IT522 – Yazılım Mühendisliği 2021

PhD Furkan Gözükara, Toros University

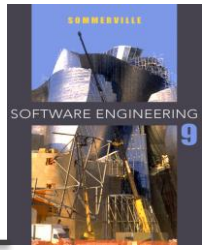
https://github.com/FurkanGozukara/Yazilim-Muhendisligi-IT522-2021

Ders 12

Güvenilebilirlik ve Güvenlik Özellikleri

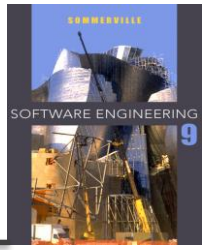
Kaynak : https://ifs.host.cs.st-andrews.ac.uk/Books/SE9/Presentations/index.html

Bölüm 1 İşlenmiş Konular



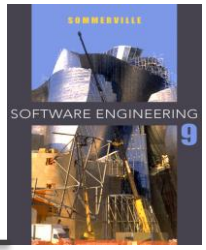
- Risk odaklı özellikler
- Güvenlik spesifikasyonu
- Güvenlik belirtimi
- Yazılım güvenilirliği özelliği

Güvenilebilirlik Gereksinimleri



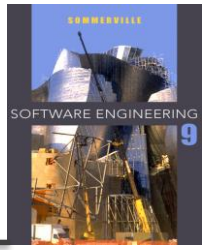
- Hata kontrol ve kurtarma olanaklarını ve sistem arızalarına karşı korumayı tanımlamak için işlevsel gereksinimler.
- Sistemin gerekli güvenilirliğini ve kullanılabilirliğini tanımlayan işlevsel olmayan gereksinimler.
- Ortaya çıkmaması gereken durumları ve koşulları tanımlayan gereksinimler hariçtir.

Risk Odaklı Özellikler



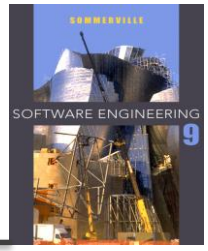
- Kritik sistem özellikleri risk odaklı olmalıdır.
- Bu yaklaşım, emniyet ve güvenlik açısından kritik sistemlerde yaygın olarak kullanılmaktadır.
- Spesifikasyon sürecinin amacı, sistemin karşı karşıya olduğu riskleri (emniyet, güvenlik vb.) anlamak ve bu riskleri azaltan gereksinimleri tanımlamak olmalıdır.

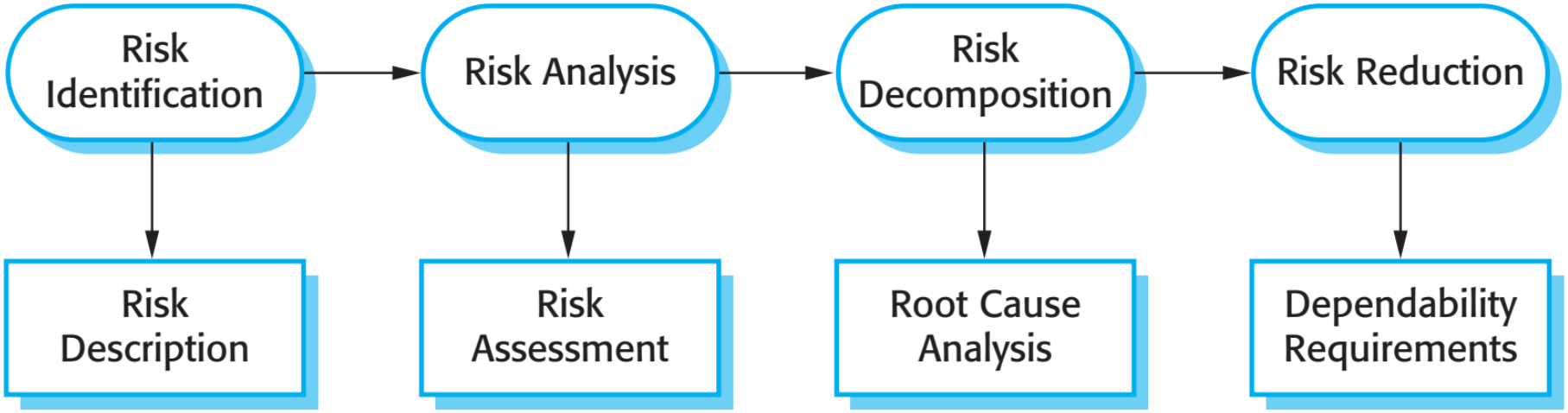
Risk Bazlı Analizin Aşamaları



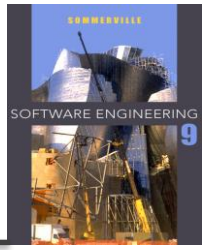
- Risk tanımlaması
  - Ortaya çıkabilecek olası riskleri belirleyin.
- Risk analizi ve sınıflandırma
  - Her bir riskin ciddiyetini değerlendirin.
- Risk ayrışımı
  - Potansiyel temel nedenlerini keşfetmek için riskleri ayrıştırın.
- Risk azaltma değerlendirmesi
  - Sistem tasarlanırken her bir riskin nasıl ortadan kaldırılması veya azaltılması gerektiğini tanımlayın.

Risk Odaklı Özellikler



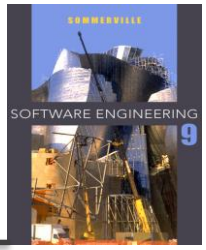


Aşamalı Risk Analizi



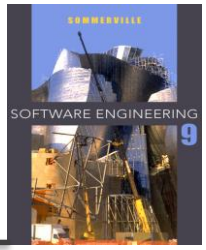
- Ön risk analizi
  - Sistem ortamından gelen riskleri belirler. Amaç, başlangıçta bir dizi sistem güvenliği ve güvenilebilirlik gereksinimleri geliştirmektir.
- Yaşam döngüsü risk analizi
  - Tasarım ve geliştirme sırasında ortaya çıkan riskleri, örneğin sistem yapımı için kullanılan teknolojilerle ilişkili riskleri tanımlar. Bu risklere karşı koruma sağlamak için gereksinimler genişletilmiştir.
- Operasyonel risk analizi
  - Sistem kullanıcı arayüzü ve operatör hatalarıyla ilişkili riskler. Bunlarla başa çıkmak için daha fazla koruma gereksinimleri eklenebilir.

Güvenlik Spesifikasyonu



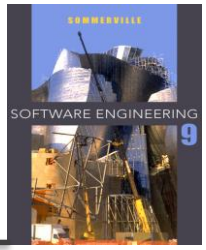
- Amaç, sistem arızalarının yaralanmaya, ölüme veya çevresel zarara neden olmamasını sağlayan koruma gereksinimlerini belirlemektir.
- Risk tanımlama = Tehlike tanımlama
- Risk analizi = Tehlike değerlendirmesi
- Risk ayrışımı = Tehlike analizi
- Risk azaltma = güvenlik gereksinimleri spesifikasyonu

Tehlike Tanımlama



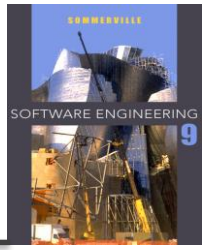
- Sistemi tehdit edebilecek tehlikeleri belirleyin.
- Tehlike tanımlaması, farklı tehlike türlerine dayalı olabilir:
  - Fiziksel riskler
  - Elektriksel tehlikeler
  - Biyolojik tehlikeler
  - Servis arızası tehlikeleri
  - Vb.

