MUH442 Bilişimde Güvenlik – 2

Prof. Dr. Hasan Hüseyin BALIK

(4. Hafta)

İçerik

- 2.Yönetim Sorunları
  - 2.1. BT Güvenlik Yönetimi ve Risk Değerlendirmesi
  - 2.2.BT Güvenlik Kontrolleri, Planları ve Prosedürleri
  - 2.3.Fiziksel ve Altyapı Güvenliği
  - 2.4. İnsan Kaynakları Güvenliği
  - 2.5. Güvenlik Denetimi
  - 2.6. Bilişim Güvenliğinde Yasal ve Etik Hususlar

2.3. Fiziksel ve Altyapı Güvenliği

2.3.İçerik

- Genel bakış
- Fiziksel Güvenlik Tehditleri
- Fiziksel Güvenlik Önleme ve Etki Azaltma Tedbirleri
- Fiziksel Güvenlik İhlallerinden Kurtulma
- Örnek: Kurumsal Fiziksel Güvenlik Politikası
- Fiziksel ve Mantıksal Güvenliğin Entegrasyonu

Fiziksel ve Altyapı Güvenliği

Mantıksal Güvenlik

- Bilgisayar tabanlı verileri yazılım tabanlı ve iletişim tabanlı tehditlerden korur

Fiziksel Güvenlik

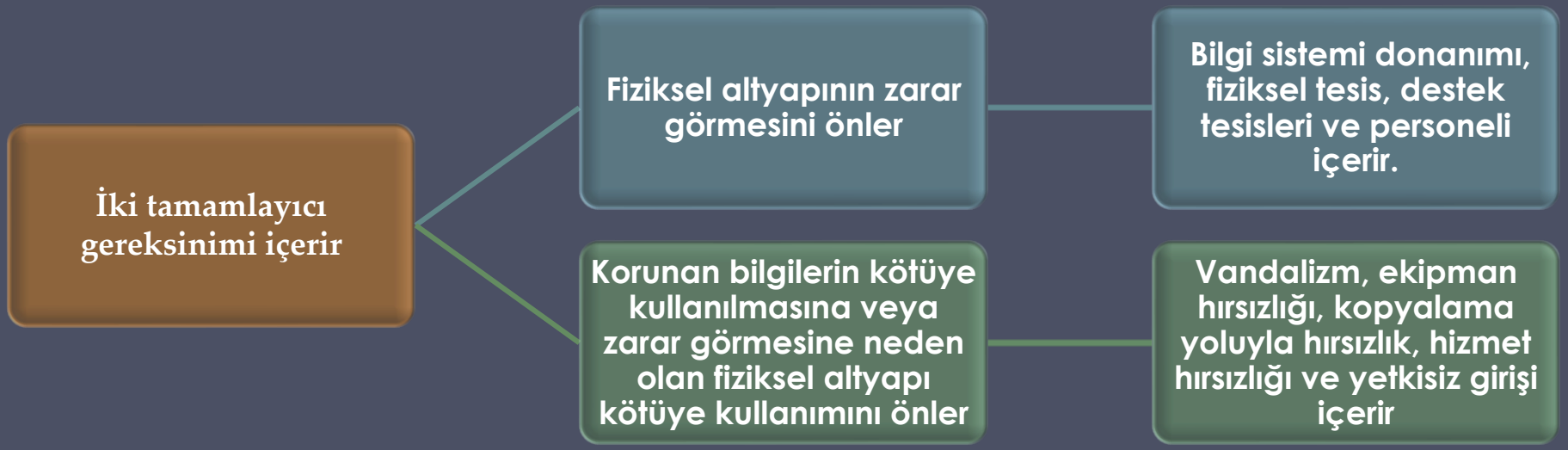
- Altyapı güvenliği de denir
- Veri içeren bilgi sistemlerini ve sistemleri kullanan, işleten ve bakımını yapan kişileri korur
- Mantıksal güvenliği tehlikeye atabilecek her türlü fiziksel erişimi veya izinsiz girişi önlemelidir

