Savunma Bilimleri Dergisi
The Journal of Defense Sciences
Kasım / November 2022, Sayı/Issue 42

Nükleer Emniyet Kapsamında Fiziksel Koruma Sistemi Tasarlamak ve Analiz Etmek İçin Yerli Yazılım Geliştirilmesi

Mahsum AKDEMİR [*] - Senem ŞENTÜRK LÜLE[**]

Öz

Nükleer enerjinin askerî amaçlar için kullanılması sonrasında nükleer silahların birçok devlet tarafından geliştirilmesi, nükleer silahların çalınması, nükleer madde ve radyoaktif maddelerin çalınması, nükleer tesislere sabotaj, nükleer maddelere taşıma sırasında sabotaj ve kirli bomba tehdidi gibi kaygılar ortaya çıkmıştır. Bu kapsamda nükleer tesis ve maddelerin korunması nükleer emniyet (nuclear security) konsepti altında değerlendirilmektedir. Kişileri, mülkleri, toplumu ve çevreyi nükleer madde ve radyoaktif madde kaynaklı hırsızlık ve sabotaj içeren kötü niyetli olaylardan korumak için nükleer emniyet rejiminin kapsamını devletler belirlemektedir. Nükleer emniyetin sağlanmasında devletin belirlediği yasal çerçeve ülkedeki yetkili kurum tarafından yürütülürken, nükleer tesisi işleten, nükleer maddeyi depolayan ve/veya taşıyan yetkilendirilen kişi de fiziksel koruma sistemi (FKS) ile nükleer emniyetin sağlanmasında rol almaktadır. Bu çalışma nükleer emniyetin sağlanmasında ve sürdürülmesinde kritik öneme sahip olan FKS'nin tasarımında ve değerlendirilmesinde kullanılabilecek yerli ve millî bir yazılım anlatılmıştır. Yazılım FKS'nin belirlenen tehdide karşı etkinliğini hesaplamakta ve tehdidin hedefine ulaşmada en çok tercih edebileceği, sistemin en zayıf halkası olan yolu belirlemektedir. En zayıf halkada yapılacak iyileştirmeler ile sistemin etkinliği arttırılabilmektedir. Test aşamalarını başarıyla geçen yazılım mevcut haliyle sadece nükleer tesislerde değil diğer kritik tesislerdeki fiziksel koruma sistemlerinin analizine de olanak vermektedir. Ayrıca ara yüzün Türkçe olması yazılımın

[*] Yüksek Lisans Öğrencisi, İstanbul Teknik Üniversitesi, Enerji Enstitüsü, akdemirm@itu.edu.tr, ORCID: 0000-0001-6224-3022.
** Doç. Dr., İstanbul Teknik Üniversitesi, Enerji Enstitüsü, senturklule@itu.edu.tr, ORCID: 0000-0002-6632-5831.

Geliş Tarihi/Received : 22.09.2021
Kabul Tarihi/Accepted : 31.05.2022
Araştırma Makalesi/ Research Article
DOI: 10.17134/khosbd.998901

Türkiye'deki nükleer emniyet eğitimlerinde kullanımının önünü açmaktadır. Gelişmeye açık olmakla birlikte, yazılım bu haliyle ülkemizdeki nükleer tesislerin FKS analizinde düzenleyici kuruluş tarafından kullanılabileceği düşünülmektedir.

***Anahtar Kelimeler**: Nükleer Emniyet, Fiziksel Koruma Sistemi, Nükleer Malzeme, Nükleer Tesis, Yerli Yazılım Geliştirme.*

The Development of Indigenous Software for Nuclear Security to Design and Analyse a Physical Protection System

Abstract

After the use of nuclear energy for military purposes, concerns on the development of nuclear weapons by many states, theft of nuclear weapons, theft of nuclear and radioactive materials, sabotage of nuclear facilities, sabotage of nuclear materials during transportation, and the threat of dirty bombs have emerged. In this context, the physical protection of nuclear facilities and materials is covered with the concept of nuclear security. States determine the scope of the nuclear security regime, whose objective is to protect people, property, society, and the environment from malicious acts, mainly theft and sabotage, towards nuclear and radioactive materials. While the legal framework determined by the state is carried out by the competent authority, the license holder who operates the nuclear facility and/or stores and/or transports the nuclear material provides nuclear security with the physical protection system (PPS). In this paper, the methodology of an indigenous and national software that can be used in the design and evaluation of PPS is explained. The software calculates the effectiveness of the PPS against the defined threat and determines the path that can be preferred by the threat to reach its target (the weakest link). The tested and verified software allows the analysis of PPS not only for nuclear but also for other critical facilities. In addition, its Turkish interface makes it an excellent tool for nuclear security trainings in Türkiye. The indigenous software can be used by the Turkish regulatory authority to evaluate the PPS of nuclear facilities in Türkiye.

***Keywords**: Nuclear Security, Physical Protection System, Nuclear Material, Nuclear Facility, Indigenous Software Development.*

Giriş

2. Dünya Savaşı sırasında Japonya'daki kullanımı sonrası yıkıcı etkisine şahit olunan nükleer enerji, tüm dünyada bir silahlanma yarışına sebebiyet vermiştir (Margulies, 2008). Bu silahlanma yarışının ortaya koyduğu tehdide yönelik olarak ortaya çıkan ilk uluslararası antlaşma Nükleer Silahların Yayılmasının Önlenmesi Antlaşması (Treaty on the Non-Proliferation of Nuclear Weapons-NPT) olup bu anlaşma 1968 yılında imzaya açılmış ve 5 Mart 1970 tarihinde yürürlüğe girmiştir (UN, 2021). Soğuk Savaş döneminde (1947-1991) bizzat devletler nükleer silah ve madde açısından odak noktasındayken, sonraki yıllarda nükleer silahların ve nükleer maddelerin devlet dışı unsurların eline geçme olasılığı ortaya çıkmış ve nükleer terör kavramı tartışılmaya başlanmıştır. Fergusan'ın çalışmasında belirtildiği şekliyle nükleer terör bağlamında dört unsur öne çıkmaktadır (Gerçeker, 2013).

- Var olan nükleer silahların yetkisiz alınması ve kullanılması,
- Nükleer silah veya ekipman yapımı ile bunların aktif hale getirilmesinde kullanılan nükleer maddelerin hırsızlık sonucu elde edilmesi,
- Nükleer tesise ve taşınır durumdaki nükleer maddeye sabotaj girişimleri,
- Radyoaktif kirliliğe sebebiyet verecek radyoaktif maddelerin çalınması ile bu maddeleri içeren araçların patlatılması.

