıca yönetimin önleme politikasının etkinliğini ve SEVESO II kuruluşundaki potansiyel amaçların hassasiyetini tanımlayarak çevrenin hassasiyetini tahmin etmektir.

Bu nedenle, -sadece etkilerinin hesaba katılmasıyla- senaryoların şiddetinin değerlendirilmesini sağlayan parametre oluşturulmuştur. Şiddet İndeksi (S) denilen bu parametre, ARAMIS projesinde geliştirilen diğer parametrelerden ve Hassasiyet İndeksi'nden (V), tamamen bağımsızdır.

Bu bölümde Risk Şiddet İndeksinin (S) hesaplanması için metodoloji anlatılmış, örnek durum sonuçları hesaplanmış ve bahsedilen bölgedeki risklerin 'haritası' hazırlanmıştır. Metodolojinin tamamı D.2.C'de tanımlanmıştır.

6.2. RİSK ŞİDDET İNDEKSİ

Risk indeksi, sayısal bir değer ya da tanımlayıcı bir sıfat olarak, tehlike ya da sistemin riski üzerinde etkisi olan faktörlerin kantitatif ya da kalitatif bir ölçüsüdür.

Risk Şiddet İndeksi; ARAMIS çerçevesinde geliştirilen MIMAH'ın (Büyük kaza tehlikelerinin belirlenmesi metodolojisi) uygulanmasında tanımlanan Tehlikeli Olaylara (Dangerous Phenomena-DP) ve bunlarla ilgili Büyük Olaylara (Major Events-ME) dayanmaktadır. Bu, farklı kaza etkileri ile ilgili benzer bir takım eşik sınır değerlerine (threshold) de açıklama getirir.

6.2.1. Eşik Sınır Değerleri (Threshold Levels)

Avrupa'nın farklı ülkelerinde kullanılan kriterler örnek alınarak dört seviye etkisi yöntemde verilmiştir. (Tablo 22).

Tablo 22: Dikkate alınan etki düzeyleri

Etki Düzeyleri	Tanım
1	Düşük ya da etkisiz
2	Telafisi olan etki
3	Telafisi olmayan etki
4	Öldürücülük ve/veya domino etkisinin başlaması

Dikkate alınan farklı etkiler:

a) Termal radyasyon:

Sürekli Radyasyon

Eşik sınır değerler 60 saniyelik maruz kalma süresi için gösterilir, farklı maruz kalma sürelerinden bahsedilirse Tablo 23'teki değerler dozun hesaba katılmasıyla değişir.

Anlık Radyasyon

Bu durumda eşik sınır değerler alevlenebilir malzemenin buluttaki konsantrasyonu ile ilişkilendirilir.

b) Patlama Basıncı Etkisi:

Dört adet maksimum yüksek basınç aralığı kullanılır. Bu durumda, direkt maksimum yüksek basınç değeri olan doz üzerinde, sürenin etkisi yoktur.

c) Şarapnel

Şarapnel fırlaması için sınır değerde sadece iki olasılıktan bahsedilir: Şarapnellerin bulunduğu mesafeden %100 daha küçük herhangi bir nokta için etkilerin maksimum değeri (4) ve daha uzak mesafeler için minimum değeri (1).

d) Toksik Etkiler:

TEEL (Geçici Acil Maruziyet Limitleri) değerleri kullanılır.

Risk Şiddet İndeksi'nin tanımlanmasında kullanılan etkilerin dört seviyesi ile ilgili eşik sınır değerleri Tablo 23'te özetlenmiştir. Şunu belirtmek gerekir ki; bu yeni harmonize (uyumlaştırılmış) eşik sınır değerleri önerisi değildir, bu her ülkenin kendi kararıdır ve ARAMIS projesinin konusu değildir. Tablo 23 sadece projenin içeriği için kullanılır ve önerilen şiddet indeksi başka herhangi bir eşik sınır değer için uygulanabilir.

Tablo 23: Farklı değerlerin etkileri için sınır tanımları

Etki seviyesi	**Radyasyon[5] (kW/m^2)**	**Anlık Radyasyon**	**Patlama Basıncı (mbar)**	**Şarapnel [6](%)**	**Toksik Etkiler**	**Tanım**
1	< 1.8	< 0.5*LFL	< 30	0	<TEEL1	Küçük ya da etkisiz
2	1.8-3		30-50		TEEL1-TEEL2	Telafisi olan etki
3	3-5		50-140		TEEL2-TEEL3	Telafisi olmayan etki
4	>5	= 0.5*LFL	> 140	100	>TEEL3	Öldürücülük ve/veya domino etkisinin başlaması

[5] Bu durum, tehlikeli olayların olasılıkları tanımlanırken ihtiyatlı bir yaklaşım uygulandığında oluşabilir.

Tablo 23'te bahsedilen etkilerin tümü sadece insanlar ve maddeleri referans alırken çevreyi dikkate almaz. Bununla birlikte, çevre üzerindeki en önemli etki toksik maddelere bağlıdır ve bu durumda çevreyi etkileyen referans konsantrasyon seviyesi de hesaba katılmalıdır.

6.2.2. Risk Şiddet İndeksi

Verilen kritik bir olay için Risk Şiddet İndeksi SCE, kritik olaylara da sahip tehlikeli olaylarla ilgili Spesifik Risk Şiddet İndeksleri'nin (SDP) kombinasyonudur. Bu durumun oluşma ihtimalleri şu şekilde hesap edilebilir;

$$S_{CE}(d) = \sum_{i=1}^{n} \left(P_{DP_i} \cdot S_{DP_i}(d) \right)$$

Eşitlik 1

Bu ifadede; n, kritik olayla ilgili olan tehlikeli olayların (DP) sayısının toplamı; PDPİ, DPİ'nin oluşma olasılığı; ve SDPİ(d), DPİ ile ilgili olan spesifik şiddet indeksidir.

SCE'nin değeri genellikle 0 ve 100 arasında (Tablo 24) olmasına rağmen bazı durumlarda, özelikle d'nin küçük değerleri, 100'den büyük (örneğin, DP ile ilgili olan olasılıkların toplamı 1'den büyük olduğunda) olabilir.

Tablo 24: Seviye etkilerinin fonksiyonu olarak spesifik risk şiddet indeks değerleri

S_{DP}	Etkilerin Seviyesi
0-24	1
25-49	2
50-74	3
75-100	4

Bütün tesis için Risk Şiddet İndeksi (S), dikkate alınan kritik olaylar ve bunların oluşum sıklıklarıyla ilgili olan Risk Şiddet İndekslerinin birleşimidir :

$$S(d) = \sum_{j=1}^{m} \left(f_{CE_j} \cdot S_{CE_j}(d) \right)$$

Eşitlik 2

Bu ifadede; m, tesisle ilgili olan kritik olayların (CE) toplam sayısı; fCEj CEj'nin oluşma frekansı ve SCEj(d)CEj ile ilgili olan risk şiddet indeksidir.

Eşitlik 2'nin uygulanmasıyla elde edilen değerler 0-100 aralığında değildir ve Tablo 24'te tanımlanan değerler daha fazla uygulanamaz. Elde edilen değerler genelde 0-1,2 aralığındadır. Bu değerler normalleştirilerek 0-1000 arasında değerler alırlar. Şu ölçü kullanılabilir;

Tablo 25: Tesis için risk şiddet indeks ölçüsü

S değeri	Risk Şiddet İndeks Seviyesi
S= 750	Son derece yüksek
300= S < 750	Yüksek
50= S <300	Orta
S<50	Düşük

S değeri uzaklığın fonksiyonu olarak değişir; bu durumda, şiddet haritası tesis için düzenlenebilir. GIS üzerindeki S değerlerini göstermek için, her bir tehlikeli olayla ilgili önerilen beş uzaklık hesaplanır (Tablo 26).

Tablo 26: S değeri ve bu değerden elde edilen uzaklık arasındaki ilişki

S_{DP}	Uzaklık
0	d_0
25	d_1
50	d_2
75	d_3
100	d_4

d_0 ve d_4 değerleri modellerin uygulanmasıyla bulunabilir, herhangi bir uzaklık için S değeri ise her aralık içindeki lineer denklemlerin uygulanmasıyla elde edilebilir (Tablo 27).

SDP, SCE ve S değerleri, direkt olarak her bir etkilenmiş bölgenin küçük kareleri içinde değerlendirilir. Bu değerlendirme özel olarak geliştirilen GIS, şiddet değerlendirme aracı ile yapılır.

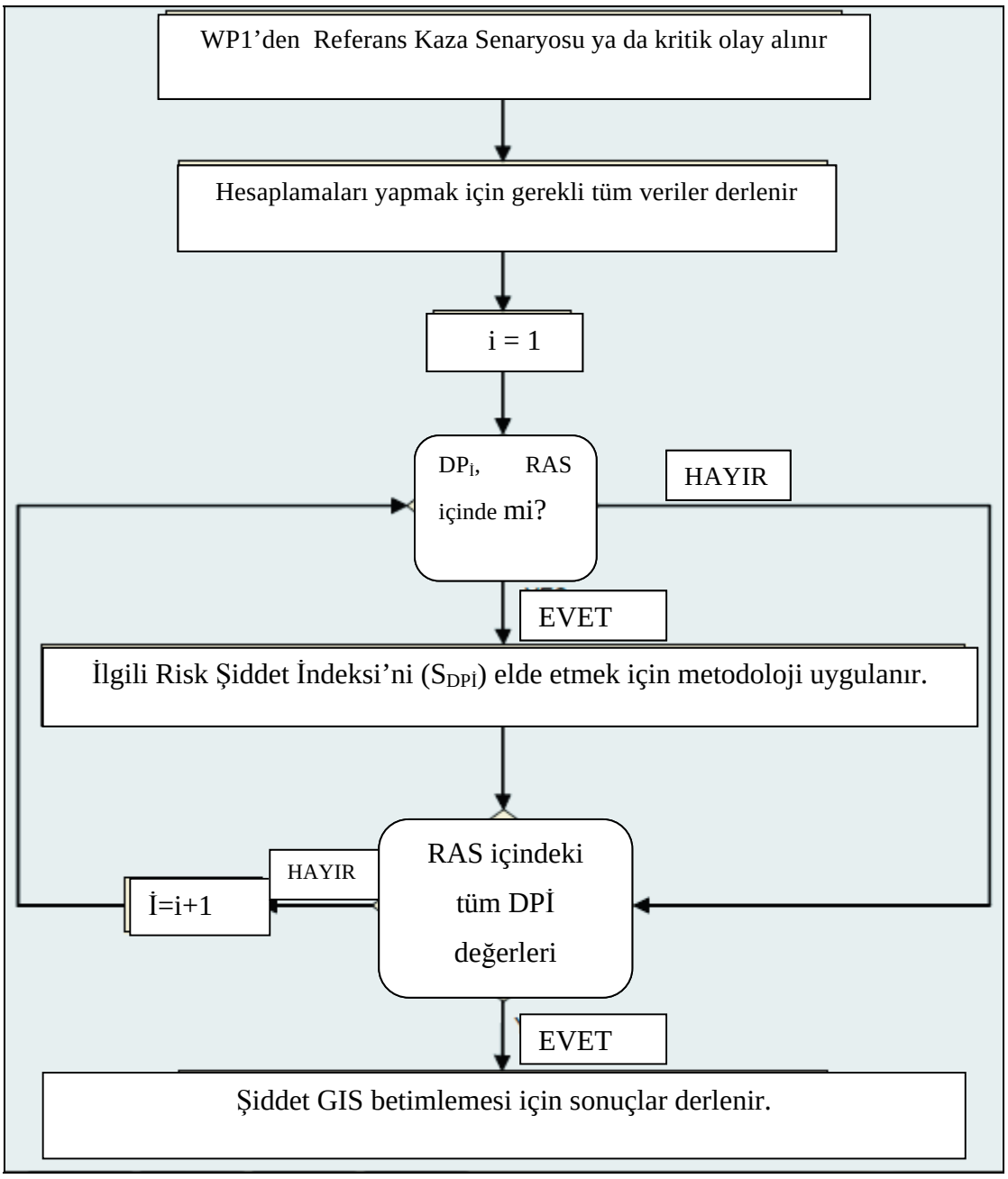
Kullanıcının sadece tesis için bahsedilen her bir DP için d_0 ve d_4 değerlerini bulması gerekir ve bunları GIS içine yerleştirerek haritaları ve verilen bir nokta için risk şiddet indekslerini elde eder.

Tablo 27: S_{DP} için lineer denklemler

$S_{DP} = \frac{25}{(d_1 - d_0)} \cdot x - \frac{25 \cdot d_0}{(d_1 - d_o)}$	$d_1 < x < d_o$	Eşitlik 6
$S_{DP} = \frac{25}{(d_2 - d_1)} \cdot x + \frac{(25 \cdot d_2 - 50 \cdot d_1)}{(d_2 - d_1)}$	$d_2 < x < d_1$	Eşitlik 3
$S_{DP} = \frac{25}{(d_3 - d_2)} \cdot x + \frac{(50 \cdot d_3 - 75 \cdot d_2)}{(d_3 - d_2)}$	$d_3 < x < d_2$	Eşitlik 5
$S_{DP} = \frac{25}{(d_4 - d_3)} \cdot x + \frac{(75 \cdot d_4 - 100 \cdot d_3)}{(d_4 - d_3)}$	$d_4 < x < d_3$	Eşitlik 4

6.3. RİSK ŞİDDET DEĞERLERİNİN HESAPLANMASI

Referans kaza senaryoları (RAS) ya da kritik olaylar (CE) ile ilgili Risk Şiddet İndeksinin belirlenmesi için genel prosedür Şekil 15'te verilmiştir. Örnek bir hesaplama ise bölüm 7.5 'te verilmiştir.

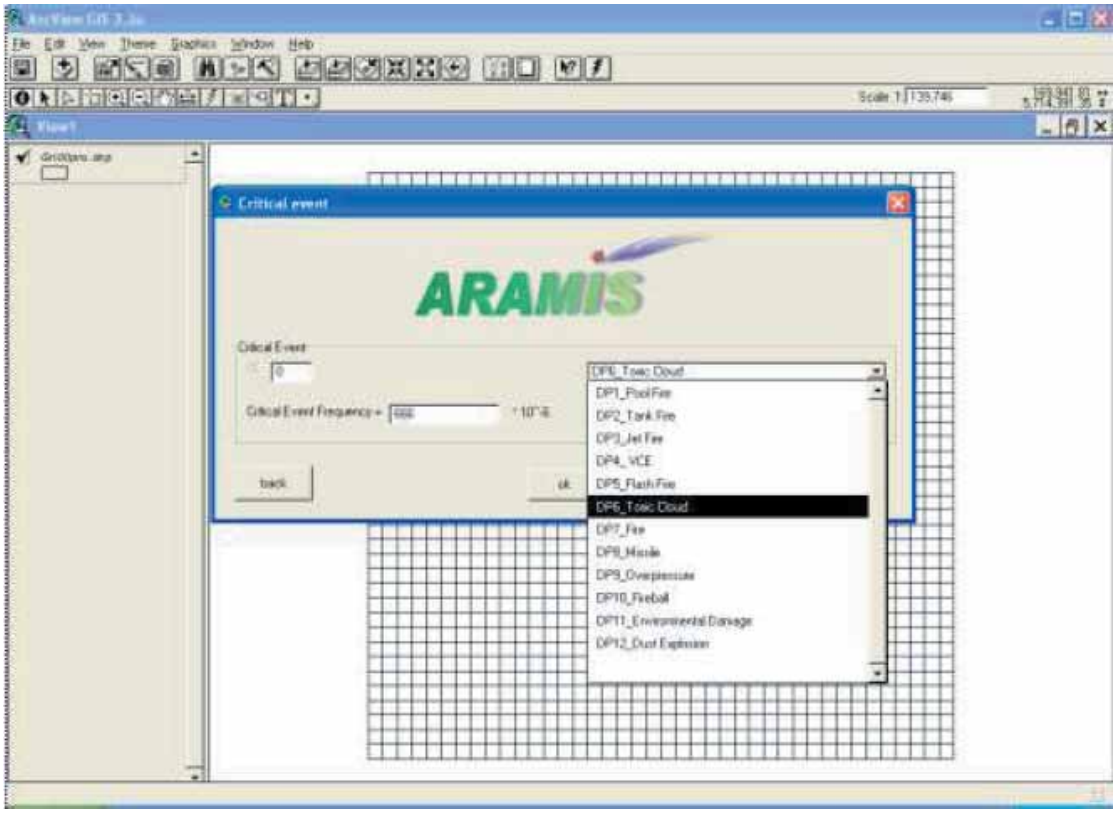


Şekil 17: Risk Şiddet İndeksinin elde edilmesi için küresel metodolojinin şematik gösterimi

[8] Örnek olay incelemesi, şiddet indeksinin dikkate alınan kritik olayların sayısına çok duyarlı olduğunu göstermiştir. Bu sonuç için iyi bir değer sağlamak amacıyla metodolojinin önceki adımları dikkatlice izlenmelidir.