Bina Güvenliği

- Kurumsal veya tesis güvenliği olarak da bilinir
- Tüm bir alan, tesis veya bina(lar) içindeki insanları ve mülkü korur ve genellikle yasalar, yönetmelikler ve güvene dayalı yükümlülükler tarafından gerekli kılınır
- Çevre güvenliği, erişim kontrolü, duman ve yangın algılama, yangın söndürme, bazı çevre koruma ve genellikle gözetim sistemleri, alarmlar ve güvenlik personeli içerir

Fiziksel Güvenliğe Genel Bakış

- Bilgilerin depolanmasını ve işlenmesini destekleyen fiziksel varlıkları korur



Fiziksel Güvenlik Tehditleri

Bilgi sistemlerini tehdit eden fiziksel durumlar ve olaylar:

- Çevresel tehditler
- Teknik tehditler
- İnsan kaynaklı tehditler

Doğal Afetlerin Özellikleri

	Uyarı	Tahliye	Süresi
Tornado	Potansiyelin önceden uyarısı; tesise özel değil	Tesiste kal	Kısa ama yoğun
Hurricane	Önemli ön uyarı	Tahliye gerekebilir	Birkaç saatten birkaç güne
Deprrem	Uyarı yok	Tahliye edilemeyebilir	Kısa süre; devam eden artçı sarsıntı tehdidi
Buz Fırtınası/Blizzard	Genellikle birkaç gün önce uyarısı beklenir	Tahliye edilemeyebilir	Birkaç gün sürebilir
Şimşek/Yıldırım	Sensörler birkaç dakika önce uyarı verebilir	Tahliye gerekebilir	Kısa ama tekrarlayabilir
Sel/Taşkın	Genellikle birkaç gün önce uyarı beklenir	Tahliye edilemeyebilir	Tasis uzun süre izole eidlebilir

Bir tornado, tornado yolu boyunca dar bir bantta hurricane gücünü aşan rüzgarlar üretebilir.

Fujita Tornado Yoğunluk Ölçeği

Katagori	Rüzgar Hızı	Hasar
F0	0–72 mil/s 64–116 km/s	Hafif hasar. Bacalarda bazı hasarlar oluşur; ağaç dalları kırılır; sığ köklü ağaçlar devrilir; tabelalar hasar görür.
F1	73– 112 mil/s 117–180 km/s	Orta hasar. Tornado rüzgar hızının başlangıcıdır; çatı yüzeyleri soyulur; mobil evler temelden sökülür veya devrilir; hareketli arabalar yollardan savrulur.
F2	113–157 mil/s 181–252 km/s	Önemli hasar. Evlerin çatıları sökülür; mobil evler yıkılır; yük vagonlar savrulur; devrilmiş veya kökünden sökülmüş büyük ağaçlar; hafif nesneler uçuşur.
F3	158–206 mil/s 253–332 km/s	Ciddi hasar. İyi yapılmış evlerin çatıları ve bazı duvarları yıkılır; trenler devrilir ormandaki ağaçların çoğu kökünden sökülür; ağır arabalar yerden kaldırılır ve fırlatılır.
F4	207–260 mil/s 333–418 km/s	Yıkıcı hasar. İyi inşa edilmiş evler tesviye edilir; zayıf temelli yapılar biraz uzağa savrulur; fırlatılan arabalar ve büyük cisimler ucuşur.
F5	261–318 mil/s 419–512 km/s	İnanılmaz hasar. Güçlü çerçeve evler temelleri kaldırılır ve hatırı sayılır bir mesafeye savrularak parçalanır; otomobil boyutunda cisimler havada 100 metreden fazla füze gibi uçuşur; ağaçlar soyulur.