Bu bağlamda, uluslararası alanda nükleer emniyet için atılan adımların başında 1980'de imzaya açılan ve 1987'de yürürlüğe giren Nükleer Maddelerin Fiziksel Korunması Sözleşmesi (Convention on Physical Protection of Nuclear Material-CPPNM) gelmektedir. Bu sözleşme, nükleer maddelerin uluslararası taşımacılıkta fiziksel olarak korunması, belirli kusurların suç kabul edilmesi ve nükleer madde hırsızlığı veya yetkisiz elde edilmesi gibi konularda uluslararası iş birliğini sağlamıştır (IAEA, 2020). 2005 yılında yapılan değişiklik ile orijinal anlaşmanın kapsamı barışçıl amaçlar için kullanılan nükleer tesislerin ve nükleer maddelerin kullanımı, depolanması ve taşınması sırasında fiziksel korunmasını da içerecek şekilde genişletilmiştir (IAEA, 2005). Ek olarak, nükleer madde kaçakçılığı ve nükleer madde ve tesislere yönelik sabotaj da suç unsuru olarak kabul edilmiştir.

İngilizce'de "Nuclear Safety", "Nuclear Safeguards" ve "Nuclear Security" Türkçe'de ise "Nükleer Güvenlik", "Nükleer Güvence" ve "Nükleer Emniyet"

olarak geçen kavramlar, nükleer enerjinin sorunsuz bir biçimde toplum yararına kullanımını sağlamaktadır. Ulusal mevzuatımıza göre:

- **Nükleer Güvenlik:** "Nükleer tesislere ilişkin faaliyetler sırasında birey, toplum ve çevrenin radyasyondan korunmasını sağlamak üzere uygun koşulların oluşturulması, kazaların önlenmesi veya kaza sonuçlarının hafifletilmesini" (TC., 2012),

- **Nükleer Güvence:** "Güvence Denetimi Anlaşması ve Ek Protokol ile Türkiye Cumhuriyeti'nin taraf olduğu diğer ikili veya çok taraflı uluslararası anlaşmalar ile üyeliklerden kaynaklananlar da dâhil olmak üzere nükleer silahların yayılmasının önlenmesine yönelik yükümlülükleri" (TC., 2020a),

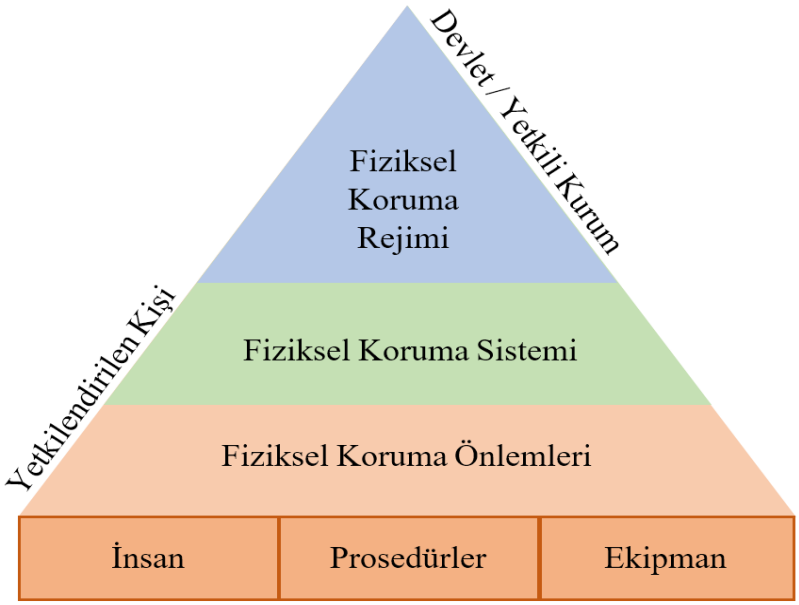
- **Nükleer Emniyet:** "Nükleer tesisleri ve nükleer maddeleri hedef alan hırsızlık, sabotaj, yetkisiz erişim ve diğer kötü niyetli girişimleri engellemek, tespit etmek ve gerektiğinde müdahale etmek üzere fiziksel koruma önlemleri ile bilgi güvenliğini ve siber güvenliği sağlamaya yönelik önlemlerin alınmasını ve bu önlemlerin etkinliğinin sürdürülmesini" (TC., 2020b) ifade etmektedir.

Bu tanımlar doğrultusunda nükleer güvenlik çevrenin ve toplumun radyasyondan korunması, nükleer emniyet nükleer tesislerin ve maddelerin kötü niyetli kişilerden korunması ve nükleer güvence de nükleer tesislerin ve maddelerin nükleer silahların yayılmasının önlenmesi amacıyla uluslararası denetim altına alınması olarak özetlenebilir.

Nükleer emniyetinin sağlanması için her devletin bir "Nükleer Emniyet Rejimi" olmalı ve bunun hedefi "kişileri, mülkleri, toplumu ve çevreyi nükleer madde ve radyoaktif madde kaynaklı temelde hırsızlık ve sabotajı içeren kötü niyetli olaylardan korumak" olmalıdır (IAEA, 2011). Nükleer emniyet rejiminin bir bileşeni olan "Fiziksel Koruma Rejimi" ülkedeki yasal ve düzenleyici çerçeve, bu yasal çerçeveyi uygulatacak ve uygulayacak kurum ve kuruluşları ve tesiste/taşıma sırasında kullanılan fiziksel koruma sistemi (FKS) bileşenlerini içerir (Şekil 1).

Nükleer emniyetin sağlanması, korunması ve sürdürülmesinde devletler birinci dereceden sorumludur. Devlet nükleer emniyet ile ilgili mevzuatı düzenleyerek konunun kapsamını ve ilgililerini belirler. Mevzuatı hayata geçirecek bir yetkili kurum görevlendirir. Görev ve yetki tanımının yapılması, devlet'in bu konudaki sorumluluğundan feragat ettiği anlamına gelmez.

Nükleer emniyette yasal ve düzenleyici çerçeveyi uygulamak yetkili kurumun sorumluluğundadır. Yetkili kurum görevini yerine getirebilecek yetkiye, yeterliliğe ve uygun finansal güce ve insan kaynaklarına sahip olmalıdır. Nükleer madde sayım ve kontrol sistemine erişimi olmalı ve düzenli denetimler yapmalıdır. Türkiye'de nükleer emniyet konusunda yetki, 702 sayılı 02/07/2018 tarihli Kanun Hükmünde Kararnamede ile Nükleer Düzenleme Kurumuna verilmiştir (TC., 2018).