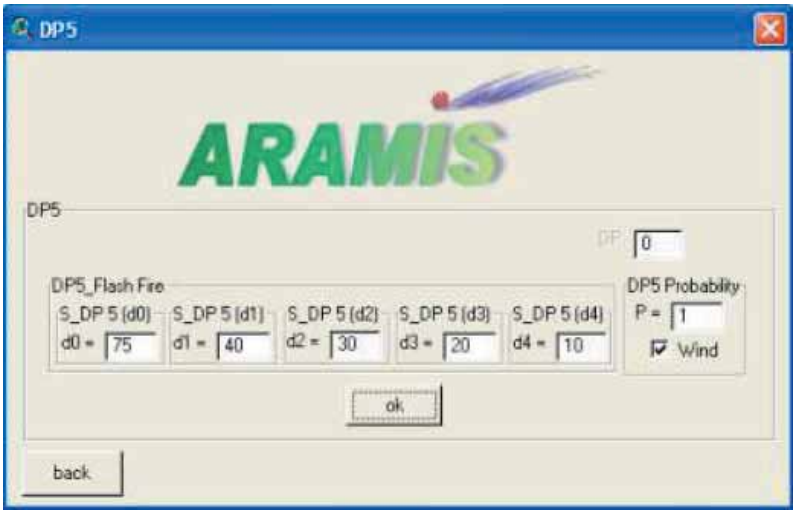
6.3.1. GIS (Coğrafi Bilgi Sistemi) Şiddet Haritası Prosedürü

GIS ArcView® aracı ile hazırlanan prosedürler farklı haritaların hazırlanması için kullanıcıyı desteklemektedir. İlk adım seçilen sistemin (hassasiyet haritasına bakınız) planlaması ve rüzgar yönü ihtimali ile ilgili verilerin girilmesidir. Daha sonra kullanıcı, ilgili menüden tehlikeli olayı seçerek kritik olayla ilgili verileri girmelidir (Şekil 18).



Şekil 18: Kritik bir olay için tehlikeli olayın seçilmesi

Her şiddet değeri ile ilgili uzaklıkların, olasılığa ve rüzgâr yönüne göre etkilenip/etkilenmediği de (flash yangınla ilgili Şekil 19'da gösterildiği gibi) her tehlikeli olayın penceresine girilmelidir.

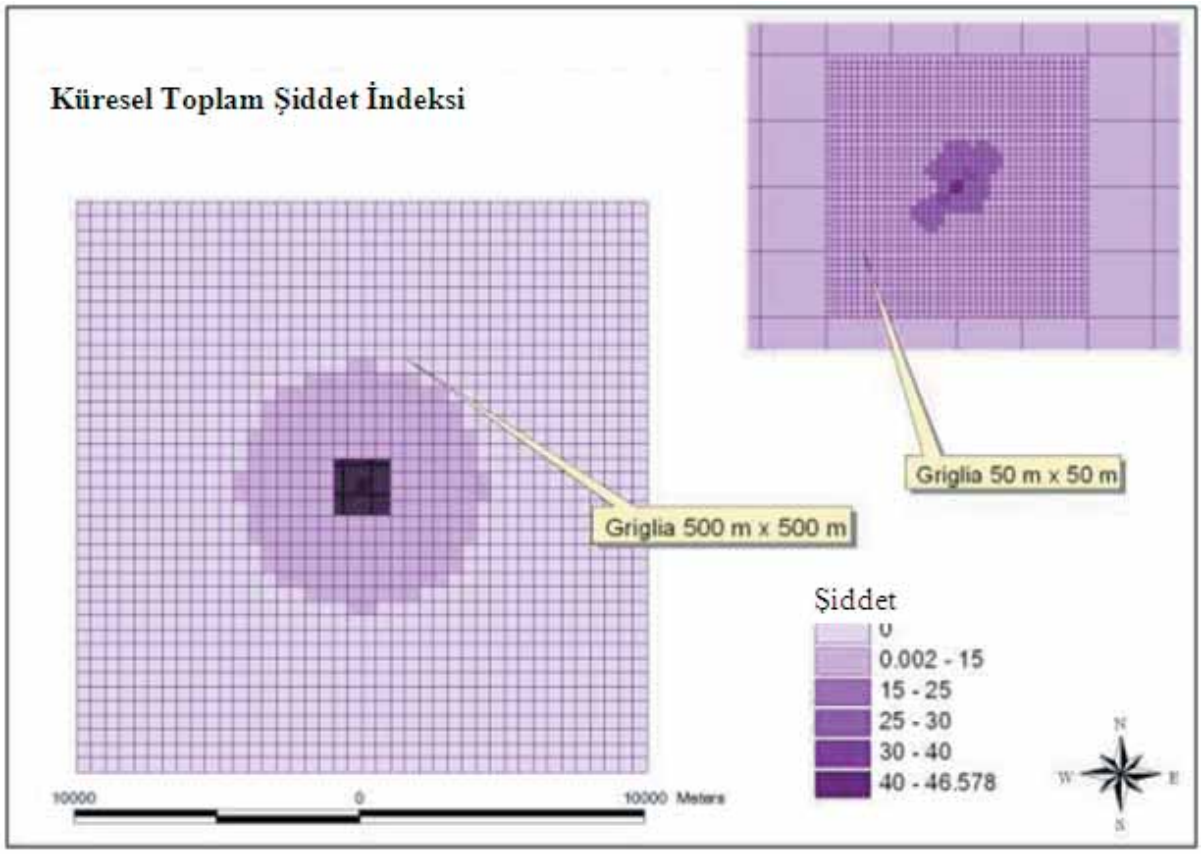


Şekil 19: Tehlikeli bir olay için veri girilmesi

Kritik olayda bahsedilen tehlikeli olayla ilgili tüm girdiler tamamlandıktan sonra, kritik olay şiddet haritası hesaplanır. Daha sonra, takip eden kritik olayların verileri girilir ve prosedür tekrarlanır. Kritik olaylarla ilgili tüm veriler girildikten sonra, toplam şiddet haritaları hesaplanır.

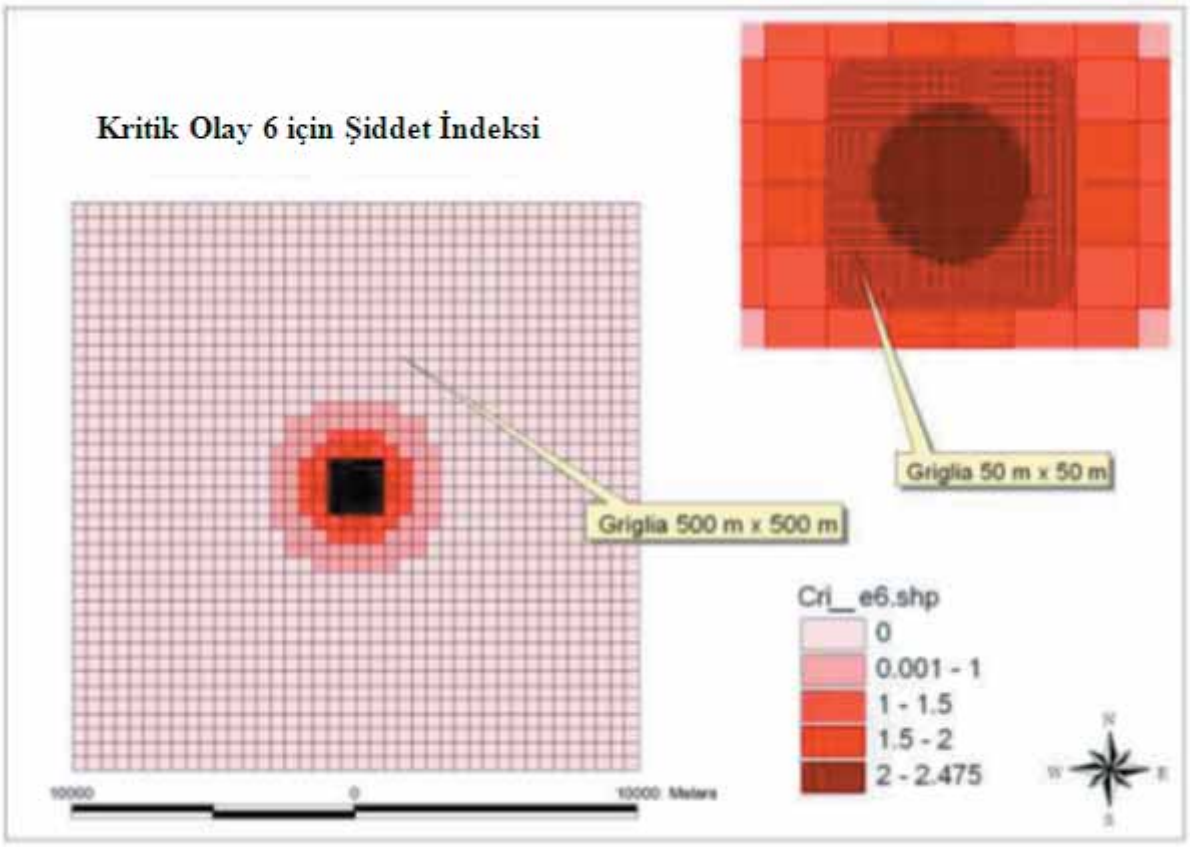
6.3.2. Sonuç: Şiddet Haritaları

GIS şiddet değerlendirme aracına bütün verilerin girilmesi ile birkaç harita elde edilir. Örneğin Şekil 18, tüm tesis için Eşitlik 2'ye göre hesaplanan Risk Şiddet İndeksinin haritasını göstermektedir. Bu tesis için risk şiddet indeks değeri, yaklaşık 750 metreden fazla olan uzaklıklar için çok düşük ve 750 metreden az olan uzaklıklar için düşük elde edilebilir. Rüzgâr yönünün etkisi iç sistem detayında fark edilebilir. Örneğin birikinti (havuz) yangını gibi tehlikeli olaylarla ilgili olan bazı kritik olaylar rüzgâr yönünden etkilenmezken (Şekil 21'da gösterilen CE6'daki gibi), flash (ani) yangın (Şekil 21'da gösterilen CE7'deki gibi) gibi tehlikeli olaylarla ilgili olanlar bu parametreye hassasiyet gösterebilir.

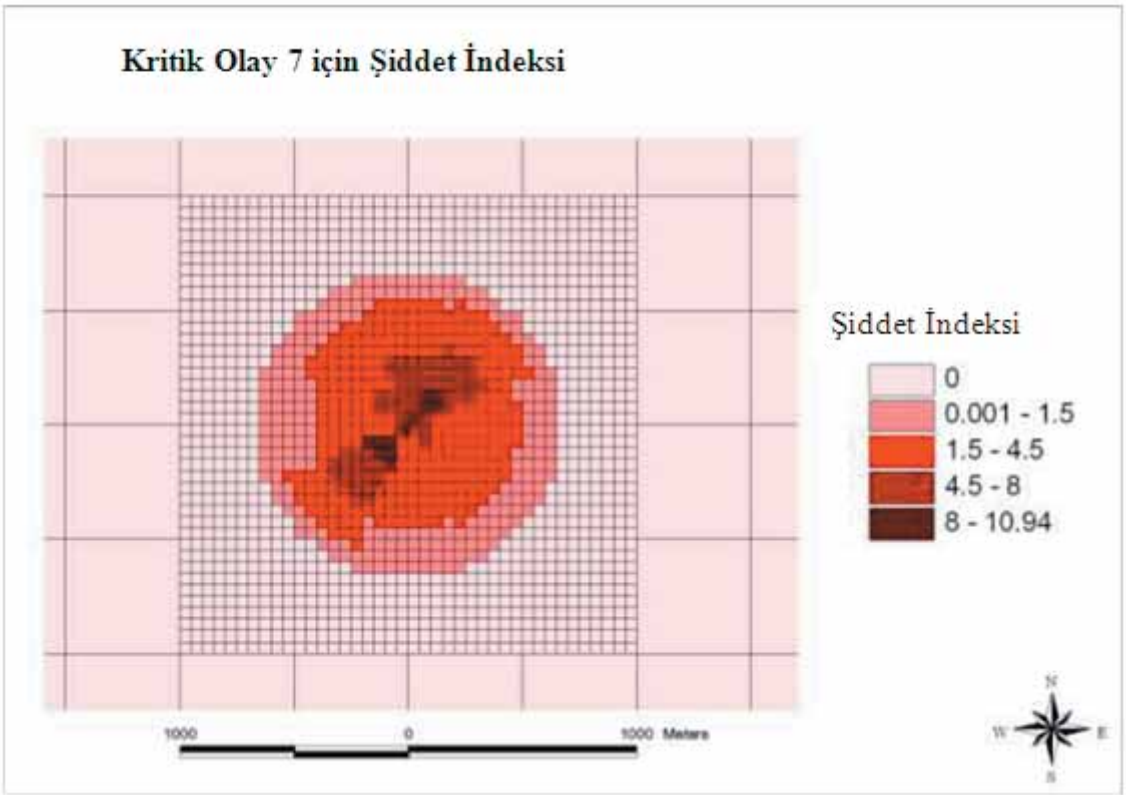


Şekil 20: Tüm tesis için küresel risk şiddet indeks haritası

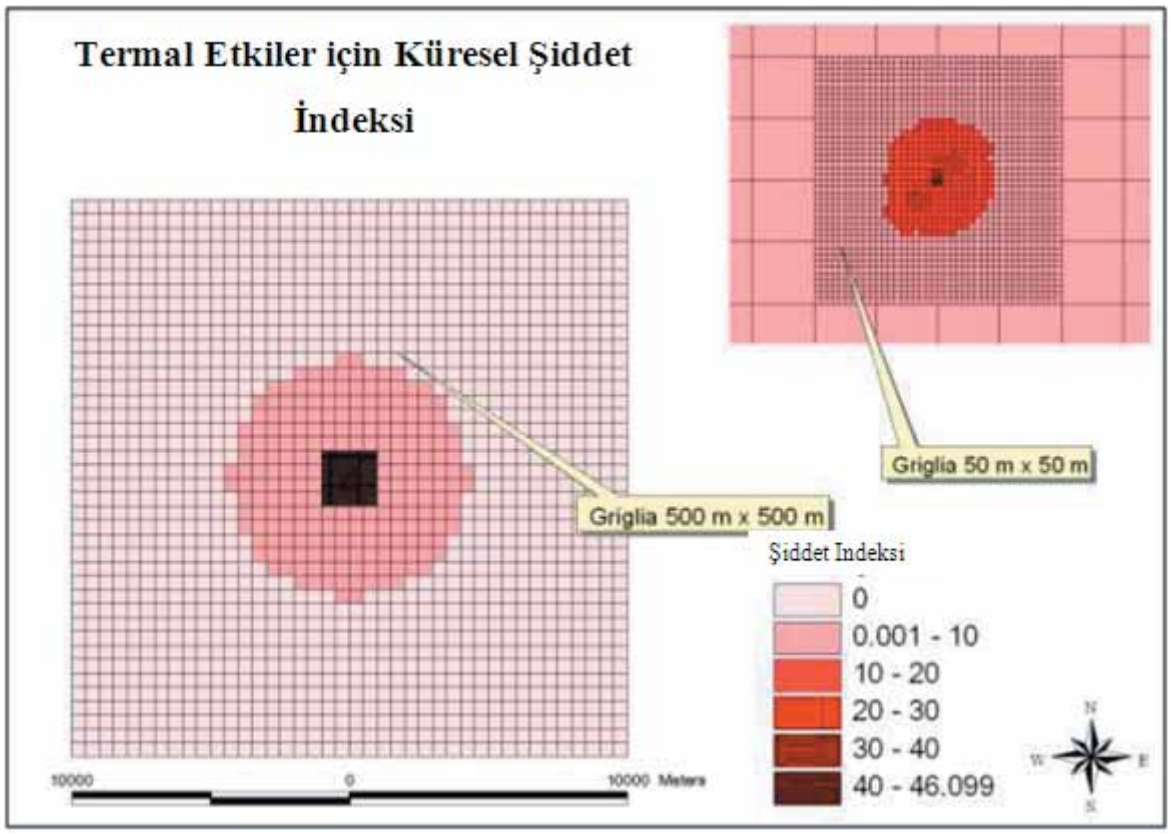
Uygulama, kritik olaylar üzerinde sadece termal ve yüksek basınç etkilerinin tesir ettiği bir sistemi işaret etmektedir: Şekil 23 ve Şekil 24, bu etkilerin etkilediği tüm tesis için risk şiddet indeksinin detaylarını göstermektedir. Yüksek basınç etkileri rüzgâr yönüne duyarlı değildir ve yüksek basınç etkilerinin risk şiddet indeksinde termal olanlara göre daha az payı vardır.