İnsülin Pompası Riskleri



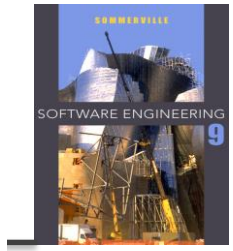
- İnsülin aşırı doz (servis hatası).
- İnsülin düşük dozu (servis hatası).
- Bitmiş pil (elektrik) nedeniyle elektrik kesintisi.
- Diğer tıbbi ekipmanlarla (elektrik) elektriksel parazit.
- Zayıf sensör ve aktüatör teması (fiziksel).
- Makinenin parçaları vücutta kırılıyor (fiziksel).
- Makinenin girişinden kaynaklanan enfeksiyon (biyolojik).
- Malzemelere veya insüline alerjik reaksiyon (biyolojik).

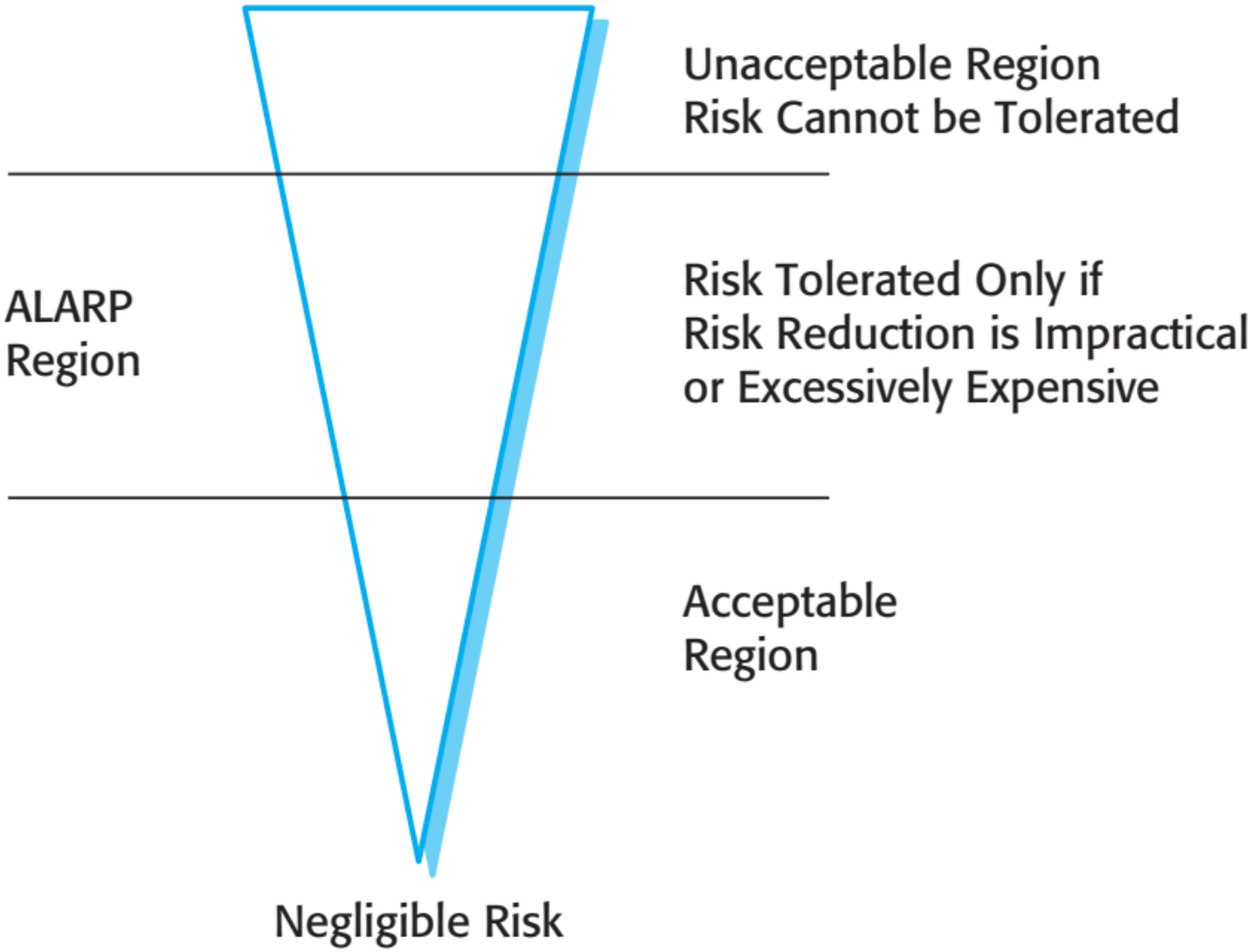
Tehlike Değerlendirmesi



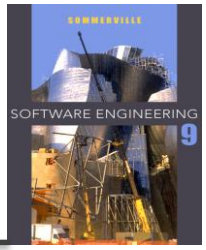
- Süreç, bir riskin ortaya çıkma olasılığını ve bir kaza veya olayın meydana gelmesi durumunda ortaya çıkabilecek olası sonuçları anlamakla ilgilidir.
- Riskler şu şekilde kategorize edilebilir:
  - Dayanılmaz. Asla ortaya çıkmamalı veya bir kazaya neden olmamalıdır
  - Makul ölçüde pratik olduğu kadar düşük (MÖPOKD). Maliyet ve program kısıtlamaları göz önüne alındığında risk olasılığını en aza indirmelidir
  - Kabul edilebilir. Riskin sonuçları kabul edilebilirdir ve tehlike olasılığını azaltmak için hiçbir ekstra maliyet yapılmamalıdır.

Risk Üçgeni


SOMMERVILLE
SOFTWARE ENGINEERING
9

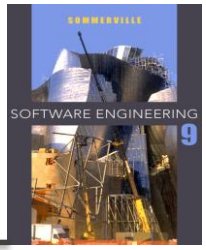

Unacceptable Region
Risk Cannot be Tolerated
ALARP
Region
Risk Tolerated Only if
Risk Reduction is Impractical
or Excessively Expensive
Acceptable
Region
Negligible Risk

Riskin Sosyal Olarak Kabul Edilebilirliği



- Bir riskin kabul edilebilirliği insani, sosyal ve politik hususlar tarafından belirlenir.
- Çoğu toplumda, bölgeler arasındaki sınırlar zamanla yukarı doğru itilir, yani toplum riski kabul etmeye daha az isteklidir
  - Örneğin, kirliliği temizlemenin maliyeti, onu önlemenin maliyetinden daha az olabilir, ancak bu sosyal olarak kabul edilebilir olmayabilir.
- Risk değerlendirmesi özneldir
  - Riskler olası, olası değil vb. olarak tanımlanır. Bu, değerlendirmeyi kimin yaptığına bağlıdır.