Şekil 1. Nükleer Emniyette Sorumlular ve Sorumluluk Alanları

Nükleer emniyette yetkilendirilen kişi, (TC., 2018) referansında "Bu Kanun Hükmünde Kararname kapsamındaki bir faaliyetin yürütülmesi için Kurum tarafından kendisine lisans, izin, onay veya yetki belgesi verilen gerçek veya tüzel kişi" olarak tanımlanmıştır. Yetkilendirilen kişi ulusal mevzuata uymak, emniyet planını hazırlamak ve ihtiyaç dâhilinde revize etmek, nükleer madde sayım ve kontrolünü yaparak olası bir tutarsızlığı yetkili kuruma bildirmek ve FKS performansını test etmek ile yükümlüdür.

Bu çalışma kapsamında "Nükleer emniyet nedir? Hedefleri nelerdir? Nükleer emniyet konusunda ilgili kurum ve kuruluşlar hangileridir? Nükleer emniyette risk temelli karar yönetimine göre ne, kime karşı, nasıl korunacak ve olası başarısızlığın sebebiyet vereceği potansiyel sonuçlar neler olacak?" sorularının

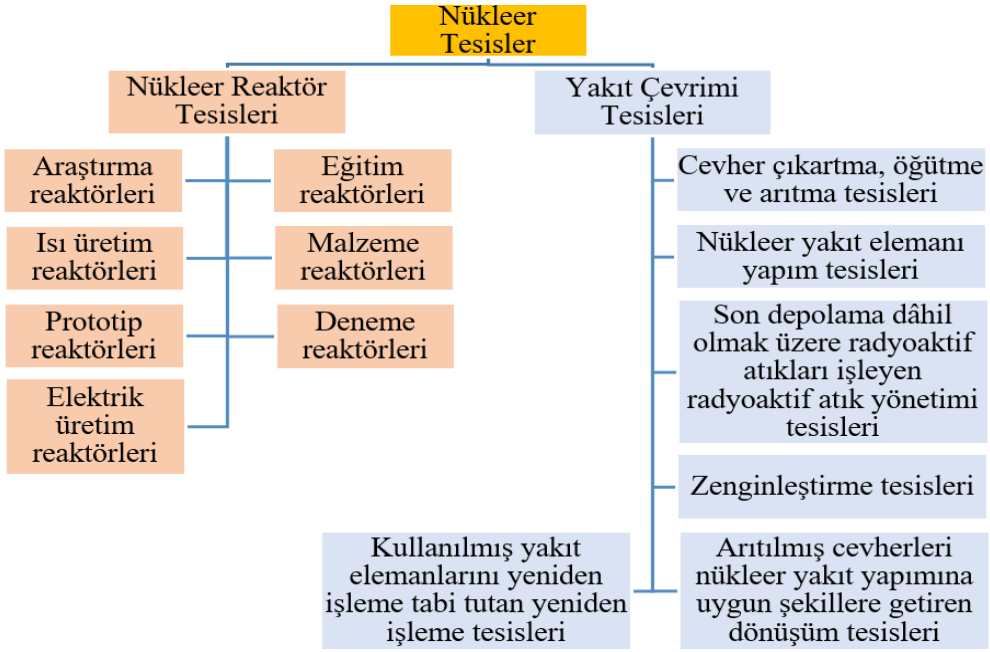
yanıtları ile nükleer emniyet kavramı anlatılmıştır. Ayrıca, bir fiziksel koruma sisteminin etkinliğini hesaplamak üzere geliştirilen yazılım tanıtılmıştır.

Materyal ve Metot

Nükleer emniyet riski, "kişi ya da kişilerden oluşan bir tehdidin istenmeyen durumlara sebebiyet vermede başarılı olma olasılığı" olarak tanımlanabilir. Nükleer tesisler için, bir nükleer patlayıcı cihaz yapmak üzere nükleer maddenin yetkisiz olarak alınması, radyolojik serpintiye sebebiyet verecek şekilde bir nükleer maddenin yetkisiz olarak alınması ve nükleer maddelerin ve nükleer tesislerin sabotajı olarak üç tip istenmeyen olay tanımlanmıştır (IAEA, 2011).

1. Ne Korunacak?

Nükleer emniyet kapsamında nükleer tesisler ve nükleer maddeler korunmalıdır. Mevzuatımıza göre nükleer tesisler, detayları Şekil 2'de gösterildiği gibi, nükleer reaktör ve nükleer yakıt çevrimi tesisleri olarak ikiye ayrılmaktadır (TC., 1983).



Şekil 2. Nükleer Emniyet Kapsamında Korunacak Tesisler

Nükleer maddeler mevzuatımızda yer aldığı şekli ile Tablo 1'de gösterilmiştir. Kategori I en sıkı koruma gerektiren maddeleri barındırırken, Kategori III korumanın en az olabileceği kategoridir.

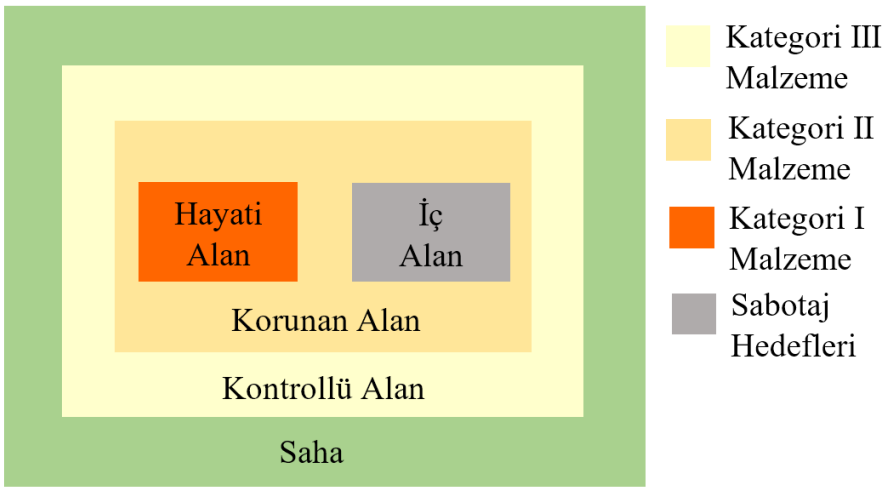
Tablo 1. Nükleer Maddelerin Nükleer Emniyet Kapsamında Sınıflandırması