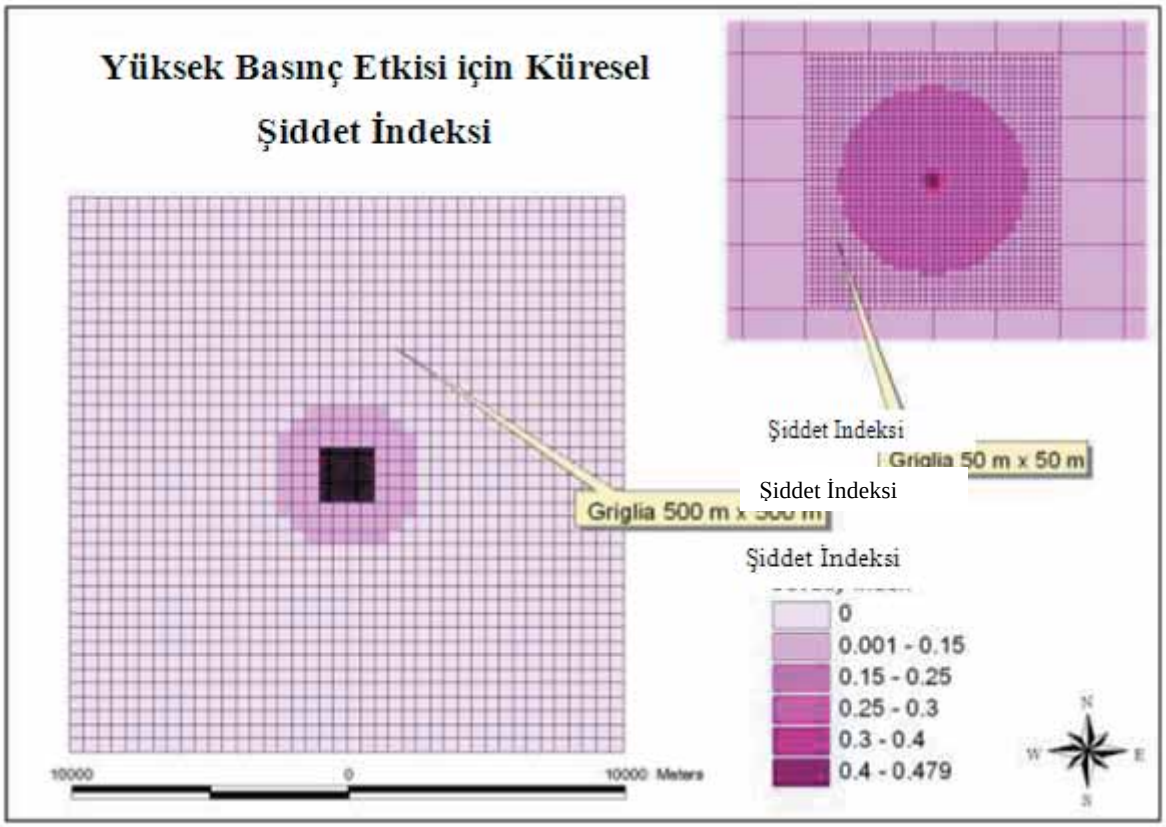
Şekil 21: CE 6 için risk şiddet indeks haritası (Tehlikeli olay: birikinti (havuz) yangını)



Şekil 22: CE 7 için risk şiddet indeks haritası (Tehlikeli olay: flash (ani) yangını)



Şekil 23: Tüm tesisi etkileyen termal etkiler için risk şiddet indeks haritası



Şekil 24: Tüm tesisi etkileyen yüksek basınç etkileri için risk şiddet indeks haritası

6.3.3. Değerlendirme

Risk Şiddet İndeksi endüstriyel tesislerle ilgili olarak pratik değerlendirme olanağı sunar. GIS kullanılarak etkilenen bölümün haritası üzerinde olasılığın grafiğinin çizilmesi, hem bölge planlamasında hem de acil durum yönetiminde kullanılabilen önemli bilgiler sağlar. Bu bilgi, tesisin çevresine olan etkisi hakkında detaylı bilgiler veren hassasiyet haritasından elde edilenler ile karşılaştırılmalıdır. Bundan başka, haritalar tek başına kritik olayların ve/veya tek başına etkilerin (toksik, termal, vb.) sonuçlarını tanımlamada da kullanılabilir.

6.4. HESAPLAMALARDA KULLANILACAK MODELLERİN SEÇİMİ

Kazalardan elde edilen etkilerin tahminleri için kullanılan modeller geniş bir çeşitlilik gösterir. ARAMIS metodolojisinde, kullanılacak en uygun modelin seçimi yapılır. Seçim yapmak için kullanılan kriterler aşağıdaki gibidir :

Modelin ve eşitliklerin çözümünün karmaşıklığı:

Örneğin birikinti (havuz) yangınları durumlarında nokta kaynaklı model (the point source model) oldukça basit ve kullanımı kolay olmasına rağmen elde edilen sonuçlar güvenilir değildir. Bu durumda katı yanma modeli seçilir.

Modelin kullanılması için gereken bilgi:

Buhar bulutu patlamalarının yüksek basınç hesaplamaları için kullanılan Çoklu Enerji Model'i, TNT Eşdeğer Modellerinden daha fazla bilgi gerektirir. Az bilginin mevcut olduğu bu tür durumlarda TNT Modeli seçilir. Aksi takdirde, gerekli tüm bilgilerin mevcut olduğu durumda Çoklu Enerji Modeli seçilir.

Bir takım eşitlikler ya da ücretsiz yazılımlar aracılığıyla modelin kullanılabilirliği:

Atmosferik dağılım hesaplamaları için seçilen modellerden Gaussian ya da İntegral Model genellikle kullanılan modellerdir. Bu modellerden bazıları ücretsiz kullanılabilir.

Kabul edilebilirlik ve bilimsel topluluk tarafından kullanım derecesi:

Büyük kabul gören ve yaygın olarak kullanılan bazı yayınlar ve kitaplar bulunmaktadır. Bu nedenle, bazı kazalarda bu yayın ve kitaplarda tavsiye edilen modeller önerilir. Örneğin, jet yangınlarındaki termal radyasyonun tahmini için kullanılan model 'Yellow Book'da (Hollanda) önerilmektedir.

Bunlara rağmen, belirtmek gerekir ki aslında büyük olayları hesaplamada kullanılan modeller şiddet indeksinin (S) tanımlanması için tasarlanan metodolojilerden tamamen bağımsızdır. Bu nedenle, kullanıcı kazanın etkilerini tahmin edebilmek için herhangi bir matematiksel model uygulayabilir.

6.5. ÖRNEK: ALEVLENEBİLİR MADDELER İÇİN DEPOLAMA TESİSİ

MIRAS (Referans kaza senaryolarının belirlenmesi metodolojisi) çalışılan şu kritik olayları verir:

Tablo 28: Alevlenebilir madde deposu için çalışılan kritik olaylar

Yükleme /boşaltma alanı (depolama vagonu)	CE_01	- Sıvı fazda cidarda delinme (bağlantı)
	CE_02	- Sıvı fazda cidarda delinme (10 mm)
	CE_03	- Sıvı fazda cidarda delinme (100 mm)
	CE_04	- Sıvı borusundan sızma (tam)
	CE_05	- Sıvı borusundan sızma (%10 eşdeğer çap)
Atmosferik depolama tankları	CE_06	- Sıvı fazda cidarda delinme (10 mm)
	CE_07	- Sıvı fazda cidarda delinme (100 mm)
	CE_08	- Katastrofik yırtılma (iç patlama)

Tablo 29: Rüzgar gülü olasılıkları

N	NE	E	SE	S	SW	W	NW
8.43	20.48	7.23	10.84	14.46	19.28	9.64	9.64

Kritik Olaylar:

Tablo 30'dan Tablo 37'ye kadar olan tablolardan elde edilen sonuçlar, dikkate alınan tüm kritik olaylar ve bunlarla ilgili tehlikeli olaylara modellerin uygulanmasıyla elde edilmiştir. Her tabloda GIS için gerekli olan tüm veriler girilmiştir; kritik olayın frekansı, her tehlikeli olay için oluşma olasılıklarıyla beraber d_0 ve d_4 uzaklıkları ve etki türü (termal, yüksek basınç, toksik ya da çevre kirliliği).

Tablo 30: Kritik olay 1 için veriler

Kritik Olay	CE_01	**Frekans**	$9.6x10^{-5}$

Tehlikeli Olay		**d0**	**d1**	**d2**	**d3**	**d4**
Birikinti (Havuz)Yangını	DP1	2413	60.6	43.9	29.1	17.9
VCE	DP2	2623	95	57	1	0
Flash Yangın	DP3	1200	57	38	29	18

Olasılık	**Tür**
0.698	Termal
0.0896	Yüksek basınç
0.0896	Termal

Tablo 31: Kritik olay 2 için veriler

Kritik Olay	CE_02	**Frekans**	$1.0x10^{-4}$

Tehlikeli Olay		**d0**	**d1**	**d2**	**d3**	**d4**
Birikinti (Havuz)Yangını	DP1	1981	48.5	35.9	25.2	16.7
Flash Yangın	DP2	495	26	17	11	10

Olasılık	**Tür**
0.005	Termal
0.027	Termal

Tablo 32: Kritik olay 3 için veriler

Kritik Olay	CE_03	**Frekans**	$1.2x10^{-5}$

Tehlikeli Olay		**d0**	**d1**	**d2**	**d3**	**d4**
Birikinti (Havuz)Yangını	DP1	4290	91	62.2	38.2	20.8
VCE	DP2	2630	95.4	57.7	1	0
Flash Yangını	DP3	1500	73	48	37	22

Olasılık	**Tür**
0.8	Termal
0.0117	Yüksek basınç
0.108	Termal

Tablo 33: Kritik olay 4 için veriler

Kritik Olay	CE_04	**Frekans**	$2.0x10^{-4}$

Tehlikeli Olay		**d0**	**d1**	**d2**	**d3**	**d4**
Birikinti (Havuz)Yangını	DP1	3080	74	53.1	35.2	20.3
Flash Yangın	DP2	1100	52	33	25	16
Birikinti (Havuz) Yangını	DP3	4290	91	62.2	38.2	20.8
VCE	DP4	2630	95.4	57.7	1	0
Flash Yangın	DP5	1500	73	48	36	22

Olasılık	**Tür**
0.7	Termal
0.16	Termal
0.0145	Termal
0.00038	Yüksek basınç
0.0034	Termal

Tablo 34: Kritik olay 5 için veriler

Kritik Olay	CE_05	**Frekans**	$2.0x10^{-3}$

Tehlikeli Olay		**d0**	**d1**	**d2**	**d3**	**d4**
Birikinti (Havuz)Yangını	DP1	1555	39.8	29.7	20.9	13.9
Flash Yangın	DP2	566	37	20	11	10
Birikinti (Havuz) Yangını	DP3	2930	72.1	51.5	33.9	19.3
Flash Yangın	DP4	1000	51	32	23	14
VCE	DP5	2630	95.4	57.7	1	0

Olasılık	**Tür**
0.1	Termal
0.5	Termal
0.0145	Termal
0.0034	Termal
0.0004	Yüksek basınç

Tablo 35: Kritik olay 6 için veriler

Kritik Olay	CE_06	**Frekans**	$1.0x10^{-4}$

Tehlikeli Olay		**d0**	**d1**	**d2**	**d3**	**d4**
Birikinti (Havuz)Yangını	DP1	3212	35	25.7	18.9	14.2

Olasılık	**Tür**
0.099	Termal

Tablo 36: Kritik olay 7 için veriler

Kritik Olay	CE_07	**Frekans**	$5.0x10^{-6}$

Tehlikeli Olay		**d0**	**d1**	**d2**	**d3**	**d4**
Flash Yangını	DP1	672	32	21	16	10

Olasılık	**Tür**
0.088	Termal

Tablo 37: Kritik olay 8 için veriler

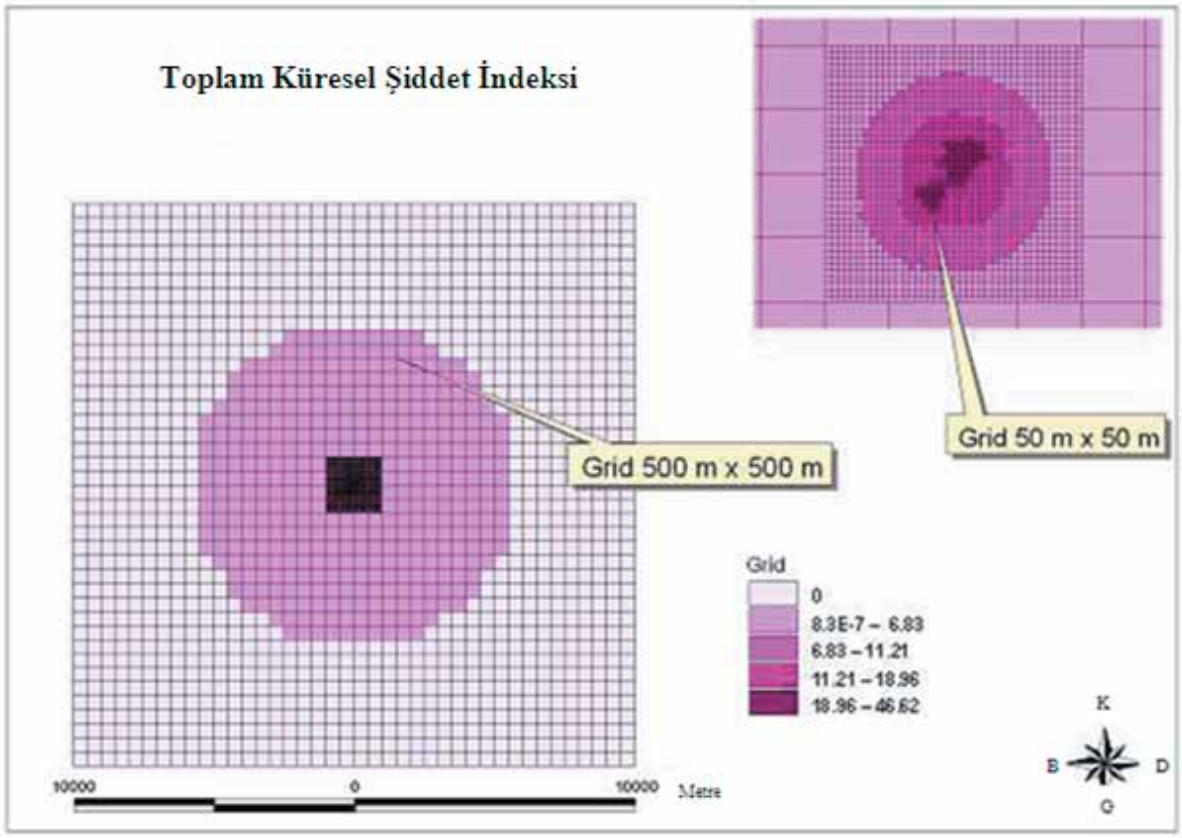
Kritik Olay	CE_08	**Frekans**	$5.0x10^{-6}$