Tehlike Değerlendirmesi

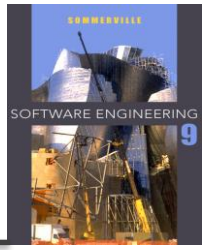


- Risk olasılığını ve risk şiddetini tahmin edin.
- Normalde bunu tam olarak yapmak mümkün değildir, bu nedenle 'olası değil', 'nadir', 'çok yüksek' gibi göreceli değerler kullanılır.
- Amaç, ortaya çıkması muhtemel veya yüksek ciddiyeti olan riskleri dışlamak olmalıdır.

İnsülin Pompası İçin Risk Sınıflandırması

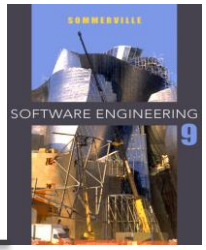
Tanımlanmış tehlike	Tehlike olasılığı	Kaza şiddeti	Tahmini risk	Kabul edilebilirlik
1. İnsülin aşırı doz hesaplaması	Orta	Yüksek	Yüksek	Tahammül edilemez
2. İnsülin düşük doz hesaplaması	Orta	Düşük	Düşük	Kabul edilebilir
3. Donanım izleme sisteminin arızalanması	Orta	Orta	Düşük	MÖPOKD
4. Elektrik kesintisi	Yüksek	Düşük	Düşük	Kabul edilebilir
5. Makine yanlış takılmış	Yüksek	Yüksek	Yüksek	Tahammül edilemez
6. Hastada makine kırılmaları	Düşük	Yüksek	Orta	MÖPOKD
7. Makine enfeksiyona neden oluyor	Orta	Orta	Orta	MÖPOKD
8. Elektriksel parazit	Düşük	Yüksek	Orta	MÖPOKD
9. Alerjik reaksiyon	Düşük	Düşük	Düşük	Kabul edilebilir

Tehlike Analizi



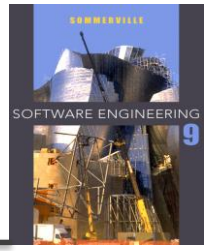
- Belirli bir sistemdeki risklerin temel nedenlerini keşfetmeyle ilgilenir.
- Teknikler çoğunlukla güvenlik açısından kritik sistemlerden türetilmiştir ve
  - Endüktif, aşağıdan yukarıya teknikler. Önerilen bir sistem arızasıyla başlayın ve bu arızadan kaynaklanabilecek tehlikeleri değerlendirin;
  - Tümdengelimli, yukarıdan aşağıya teknikler. Bir tehlike ile başlayın ve bunun nedenlerinin ne olabileceğini belirleyin.

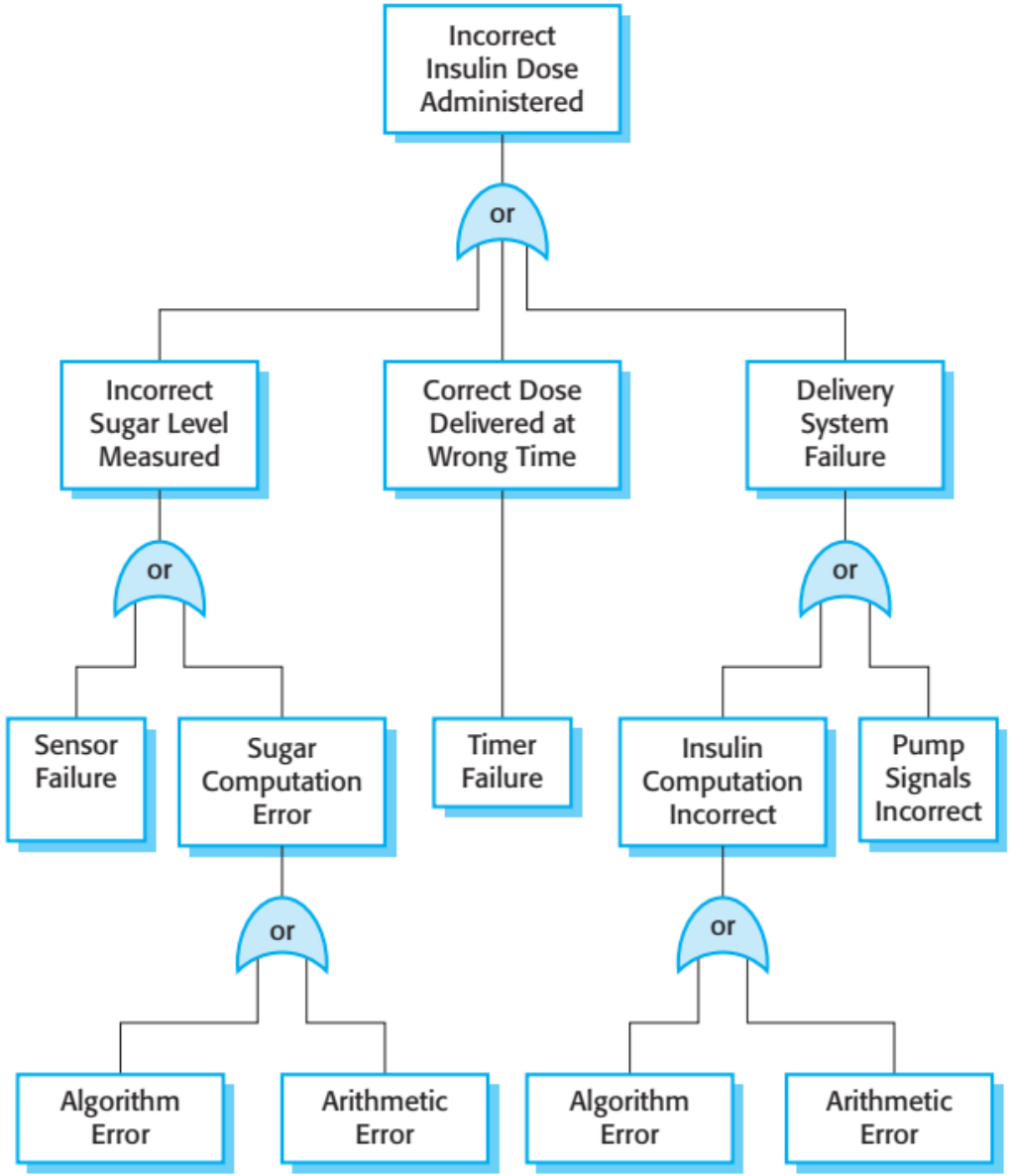
Hata Ağacı Analizi



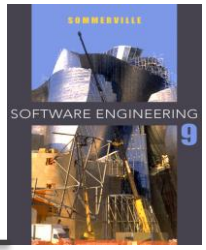
- Tümdengelimli yukarıdan aşağıya bir teknik.
- Riski veya tehlikeyi ağacın köküne koyun ve bu tehlikeye yol açabilecek sistem durumlarını belirleyin.
- Uygun olduğu durumlarda, bunları 've' veya 'veya' koşullarıyla ilişkilendirin.
- Hedef, sistem arızasının tekil nedenlerinin sayısını en aza indirmek olmalıdır.