Safir/Simpson Hurricane Ölçeği

Katagori	Rüzgar Hızı	Fırtına Dalgalanması	Potansiyel Hasar
1	74–95 mil/s 119–153 km/s	4-5 ft 1-2 m	Minimal
1	96– 110 mil/s 154–177 km/s	6-8 ft 2-3 m	Orta
3	111–130 mil/s 178–209 km/s	9-12 ft 3-4 m	Yaygın
4	131–155 mil/s 210–249 km/s	13-18 ft >5 m	Yaygın
5	>155 mil/s >249 km/s	>18 ft >5 m	Katastrofik/Felaket

Bilişim Kaynaklarına Zarar Verecek Sıcaklık Eşikleri

Bileşen veya Ortam (Medya)	Hasarın Başlayabileceği Sürekli Ortam Sıcaklığı
Floppy Diskler ve manyetik kasetler vb.	38 °C (100 °F)
Optik Diskler	49 °C (120 °F)
Hard Diskler	66 °C (150 °F)
Bilgisayar bileşenleri	79 °C (175 °F)
Tehlikeli voltaj taşıyan teller üzerinde termoplastik yalıtım	125 °C (257 °F)
Kağıt ürünleri	177 °C (350 °F)

*Kaynak:*National Fire Protection Association.

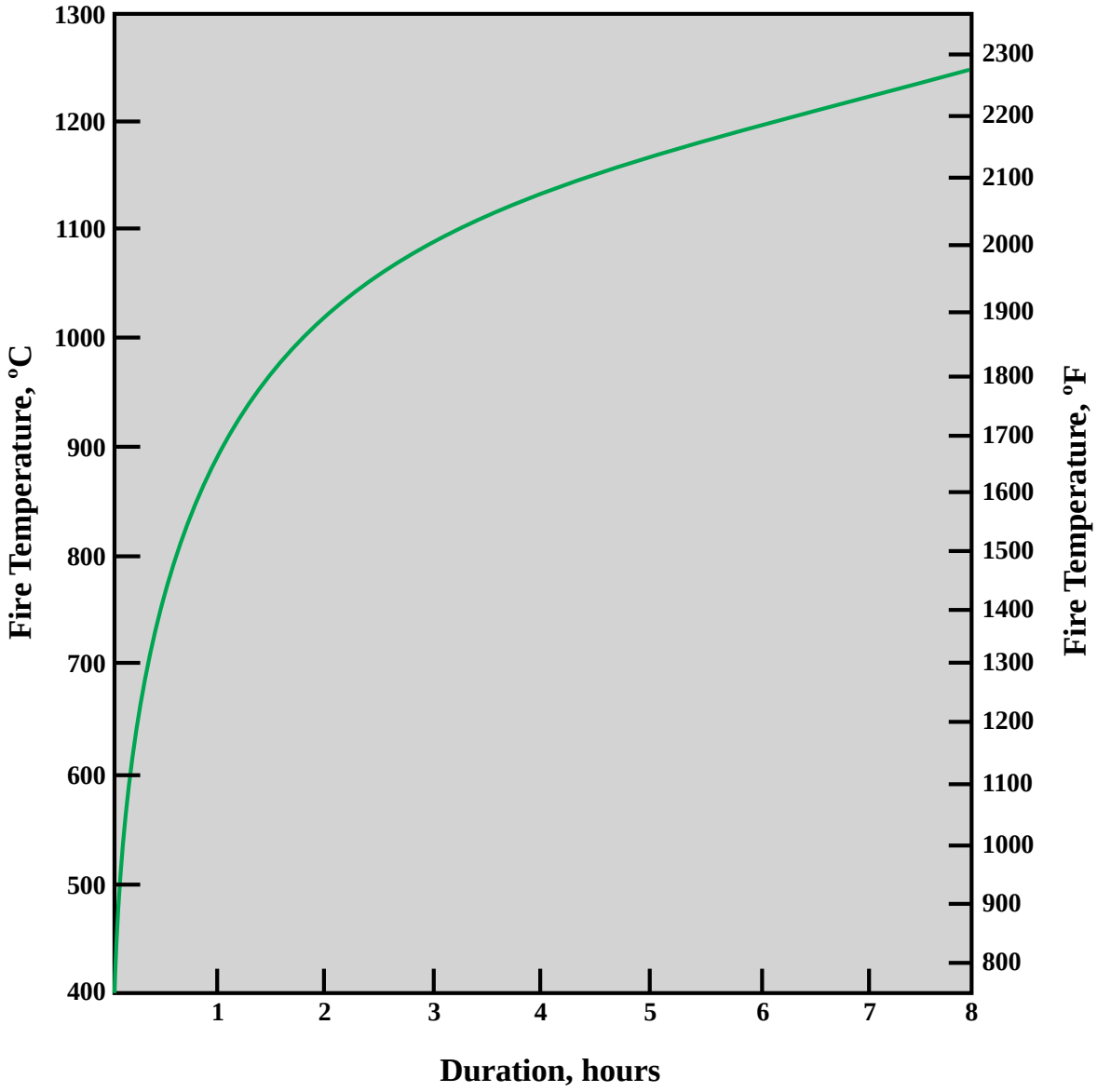


Figure 16.1 Standard Fire Temperature-Time Relations Used for Testing of Building Elements

Sıcaklığın Etkileri

Sıcaklık	Etki
260 °C (500 °F)	Ahşap tutuşur
326 °C (618 °F)	Kurşun erir
415 °C (770 °F)	Çinko erir
480 °C (896 °F)	Yalıtılmamış bir çelik malzeme bükülme ve içeriğini açığa çıkarma eğilimindedir.
625 °C (1157 °F)	Alüminyum erir
1220 °C (2228 °F)	Dökme demir erir
1410 °C (2570 °F)	Sert çelik erir

Su Hasarı

Birincil tehlike elektriksel kısa devredir

Su borusu, hattaki bir arızadan veya donmadan patlayabilir.

Sprinkler sistemleri (yangın söndürme sistemleri) yanlışlıkla devreye girebilir

Sel suyu balçık bırakır ve katı parça sürükler