Madde	**Biçim**	**Nükleer Maddenin Sınıfı**		
		I	**II**	**III**
Plütonyum[a]	Işınlanmamış veya az ışınlanmış[b]	2 kg veya daha fazla	500 g dan fazla ve 2 kg dan az	15 g dan fazla ve 500 g veya daha az
Uranyum-235	Işınlanmamış veya az ışınlanmış[b] %20 veya daha fazla zenginleştirilmiş uranyum	5 kg veya daha fazla	1 kg dan fazla ve 5 kg dan az	15 g dan fazla ve 1 kg veya daha az
	Işınlanmamış veya az ışınlanmış[b] %10 veya daha fazla ve %20 den daha az zenginleştirilmiş uranyum	-	10 kg veya daha fazla	1 kg dan fazla ve 1 kg veya daha az
	Işınlanmamış veya az ışınlanmış[b] Doğal uranyumdan fazla %10 dan az zenginleştirilmiş uranyum	-	-	10 kg veya daha fazla
Uranyum-233	Işınlanmamış veya az ışınlanmış[b]	2 kg veya daha fazla	500 g dan fazla ve 2 kg dan az	15 g dan fazla ve 500 g veya daha az
Işınlanmış Yakıt			Tüketilmiş veya doğal uranyum, toryum veya düşük zenginlikli yakıt (fisil içeriği %10 dan az)	

a) Plütonyum-238 içeriği %80 veya daha az olan plütonyum.

b) Reaktörde ışınlanmamış nükleer maddeler ile reaktörde ışınlanmış ancak zırhlama olmaksızın 1 Gy/saat (100 rad/saat) değerine eşit veya daha az radyasyon doz hızına sahip maddeler.

Nükleer maddelerin kategorileri, bu maddelerin tesiste hangi alanlarda bulunması gerektiğini belirler. Şekil 3'te mevzuatımıza göre belirlenen farklı alanlar gösterilmiştir (TC., 2020).



Şekil 3. Nükleer Maddelerin Kategorilerine Göre Tesis İçindeki Alanlar

2. Kime Karşı Koruma Sağlanacak?

Korumanın kime karşı yapılacağı konusunda belirleyici olan tasarıma esas tehdittir (TET). TET mevzuatımızda "Nükleer tesislerde fiziksel koruma sisteminin tasarımına ve değerlendirilmesine temel teşkil eden, nükleer tesisler ve nükleer maddeleri hedef alan hırsızlık, sabotaj, yetkisiz erişim ve diğer kötü niyetli girişimlerle sonuçlanabilecek, nükleer tesis içinden ve/veya dışından kaynaklanabilecek potansiyel en güçlü tehdit" olarak tanımlanmıştır (TC., 2020).

Yetkili kurum tarafından kurulan ve tesise özgü TET belgesini hazırlayacak olan TET komisyonunda emniyet ve istihbarat ile ilgili kurum ve kuruluşlar yer alır. TET'in doğru olarak tespiti için tehdidin türü, motivasyonu, niyeti, taktikleri, sahip olduğu araç-gereçler ve yetenekleri gibi konular detaylıca irdelenir.

3. Koruma Nasıl Sağlanacak?

Korumanın sağlanmasında, bir kötü niyet eyleminin caydırma ve hassas bilgilerin korunması ile önlenmesi ve FKS'ye tespit, geciktirme ve müdahale gücü

entegre edilerek kötü niyetli eyleme zamanında müdahale etmek ve tehdidi etkisiz hale getirmek olarak ifade edilebilecek iki yöntem uygulanır.

a. Bir kötü niyet eyleminin caydırma ve hassas bilgilerin korunması ile önlenmesi:

Nükleer tesislere ve maddelere yapılması planlanan kötü niyetli eylemler önceden belirlenip engellenmelidir. Ayrıca, tesis özelinde potansiyel tehditleri önlemek ve bir saldırının gerçekleşme olasılığını azaltmak üzere fiziksel koruma önlemleri ile caydırıcılık sağlanmalıdır.

b. FKS'ye tespit, geciktirme ve müdahale gücü entegre edilerek kötü niyetli eyleme zamanında müdahale etmek ve tehdidi etkisiz hale getirmek:

FKS, mevzuatımızda şu şekilde tanımlanmıştır: "Nükleer tesisleri ve nükleer maddeleri hedef alan hırsızlık, sabotaj, yetkisiz erişim ve diğer kötü niyetli girişimleri engelleme, tespit etme, geciktirme ve gerektiğinde müdahale fonksiyonlarını yerine getirmek üzere oluşturulan, etkinliği ve yeterliliği sürekli analiz edilen ve güncellenen idari, teknik ve organizasyonel bütünleşik önlemler içeren geniş kapsamlı koruma sistemidir" (TC., 2020).

4. Korumayı kim sağlayacak?

Tehdit seviyesine göre nükleer emniyetin sağlanmasında sorumluluk devlet ile yetkilendirilmiş kişi arasında paylaşılmaktadır. Bu sorumluluk derecesinin belirleyicisi TET'dir. TET ve TET seviyesinin altındaki tehditler daha düşük kapasitelidir ve yetkilendirilen kişinin, TET seviyesinin üstündeki yüksek kapasiteli tehditler devletin sorumluluğundadır.

Konuya tesis özelinde bakıldığında korumanın sağlanmasında FKS'nin en etkili unsurunun müdahale gücü olduğu anlaşılır. Müdahale gücü hırsızlık veya sabotaj riskine karşı geciktirme, müdahalede bulunma ve kötü niyetli kişinin etkisiz hale getirilmesi işlerini yapan personelin oluşturduğu ekiptir. Müdahale gücü kapasite olarak TET'de tanımlanan tehdidi etkisiz hale getirecek yeterli sayıda, iyi eğitilmiş ve fiziki durumu iyi personeli içermeli ayrıca yeterli teçhizatla donatılmış olmalıdır.

5. Nükleer emniyet sağlanamazsa oluşacak potansiyel tehlikeler ve çözüm yaklaşımları nelerdir?

FKS'nin başarısız olması ve kötü niyetli kişilerin hedeflerine ulaşmaları sonucu ortaya çıkabilecek potansiyel tehlikeler hırsızlık ve sabotaj olayları için ayrı ayrı değerlendirilmelidir.

Hırsızlık eyleminin başarılı olması durumunda çalınan nükleer maddelerin nükleer patlayıcı yapımında kullanılması veya kirli bomba ile radyoaktif kirliliğe sebep olması mümkündür. Sabotaj eylemi başarılı olursa da çevreye radyasyon yayılması olasıdır. Sabotaj sonuçları yüksek radyolojik sonuçlar ve kabul edilemez radyolojik sonuçlar olmak üzere iki kategoride değerlendirilir. Sabotaj sonunda hangi seviyeden radyolojik sonuçlar açığa çıkacağı tesisin radyoaktivite envanteri ile doğrudan ilişkilidir.

Hırsızlık durumunda, çalınan nükleer maddenin yerinin tespitinden ve geri alınmasından sorumlu kurumların önceden belirlenmesi, görev, yetki ve sorumluluklarının net bir şekilde bir protokol çerçevesinde resmiyete kavuşturulması gereklidir. Sabotaj durumunda ise nükleer tesisin emniyete alınması, acil durum ekipmanını ve personelini korumaya ve hasarın artmasını önlemeye yönelik önlemleri içeren beklenmedik olay planının hazırlanmış olması gerekmektedir.