Tehlikeli Olay		**d0**	**d1**	**d2**	**d3**	**d4**
Yüksek Basınç Oluşumu	DP1	5740	212.2	129.3	47.7	29.2

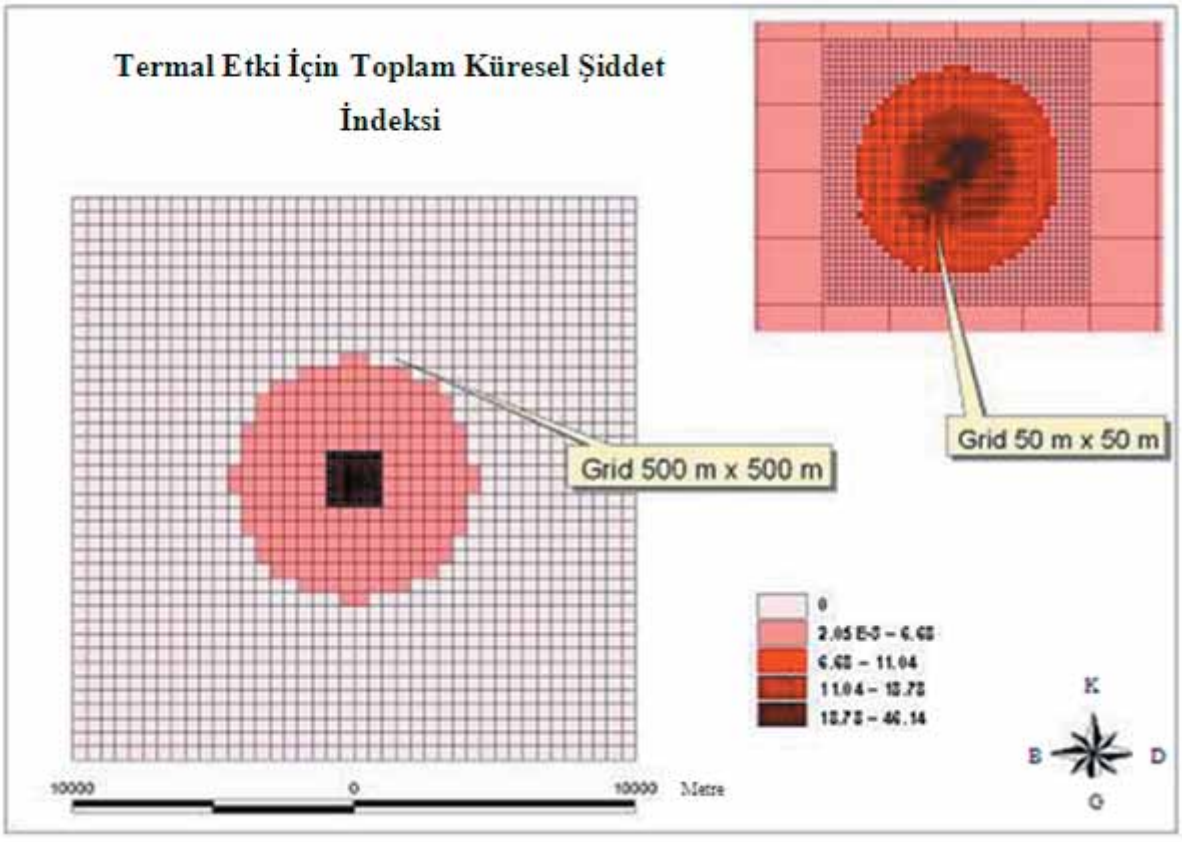
Olasılık	**Tür**
1	Yüksek Basınç

Sonuçlar: Şiddet Haritaları

Tüm verilerin, GIS aracına girişinden sonra birkaç harita çizilebilir. Aşağıda verilen iki şekil, örnek olarak gösterilmektedir. Şekil 25, Eşitlik 2'ye göre yapılan tüm tesisin Risk Şiddet İndeksini göstermektedir. Bu tesis için risk şiddet indeksinin, yaklaşık olarak 750 metreden daha yüksek mesafeler için çok düşük ve 750 metrenin altındaki mesafeler içinse düşük olduğu görülebilmektedir. Şekil 26 ise, termal etkilere karşılık gelen tüm tesis için risk şiddet indeksini göstermektedir.



Şekil 25: Tüm tesis için toplam risk şiddet indeksi



Şekil 26: Termal etkiye karşılık gelen tüm tesis için risk şiddet indeksi

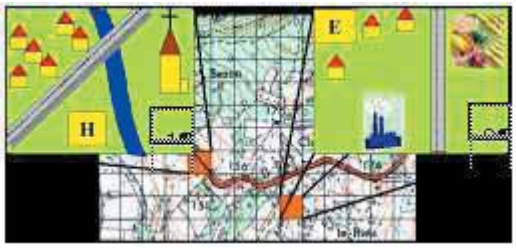
6.6. DEĞERLENDİRME

Risk Şiddet indeksi, endüstriyel tesislerle ilgili riskin uygulamalı olarak ölçülmesini olanaklı hale getirmektedir. GIS kullanmak suretiyle, etkilenen bir bölge(zone)nin haritası üzerinde bunu grafiksel olarak ifade etme imkânı, hem bölge planlamasında hem de acil durum yönetiminde kullanılabilecek oldukça ilginç bilgileri de beraberinde getirmektedir.

7. BİR TESİSİN ÇEVRESİNİN GÜVENLİK AÇIĞINI HARİTALANDIRMA

7.1. AMAÇ

ARAMIS projesi, diğerlerinin yanı sıra bir endüstriyel sahayı çevreleyen alanın güvenlik açığına dayalı olarak bütünleştirilmiş bir risk indeksinin geliştirilmesini amaçlamaktadır. Aslında çevresel güvenlik açığı, risk değerlendirmesinde nadiren dikkate alınmaktadır ve ARAMIS projesindeki bu bütünleştirme büyük bir ilgiyle birlikte yenilikçi bir yaklaşımı temsil etmektedir. Şekil 27, çevresel güvenlik açığının tanımlanması esnasında yönlendirilen sorunlu konuları daha iyi açıklamaktadır. Bu konular aşağıda belirtilen biçimde özetlenebilir: İnsan, çevre ve maddi unsur hedeflerinden oluşan Alan 1 ve daha fazla veya daha az güvenlik açığı olan ve yine insan, çevre ve maddi unsur hedeflerinden oluşan ancak miktar ve doğası açısından farklı olan Alan 2.



Şekil 27: Çevresel güvenlik açığı tanımlaması

Burada geliştirilen fikir, Seveso endüstri sahası çevresinde yerleşik bulunan tüm muhtemel hedeflerin güvenlik açığını belirleyecek ve karakterize edecek bir güvenlik açığı indeksi tanımlamaktır (güvenlik açığı haritalandırma). Bu öncelikle, çalışma alanının tesis edilmesini ve ilgili hedeflerinin belirlenmesini, ardından çalışma alanındaki hedeflerin tanımlanması ve ölçülmesini ve son olarak bunların güvenlik açığının değerlendirmesini gerektirecektir. Bu son adım spesifik bir metodoloji gerektirir. Bu çalışmada, güvenlik açığı için yarı-kantitatif bir yöntem benimsenmiştir. Bu yöntem uzman görüşlerine dayanan çok kriterli karar yöntemidir (SAATY Metodu). Bu yöntem, hem spesifik bir hedefin "durum"unun (kalitatif yaklaşım) hem de hedefin "sayısı"nın (kantitatif yaklaşım) dikkate alınmasına izin vermektedir.

7.2. GÜVENLİK AÇIĞININ TİPOLOJİSİ

Bu bölümün amacı; endüstriyel bir tesis nedeniyle oluşan bir kaza durumunda etkilenebilen endüstriyel sahanın çevresini tanımlamaktır. Bu nedenle, çevre hassasiyeti ile birlikte karakterize etmek için bir takım hedef tipleri kümesinin önerilmesi gerekmektedir. Bu yapılırken yöntemin transfer edilebilirliği ve bunun esnekliğinin öneminin unutulmaması gereklidir. Aslında dikkate alınacak hedef sayısı ile çok kriterli karar yöntemi sebebiyle oluşan sınırlamalar arasında uygun bir denge bulmak gereklidir.
Öncelikle hedefler üç kategoriye ayrılmakta ve sonrasında bu kategorilerden her biri hedef tipleri listesinde detaylandırılmaktadır:

- ✓ İnsan (H)
- Sahadaki personel (H1)
- Bölgesel nüfus (H2)
- Halka açık bir kuruluştaki nüfus (H3)
- İletişim yolu kullanıcıları (H4)

✓ Çevresel (E)
- Zirai alanlar (E1)
- Doğal alanlar (E2)
- Spesifik doğal alanlar (E3)
- Sulak alanlar ve su yapıları (E4)

✓ Maddi unsurlar(M)
- Sanayi siteleri (M1)
- Kamu hizmet kuruluşları ve altyapılar (M2)
- Özel yapılar (M3)
- Kamu yapıları (M4)

Bu hedeflerle ilgili maksimum bilgiye ulaşmak için iki veri tabanı kullanılmıştır.

Corine Land Cover (IFEN, 2002) veri tabanı, her Avrupa ülkesinde arazi kullanımı hakkında homojen coğrafik bilgi sağlamaktadır. Bu veri tabanının kapsadığı esas bilgi; topografik harita, bitki örtüsü ve orman tipi haritası ve son olarak da toprak ve ağ tanımlamasını içermektedir.

Bölge tanımlamasının beş ana tipi söz konusudur:
- Yapay bölge
- Zirai olarak kullanılan arazi
- Orman ve doğal alanlar
- Nemli alanlar
- Su alanları

Bu ilk beş alan tipi, doğal çevrenin karakterize edilmesi amacıyla kırk dört sınıfa ayrılmaktadır.

TeleAtlas veri tabanı, tüm Avrupa ülkelerinde ve ABD'de gerçekleştirilen bölgesel veri toplama çalışmalarından oluşmaktadır (TeleAtlas, 1996).

Bu çalışmaların içerdiği temalar:
- Yol ve sokak ana arterler
- Adres alanları
- İdari alanlar
- Posta bölgeleri
- Arazi kullanımı ve kapsamı
- Tren yolları
- Taşıma bağlantıları
- İlgi noktaları: yerleşim alanları
- Yerleşim merkezleri
- Su

Doğal çevrenin ve insan yapımı hedeflerin tanımlanması için bu iki veri tabanı amaçlarımızın çoğunu yerine getirmektedir. İnsan hedefleri ile ilgili olarak, her bir ülkeden sağlanan spesifik veriler kullanılmalıdır. Nüfusla ilgili bilgi, 1999 yılında bölge bazında Fransa nüfusunun statüsünü içeren INSEE tarafından sağlanan verilerden elde edilecektir (INSEE, 1999). İtalya'da, ISTAT (Ulusal İstatistik Enstitüsü) 1991'de, sonrasında da 2001'de bölge veya nüfus sayımı birimi tarafından yapılan İtalyan nüfus sayımına dayalı bu tip verileri sağlamaktadır.

Bu nüfus verilerinin kullanılabilmesi için, çevresel hedeflerin sayısal hale dönüştürülmesi ile ilgili olan paragrafta ele alındığı gibi, her bir küçük kareye karşılık gelen bir nüfus sayısının atandığının varsayılması gereklidir. Eğer çok hassas sonuçlara ulaşılması gerekliyse, kadastroyla ilgili bilgilerin de dikkate alınması gereklidir. Bu ikinci yaklaşım için ilkine göre daha fazla zaman gereklidir.

Parklar veya koruma altındaki alanlar gibi bazı önemli çevresel özelliklerle ilgili diğer spesifik bilgilerin, İtalya'da APAT veya Fransa'da ZNIEFF gibi fauna ve floranın doğal bölgesi(zone) ile ilgili ulusal çevre kuruluşlarından elde edilebileceğini de belirtmek gerekir.

Son olarak; endüstriyel saha ile ilgili olanlar gibi bazı diğer bilgiler de, kamusal olarak sağlanamadığı için, doğrudan kullanıcısından sağlanmalıdır. Nüfusun yoğunlaştığı alanlar, yaşamla ilgili altyapılar, anıtlar ve benzerleri gibi özel hedeflerle ilgili bilgilerin eklenmesi için de kullanılabilen verilerin karşılanması amacıyla spesifik bir prosedür önerilmektedir.

7.3 GÜVENLİK AÇIĞI YÖNTEMİ VE HEDEF GÜVENLİK AÇIĞININ ÖNCELİKLENDİRİLMESİ

Amaç, çevresel güvenlik açığını sayısal olarak değerlendirmektir. Bu amaçla, aşağıda belirtilen dört ana adıma dayalı olarak uzman görüşlerini ve ikili karşılaştırmaları kullanarak sıralama yapan SAATY Çok Kriterli Karar Yöntemi uygulanmaktadır:

- Amacın tanımlanması
- Çevrenin belirlenmesi
- Probleme cevap vermek için bilginin organizasyonu
- Uzman görüşlerine dayalı güvenlik açığı faktörlerinin kantitatif değerlendirmesi

Bu düşünceyle, çevre, üç tipoloji aracılığıyla tanımlanmaktadır:

- Hedef kategorilerinin tanımlanması: insan, çevre ve maddi unsur. Her bir hedef kategorisi dört tipte alt hedef kategorisine bölümlenmektedir. İnsan hedefleri için: sahadaki personel, bölgesel nüfus, halk tarafından ziyaret edilen kuruluşlardaki nüfus ve iletişim yollarını kullananlar. Çevresel hedefler için: zirai alanlar, doğal alanlar, spesifik doğal alanlar, sulak alanlar ve su yapıları. Maddi unsur hedefleri için: endüstriyel sahalar, kamu hizmet kuruluşları ve alt yapılar, özel yapılar ve kamu yapıları.
- Fiziksel etkilerin tanımlanması: yüksek basınç, termal radyasyon, gaz toksisitesi ve sıvı kirliliği.
- Etkilerin tanımlanması: bütünlük, ekonomik ve psikolojik etkiler.