İki kat yukarıdan gelen suyun tehlike oluşturmaması için gerekli özen gösterilmelidir.

Kimyasal, Radyolojik ve Biyolojik Tehlikeler

- Kasıtlı saldırıdan ve kazara tahliyeden tehdit oluşturma
- Deşarjlar havalandırma sistemi veya açık pencerelerden ve radyasyon durumunda çevre duvarlarından yapılabilir.
- Sel, biyolojik veya kimyasal kirleticileri de beraberinde getirebilir.

Toz ve İstila

Toz

- Sıklıkla gözden kaçar
- Dönen depolama ortamı ve bilgisayar fanları, hasara karşı en savunmasız olanlardır.
- Havalandırmayı da engelleyebilir
- Akışlar bir dizi şeyden kaynaklanabilir:
  - Yakındaki bir binanın kontrollü patlaması
  - Fırtına taşıyan enkaz
  - Binada inşaat veya bakım çalışmaları

İstila

- Çok çeşitli canlı organizmaları kapsar:
  - Yüksek nem koşulları küflenmeye neden olabilir
  - Böcekler, özellikle tahta ve kağıda saldıranlar

Teknik Tehditler

- Ekipmanı çalıştırmak için elektrik gücü gereklidir
  - Güç hizmeti sorunları:
    - Düşük voltaj - düşüklük/ kesintiler, hizmeti kesintiye uğratıyor
    - Aşırı voltaj - dalgalanmalar/arızalar/parlama, çipleri yok edebilir
    - Gürültü - elektrik hatlarında, cihazın çalışmasını engelleyebilir

Elektromanyetik girişim (EMI)

- Güç kaynağı hattı, motorlar, fanlar, ağır ekipman, diğer bilgisayarlar, cep telefonları, mikrodalga röle antenleri, yakındaki radyo istasyonları gürültüüretir
- Gürültü, elektrik hatlarının yanı sıra boşlıktada iletilebilir
- Bilgisayarlarda aralıklı sorunlara neden olabilir