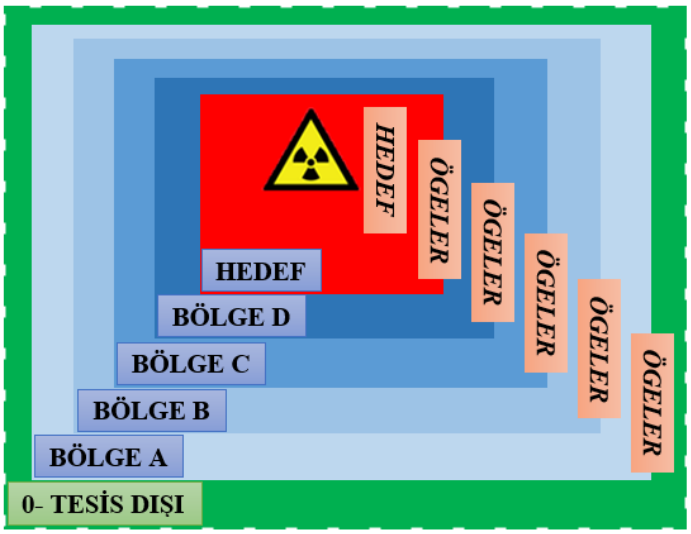
6. FKS Tasarım Değerlendirmesi

Etkin bir fiziksel koruma sistemi için FKS gereklilikleri belirlenmeli, FKS tasarımı yapılmalı, bu tasarım değerlendirilmeli ve değerlendirme sonucuna göre ya tasarıma son şekli verilmeli ya da tasarım süreci yeniden başlatılmalıdır. Bu bölümde, bir FKS tasarımının yapılmasında veya tasarımı yapılmış bir fiziksel koruma sisteminin değerlendirilmesinde kullanılabilecek ve bu makaleye konu olan yerli ve millî yazılımın temelini aldığı yukarıda anlatılan ilk 4 konu başlığı dikkate alınarak ortaya çıkarılmış yöntem anlatılacaktır. Yazılımın ortaya çıkmasındaki gereklilik nükleer emniyetin sağlanmasında en önemli faktör olan FKS etkinliğinin değerlendirilmesidir.

FKS etkinliği değerlendirilirken, FKS'nin belirlenmiş bir hedefi, belirli bir tehdide (genellikle TET) karşı başarılı bir şekilde koruyup korumadığı incelenir. FKS'nin nihai etkinliğinin anlaşılması için hedefler, tehditler ve saldırı senaryolarının oluşturduğu kombinasyonlar göz önünde bulundurulur.

Sayısal analizde kötü niyetli eylemi tamamlamak için kötü niyetli kişinin tesis dışından hedefine doğru bir yol izlediği varsayılır. Bu yol, hedefe giderken geçilmesi gereken fiziksel alanlar ve yol boyunca hem fiziksel alanlarda hem de FKS ögelerini etkisiz hale getirmede harcaması gereken süre dikkate alınarak hem mekânsal hem de zamansal olarak tanımlanır. Burada kötü niyetli kişinin başarıya ulaşması için sabotaj durumu için hedefine ulaşmasının yeterli olduğu, hırsızlık durumu için ise tesisi hedefi ile terk etmesi gerektiği varsayılır.

Sayısal analiz için tesiste hedefin etrafını çevreleyen bölgeler ve bölgelerin sınırlarında da FKS ögeleri olduğu varsayılır. Geliştirilen yazılımda kullanılan tesis şeması Şekil 4'te gösterilmiştir. Şekil 4'e göre "bölgeler" kötü niyetli kişinin hedefe ulaşmak için geçmesi gereken fiziki alanları, "ögeler" ise bu alanların sınırındaki FKS ekipmanlarını ifade etmektedir.



Şekil 4. Örnek Tesis Şeması

Ögeler, izinsiz girişi tespit edecek ekipmanları (dış sensörler-sismik gömülü kablo, elektrik alanı, kızılötesi, mikrodalga, vb., iç sensörler-sonik, kapasitans, video hareketi, infrared, ultrasonik, vb.), erişim kontrolü ekipmanları/prosedürleri, nöbetçilerin gözlem yapması, patlayıcı tespit ekipmanları, metal dedektörleri, duvarlar, kapılar, nöbetçiler vb. olarak gruplandırılabilir. Her öge hem tespit olasılığına hem de geciktirme süresine sahiptir. Yazılımın çalışabilmesi için bu

ögelerin tespit olasılıkları ve geciktirme süresi verilerinin ekipman üreticilerinden ve/veya bireysel olarak yapılan deneylerden elde edilmesi gereklidir.

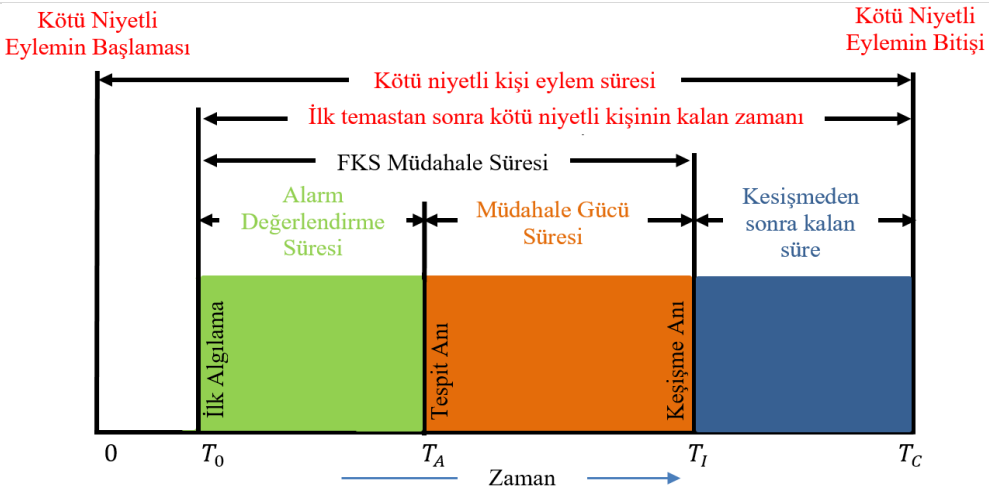
FKS etkinlik olasılığı (P_E) hesaplanırken kötü niyetli kişinin hedefine ulaşmak için kullanabileceği tüm yollar ve bu yollar üzerindeki tüm ögelerin geciktirme süreleri ve tespit olasılıkları dikkate alınır. Burada amaç kötü niyetli kişinin amacını gerçekleştirmek için tercih edeceği yolun bulunmasıdır. FKS etkinlik olasılığı (P_E), kesişme olasılığı (P_I) ve etkisiz hale getirme olasılığı (P_N) değerlerinin çarpımıyla Eşitlik 1'de gösterildiği şekilde hesaplanır (Sandia, 2021a).

$$P_E = P_I \times P_N \tag{1}$$

Burada P_I müdahale gücünün kötü niyetli girişim tamamlanmadan kötü niyetli kişilerin önünü kesme olasılığını ifade eden "kesişme olasılığını", P_N ise müdahale gücünün kötü niyetli kişileri eylemlerini tamamlamadan etkisiz hale getirme olasılığını ifade eden "etkisiz hale getirme olasılığını" işaret etmektedir.