Bilgi, aşağıda belirtilen güvenlik açığı tanımlarının benimsenmesi yoluyla ve çalışma amacı doğrultusunda yapılandırılmaktadır:

- Hedef sınıfı ve getirdiği fiziksel etki için; her bir hedef tipinin diğerleri ile ilgili olarak güvenlik açığı, ikili karşılaştırmalar yoluyla değerlendirilmekte olup, her bir fiziksel etki için her bir hedef sınıfının güvenlik açığı elde edilmektedir.
- Hedef sınıfı için; diğerleri ile ilgili olarak her bir fiziksel etkinin önemi, ikili karşılaştırmalar ile değerlendirilmekte olup, hedef sınıflarının her birinin tüm güvenlik açığı elde edilmektedir.
- Son olarak, hedeflerin her bir sınıfının güvenlik açığı diğerleri ile karşılaştırılarak, toplam güvenlik açığı elde edilmektedir.

Bu yaklaşımdan yola çıkarak, güvenlik açığı indeksini oluşturacak güvenlik açığı faktörleri (52 adet fonksiyon tanımlamıştır) ve hedeflerin sayısallaştırılmış faktörlerinin bir araya getirilmesi yoluyla,

matrisler ve fonksiyonlar türetilmektedir. Bu matrisler ve fonksiyonlar, her bir güvenlik açığı fonksiyonunun güvenlik açığı faktörlerinin saptanması için uzman görüşlerinin oluşmasını mümkün kılmaktadır. Bu amaçla, çeşitli uzmanlık alanlarına (risk analisti, yetkili kuruluşlar, sanayiciler) sahip ve çeşitli ülkelerden gelen 38 uzmana ayrı ayrı danışılmıştır. Uzman görüşlerine göre doldurulan anketlerin işlenmesinden sonra, 52 adet fonksiyonun güvenlik açığı faktörleri, matrislerin özgün vektörlerinden hesaplanmıştır. Örneğin, çalışma alanının toplam güvenlik açığı (Vglobal), insan, doğal çevre ve maddi unsur güvenlik açığı (VH, VE ve VM)'nın aşağıda belirtilen kombinasyonundan oluşmaktadır:

$$V_{global} = 0.752 \text{ x } VH + 0.197 \text{ x } VE + 0.051 \text{ x } VM \quad (1)$$

Burada, hedeflerin her bir sınıfının güvenlik açığı, fiziksel etkinin kendi güvenlik açığına bağlıdır (yüksek basınç= op, termal radyasyon =tr, toksisite= tox, kirlenme= poll).

$$V_H = 0.242 \text{ x } V_H^{op} + 0.225 \text{ x } V_H^{tr} + 0.466 \text{ x } V_H^{tox} + 0.067 \text{ x } V_H^{poll} \quad (2)$$

$$V_E = 0.071 \text{ x } V_E^{op} + 0.148 \text{ x } V_E^{tr} \; 0.277 \text{ x } V_E^{tox} + 0.503 \text{ x } V_E^{poll} \quad (3)$$

$$V_M = 0.446 \text{ x } V_M^{op} + 0.410 \text{ x } V_M^{tr} + 0.069 \text{ x } V_M^{tox} + 0.075 \text{ x } V_M^{poll} \quad (4)$$

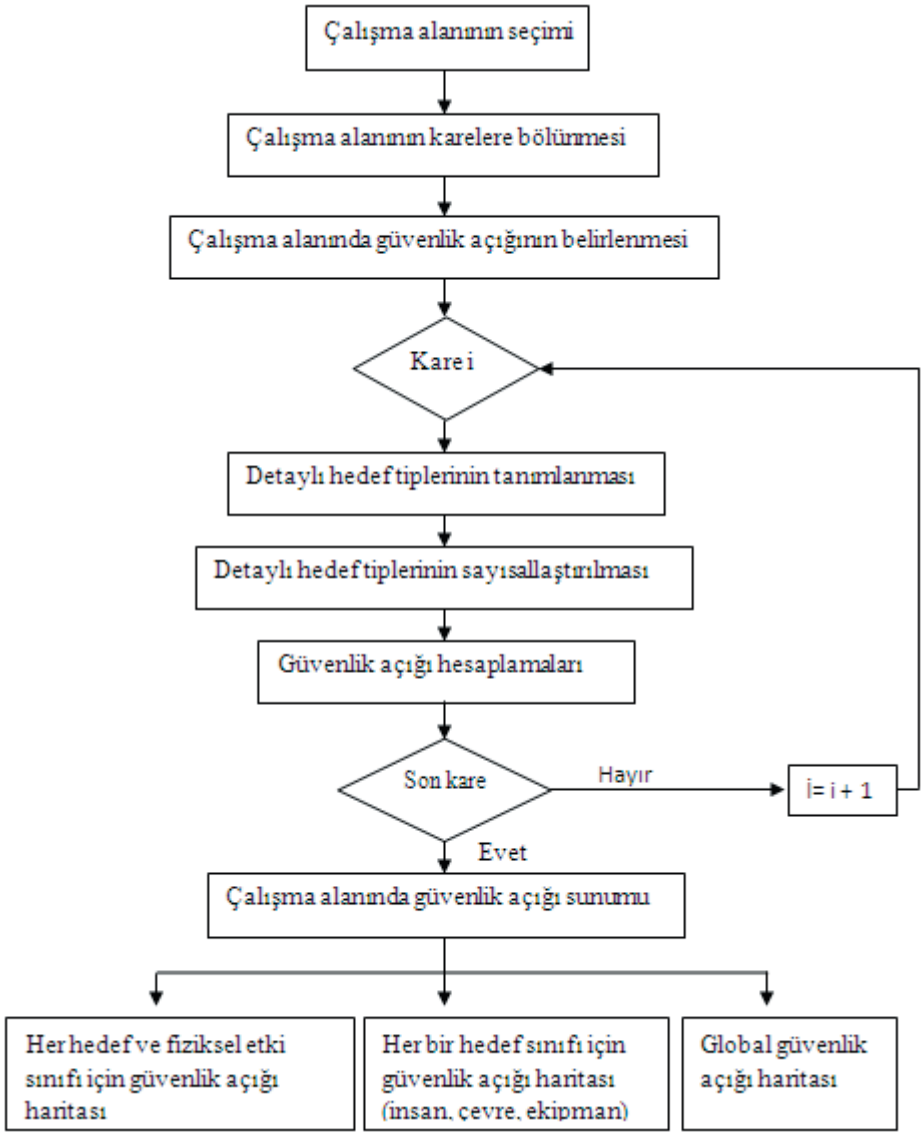
Bu metodolojinin uygulanması ve alan güvenlik açığının değerlendirilmesi için; ilk adım, çalışma alanının özelliklerinin belirlenmesinden oluşmaktadır; bunun ölçülerinin endüstriyel saha için kurgulanan, beklenen kaza senaryolarının etkilerini kapsamaya yetecek kadar geniş olması ve güvenlik açığı haritalandırması açısından küçük karelere ayrılmış olması gereklidir. 20 km x 20 km'lik çalışma alanının, 500 m x 500 m veya daha az ölçülerde küçük karelere bölünmesi önerilmektedir. Burada, bu bölgenin(zone) güvenlik açığının daha iyi görüntülenebilmesi maksadıyla, endüstriyel sahanın yakınında, küçük kare ölçüleri, azaltılabilir. Sonrasında, güvenlik açığı fonksiyonuna dâhil edilecek her bir hedef tipi faktörünün sayısallaştırılmasını belirlemek üzere; muhtemelen kullanıcı bilgileriyle tamamlanmış uygun ticari veri tabanlarından, bu alanlardaki çeşitli hedefler hakkında bilgi elde edilmesi gereklidir. Bu, çalışma alanındaki her bir küçük karede, hedef kategorisinin ve tipinin sayımının yapılmasını gerektirir. Özellikle, sayısallaştırma faktörü, "0-1" aralığında bir değer olduğu kabul edilen boyutsuz bir değişkendir. Burada;"0" inceleme altındaki alanda hedefin olmadığına işaret eder. "1" ise alandaki bu hedefin miktarının beklenen maksimum değerine ulaştığını göstermektedir. Güvenlik açığı fonksiyonlarının tümü, çoğaltılabilir doküman D.4.A'da belirtilmektedir.

7.4. GÜVENLİK AÇIĞI HARİTALANDIRMA

Yukarıda tanımlanan yaklaşım, uygun şekilde bir GIS aracı olarak geliştirilmiştir. İlgili bölgedeki (zone) güvenlik açığını değerlendirmek amacıyla; aşağıda belirtilen adımların gerçekleştirilmesi gereklidir (bkz. şekil 28):

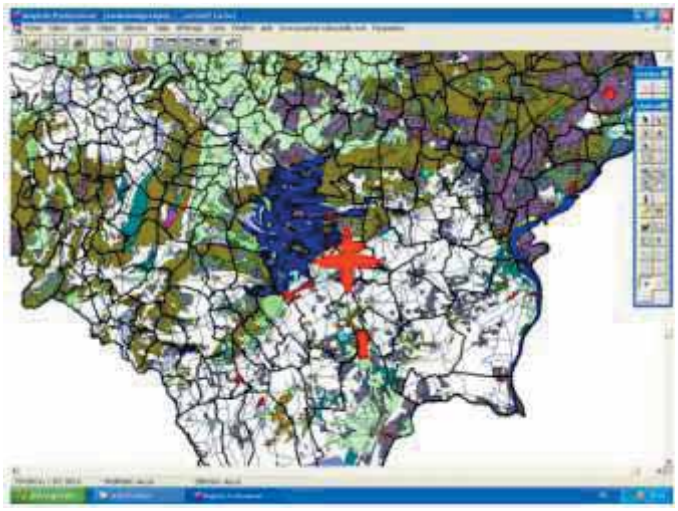
- Çalışma alanı seçilir ve küçük karelere bölünür;
- Küçük karelere dahil edilen insan, çevre ve maddi unsur kategorilerinin detaylı hedef tiplerinin belirlenmesi ve sayısal hale dönüştürülmesi yoluyla her bir küçük karenin güvenlik açığı değerlendirilir;
- Küçük karelerin güvenlik açığı indeksleri hesaplanır.
- Sonuçlar haritalandırılır.

Bu adımlar, araştırılan alanın her bir küçük karesi için tekrarlanmalıdır.

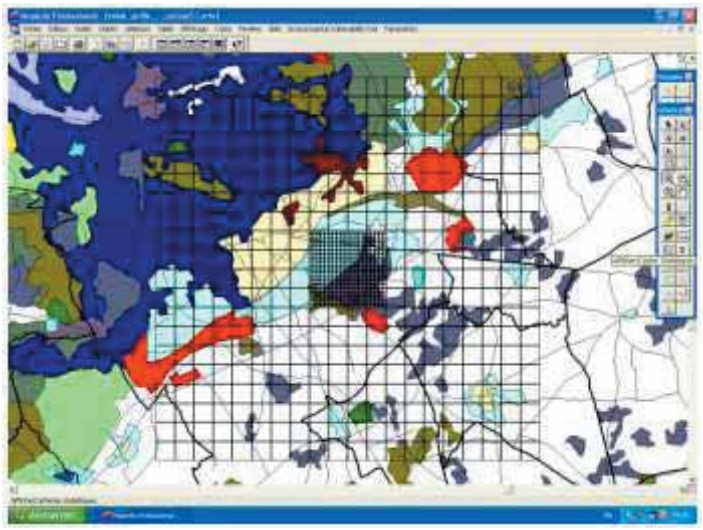


Şekil 28: Güvenlik açığı haritalandırma için GIS aracının yapısı

Çalışma alanı, endüstriyel sahada küçük kare merkezli olacaktır (Şekil 29 ve Şekil 30). Çeşitli hedef tipleri ve yerleşimi ile ilgili gerekli bilgi; arazi kullanımı, ulaşım ağı ve ilgi noktası da dahil olmak üzere oldukça kolay erişilebilen ticari veri tabanlarından (Corine Land Cover, 2002, TeleAtlas, 1996, vs.) ve ikamet eden nüfusun sayım datalarından (Fransa'da INSEE'den ulaşılabilir, 1999) oldukça kolay bir şekilde sağlanabilmektedir. Doğal çevreyle ilgili diğer faydalı bilgiler, çevreyle ilgili kuruluşlardan elde edilebilmektedir. Kendi sınırları veya özel hedeflerin kesin konumu (örneğin; sanayi sitelerindeki ofis binaları) gibi endüstriyel saha ile ilgili olan ancak ticari veri tabanlarına dâhil edilmemiş bilgiler, kullanıcıları tarafından kolaylıkla verilebilir.



Şekil 29: Endüstriyel sahanın haritada yerini belirleme



Şekil 30: 10 kmx10 km çalışma alanı (küçük kare 500 m);
iç taraftaki ızgara 2 km x 2 km (küçük kare 100 m)

GIS aracı, herhangi bir GIS yazılımı (MapInfo, 2002; ArcView, 2000 vs.) ile kolaylıkla geliştirilebilir. Burada gösterilen örnekler, MapInfo'dan elde edilmiştir, ancak ArcView aracı da kullanılabilir. Her iki durumda da araçlar; kullanıcıya, çalışma alanının seçimini, bu alanın küçük karelere bölünmesini ve her bir küçük karenin içerisine hedeflerin farklı tiplerinin tanımlanmasını ve sayısallaştırılmasını yapma imkânını vermektedir. Sayısallaştırma adımı; inceleme altındaki alan için bu tipin her bir hedefi tarafından kapsanan alanın oranına dayalı olarak doğal ve yerleşim alanlarına ait hedefler için, tamamen otomatik hale getirilmiştir. İnsan hedefleri için aynı prosedür benimsenemez. Buralarda sayısallaştırma faktörlerinin, alanda beklenen maksimum kişi sayısına dayalı olarak belirlenmesi gerekmektedir (Detaylar için bakınız: Tixier ve diğerleri, 2003). Sayısal faktörlerin elde edilmesi için, kullanıcı tarafından uyarlanabilen uygun hazır değerler önerilmektedir.

7.5. ÖRNEK

Güvenlik açığının değerlendirmesinin önemine vurgu yapılması ve doğrulamasının yapılması amacıyla, metodoloji birkaç test vakasında uygulanmıştır.

Bu bölümün sonraki kısmında, hem ARAMIS projesine ait Fransız test vakasının çevresi, hem de buradan çıkarılan güvenlik açığı haritası sunulmaktadır.

Fransız test alanı, Fransa Haute-Normandie bölgesinde bulunmaktadır.

7.5.1. Fransız test sahasının çevresinin tanımlanması

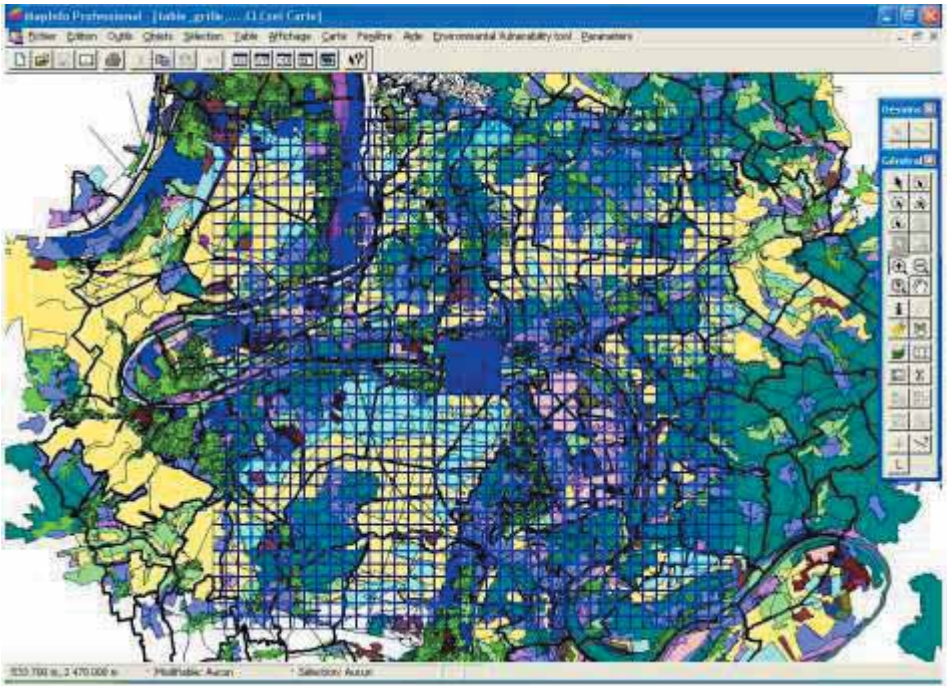
Çalışma alanı (Şekil 31) iki grid (ızgara)'ten oluşmaktadır:

- Ana grid: 500 m x 500 m küçük karelere bölünmüş 20 km x 20 km'lik bir karedir.
- İç grid: 50 m x 50 m küçük karelere bölünmüş 2 km x 2 km'lik bir karedir.