İnsan Kaynaklı Tehditler

- Daha az öngörülebilir, önleme yöntemlerinin üstesinden gelmek için tasarlanmış, başa çıkması daha zor
- …. içerir:
  - Yetkisiz fiziksel erişim
    - Bilgi varlıkları genellikle kısıtlı alanlarda bulunur
    - Hırsızlık, vandalizm veya kötüye kullanım gibi diğer tehditlere yol açabilir
  - Ekipman/veri hırsızlığı
    - Gizli dinleme ve telefon dinleme bu kategoriye girer
    - İçeriden veya yetkisiz erişim kazanmış bir yabancı kaynaklı olabilir
  - Ekipman/veri vandalizmi
  - Kaynakların kötüye kullanılması

Fiziksel Güvenlik Önleme ve Etki Azaltma Yöntemleri

- İlk önleme önlemi, bulut bilişimin kullanılmasıdır
- Uygun olmayan sıcaklık ve nem
  - Çevre kontrol ekipmanı, güç kaynağı
- Ateş ve duman
  - Alarmlar, önleyici tedbirler, yangın azaltma
  - Duman dedektörleri, sigara içilmez
- Su
  - Hatları, ekipman konumunu, kesme sensörlerini yönet
- Diğer tehditler
  - Uygun teknik karşı önlemler, toz girişini sınırlama, haşere kontrolü

Etki Azaltma Önlemleri

Teknik Tehditler

Her kritik ekipman için kesintisiz güç kaynağı (UPS)

Kritik ekipman bir acil durum güç kaynağına (jeneratö gibi) bağlanmalıdır

Elektromanyetik parazit (EMI) ile başa çıkmak için bir filtre ve ekranlama kombinasyonu kullanılabilir

Etki Azaltma Önlemleri İnsan Kaynaklı Fiziksel Tehditler

Fiziksel erişim kontrolü

- **Bina erişimini kısıtla**
- **Kontrollü alanları korumak için güvenlik devriyesi gezdir**
- **Giriş noktalarında kilitler veya perdeleme önlemleri**
- **Hareketli kaynakları bir izleme cihazı ile donat**
- **Bir güvenlik cihazı tarafından kontrol edilen güç anahtarı kullan**
- **Hırsız sensörleri ve alarmları kullan**
- **Kayıt ve gerçek zamanlı uzaktan görüntüleme sağlayan gözetim sistemleri kur**

Kurtarma
Fiziksel Güvenlik İhlalleri

Kurtarmanın en temel unsuru yedeklemedir

- Veri kaybından kurtarma sağlar
- İdeal olarak, tüm önemli veriler saha dışında bulunmalı ve mümkün olduğunca sık güncellenmelidir.
- Toplu şifreli uzaktan yedekleme kullanabilir
- Kritik durumlar için, operasyonu anında devralmaya hazır bir uzak sıcak site oluşturulabilir.

Fiziksel ekipman hasar kurtarma

- Hasarın ve temizlemenin doğasına bağlıdır
- Olağanüstü durum kurtarma uzmanlarına ihtiyaç duyabilir

Fiziksel ve Mantıksal Güvenlik Entegrasyonu

- Çok sayıda algılama ve önleme cihazı
- Merkezi bir kontrol varsa daha etkilidir
- Otomatikleştirilmiş fiziksel ve mantıksal güvenlik işlevlerini entegre edin
  - Tek bir kimlik kartı kullanın
  - Tek adımlı kart kaydı ve sonlandırma
  - Merkezi kimlik yönetim sistemi
  - Birleşik olay izleme ve korelasyon
- Bu alanda standartlara ihtiyaç var
  - FIPS 201-1 *"Federal Çalışanların ve Yüklenicilerin Kişisel Kimlik Doğrulaması (PIV)"*