Yazılım Hatası Ağacına Bir Örnek



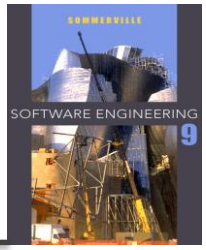


Hata Ağacı Analizi



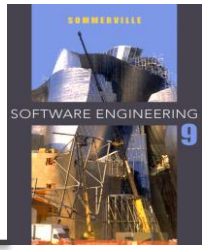
- Yanlış insülin dozunun verilmesine yol açabilecek üç olası durum
  - Kan şekeri seviyesinin yanlış ölçümü
  - Teslimat sisteminin başarısızlığı
  - Yanlış zamanda verilen doz
- Hata ağacının analizi ile, yazılımla ilgili bu tehlikelerin temel nedenleri şunlardır:
  - Algoritma hatası
  - Aritmetik hata

Risk Azaltma



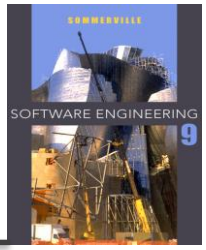
- Bu sürecin amacı, risklerin nasıl yönetilmesi gerektiğini belirleyen ve kazaların / olayların ortaya çıkmamasını sağlayan güvenilirlik gereksinimlerini belirlemektir.
- Risk azaltma stratejileri
  - Riskten kaçınma;
  - Risk tespiti ve ortadan kaldırılması;
  - Hasar sınırlaması.

Strateji Kullanımı



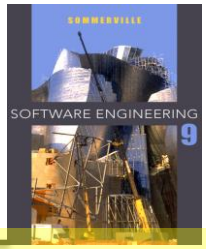
- Normalde, kritik sistemlerde, risk azaltma stratejilerinin bir karışımı kullanılır.
- Bir kimyasal tesis kontrol sisteminde, sistem reaktördeki aşırı basıncı tespit etmek ve düzeltmek için sensörler içerecektir.
- Bununla birlikte, tehlikeli derecede yüksek basınç algılandığında bir tahliye vanası açan bağımsız bir koruma sistemi de içerecektir.

İnsülin Pompası - Yazılım Riskleri



- Aritmetik hata
  - Bir hesaplama, bir değişkenin değerinin taşmasına veya yetersiz kalmasına neden olur;
  - Belki her aritmetik hata türü için bir istisna işleyicisi içerebilir.
- Algoritmik hata
  - Verilecek dozu önceki dozla veya güvenli maksimum dozlarla karşılaştırın. Çok yüksekse dozu azaltın.

Güvenlik Gereksinimleri Örnekleri



SR1 : Sistem, bir sistem kullanıcısı için belirtilen maksimum dozdan daha fazla olan tek bir doz insülin vermeyecektir.

SR2 : Sistem, bir sistem kullanıcısı için belirtilen maksimum günlük dozdan daha fazla olan günlük kümülatif bir insülin dozu vermeyecektir.

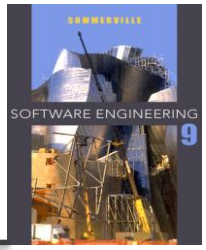
SR3 : Sistem, saatte en az dört kez çalıştırılacak bir donanım control / doğrulama olanağı içerecektir.

SR4 : Sistem, Tablo 3'te tanımlanan tüm istisnalar için bir istisna işleyicisi **içermelidir** .

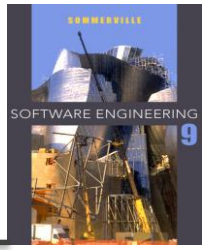
SR5 : Herhangi bir donanım veya yazılım anormalliği tespit edildiğinde sesli alarm **çalacak** ve Tablo 4'te tanımlandığı gibi bir teşhis mesajı görüntülenecektir.

SR6 : Bir alarm durumunda, kullanıcı sistemi sıfırlayıp alarmı temizleyene kadar insülin iletimi askıya alınacaktır.

Bölüm 1'in Anahtar Noktaları



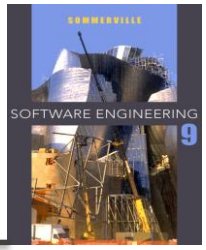
- Risk analizi, güvenlik ve güvenilirlik gereksinimlerinin belirlenmesinde önemli bir faaliyettir. Kazalara veya olaylara neden olabilecek risklerin tanımlanmasını içerir.
- Bir sistemin güvenlik gereksinimlerini anlamak için tehlike odaklı bir yaklaşım kullanılabilir. Potansiyel tehlikeleri belirler ve kök nedenlerini keşfetmek için bunları (hata ağacı analizi gibi yöntemleri kullanarak) ayrıştırırsınız.
- Tehlikelerin ve kazaların ortaya çıkmamasını sağlamak veya bu imkansızsa, sistem arızasının neden olduğu hasarı sınırlamak için güvenlik gereksinimleri dahil edilmelidir.



Ders 12 - Güvenilirlik ve Güvenlik Özellikleri

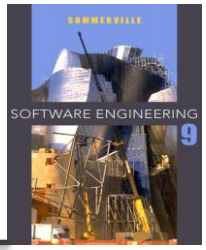
Bölüm 2

Sistem Güvenilirliği Özelliği



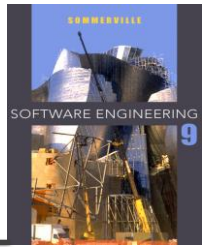
- Güvenilirlik ölçülebilir bir sistem özelliğidir, bu nedenle işlevsel olmayan güvenilirlik gereksinimleri nicel olarak belirtilebilir. Bunlar, sistemin normal kullanımı sırasında kabul edilebilir arıza sayısını veya sistemin mevcut olması gereken zamanı tanımlar.
- İşlevsel güvenilirlik gereksinimleri, yazılımdaki hataları önleyen, algılayan veya tolere eden sistem ve yazılım işlevlerini tanımlar ve böylece bu hataların sistem arızasına yol açmamasını sağlar.
- Donanım hatası veya operatör hatasıyla başa çıkmak için yazılım güvenilirliği gereksinimleri de dahil edilebilir.

Güvenilirlik Şartname Süreci



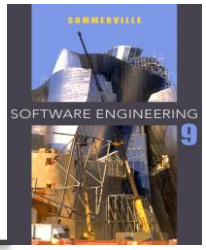
- Risk tanımlaması
  - Ekonomik kayıplara yol açabilecek sistem arızası türlerini belirleyin.
- Risk analizi
  - Farklı yazılım hatası türlerinin maliyetlerini ve sonuçlarını tahmin edin.
- Risk ayrışımı
  - Sistem arızasının temel nedenlerini belirleyin.
- Risk azaltma
  - Kabul edilebilir arıza seviyelerini tanımlayan nicel gereksinimler dahil olmak üzere güvenilirlik spesifikasyonları oluşturun.

Sistem Arızası Türleri



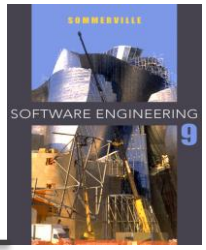
Başarısızlık türü	Açıklama
Hizmet kaybı	Sistem kullanılamıyor ve hizmetlerini kullanıcılara sunamıyor. Kritik olmayan hizmetlerdeki bir arızanın sonuçlarının kritik hizmet arızasının sonuçlarından daha az olduğu durumlarda, bunu kritik hizmetlerin kaybına ve kritik olmayan hizmetlerin kaybına ayırabilirsiniz.
Hatalı hizmet teslimi	Sistem kullanıcılara doğru bir hizmet sunmuyor. Yine bu, kritik ve kritik olmayan hizmetlerin sunumundaki küçük ve büyük hatalar veya hatalar açısından belirtilebilir.
Sistem / veri bozulması	Sistemin arızalanması, sistemin kendisine veya verilerine zarar verir. Bu genellikle, ancak zorunlu olarak diğer arıza türleri ile bağlantılı olacaktır.