FKS tasarım analizi çerçevesinde iki zaman akışından bahsedilebilir. Bunlardan ilki "kötü niyetli kişi zaman akışı" diğeri ise "fiziksel koruma sistemi zaman akışı" olarak ifade edilir. Her iki zaman akışı Şekil 5'te gösterilmiştir. Kötü niyetli kişi zaman akışı, kötü niyetli eylemi gerçekleştirecek kişinin harekete geçmesi ile başlar, tesis içindeki alanları geçmesi, geciktirme ögelerini aşması ve sabotaj ya da hırsızlık eylemini başarması ile sona erer. Fiziksel koruma sistemi zaman akışı ise tespit, geciktirme ve müdahale süreçlerini içerir.

Şekil 5'te 0 kötü niyetli kişinin harekete geçme anıdır ve henüz kimse kötü niyetli kişinin varlığından haberdar değildir. T_0 kötü niyetli eylemin ilk algılandığı andır. Bu an sensörlerin tetiklendiği veya kötü niyetli kişinin görüldüğü an olabilir. Algılanan durumun değerlendirmesi yapılmadığından henüz tespit yapılmamış sayılır. T_A alarm değerlendirilmesinin yapılıp tespitin tamamlandığı ve müdahale gücüne bilgilendirmenin yapıldığı anı, T_I ise müdahale gücünün olay mahalline varıp kötü niyetli kişiler ile kesiştiği anı ifade eder. T_I ile T_A arasındaki süre müdahale gücü süresi olarak ifade edilir. Bu süre harekete geçme ve kesişme süreçleri için gerekli sürelerin toplamıdır. T_O ile T_I arasındaki süre FKS müdahale süresidir. Bu süre alarm değerlendirme süresini de içermesinden dolayı müdahale gücü süresinden farklıdır. T_C ise kötü niyet kişisinin eylemini başarılı bir şekilde gerçekleştirmesi için ihtiyaç duyacağı toplam süreyi ifade etmektedir.



Şekil 5. FKS Değerlendirmesinde Kullanılan Zaman Akış Şeması

FKS zaman çizelgesinde FKS'nin müdahale gücüne kötü niyetli kişiyi etkisiz hale getirmesi için yeterince zaman verecek son tespit noktası "fark edilme kritik noktası (FKN)" olarak adlandırılır. FKN'den sonra müdahale ekibinin kötü niyetli girişimi başarılı bir şekilde engelleyebilmesi için ihtiyaç duyacağı zaman, kötü niyetli kişinin amacına ulaşma başarısı için gereken zamandan daha uzun olduğundan FKS başarısız olacaktır.

Tablo 2. P_N Hesabında Kullanılabilecek Örnek Matris (Sandia, 2021b)

Kötü niyetli kişi sayısı	**Müdahale ekibi kişi sayısı**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	0,5	0,83	0,96	0,99	1,00	1,00	1,00	1,00	1,00	1,00
2	0,17	0,50	0,78	0,92	0,98	0,99	1,00	1,00	1,00	1,00
3	0,04	0,23	0,50	0,74	0,89	0,96	0,99	1,00	1,00	1,00
4	0,01	0,08	0,26	0,50	0,72	0,86	0,94	0,98	0,99	1,00
5	0	0,02	0,11	0,28	0,50	0,70	0,84	0,92	0,97	0,99
6	0	0,01	0,04	0,14	0,30	0,50	0,68	0,82	0,91	0,96
7	0	0	0,01	0,06	0,16	0,32	0,50	0,67	0,81	0,90
8	0	0	0	0,02	0,08	0,18	0,33	0,50	0,66	0,79
9	0	0	0	0,01	0,03	0,09	0,19	0,34	0,50	0,65
10	0	0	0	0	0,01	0,04	0,10	0,21	0,35	0,50

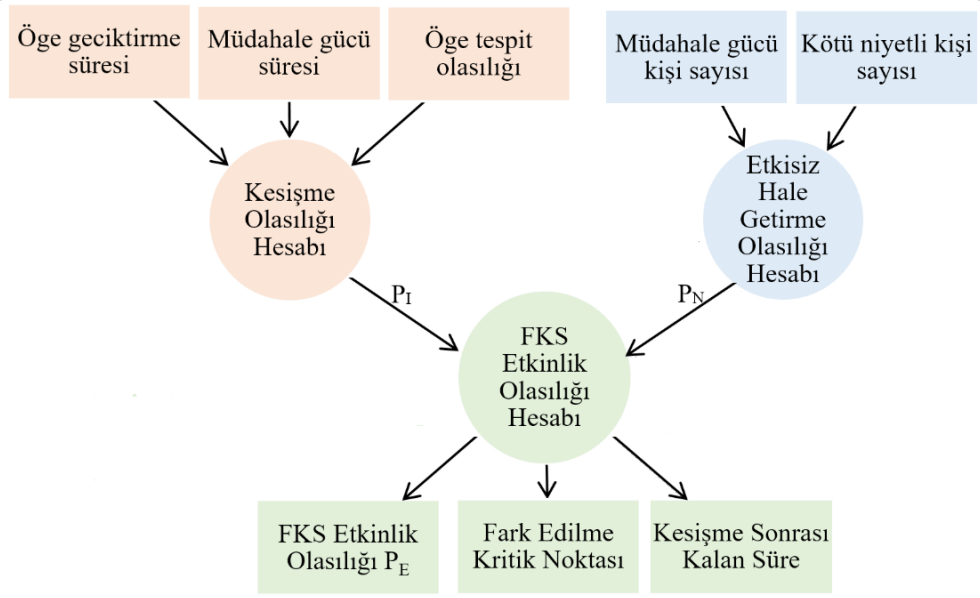
Eşitlik 1'de gösterildiği üzere FKS'nin etkinlik olasılığı P_I ve P_N şeklinde iki farklı bileşenin çarpımı ile hesaplanmaktadır. Bunlardan P_N olasılık değeri hesaplanırken uzman görüşleri, basit hesaplamaların, karmaşık simülasyonların ve güce-güç tatbikatlarının sonuçları teker teker kullanılabileceği gibi farklı kombinasyonlarda da kullanılabilir. Burada önemli olan kötü niyetli kişi sayısı arttıkça müdahale gücünün başarılı olma olasılığının azaldığının bilinmesidir. Tablo 2 örnek bir P_N matrisini göstermektedir.