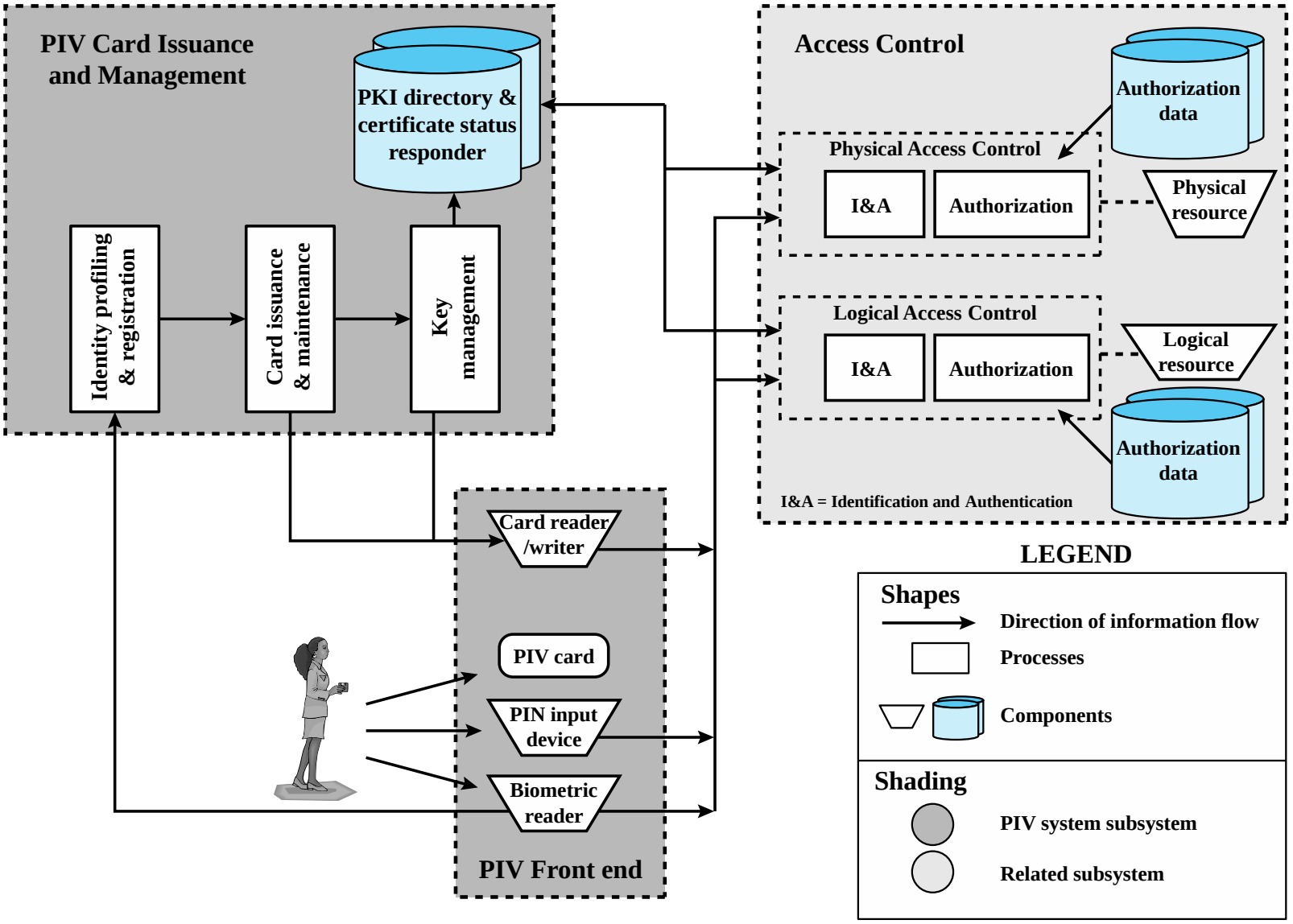


Figure 16.2 FIPS 201 PIV System Model