Güvenilirlik Ölçütleri



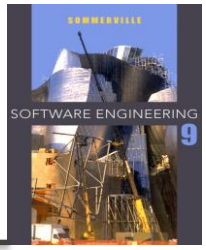
- Güvenilirlik ölçütleri, sistem güvenilirliğinin ölçü birimleridir.
- Sistem güvenilirliği, operasyonel arızaların sayısı sayılarak ve uygun olduğu durumlarda, bunlar sistem üzerinde yapılan talepler ve sistemin operasyonel olduğu süre ile ilişkilendirilerek ölçülür.
- Kritik sistemlerin güvenilirliğini değerlendirmek için uzun vadeli bir ölçüm programı gereklidir.
- Metrikler
  - Talep üzerine arıza olasılığı
  - Arızaların gerçekleşme oranı / Ortalama arızaya kadar geçen süre
  - Kullanılabilirlik

Talep Üzerine Arıza Olasılığı (TÜAO)



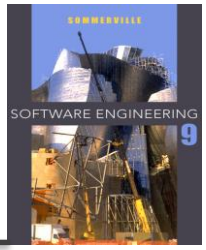
- Bu, bir servis talebi yapıldığında sistemin başarısız olma olasılığıdır. Servis talepleri aralıklı ve nispeten seyrek olduğunda kullanışlıdır.
- Hizmetlerin ara sıra talep edildiği ve hizmetin teslim edilmemesi durumunda ciddi sonuçların olduğu koruma sistemleri için uygundur.
- İstisna yönetimi bileşenlerine sahip birçok güvenlik açısından kritik sistemle ilgilidir
  - Bir kimya tesisinde acil kapatma sistemi.

Arıza Oluşma Oranı (AOO)



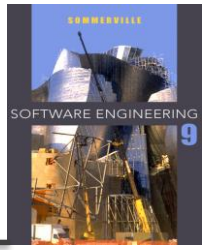
- Sistemde arıza oluşma oranını yansıtır.
- 0,002'lik AOO, her 1000 operasyonel zaman biriminde 2 arızanın muhtemel olduğu anlamına gelir, örn. 1000 saatlik çalışma başına 2 arıza.
- Sistemin kısa sürede çok sayıda benzer isteği işlemek zorunda olduğu sistemler için geçerlidir
  - Kredi kartı işlem sistemi, havayolu rezervasyon sistemi.
- AOO'nun Karşılıklı Ortalama Başarısız Olma Süresidir (KOBOS)
  - Uzun işlemlerin olduğu sistemler için geçerlidir, yani sistem işlemenin uzun sürdüğü yerler (örneğin CAD sistemleri). MTTF, beklenen işlem uzunluğundan daha uzun olmalıdır.

Kullanılabilirlik



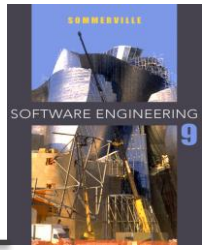
- Sistemin kullanıma hazır olduğu sürenin ölçüsü.
- Onarım ve yeniden başlatma zamanını hesaba katar
- 0,998'in kullanılabilirliği, yazılımın 1000 zaman biriminden 998'i için kullanılabilir olduğu anlamına gelir.
- Kesintisiz, sürekli çalışan sistemler için geçerlidir
  - telefon anahtarlama sistemleri, demiryolu sinyalizasyon sistemleri.

Kullanılabilirlik Belirtimi



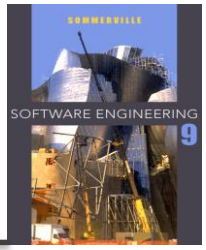
Kullanılabilirlik	Açıklama
0,9	Sistem, zamanın %90'ı için kullanılabilir. Bu, 24 saatlik bir süre içinde (1.440 dakika) sistemin 144 dakika süreyle kullanılamayacağı anlamına gelir.
0,99	24 saatlik bir süre içinde, sistem 14,4 dakika süreyle kullanılamaz.
0,999	Sistem, 24 saatlik bir süre içinde 84 saniye süreyle kullanılamaz.
0,9999	Sistem 24 saatlik bir süre içinde 8,4 saniye süreyle kullanılamaz. Kabaca haftada bir dakika.

Başarısızlık Sonuçları



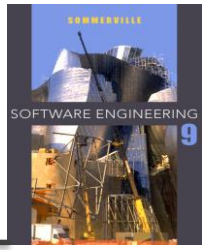
- Güvenilirliği belirtirken, önemli olan sadece sistem arızalarının sayısı değil, aynı zamanda bu arızaların sonuçlarıdır.
- Ciddi sonuçları olan arızalar, onarım ve kurtarmanın basit olduğu durumlara göre açıkça daha zarar vericidir.
- Bu nedenle bazı durumlarda, farklı arıza türleri için farklı güvenilirlik özellikleri tanımlanabilir.

Güvenilirliğin Aşırı Spesifikasyonu



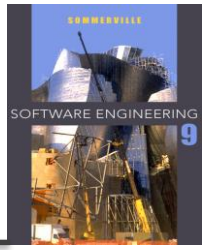
- Güvenilirliğin aşırı belirtilmesi, yüksek düzeyde güvenilirliğin belirlendiği bir durumdur, ancak bunu başarmak uygun maliyetli değildir.
- Çoğu durumda, hataların meydana gelmesini önlemek yerine kabul etmek ve bunlarla başa çıkmak daha ucuzdur.
- Aşırı spesifikasyonu önlemek için
  - Farklı arıza türleri için güvenilirlik gereksinimlerini belirtin. Küçük hatalar kabul edilebilir.
  - Farklı hizmetler için gereksinimleri ayrı ayrı belirtin. Kritik hizmetler, en yüksek güvenilirlik gereksinimlerine sahip olmalıdır.
  - Yüksek güvenilirliğin gerçekten gerekli olup olmadığına veya güvenilirlik hedeflerine başka bir yolla ulaşılıp ulaşılamayacağına karar verin.

Güvenilirlik Spesifikasyonuna Giden Adımlar



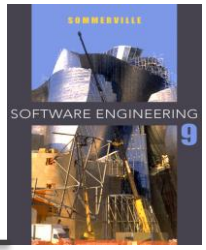
- Her bir alt sistem için olası sistem arızalarının sonuçlarını analiz edin.
- Sistem arızası analizinden, arızaları uygun sınıflara ayırın.
- Tanımlanan her bir başarısızlık sınıfı için, uygun bir ölçüt kullanarak güvenilirliği belirleyin. Farklı güvenilirlik gereksinimleri için farklı ölçütler kullanılabilir.
- Kritik arıza olasılığını azaltmak için işlevsel güvenilirlik gereksinimlerini belirleyin.