FKS Tasarım ve Analiz Yazılımı Geliştirilmesi

FKS tasarım yazılımının geliştirilmesinde açık kaynak Python yazılım dili (Python, 2021), MySQL veri tabanı (MySQL, 2021) ve PyCharm entegre gelişim ortamı (IDE) (Jetbrains, 2021) kullanılmıştır.

Yazılım kesişme olasılığını hesaplamak için kullanıcıdan tesis içinde hedef etrafında bulunan bölgelerin ve bölge sınırlarındaki tespit ve/veya geciktirmede kullanılan ögelerin tespit olasılığı ve geciktirme süreleri ile müdahale gücü süresinin değerlerini girdi olarak istenirken, etkisiz hale getirme olasılığını hesaplamak için ise müdahale gücündeki kişi sayısı ile kötü niyetli kişilerin sayısını girdi olarak istemektedir. Geliştirilen yazılım çoklu güzergâh analizi ile kötü niyetli kişinin hedefine ulaşmak için kullanacağı en kritik yol ve bu yol üzerindeki fark edilme kritik noktasını hesaplamaktadır. Arka planda yapılan hesaplamalar sonucunda elde edilen bu iki olasılık çarpılarak FKS etkinlik olasılığı hesaplanarak en kritik yol ve bu yoldaki ögeler kullanıcıya bildirilmektedir. Yazılımda kullanılan veri akış şeması Şekil 6'da özetlenmiştir.

Yazılımı kullanmak için herhangi bir tesisi Şekil 4'teki formda yapılandırmak gerekmektedir. Burada tespit ve geciktirme için kullanılan koruma ögelerinin konumlandığı fiziksel alanlar bölgeler olarak tanımlanmış olup O-tesisin dışı olmak üzere tesis içinde hedef bölgeye doğru sırasıyla A, B, C, D, HEDEF şeklinde toplamda altı bölge tanımlanmıştır. Bu bölge sınırlarında FKS ögelerinin konumlandığı varsayılmıştır. Her bir sınır için istenilen sayıda öge tanımlamak mümkün kılınmıştır. Tesis yapısının bu düzeni ile hedefe ulaşmak için farklı güzergâhlar mümkündür. Yazılımda olası tüm güzergâh seçeneklerini bulunduracak şekilde bir algoritma oluşturulmuş olup bu bağlamda olası tüm durumların değerlendirilmesi sağlanmıştır.



Şekil 6. Yazılım Veri Akış Şeması

Yazılımda ayrıca sabotaj ve hırsızlık eylemleri için ayrı ayrı hesaplar yapılmasına imkân verilmiştir. Sabotaj senaryosunda hedefe ulaşmak kötü niyetli eylemin tamamlanması için yeterli iken hırsızlık senaryosunda kötü niyetli kişinin hedef ile tesisi terk etmesi eylemi tamamlaması için gerekli şarttır.

Yazılımın algoritmasının beklenildiği gibi çalışıp çalışmadığı hırsızlık ve sabotaj durumları için oluşturulan senaryolar ile test edilmiştir. Bu senaryolar oluşturulurken yazılımı zorlayacak şekilde öge ve bölgelere veri ataması yapılmıştır. Tüm senaryolara ait yazılımdan elde edilen analiz sonuçları ile bu analizlerin elle hesaplanan değerleri tamamen örtüşmüştür. Bu bağlamda algoritmanın beklenildiği şekilde eksiksiz çalıştığı anlaşılmıştır.

Ek olarak yazılım sanal bir tesise ait FKS testinde kullanılmıştır. Bu bağlamda sanal tesise ait veriler Sandia Ulusal Laboratuvarı ve UAEA tarafından 2019 yılında gerçekleştirilen nükleer emniyet kursu ITC-27'de dağıtılan "LIMP Exercise Data Handbook, The Hypothetical Facility Twenty-Seventh International Training Course" kitapçığından alınmıştır (Sandia, 2021c). Bu kitapçıkta sanal bir devlette yer alan sanal bir tesis tanıtılmış ve kurs katılımcıları bu tesis üzerinde analizler gerçekleştirmiştir. Yerli ve millî yazılımdan elde edilen analiz sonuçları

kurs sürecinde kullanılan Sandia Laboratuvarına ait olan yazılımın sonuçları ile karşılaştırılmıştır. Sonuçların bu sanal tesis için de örtüştüğü görülmüştür. Sonuç olarak yazılımın bu haliyle beklenildiği gibi çalıştığı doğrulanmıştır.

Sonuç

Bu çalışmada nükleer emniyetin sağlanmasında ve sürdürülmesinde kritik öneme sahip olan fiziksel koruma sisteminin tasarımı ve değerlendirilmesinde öncü rol üstlenmesi beklenen yerli ve millî bir yazılım geliştirilmiştir.

Nükleer emniyet kapsamında nükleer tesislerin ve nükleer maddelerin korumasına destek olmayı hedefleyen yazılım, herhangi bir işletmenin fiziksel koruma sistemi tasarım ve değerlendirilmesinde bu haliyle temel hesaplar yapmak için kullanılabilir durumdadır. Özellikle Türkçe olarak hazırlanan yazılım Türkiye'de düzenlenecek nükleer emniyet eğitimlerinde fiziksel koruma sistemi tasarım ve değerlendirilmesi konusunun anlaşılması açısından oldukça iyi bir araç olacaktır. Yazılımın gerçek bir nükleer tesisin fiziksel koruma sisteminin değerlendirilmesinde yerli ve millî bir kaynak olarak düzenleyici kuruluş tarafından kullanılabilir olacağı düşünülmektedir.

Yazılım mevcut durumda sadece 6 bölgeye ayrılabilen bir fiziksel koruma sistemi için analize olanak vermektedir. Ancak, bu konudaki limit istenmesi halinde algoritmanın tekrar tasarlanmasıyla giderilebilir. Yazılımın İngilizce sürümü yapılabilir. Yazılımın geliştirilmesi aşamasında kullanıcıya kolaylık sağlama ve istediği tespit/geciktirme ögesini seçmesine olanak verecek şekilde bir veri tabanı oluşturulması düşünülmektedir. Böylece, kullanıcıya tesisini tasarlarken veya analizini yaparken listeden en uygun ögeyi seçerek pek çok deneme yapma şansı verilecektir. Ayrıca, mevcut nükleer tesis fiziksel koruma sistemini güçlendirmek adına çözüm önerisi sunabilecek, yani belirli bir fiziksel koruma sistemi etkinlik olasılığı değerini sağlayacak şekilde ilgili ögelerin geciktirme süreleri ile tespit olasılık değerlerinde yapılması gereken iyileştirmeleri önerecek bir analiz programının tasarlanması da düşünülmektedir.