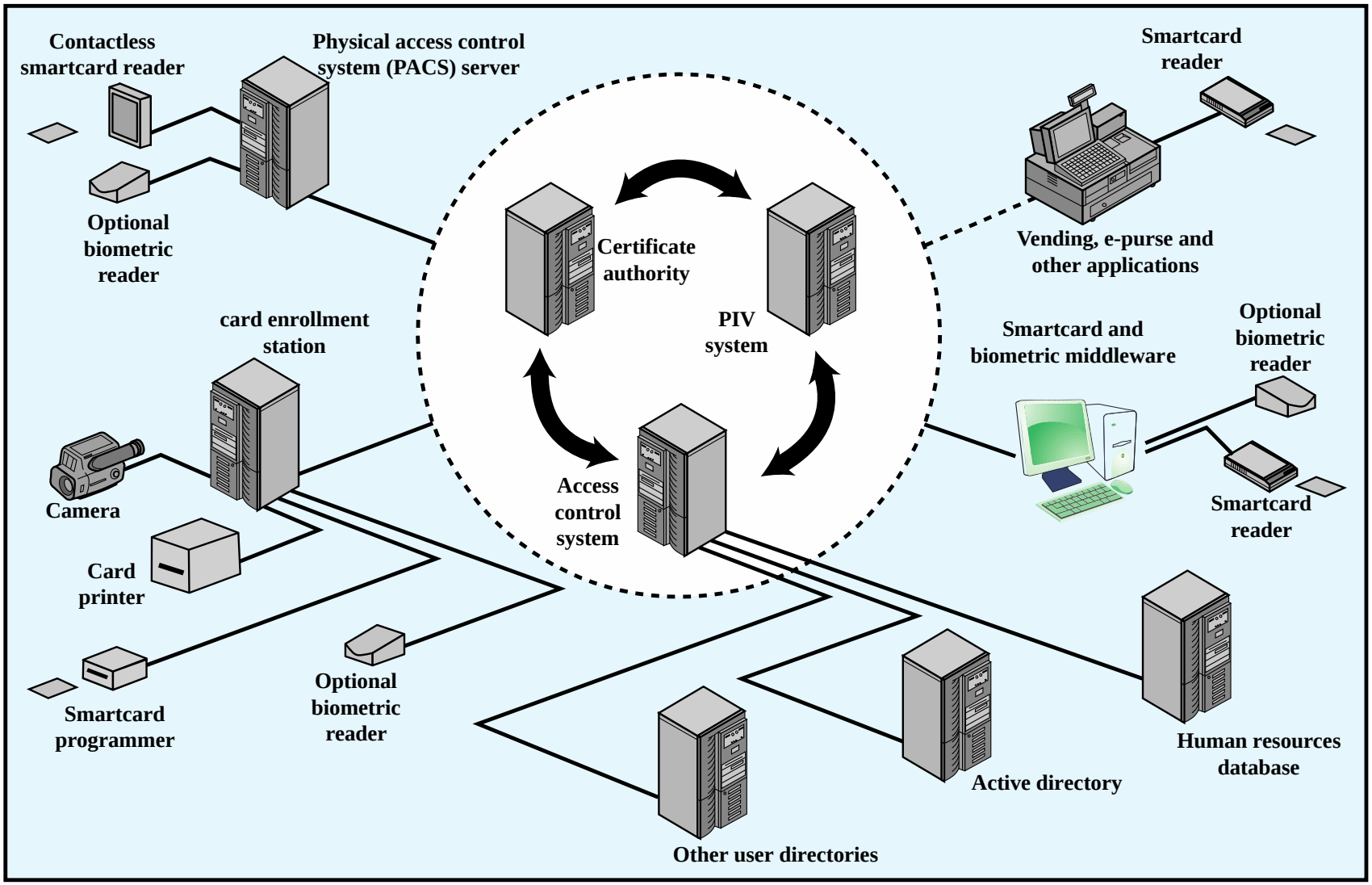
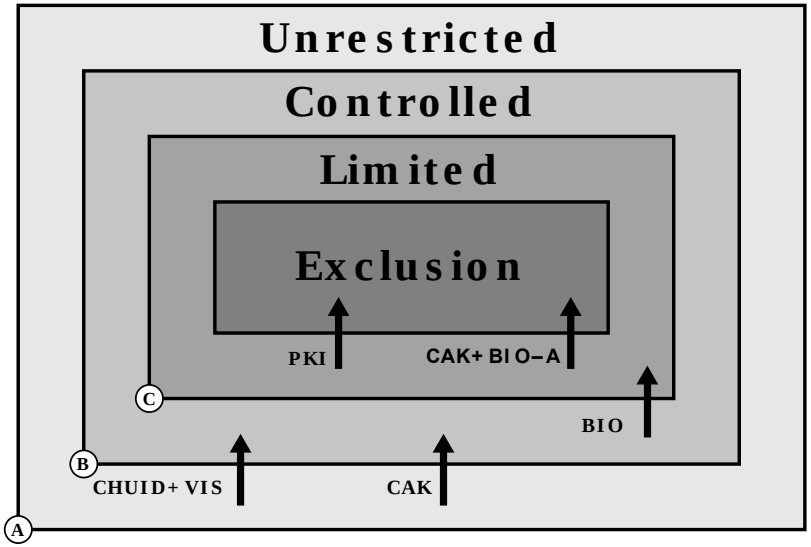