İnsülin Pompası Özellikleri



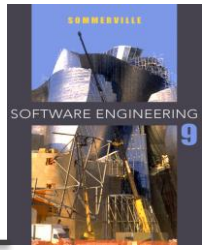
- Başarısızlık olasılığı (TÜAO) en uygun ölçüdür.
- Makinenin yeniden kalibrasyonu gibi kullanıcı eylemleriyle onarılabilen geçici arızalar. Nispeten düşük bir TÜAO değeri kabul edilebilir (örneğin 0,002) - her 500 talepte bir arıza meydana gelebilir.
- Kalıcı arızalar, yazılımın üretici tarafından yeniden yüklenmesini gerektirir. Bu, yılda bir defadan fazla olmamalıdır. Bu durum için TÜAO 0,00002'den az olmalıdır.

İşlevsel Güvenilirlik Gereksinimleri



- Bir arızaya yol açmadan önce yanlış verilerin tespit edilmesini sağlamak için kontrolleri tanımlayan gereksinimleri kontrol etmek.
- Bir arıza meydana geldikten sonra sistemin kurtarılmasına yardımcı olmak için düzenlenmiş kurtarma gereksinimleri.
- Dahil edilecek sistemin yedek özelliklerini belirten yedeklilik gereksinimleri.
- Kullanılacak geliştirme sürecini belirleyen güvenilirlik için süreç gereksinimleri de dahil edilebilir.

AS-HYS İçin İşlevsel Güvenilirlik Gereksinimlerine Örnekler



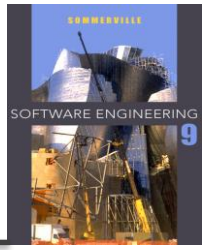
RR1 : Tüm operatör girişleri (örneğin ilaç dozu) için önceden tanımlanmış bir aralık tanımlanacak ve sistem, tüm operatör girişlerinin bu önceden tanımlanmış aralığa girdiğini kontrol etmelidir. (Kontrol etme)

RR2: Hasta veri tabanının kopyaları, aynı binada bulunmayan iki ayrı sunucuda saklanacaktır. (Kurtarma, artıklık)

RR3: N-versiyonu (örneğin sistemin 2 farklı versiyonu) programlama, frenleme kontrol sistemini uygulamak için kullanılacaktır. (Yedeklilik)

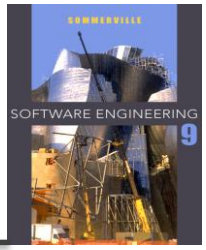
RR4: Sistem, Ada'nın güvenli bir alt kümesinde uygulanmalı ve statik analiz kullanılarak kontrol edilmelidir. (Süreç)

Güvenlik Özellikleri



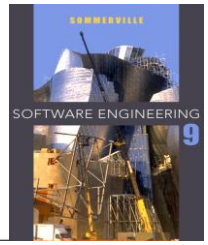
- Güvenlik spesifikasyonunun güvenlik gereksinimleri spesifikasyonuyla ortak bir yönü vardır - her iki durumda da endişeniz kötü bir şey olmasını önlemektir.
- Dört büyük fark
  - Emniyet sorunları tesadüfi - yazılım düşmanca bir ortamda çalışmıyor. Güvenlik açısından, saldırganların sistem zayıflıkları hakkında bilgi sahibi olduğunu varsaymalısınız.
  - Güvenlik arızaları meydana geldiğinde, başarısızlığa neden olan temel nedeni veya zayıflığı arayabilirsiniz. Başarısızlık kasıtlı bir saldırıdan kaynaklandığında, saldırgan başarısızlığın nedenini gizleyebilir.
  - Bir sistemi kapatmak, güvenlikle ilgili bir arızayı önleyebilir. Kapanmaya neden olmak bir saldırının amacı olabilir.
  - Emniyetle ilgili olaylar zeki bir düşman tarafından oluşturulmaz. Bir saldırgan, zayıflıkları keşfetmek için zaman içinde savunmaları araştırabilir.

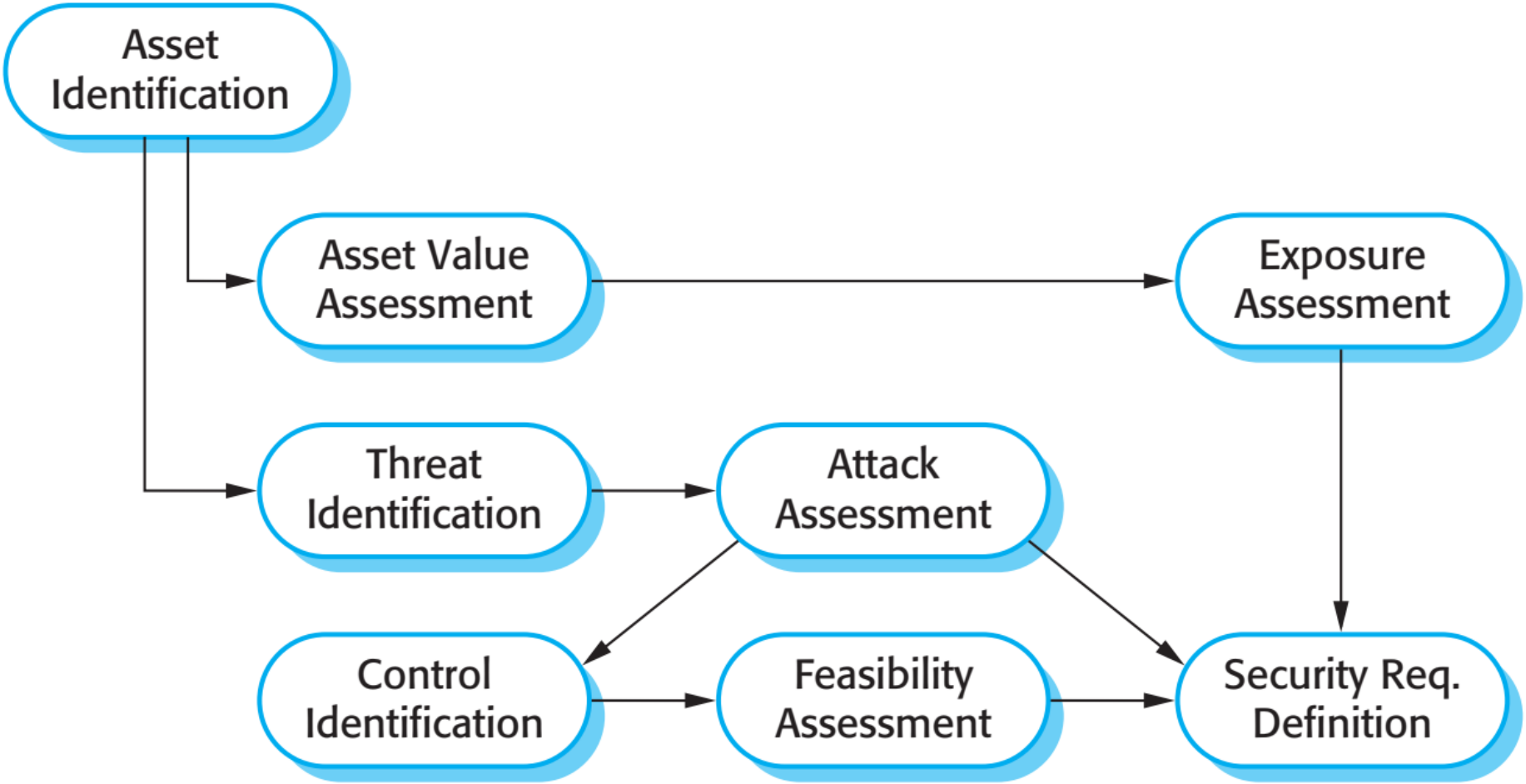
Güvenlik Gereksinimi Türleri



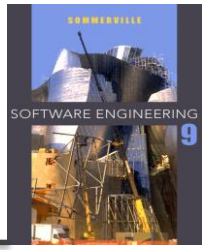
- Tanımlama gereksinimleri.
- Kimlik doğrulama gereksinimleri.
- Yetkilendirme gereksinimleri.
- Bağışıklık gereksinimleri.
- Bütünlük gereksinimleri.
- Saldırı tespiti gereksinimleri.
- Reddetmeme gereksinimleri.
- Gizlilik gereksinimleri.
- Güvenlik denetimi gereksinimleri.
- Sistem bakımı güvenlik gereksinimleri.