Extended Summary

Introduction

Nuclear security deals with the physical protection of nuclear facilities and nuclear materials. In this respect, it is important to know who has what responsibilities in the hierarchy, how they are determined, what the nuclear security risk means, what is going to be protected and against who, how, and by whom, and if the protection fails what could be the potential consequences and what are the actions for mitigation.

The responsibility of the nuclear security is with the State. State must define the nuclear security regime, assign a competent authority to execute the regulations, and make sure that the competent authority is independent. The competent authority implements the regulations, issues licenses, performs inspections, and must have access to systems of accounting and control of nuclear material. The license holder is responsible for the physical protection of nuclear facilities and nuclear material that it owns.

Although there are many ways to provide nuclear security, the burden is on the physical protection system (PPS). PPS is the complete set of equipment, procedures, and behaviors. Its effectiveness must be tested and approved by the competent authority. PPS is based on detection, delay, and response.

Material and Method

The "Effectiveness Probability (P_E)" of physical protection system shows how effective is the PPS against threats especially to the design basis threat. The effectiveness probability can be calculated by multiplying the values of "Interruption Probability (P_I)" that is a measure of interruption of adversary before completing his/her task by response force and "Neutralization Probability (P_N)" that is a measure of response force's ability to neutralize the adversary. Several methods can be used to define these probabilities.

"Path Interruption Analysis" determines the path that can be used by adversary by using delay time and detection probability of each component along the path. Afterwards, P_I is calculated. On the other hand, "Adversary Sequence Diagram" is applied to figure out all possible adversary paths. These paths for theft

are assumed being bi-directional since adversary is expected to leave the facility with nuclear material while the sabotage is being one-way. By "Multipath Analysis", it is possible to figure out all adversary paths with their P_I values.

The PPS Design and Analysis Software Development

The software asks the user the detection probability and delay time of the regions around the target and the equipment used in detection and/or delay at the boundaries of these region together with response force time and the number of response force staff and adversary. At the end, the probability of effectiveness is calculated by multiplication of P_I and P_N.

The developed software calculates and reports the most critical path that the adversary will use to reach his/her goal and the critical detection point on this path.

The software is tested against theft and sabotage with 26 scenarios for each case. The results showed that the software is verified. In addition, the performance of the software for a fictitious facility used in international trainings at Sandia National Laboratory, USA was evaluated. This test proved that the software is capable of analyzing complex facilities with PPS having several components.

Conclusions

In this paper, the methodology of an indigenous and national software that can be used in the design and evaluation of PPS is explained. The software calculates the effectiveness of the PPS against a threat and determines the path that can be preferred by this threat to reach its target (the weakest link). The software is tested and verified with several scenarios.

The software, which aims to support the physical protection of nuclear facilities and nuclear materials within the scope of nuclear security, can be used to make basic analyzes for the design and evaluation of the PPS of any critical facility. Since the language of the software is Turkish, it can be used as an important tool in understanding the topic of PPS design and evaluation for nuclear security courses to be held in Türkiye. In addition, the indigenous software can be used by the regulatory authority in Türkiye to evaluate the physical protection system of nuclear facilities in Türkiye.

As future work, it is considered to create a database for PPS equipment to allow users to select the desired detection/delay item from the database. Thus, the user will be given a chance to design or analyze a facility with many scenarios. In addition, English version of the software can be made as well.

Kaynakça

Kitaplar

IAEA. (2020). *The Legal Framework for Nuclear Security*, Vienna: International Atomic Energy Agency.

IAEA. (2005). *The Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment.* Vienna: International Atomic Energy Agency.

IAEA. (2011). N*uclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*, Vienna: International Atomic Energy Agency.

Margulies, P. (2008). *Global Issues: Nuclear Nonproliferation* (sf. 3). New York: Infobase Publishing

Türkiye Cumhuriyeti Atom Enerjisi Kurumu, TC. (2012). *Nükleer Tesislerin ve Nükleer Maddelerin Fiziksel Korunması Yönetmeliği,* Ankara: T. C. Resmi Gazete 28300.

Türkiye Cumhuriyeti Nükleer Düzenleme Kurumu, TC. (2020a). *Nükleer Güvence Yönetmeliği* (2020), Ankara: T. C. Resmi Gazete 31019.

Türkiye Cumhuriyeti Nükleer Düzenleme Kurumu, TC. (2020b). *Nükleer Tesislerin ve Nükleer Maddelerin Emniyetine İlişkin Yönetmelik,* Ankara: T. C. Resmi Gazete 31207.

Türkiye Cumhuriyeti Bakanlar Kurulu, TC. (2018). *Nükleer Düzenleme Kurumunun Teşkilat ve Görevleri İle Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun Hükmünde Karaname*, Ankara: T. C. Resmi Gazete 30473.

Türkiye Cumhuriyeti Atom Enerjisi Kurumu, TC. (1983). *Nükleer Tesislere Lisans Verilmesine İlişkin Tüzük*, Ankara: T. C. Resmi Gazete 18256.

Makaleler

Gerçeker, N. (2013). Küresel Felaket: Nükleer Terörizm, Uluslararası Hukuk Çerçevesine İlişkin Bir Değerlendirme. *Savunma Bilimleri Dergisi, 12* (1). 91-95.

Elektronik Kaynaklar

Jetbrains. 25.05.2021 tarihinde https://resources.jetbrains.com/storage/products/jetbrains/docs/jet brains_corporate_overview.pdf adresinden alınmıştır.

MySQL. 25.05.2021 tarihinde http://www.mysql.com/ adresinden alınmıştır.

Python. 25.05.2021 tarihinde https://www.python.org/doc/essays/blurb/ adresinden alınmıştır.

Sandia. 25.05.2021c tarihinde https://share-ng.sandia.gov/itc/assets/hypo_fac_limp.pdf adresinden alınmıştır.

Sandia. 25.05.2021a tarihinde https://share-ng.sandia.gov/itc/assets/18_path-interruption-analysis.pdf adresinden alınmıştır.

Sandia. 25.05.2021b tarihinde https://share-ng.sandia.gov/itc/assets/21_neutralization-analysis.pdf adresinden alınmıştır.

UN. 06.06.2021'de https://www.un.org/en/conf/npt/2015/pdf/background%20info.pdf adresinden alınmştır.