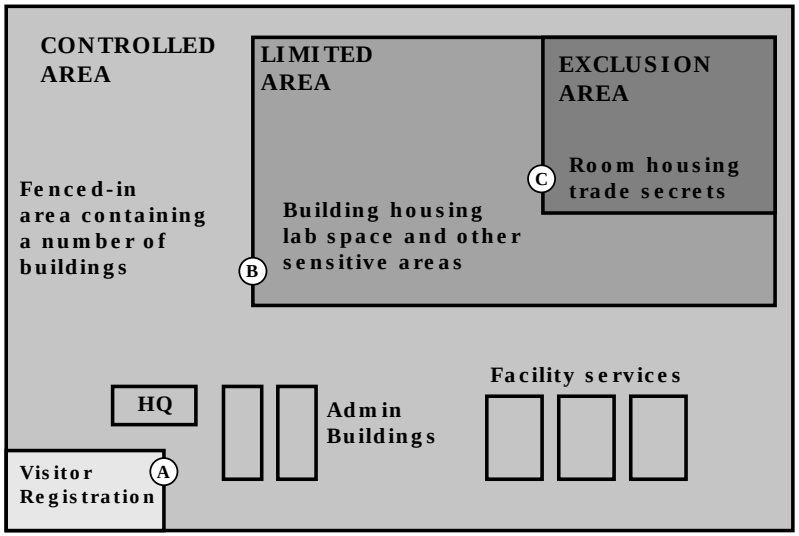
Figure 16.3 Convergence Example

Korunan Alanlar için Güvenlik ve Kontrol Dereceleri

Sınıfı	Tanım
Sınırsız	Güvenlikle ilgisi olmayan bir tesis alanı.
Kontrollü	Kısıtlı bir alanın, genellikle sınırlı veya hariç tutulan bir alana yakın veya onu çevreleyen bölümü. Kontrollü alana giriş, erişim ihtiyacı olan personel ile sınırlıdır. Yetkili personelin bu alan içindeki hareketi mutlaka kontrol edilmez, çünkü alana yalnızca giriş güvenlik çıkarlarına erişim sağlamaz. Kontrollü alan, idari kontrol için, güvenlik için veya sınırlı veya hariç tutulan alan için derinlemesine güvenlik için bir tampon bölge olarak sağlanır.
Kısıtlı	Bir güvenlik bölgesinin yakınında bulunan kısıtlı alan. Kontrolsüz hareket, menkul kıymet çıkarlarına erişime izin verebilir. Eskortlar ve diğer dahili kısıtlamalar, sınırlı alanlarda erişimi engelleyebilir.
Girilmez	Bir güvenlik alanı. Kontrolsüz hareket, güvenliğe doğrudan tecavüz anlamına gelir.



(a) Access Control Model



(b) Example Use

Figure 16.4 Use of Authentication Mechanisms for Physical Access Control