Güvenlik Gereksinimleri İçin Ön Risk Değerlendirme Süreci



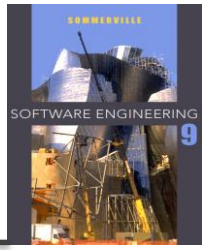


Güvenlik Riski Değerlendirmesi



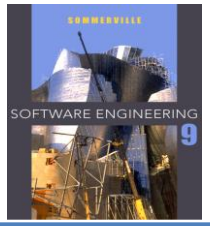
- Varlık kimliği
  - Korunması gereken temel sistem varlıklarını (veya hizmetleri) tanımlayın.
- Varlık değeri değerlendirmesi
  - Tanımlanan varlıkların değerini tahmin edin.
- Maruz kalma değerlendirmesi
  - Her bir varlıkla ilişkili potansiyel kayıpları değerlendirin.
- Tehdit tanımlama
  - Sistem varlıklarına yönelik en olası tehditleri belirleyin

Güvenlik Riski Değerlendirmesi



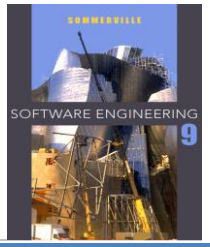
- Saldırı değerlendirmesi
  - Tehditleri, sisteme yönelik olası saldırılara ve bunların gerçekleşme yollarına ayırın.
- Kontrol kimliği
  - Bir varlığı korumak için uygulanabilecek kontrolleri önerin.
- Fizibilite değerlendirmesi
  - Kontrollerin teknik fizibilitesini ve maliyetini değerlendirin.
- Güvenlik gereksinimleri tanımı
  - Sistem güvenlik gereksinimlerini tanımlayın. Bunlar altyapı veya uygulama sistem gereksinimleri olabilir.

AS-HYS İçin Ön Risk Değerlendirme Raporunda Varlık Analizi



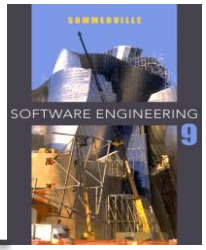
Varlık	Değer	Maruziyet
Bilgi sistemi	Yüksek. Tüm klinik konsültasyonları desteklemek için gereklidir. Potansiyel olarak güvenlik açısından kritik.	Yüksek. Kliniklerin iptal edilmesi gerekebileceğinden mali kayıp. Sistemi geri yükleme maliyetleri. Tedavi reçete edilemezse olası hastaya zarar verir.
Hasta veritabanı	Yüksek. Tüm klinik konsültasyonları desteklemek için gereklidir. Potansiyel olarak güvenlik açısından kritik.	Yüksek. Kliniklerin iptal edilmesi gerekebileceğinden mali kayıp. Sistemi geri yükleme maliyetleri. Tedavi reçete edilemezse olası hastaya zarar verir.
Bireysel bir hasta kaydı	Normalde düşük olmasına rağmen belirli yüksek profilli hastalar için yüksek olabilir.	Düşük doğrudan kayıplar ancak olası itibar kaybı.

Ön Risk Değerlendirme Raporunda Tehdit Ve Kontrol Analizi



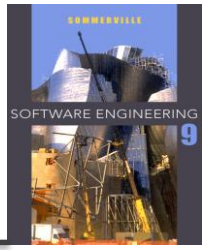
Tehdit	Olasılık	Kontrol	Fizibilite
Yetkisiz kullanıcı, sistem yöneticisi olarak erişim kazanır ve sistemi kullanılamaz hale getirir	Düşük	Sistem yönetimine yalnızca fiziksel olarak güvenli olan belirli konumlardan izin verin.	Düşük uygulama maliyeti, ancak anahtar dağıtımına ve acil bir durumda anahtarların mevcut olmasını sağlamak için özen gösterilmelidir.
Yetkisiz kullanıcı, sistem kullanıcısı olarak erişim kazanır ve gizli bilgilere erişir	Yüksek	Tüm kullanıcıların bir biyometrik mekanizma kullanarak kendi kimliklerini doğrulamasını isteyin. Sistem kullanımını izlemek için hasta bilgilerindeki tüm değişiklikleri günlüğe kaydedin.	Teknik olarak uygulanabilir ancak yüksek maliyetli çözüm. Olası kullanıcı direnci. Uygulaması basit ve şeffaftır ve ayrıca kurtarmayı destekler.

Güvenlik Politikası



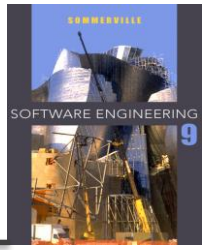
- Bir organizasyonel güvenlik politikası tüm sistemler için geçerlidir ve neye izin verilip verilmemesi gerektiğini belirler.
- Örneğin, bir askeri politika şöyle olabilir:
  - Okuyucular, yalnızca sınıflandırması okuyucuların inceleme düzeyiyle aynı veya altında olan belgeleri inceleyebilir.
- Bir güvenlik politikası, bir güvenlik sistemi tarafından sürdürülmesi gereken koşulları belirler ve böylece sistem güvenlik gereksinimlerinin belirlenmesine yardımcı olur.

AS-HYS İçin Güvenlik Gereksinimleri



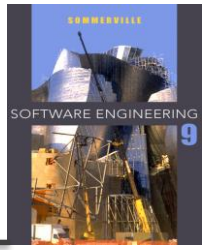
- Hasta bilgileri, bir klinik seansının başlangıcında, klinik personel tarafından kullanılan sistem istemcisinde güvenli bir alana indirilecektir.
- Sistem istemcisindeki tüm hasta bilgileri şifrelenecektir.
- Hasta bilgileri, bir klinik oturumu bittikten ve istemci bilgisayardan silindikten sonra veri tabanına yüklenecektir.
- Sistem veritabanında yapılan tüm değişikliklerin veritabanı sunucusundan ayrı bir bilgisayardaki günlük kaydı tutulmalıdır.

Biçimsel Şartname



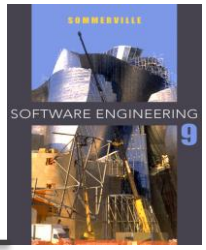
- Biçimsel belirtim, 'biçimsel yöntemler' olarak bilinen daha genel bir teknikler koleksiyonunun parçasıdır.
- Bunların tümü, yazılımın matematiksel temsiline ve analizine dayanmaktadır.
- Biçimsel yöntemler şunları içerir:
  - Biçimsel şartname;
  - Spesifikasyon analizi ve ispat;
  - Dönüşümsel gelişme;
  - Program doğrulama.