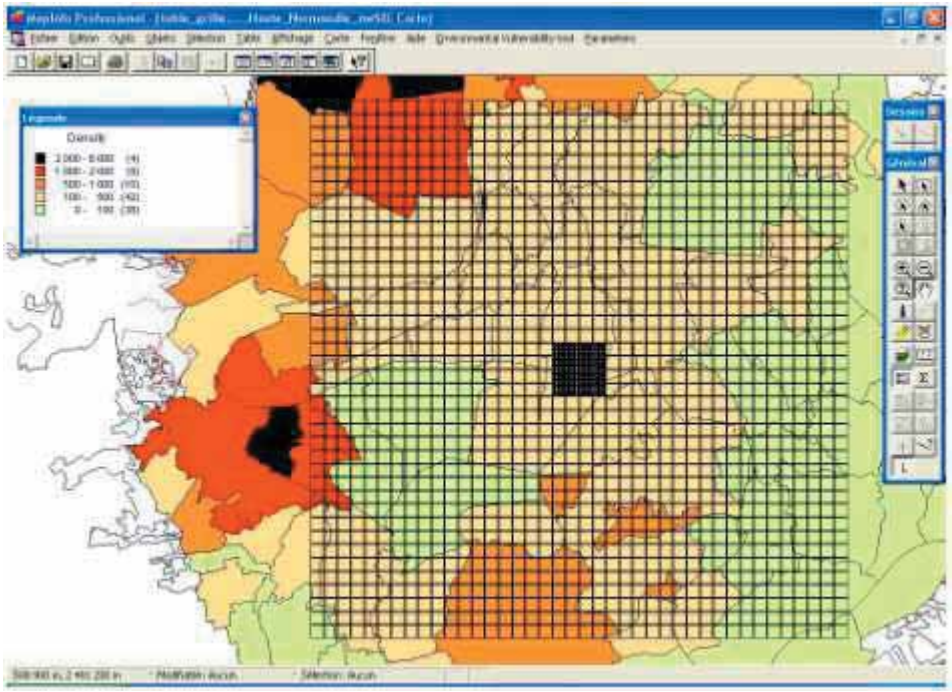
İç grid, endüstriyel sahaya yakın yerde çok daha hassas bir güvenlik açığının belirlenmesini olanaklı kılmaktadır.

Bu çevre, Şekil 32 ve Şekil 33'de detayları belirtilen çeşitli sınırlar içermektedir.

Beşeri alan sınırları (Şekil 32), esas olarak çok düşük ve düşük yoğunluklu (her bir km2 başına 0 ila 1000 kişi arasında değişen) bölgelerden oluşmaktadır. Çalışma alanının yalnızca % 20'si orta yoğunluklu bölge (her bir km^2 başına 1000 ila 2000 kişi arasında) olarak temsil edilmektedir.

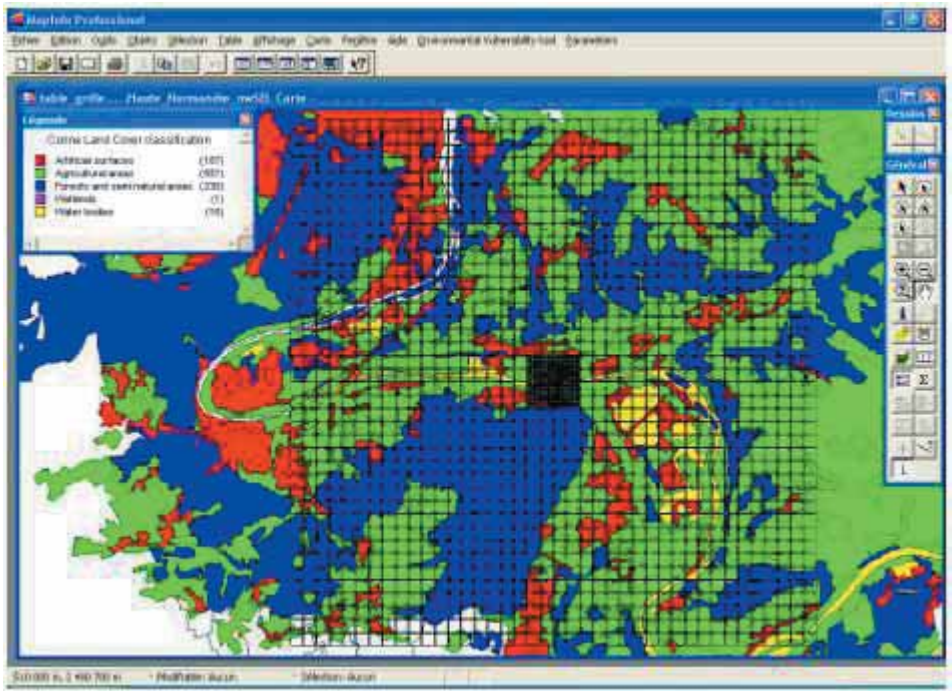


Şekil 31: Fransız test sahasının çalışma sahası



Şekil 32: Çalışma alanının insan bölgeleri

Doğal bölgeler ve maddi unsur bölgeleri (zone), esas olarak zirai alanlar, orman alanları ve yarı doğal alanlardan oluşmaktadır (Şekil 33). Çalışma alanının diğer kısmı, suni alanlar, sulak alanlar ve su yapıları olarak karakterize edilmektedir.



Şekil 33: Çalışma alanının doğal ve maddi bölgeleri

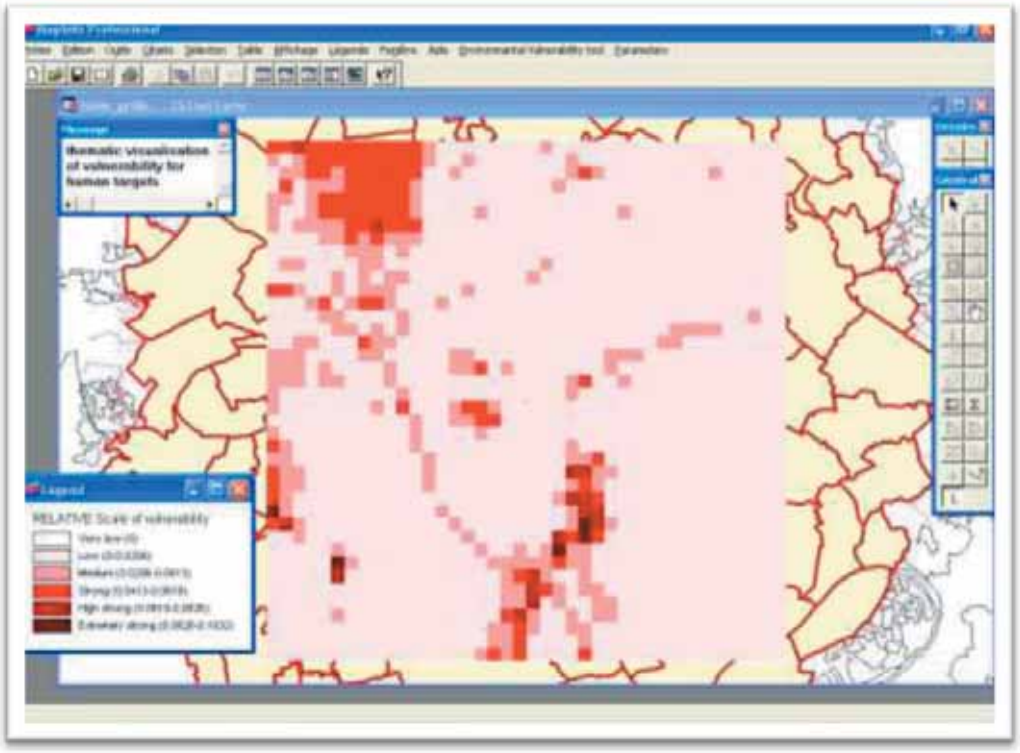
Bu analizden yola çıkılarak, genelde, tüm alanın güvenlik açığının düşük veya orta düzeyde olduğu söylenebilir.

Ancak aşağıda belirtilen güvenlik açığı haritaları, bunun kesin bir değeri ile birlikte hassas noktaların konumunu da göstermektedir.

Güvenlik açığı sonuçlarının sunumu ve analizi

Bu bölümde; iki farklı güvenlik açığı harita kümesi sunulmakta ve yorumlanmaktadır. Bunlar:

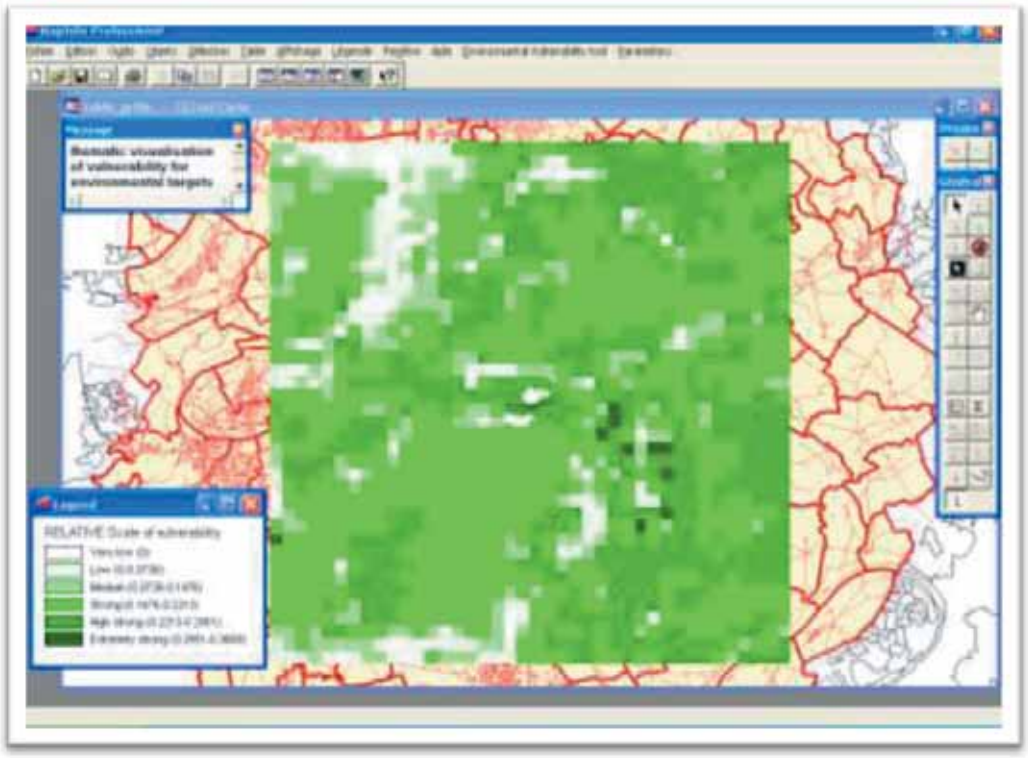
- Hedeflerin her bir tipi (insan, çevre ve maddi unsur) için bir grup güvenlik açığı haritası ve toplam güvenlik açığı haritası kümesi
- Her bir fiziksel etki (yüksek basınç, termal radyasyon, toksisite ve kirlenme) için güvenlik açığı haritası kümesi



Şekil 34: Beşeri unsurların tehlikeye maruziyet haritası

Çalışma alanının büyük kısmında insanların tehlikeye maruz kalma riski düşüktür. Aslında insanların tehlikeye maruz kalma riski büyük ölçüde, nüfus yoğunluğu ve kentsel ya da yarı-kentsel alanlarla (yapay alanlar) bağlantılıdır. Çalışma alanındaki nüfus yoğunluğunun düşük olmasından dolayı, yapay alanların bazı kısımları küçük bir tehlikeye maruz kalma riski taşımaktadır.

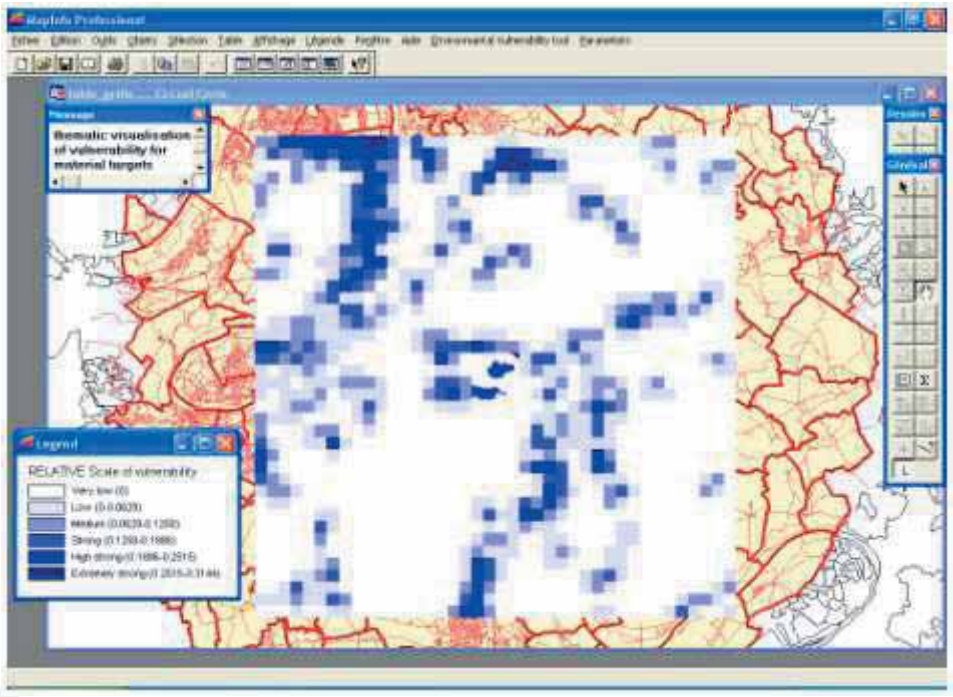
İç bölgeler yaklaşık olarak 600 işçinin çalıştığı sanayi bölgesi için çok düşük tehlikeye maruz kalma riski ile karakterize edilmiştir.



Şekil 35: Çevresel unsurların tehlikeye maruziyet haritası

Çalışma alanının büyük bir kısmı orta seviyede tehlikeye maruz kalma riski ile karakterize edilmiştir.

Sadece yapay alanlara karşılık gelen kısmın tehlikeye maruz kalma risk değeri düşüktür. İç bölgede su birikintilerinin varlığı çevrenin tehlikeye maruz kalma riskini yükseltmektedir.



Şekil 36: Maddi unsurların tehlikeye maruziyet haritası

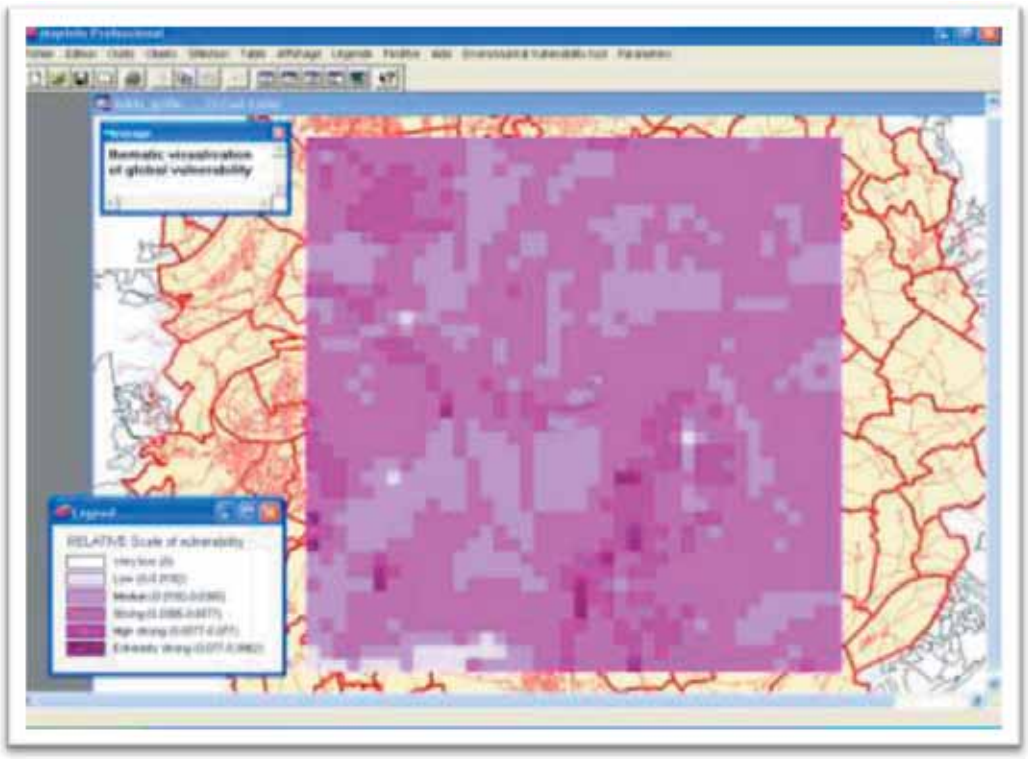
Maddi unsurların tehlikeye maruz kalma riskini gösteren haritada, büyük ölçüde çalışma alanındaki yapay alanların konumundan dolayı orta seviyede tehlikeye maruz kalma riski olan bazı spesifik alanlara dikkat çekilmektedir. İç bölgede sanayi bölgesine yakın, tehlikeye maruz kalma riski yüksek olan iki alan bulunmaktadır.

Yukarıda bahsedilen üç harita karşılaştırıldığında, en korunmasız alanların haritadaki konumlarının, beşeri ve maddi unsur hedefleri için çok benzer olduğu görülmektedir. Ayrıca, çevresel tehlike haritasındaki tehlikeye maruz kalma riski en yüksek olan alanlar, insan ve maddi unsur tehlike haritalarında belirtilen yüksek maruziyet riski olan alanlarla karşıtlık oluşturmaktadır.

Şimdiye kadar gösterilen üç tehlike maruziyet haritası (beşeri, çevresel ve maddi unsur), kullanılarak genel tehlike maruziyet haritası oluşturulabilir.

Bu çalışma alanı için genel tehlike maruziyet riski düşüktür. Bu harita yüksek tehlikeye maruziyet riski olan alanlar da dâhil olmak üzere, genel maruziyet riskinin %75'ini oluşturan beşeri tehlike maruziyet haritasıyla açıkça bağlantılıdır.

Fiziksel etkilerin maruziyet risk değerleri yüksek basınç ve termal radyasyon için düşük, toksisite ve kirlilik etkileri için orta seviyededir. Yüksek basınç, termal radyasyon ve toksisite için hazırlanan tehlike maruziyet haritalarında belirtilen, tehlikeye maruz kalma riski en yüksek yerlerin konumları beşeri unsurların tehlikeye maruziyet riskiyle ilişkilidir. Kirlilik etkisi için ise, tehlikeye maruziyet risk alanları doğal çevreyle bağlantılıdır.



Şekil 37: Genel tehlike maruziyet haritası

7.6. DEĞERLENDİRME

Her bir küçük kare için, ayırt edici renkle gösterilen tehlike maruziyet risk sınıfının hesaplanmış değerlerinin birleştirilmesiyle önceki aşamalarda elde edilen tehlike maruziyet değerleri haritada gösterilebilir.

Burada üç tehlike maruziyet haritası elde edilebilir:

- Çalışma alanındaki genel tehlikeye maruziyet haritası,
- Tüm fiziksel etkiler için bir hedef (beşeri, çevresel ve maddi) sınıfının tehlikeye maruziyet haritası,
- Belirli bir fiziksel etki (yüksek basınç, termal radyasyon, toksisite ve kirlilik) için bütün hedeflerin tehlikeye maruziyet haritası.

Her bir fiziksel etki ile ilgili tehlike maruziyet harita katmanları bunlara karşılık gelen maruziyetin şiddet haritalarıyla karşılaştırılmalıdır. Bu her iki harita, sanayi bölgesini çevreleyen alandaki son durumu gösteren çizimle beraber son kullanıcılara(tesis yöneticileri, risk analizi yapan uzmanlar ve/veya yetkili kurum ve kuruluşlar) verilmelidir.

Bu bilgi yalnızca güvenlik seviyesinin onaylanması için belirli bir sanayi bölgesinin içerdiği riskle ilgili olarak dikkate alınacak hususların kağıt üzerinde gösterilmesini sağlamakla kalmayacaktır. Ayrıca tehlikeye maruziyet durumları ya da maruziyetin şiddeti, alanın tehlike durumunu ortaya koyacaktır. Bu nedenle, çıkacak sonuçlara göre sanayi bölgesinin güvenlik seviyesini yükseltmek özel çaba gerektirir.

Gelecekte, birtakım bölgeler arasındaki tehlikeye maruziyetlerin karşılaştırılmasını sağlamak için haritalar, uygun renkler ve normalleştirilmiş bir ölçek ile geliştirilebilir.

8. DİĞER UYGULAMALAR VE ARAŞTIRMA SAHALARI İÇİN ARAMIS'İN KULANIMI

8.1. PAPYON MODELLERİNİN VE SENARYOLARIN GELİŞTİRİLMESİ

Genel hatalar; olay ağacı, güvenlik işlevleri ve bariyerlerin birleşik listeleri gibi araçların sağlanması yanında, MIMAH ve MIRAS risk analizleri için yöntemsel ve kavramsal bir çerçeve de sunar. Bu belgede kısaca bahsedilen elemanlar genelleştirilmiş papyon, güvenlik işlevleri ve bariyerler; tüm proje ortaklarının ve kontrol takımının hali hazırda kullandığı kesin olan tanımlamaları verir. Bunlar, maruziyetin şiddetinin hesaplanması ya da yönetim verimliliğinin değerlendirilmesi gibi metodolojinin diğer temel parçalarının geliştirilmesi için kullanılır.

Paralel olarak, olasılıklar (frekanslar/başlatan olayların olasılıkları, kritik olayların sıklığı, geçiş olasılıkları) hata ve olay ağacının tüm dalları boyunca incelenmiştir. Birtakım sonuçlar bulunmuş olsa bile, ARAMIS'in bu bölümü şunu göstermektedir: Bir taraftan güvenilir verilerin olmaması ve diğer taraftan eldeki veriler ile genelleştirilmiş ağaçlar arasındaki eşleşme başlıca bir zorluktur. Tasarlanmış bir "Avrupa Veri Toplama Programı" ARAMIS'in gelişmesine gerçekten katkıda bulunabilir.

Bununla beraber ARAMIS'in ortaya koyduğu diğer bir şey; Avrupa Birliği'ndeki farklı ülkelerde risk kabul kriterlerinin uyumlaştırma ihtiyacı olduğudur. Risklerin kabul edilebilirliği için değişik yaklaşımların uyumlaştırılması amacıyla birtakım bilimsel kriterler belirlenmelidir.

JRC-MAHB'nin koordinatörlüğünde Arazi Kullanım Planlanması temelinde Avrupa Çalışma Grubunda yapılacak çalışmalarda bu konuda gelişme sağlanması mümkün olacaktır.

Papyon yaklaşımı "güvenlik bariyerleri ve güvenlik fonksiyonları" konsepti ile birlikte iş güvenliği, tehlikeli maddeler ya da taşıma güvenliği gibi alanlarda gelecekte kullanılması muhtemel uygulamaların elde edilebilmesine katkıda bulunabilir.

8.2. BARİYER PERFORMANSININ DEĞERLENDİRİLMESİ

Sanayide kaza senaryolarının tanımlanması risk değerlendirmesinin kilit noktasıdır. Ancak, özellikle deterministik bir yaklaşım içinde, çoğunlukla uygulanmış güvenlik politikaları ve kullanılmış güvenlik cihazları dikkate alınmadan, genellikle en kötü senaryolar göz önünde bulundurulur. ARAMIS'in önemli bir özelliği, kaza senaryolarının tanımlanmasında güvenlik yönetimi ve güvenlik sistemlerinin etkisine odaklanmasıdır. Bu yaklaşım risk seviyesi tayininin kesin bir şekilde yapılmasını amaçlamaktadır.

Referans Kaza Senaryolarının tanımlanması için, sahada var olan güvenlik yönetimi ve güvenlik sistemlerinin göz önünde bulundurulması ve sanayi sektörünün mevcut çabaları, güvenlik sistemlerine ilave yatırımların yapılmasını sağlayacaktır.

Bu yaklaşım, çoğunlukla güvenlik sistemlerinin performanslarının ölçülmesine dayanır. Ancak, IEC 61508 ve 61511 standartları; emniyet donanımlı sistemin güvenilirlik seviyesini değerlendirmek için kriterleri belirlemiş olsa bile, bir alt sistem için hata kabul edilebilirliği ve güvenli hata oranı gibi

parametreleri belirlemek zordur. Bu parametreleri belirlemek için ekipmanla ilgili elle tutulur veriler ya da yöntemlerin oluşturulması ve kullanıma sunulması gerekmektedir.

Bununla birlikte, birtakım etkin güvenlik bariyerleri tam otomatik değildir ve kişilerin bizzat müdahale ve teşhisine ihtiyaç duymaktadır. Bu bariyerlerin performansının ölçülmesinde insan faktörünü dahil etmek için, açık bir kritere gereksinim duyulmaktadır.

8.3. GÜVENLİK YÖNETİM YAPISI VE KÜLTÜRÜNÜN ÖLÇÜLMESİ

8.3.1. Genel

Vaka çalışmalarından edinilen tecrübeler, gözden geçirme panellerinden elde edilen geri bildirimler ile ARAMIS metodolojisinin güvenlik yönetimi yapısının ve kültürünün ölçülmesindeki başarısı, denetimlerden alınan kalitatif geri bildirimler, şirket içi zayıf noktalara odaklı güvenlik kültürü araştırması ile yönetimde mümkün olan iyileştirmelere dayanmaktadır.

Prosesin şeffaf olmasına ve alana özel şartlardaki belirli güvenlik bariyerleri ile ilişkili güvenlik yönetim meselelerine öncelik vermeye yardım etmesine rağmen, kantitatif hale getirme süreci hala pek çok belirsizlik içermektedir. Güvenlik yönetimini tanımlama ve oluşturma bağlamında, güvenlik yönetiminin temel, önemli, dikey etkenleri ve işlevleri hala tam olarak kurulmamıştır. ARAMIS uzun süreli araştırmalar sonucunda ulaşılan tek başarıdır. Ancak, bilinen güvenlik yönetiminin yapısal etkenleri ve güvenlik kültürü birikimi olan ARAMIS ilerleyen zamanlarda değişime uğrayacak ve bilimsel bilgimiz arttıkça daha da belirginleşecektir. ARAMIS yöntemi güvenlik yönetimi etkinliğini değerlendiren, gelecek vaat eden bir yönteme dikkat çekmektedir:

- Yorucu olmayan, bir miktar çabayla değerlendirmenin yapılabileceği bilinmektedir,
- Somut güvenlik bariyerleri ve güvenlik yönetim etkinlikleri arasındaki ilişkiye odaklanma ile şirketlerin kolaylıkla anlayabileceği ve onların gelişim süreçleri için elle tutulur, faydalı prosesler ve somut etkinlikler haline gelecektir.

8.3.2. Güvenlik Yönetim Denetimi

ARAMIS denetim projesinin genel sonucu "araçların" önemli bir potansiyelinin olmasıdır. Belirli senaryo ve bariyerler üzerine odaklanma düşüncesi, yönetim etkilerinin değerlendirilmesi, şirketlerin değerlendirme araçlarına yardımcı olarak şirketten ek bir genel destek almalıdır. Ancak, hala bu araçları netleştirmek ve kullanıcı dostu haline getirmek büyük çaba gerektirir.

8.3.3. Güvenlik Kültürü Anketi

Anket, bir şirketin veya bölgenin güvenlik seviyesiyle ilgili kesin teşhis değerlerine haiz birkaç sonuçtan oluşan kanıtları veren ve benzer kritik güvenlikli tanımlanmış alanlarda yapılan önceki çalışmalar yoluyla geliştirilmiştir. Şimdiye kadar bu araçlar genel olarak bir karşılaştırma yoluyla kalitatif araçlar olarak da kullanılmıştır. ARAMIS kapsamında mutlak bir referans noktası verilmelidir. Böyle bir referans noktası için daha fazla araştırmanın kapsamlı bir temel oluşturularak yapılması gerekmektedir. Bu nedenle veri bankasını genişletmek ve hem gerçek güvenlik performansının (kazalar ve olaylar) hem de güvenlik yönetim denetiminin sonuçlarına ışık tutan bir veri haznesinin geliştirilmesi amaçlanmıştır.

8.3.4. Verimliliğin Kantitatif Hale Getirilmesi

Başlatıcı olayların gerçekleşmesi ya da bariyerlerin güvenirliliğine ilişkin güvenlik yönetimi etkenlerinin göreceli önemiyle ilgili objektif deneysel bilgi bulunmamaktadır. Şimdiye kadar bu türdeki bilgiler uzman görüşlerinin paylaşılmasından elde edilmiştir. Buna karşın, sanayi güvenliğinde uzman kişilerin bildiği önemli bilgilerin bazı bağımsız veri kaynaklarıyla desteklenemeyen kendini doğrulayan bir eğilimi de vardır.

Prensip olarak, kaza analizleri ve olaylardan faydalı deneysel bilgiler toplamak mümkündür, ancak bu olay verilerine katkıda bulunan tesislerdeki (denetim ve anket kullanımı) gerçek güvenlik yönetim performans araştırmaları ile bu bilgilerin tamamlanması gerekmektedir. Bu bize, Bayes'in koşullu olasılık teoremi kullanılarak belirli yönetim faktörlerinin yetersizlik koşulu altındaki hata sıklığı ile yetersizlik koşulu olmaksızın elde edilen hata sıklığı arasındaki oran, aranan etki faktörünü ifade eder.

Bu tür birleştirilmiş olay/kaza analizleri, istatistikî olaylar ve güvenlik yönetim araştırmaları kullanılarak hem olay/kaza analizleri hem de güvenlik yönetim araştırmaları için kullanılması planlanan yönetim faktörlerinin tutarlı bir şekilde sınıflandırılmasına ihtiyaç duyulmaktadır.