Resmi Yöntemlerin Kullanımı



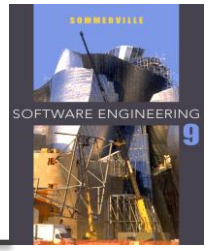
- Biçimsel yöntemlerin temel faydaları, sistemlerdeki hata sayısını azaltmaktır.
- Sonuç olarak, temel uygulama alanları kritik sistem mühendisliğidir. Bu alanda resmi yöntemlerin kullanıldığı birkaç başarılı proje olmuştur.
- Bu alanda, resmi yöntemlerin kullanımı büyük olasılıkla maliyet etkin olacaktır çünkü yüksek sistem hatası maliyetlerinden kaçınılmalıdır.

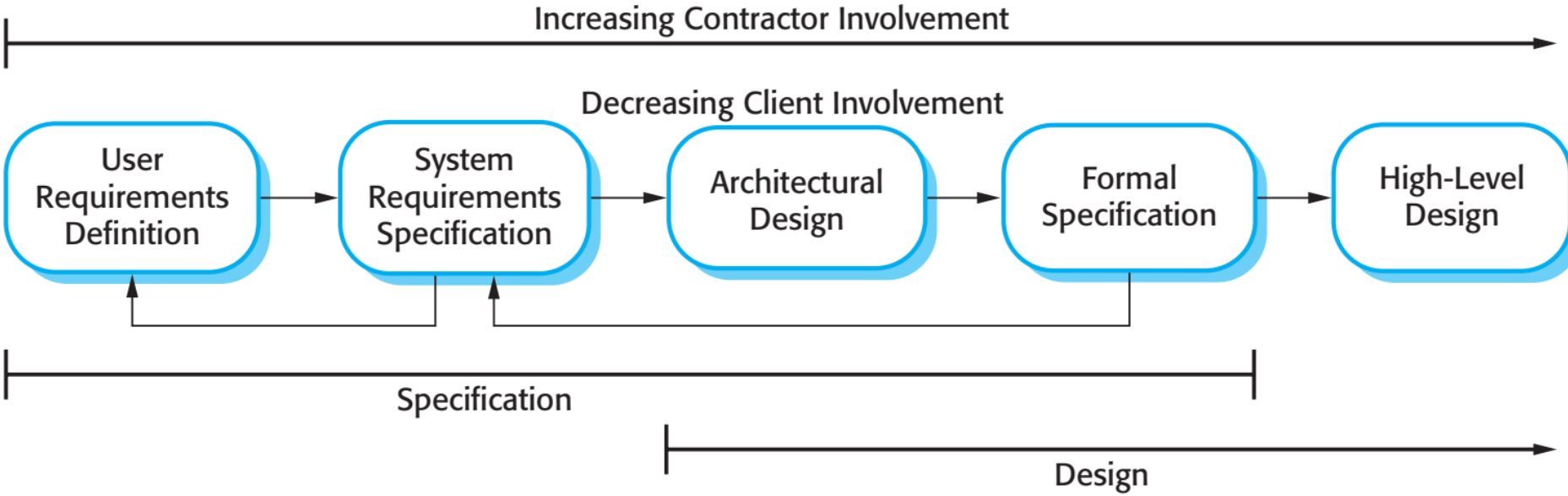
Yazılım Sürecindeki Şartname



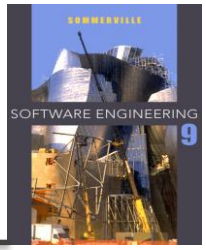
- Spesifikasyon ve tasarım ayrılmaz bir şekilde iç içe geçmiştir.
- Bir şartname ve şartname sürecini yapılandırmak için mimari tasarım esastır.
- Biçimsel belirtimler, kesin olarak tanımlanmış kelime dağarcığı, sözdizimi ve anlambilim ile matematiksel bir gösterimle ifade edilir.

Plan Tabanlı Bir Yazılım Sürecinde Resmi Şartname



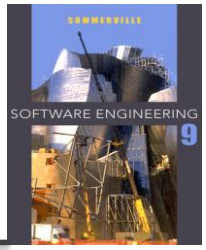


Resmi Spesifikasyonun Faydaları



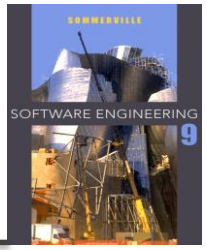
- Resmi bir spesifikasyon geliştirmek, sistem gereksinimlerinin ayrıntılı olarak analiz edilmesini gerektirir. Bu, gereksinimlerdeki sorunları, tutarsızlıkları ve eksiklikleri tespit etmeye yardımcı olur.
- Spesifikasyon resmi bir dilde ifade edildiğinden, tutarsızlıkları ve eksiklikleri keşfetmek için otomatik olarak analiz edilebilir.
- B yöntemi gibi resmi bir yöntem kullanırsanız, resmi belirtimi 'doğru' bir programa dönüştürebilirsiniz.
- Program, spesifikasyonuna göre resmi olarak doğrulanırsa, program test maliyetleri düşebilir.

Resmi Yöntemlerin Kabulü



- Biçimsel yöntemler, pratik yazılım geliştirme üzerinde sınırlı etkiye sahiptir:
  - Sorun sahipleri resmi bir şartnameyi anlayamazlar ve bu nedenle, gereksinimlerinin doğru bir şekilde temsil edilip edilmediğini değerlendiremezler.
  - Resmi bir şartname geliştirmenin maliyetlerini değerlendirmek kolaydır, ancak faydaları değerlendirmek daha zordur. Yöneticiler bu nedenle resmi yöntemlere yatırım yapma konusunda isteksiz olabilirler.
  - Yazılım mühendisleri bu yaklaşıma aşina değiller ve bu nedenle resmi metot kullanımını önermeye isteksizler.
  - Biçimsel yöntemlerin büyük sistemlere ölçeklendirilmesi hala zordur.
  - Biçimsel belirtim, Agile geliştirme yöntemleriyle gerçekten uyumlu değildir.

Bölüm 2'nin Anahtar Noktaları



- Güvenilirlik gereksinimleri nicel olarak tanımlanabilir. Talep üzerine arıza olasılığını, arızanın meydana gelme oranını ve kullanılabilirliği içerir.
- Bir sistem saldırganı bir sistem saldırısı planlamak için sistem güvenlik açıkları bilgisini kullandığından ve başarısız saldırılardan gelen güvenlik açıkları hakkında bilgi edindiğinden, güvenlik gereksinimlerinin belirlenmesi emniyet gereksinimlerinden daha zordur.
- Güvenlik gereksinimlerini belirlemek için, korunacak varlıkları tanımlamalı ve bu varlıkları korumak için güvenlik tekniklerinin ve teknolojisinin nasıl kullanılması gerektiğini tanımlamalısınız.
- Biçimsel yazılım geliştirme yöntemleri, matematiksel bir model olarak ifade edilen bir sistem spesifikasyonuna dayanır. Biçimsel yöntemlerin kullanımı, kritik bir sistem spesifikasyonundaki belirsizliği önler.