8.4. BİR TESİSİN RİSK ŞİDDETİ VE ETRAFININ TEHLİKEYE AÇIKLIK DURUMLARININ HARİTALANDIRILMASI

Risk şiddetleri ve tehlikeye maruziyet değerlendirilmesi için pek çok ilerleme, gelişme hali hazırda mevcuttur. Bunlar kullanıcı rehberinde karşılık gelen kısımlarda irdelenmiştir. Ancak muhtemelen en önemli şey, arazi kullanımı planlamasının kararlaştırılması sürecinde bu sonuçları kullanabilmektir. Tehlikenin şiddeti ve tehlike maruziyet haritalarının çakışması, tesisin/organizasyonun modifiye edilerek tehlikenin şiddetinin azaltılması veya hedeflerin uzaklaştırılması, yapıların güçlendirilmesi gibi önlemlerle tehlike maruziyetinin azaltılması için karar almayı mümkün kılar.

Bu kuralların oluşturulması sadece bilimsel bir mesele değildir. Bunun arazi kullanım planlaması politikaları göz önünde bulundurularak yapılması gerekir. Ancak kurallar belirlenir belirlenmez, bunların uygulanması ARAMIS'in araçlarında, maruziyet şiddetinin eşik değerinin belirlenmesi ya da tehlikeye maruziyetin değerlendirmesinin netleştirilmesi gibi birtakım uyum çalışmalarını gerektirebilir. Bunlar son kullanıcıların ihtiyaçları doğrultusunda daha kolaylaşacaktır. Son kullanıcılar ARAMIS gibi bir yöntemin kullanımı ile kendi bilgi ve donanımlarını güncel tutabilirler. Uzun vadede elde edilen sonuçlar arazi kullanım planlama sonuçlarının bir küresel gelişimi olacaktır.

SONUÇ: ARAMIS PROJESİNİN SEVESO DİREKTİFİNE KATKISI

ARAMIS Projesi, Avrupa Araştırma Alanında bilgi birikiminin ilerlemesini desteklemekte, bilim adamları ile endüstri diyalogunu teşvik etmekte ve tehlikeli tesisler ile ilgili karar verme prosesini uyumlu hale getirmektedir.

ARAMIS metodu, risk uzmanları tarafından tavsiye edilen ve uyumlu hale getirilmiş bir araç olarak doğrudan önerilmekte ve AB'de risk karar vericileri tarafından geçerliliği olan bir metot olarak kabul edilmektedir.
Avrupa'da risk değerlendirmelerinin uyumlaştırılması projesi olarak adlandırabileceğimiz ARAMIS Projesi, SEVESO II direktifinin uygulanması, büyük kazaların önlenmesi hususunda Avrupa Komisyonunun çalışmalarına önemli ölçüde katkıda bulunmuştur. Uyumlaştırılmış bir risk değerlendirme metodolojisi olarak ARAMIS, yetkili kuruluşlar ve sanayi açısından önemli bir ilgi kaynağı olarak aşağıdaki hususlar için kılavuz niteliğindedir:

- Endüstri bölgelerinde, olasılığa dayanan ve belirleyici olan yaklaşımların güçlü taraflarını birleştirerek, bir risk değerlendirme ve karşılaştırma aracı oluşturmuştur,
- Prosedür, güvenlik yönetim sistemi çerçevesinde ilerleme planlarına olanak sağlayacaktır,
- Koruyucu önlemler ve gerçekçi verilerle, senaryo seçimlerinin azaltılmasına imkân vermiştir,
- Güvenlik raporlarında gerek duyulduğu üzere, tesise özgü güvenlik araçlarının ve güvenlik yönetim etkinliğinin öneminin değerlendirilmesine imkân verecektir.

SÖZLÜK

Alt tutuşabilirlik sınırı (LFL): Yanıcı gaz veya buharın havadaki karışımının alev alabileceği minimum konsantrasyondur.

Basınçlı depolama: 1 bar basıncın üstünde ve ortam sıcaklığında çalışan depolama tankları. Depolanan madde basınç (iki faz dengeleri) altında sıvılaştırılmış gaz veya basınç (tek fazlı) altında bir gaz olabilir.

Başlatıcı olay (kök neden): Hata ağacında kritik olayın ilk nedenidir.

Birikinti yangını: Sıvı yakıt birikintisinin yanmasıdır. Birikinti yangını sıvı yakıt içeren bir tankın içinde de olabilir.

BLEVE: Normal atmosferik basınç altındaki kaynama noktasının oldukça üzerinde bir sıcaklıkta sıvı içeren kabın yarılması sonucu meydana gelen patlamadır.

Dağıtım sistemi: Dağıtım sistemi, yaşam döngüsü boyunca bir bariyerin optimum performans için gerekli olan kaynakları (davranış, donanım veya yazılım ile) sağlayan güvenlik yönetim sisteminin yapısal parçasıdır.

Denetim: Gerçek durum ile güvenli olarak belirtilen durumun uyumlu olup olmadığının sistematik olarak gözden geçirilmesi ve incelenmesidir.

Eşik sınır değerleri: Tablo 23'te tanımlandığı gibi farklı etki düzeyleri için sınır değerlerdir.

Etki düzeyleri: Kazaların etkilerinin kalitatif kategorileridir.

Etkisi sınırlı tehlikeli olay: Doğrudan kritik olaydan sonra olmayan ancak olay ağacında sınırlayıcı bariyerin çalışmasıyla tehlikesi sınırlanan olaydır. (Örneğin, bulut oluşturan gaz miktarını sınırlayan bir su perdesi).

Flash yangını: Hava ile karışan yanıcı gaz veya buhar bulutlarının hızlıca tutuşmasıdır.

GIS: Coğrafik bilgi sistemi.

Güvenli hata kesri (Safe failure fraction, SFF): Bileşendeki güvenli durum arıza frekansının toplam arıza frekansına oranıdır. Güvenli durum, güvenlik bariyerini tehlikeli veya başarısız fonksiyon durumuna düşürme potansiyeli olmayan arızadır.

Güvenlik bariyeri: Güvenlik bariyerleri özel süreçlere veya yönetimsel kontrollere dayalı olan fiziksel ve mühendislik sistemleri veya insan davranışları olabilir. Güvenlik bariyeri doğrudan güvenlik fonksiyonunu yerine getirir. Güvenlik bariyerleri güvenlik fonksiyonlarının nasıl uygulandığı ile ilgilidir.

Güvenlik bariyerinin etkinliği: Etkinlik, güvenlik bariyerinin belirli koşullarda performansında azalma olmaksızın bir süre için bir güvenlik fonksiyonunu yerine getirebilme yeteneğidir. Etkinlik tanımlı güvenlik fonksiyonunun performansının olasılığı veya yüzdesidir. Güvenlik bariyerinin

etkinliği yüzdesel olarak ifade edilmek istenirse bu değer çalışma süresi boyunca değişebilir. Örneğin bir güvenlik talebinde tam olarak kapanmayacak bir valfin (donanım veya metot tasarımı) etkinliği %100 olmayacaktır.

Güvenlik bariyerinin güvenirlilik seviyesi: Belli bir zaman dilimi içerisinde belirtilen koşullar altında belli bir etkinlik ve tepki zamanına göre gerekli bir güvenlik fonksiyonu doğru şekilde çalışması istendiği anda (talep üzerine) meydana gelen hata olasılığıdır (the probability of failure on demand, PFD). Bu kavram Güvenlik Enstrümanlı Sistem standardı IEC 61511 tanımlanan SIL kavramına (Safety Integrity Level) benzer ancak, ARAMİS metodunda tam veya kısmi insan davranışına dayanan güvenlik bariyerlerine de uygulanır.

"Tasarım" güvenirlilik seviyesi Ekte 8'de verilen yönerge yardımıyla değerlendirilir. Bu seviye, bariyerin kurulduğu andaki tepki süresi ve talep üzerine başarısızlık olasılığı veya aynı güvenirlilik seviyesinde olması için ilk kurulduğu andaki gibi etkin olduğu varsayımı anlamına gelir.

"Operasyonel" güvenirlilik seviyesi güvenlik yönetim sisteminin etkisini içerir.

"Operasyonel" güvenirlilik seviyesi güvenlik yönetim sisteminin denetimi sırasında bazı sorunlar tespit edildiği durumda "tasarım" güvenirlilik seviyesinden daha düşük olabilir.

Güvenlik bütünlük seviyesi (SIL): Güvenlik ile ilgili elektrik/ elektronik/ programlanabilir elektronik sistemlerin fonksiyonel güvenliği ile ilgili IEC 61508 ve IEC 61511 standartlarında tanımlanan güvenirlilik seviye kademeleridir. SIL, SIL = -log(PFD) ile tanımlanır (PFD, çalışması istendiği anda (talep üzerine) hata olasılığıdır).

Güvenlik fonksiyonu: Güvenlik fonksiyonu, teknik veya prosedürlerle ilgili bir eylem olup, bir nesne ya da fiziksel bir sistem değildir. Bir olaydan kaçınmak, olayı önlemek veya olayın oluşmasını kontrol etmek ya da sınırlamak için gerçekleştirilmesi gereken bir eylemdir. Bu eylem, bir güvenlik bariyeri sayesinde gerçekleştirilecektir. Güvenlik fonksiyonu güvenliği garanti etmek, artırmak ve/veya teşvik etmek için gerekli olan fonksiyonlardır.

Güvenlik kültürü: Bir çalışma grubunun üyeleri arasında çalışmalarının güvenliği üzerinde gerçek ya da potansiyel etkiye sahip olan, paylaşılan ve birbiri ile bağlantılı inançlar, normlar ve eylemler dizisidir.
Güvenlik yönetim sistemi: Etkin bir güvenlik sistemini ve sürekli gelişimini sağlayan ilkeler, planlı görevler, süreçler ve sorumlulukların belgelendirilmesi veya kalite yönetim sisteminin (ISO 9000) uyumlaştırılmasıdır. Güvenlik politikasını geliştirmek, uygulamak, başarmak, gözden geçirmek ve sürdürebilmek için gerekli süreçler ve kaynaklar, prosedürler, eylemler, sorumluluklar, planlama eylemleri ve organizasyonel yapıyı içeren yönetim sistemini içeren bir parçasıdır.

Güvenlik yönetimi: Tehlikelerin etkin bir şekilde tanımlandığı, anlaşıldığı ve makul başarılabilir bir seviyeye indirilmesini sağlayan yönetim faaliyetleri kümesidir. Bu durum ARAMIS çerçevesinde güvenlik bariyerlerinin belirtildiği, tasarlandığı ve gerektiği gibi çalışmasını sağlayan yönetimsel eylemler bütünü olarak genişletilebilir.

Hata ağacı: Papyonun sol parçasıdır ve kritik olayın olası nedenlerini belirler.

Hata toleransı: Bariyeri oluşturan bir ya da daha fazla sistem arızası durumunda bariyerin güvenlik

fonksiyonunu sürdürebilme kapasitesiyle bağlantılıdır. Hata toleransı yedeklilik ile bağlantılıdır. Örneğin hata toleransı 1 ise, bir bileşen arızalanması durumunda dahi güvenlik fonksiyonu çalışmaya devam eder.

Hedef: Tesiste meydana gelen büyük bir kaza durumunda etkiye maruz kalan endüstriyel bölge çevresinin elemanıdır. Hedef 3 ana kategoriye ayrılır. İnsan, maddi unsurlar ve doğal çevre.

İkincil kritik olay (papyonda, olay ağacı tarafında): Kritik olayı takip eden olaydır. (örneğin: kapta delinmeden sonra birikinti oluşması)

Kaynağı sınırlı tehlikeli olay: Kritik olayın sonucu oluşan tehlike olayın sonucunun başarılı güvenlik bariyerleri tarafından sınırlanması(örneğin: birikintinin hacminin veya salım süresinin sınırlanması).

Kritik olay: Genel olarak sınırlama kaybı (LOC) olarak tanımlanır ve bu sıvılar için oldukça doğrudur. Bu tanımı katılar için ve özellikle katı kütle depolayanlar için maddenin fiziksel ve/veya kimyasal özellikleri değiştiği düşünülerek fiziksel bütünlük kaybı(LPI) olarak kullanılabilir. Kritik olay papyonun merkezinde yer alır.

MIMAH: Büyük kaza tehlikelerinin belirlenmesi metodolojisi.

MIRAS: Referans kaza senaryolarının belirlenmesi metodolojisi.

Olay ağacı: Papyonun sağ kısmını oluşturur, kritik olayın olası sonuçlarını belirler.

Patlama basıncı (Blast): Patlamadan kaynaklı yüksek basınç(bar).

Radyasyon: Alevden kaynaklanan termal radyasyon (kW m-2).

Risk indeksi: Bir sistemin riski veya tehlikeleri üzerinde etkili olan faktörler dizisinden oluşan kantitatif ya da kalitatif bir ölçüdür.

Risk şiddet indeksi: Eşitlik 1 ile tanımlanan risk indeksidir (Bölüm 7.2.2).

Sıvı fazda cidarda delinme: Ekipmanın içinde sıvı faz bulunurken cidarın üzerinde belirli bir çapa sahip sürekli salıma sebep olan delinme olayıdır. Bu delik yapının mekanik özelliklerinden dolayı bozulmadan veya iç/dış nedenlerden dolayı mekanik stresten oluşabilir.

Şarapnel (missiles): Patlama sonucu saçılan kap parçacıklarıdır.

"Tam gelişmiş" tehlikeli olay: Kritik olayın sonucunu sınırlayan veya etkilerini azaltan güvenlik sisteminin olmadığı tehlikeli olaydır.

TEEL: Geçici Acil Maruziyet Limitleri.

Tehlikeli madde: SEVESO II direktifi tehlikeli maddeleri, Ek 1 - Bölüm 1'de listelenen veya Ek 1 - Bölüm 2'de verilen kriterleri karşılayan madde veya karışım olarak tanımlar ve hammadde, ürün, yan ürün, artık madde veya kaza durumunda oluşabilecek ara ürünleri de belirtir. Son olarak, tehlikeli bir madde insana, çevreye ya da ekipmana zarar verme kapasitesi olan toksik, yanıcı kararsız veya patlayıcı olan

maddelerdir. Kullanılan tehlikeli özelliklerinin SEVESO II Direktifinin tehlikeli kategorileri ve 67/548/EEC sayılı Direktifin risk ibarelerine dayanmaktadır.

Tehlikeli olay (papyonda, olay ağacı tarafı): Üçüncül kritik olayı takıp eden olaydır (Örneğin: Birikintinin tutuşmasından sonra birikinti yangınıdır.). Tehlikeli olayın örnekleri: buhar bulutu patlaması, flaş yangını, tank yangını, toksik bulutun yayılması vb.

Tepki süresi: Güvenlik bariyeri tarafından gerçekleştirilen güvenlik fonksiyonunun tam olarak başarılması (etkinliğe eşit) ile güvenlik bariyerinin çalışmaya başlaması arasındaki süredir.

Uygun tehlikeli ekipman: Eşik sınır değerine eşit veya daha yüksek miktarda tehlikeli madde içeren ekipman.

Üçüncül kritik olay (papyonda, olay ağacı tarafında): İkincil kritik olayı takip eden olaydır (örneğin: birikintinin oluşmasından sonra tutuşması).

Yüksek basınç: Patlama kaynaklı ani basın artışı (bar).

REFERANSLAR

1. http://mahb.jrc.it/index.php?id=418

2. http://f-seveso.eu-vri.eu/

3. http://mahb.jrc.it/index.php?id=517

4. ARAMIS - ACCIDENTAL RISK ASSESSMENT METHODOLOGY FOR INDUSTRIES IN THE CONTEXT OF THE SEVESO II DIRECTIVE, Contract number : EVG1 – CT – 2001 – 00036, USER GUIDE

ÇALIŞMA ve SOSYAL GÜVENLİK BAKANLIĞI
İş Teftiş Kurulu Başkanlığı
İnönü Bulvarı No:42 B Blok
Kat:5 Emek / ANKARA
Tel : 0312 296 62 31
web : www.itkb.gov.tr
e-posta : isteftis@csgb.gov.tr

İŞ TEFTİŞ KURULU BAŞKANLIĞI YAYINIDIR
PARA İLE SATILMAZ.