Denizcilik Teknoloji Yol Haritası

Denizcilik Sektöründe Siber Güvenlik ve Dayanıklılık

IACS UR E26-E27 Standartları ile Denizel Alanda Siber Güvenlik Çerçevesi ve Yeni Yetenek ve Yeterlilik Gereksinimi

Konuşmacı: Doç. Dr. Pelin Bolat

Deniz Güvenliği ve Siber Tehditler Araştırma (CyberMarSec) Laboratuvarı

İstanbul Teknik Üniversitesi Denizcilik Fakültesi

İçerik

- Gemi BT-OT Sistemleri
- Denizel Alanda Siber Risk
- Denizel Alanda Siber Olaylar
- IACS UR E26 ve E27
- Denizel Alanda İnsan Faktörü

Biz Kimiz?

- İTÜ-DF-CYBERMARSEC LAB

İTÜ-DF-CYBERMARSEC LAB

İTÜ DENİZ GÜVENLİĞİ ve SİBER TEHDİTLER ARAŞTIRMA LABORATUVARI

İTÜ ANASAYFA NİNOVA ÖĞRENCİ İŞLERİ WEBMAIL KÜTÜPHANE REHBER ENGLISH

ANASAYFA Dr. BOLAT HK. ARAŞTIRMA KONULARI ARAŞTIRMA EKİBİ YAYINLAR TESİSLER İŞBİRLİKLERİ HABERLER

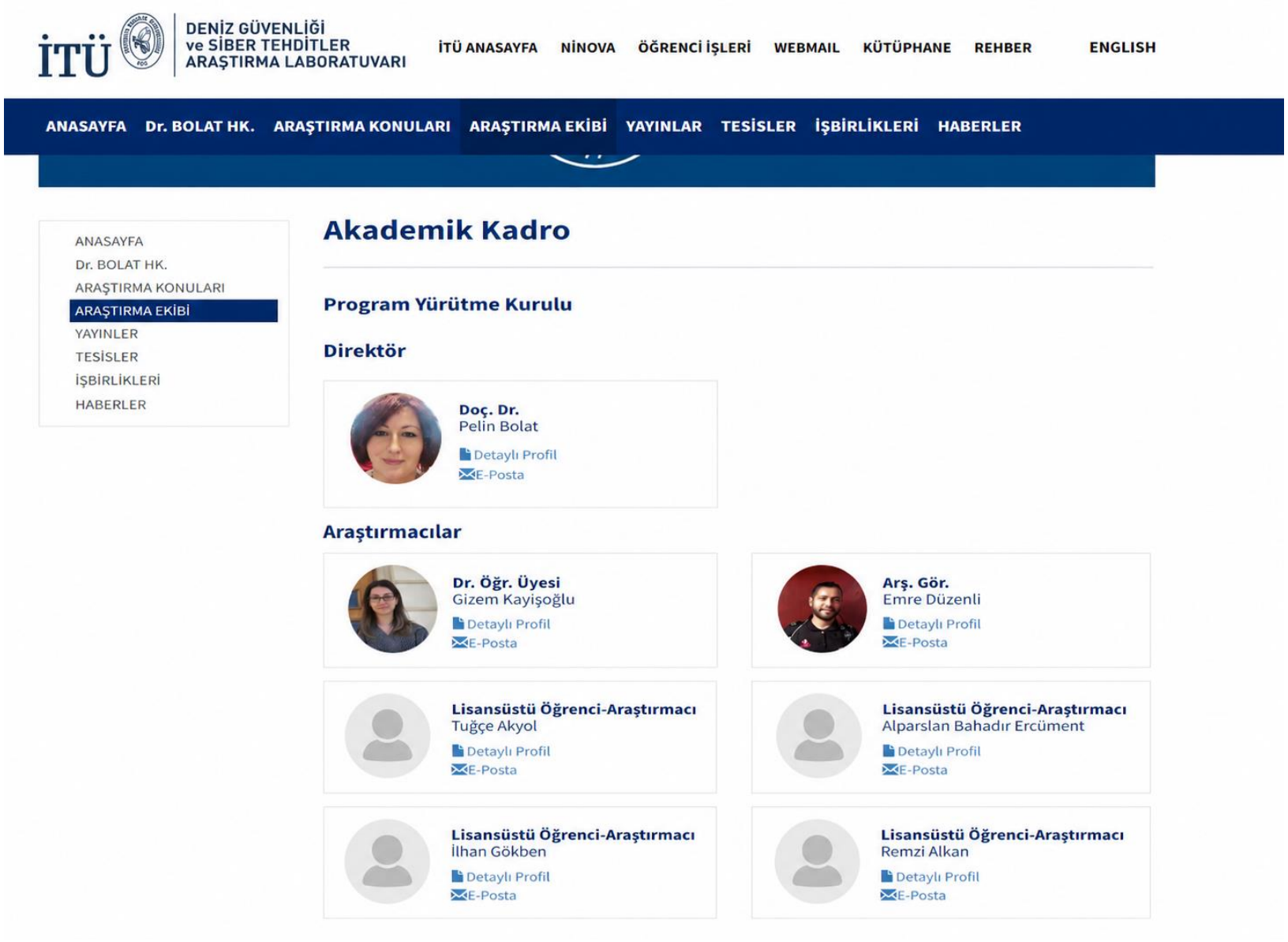
Deniz Güvenliği ve Siber Tehditler Araştırma Laboratuvarı (CyberMarsec), İstanbul Teknik Üniversitesi Denizcilik Fakütesinde deniz güvenliği ve siber tehditler üzerine araştırmalar yapmak amacıyla dünyanın önde gelen araştırma laboratuvarı olmak üzere kurulmuştur.

CyberMarSec laboratuvarının vizyonu, deniz güvenliği ve deniz siber güvenliği alanında araştırma, geliştirme ve inovasyonda dünya çapında tanınan bir mükemmellik merkezi olmaktır. Laboratuvar, denizcilik operasyonlarının, denizel kritik altyapıların, fiziksel ve siber ortamdaki varlıkların güvenliğini artırmak için bilgi ve teknolojiyi geliştirmeye odaklanmıştır.

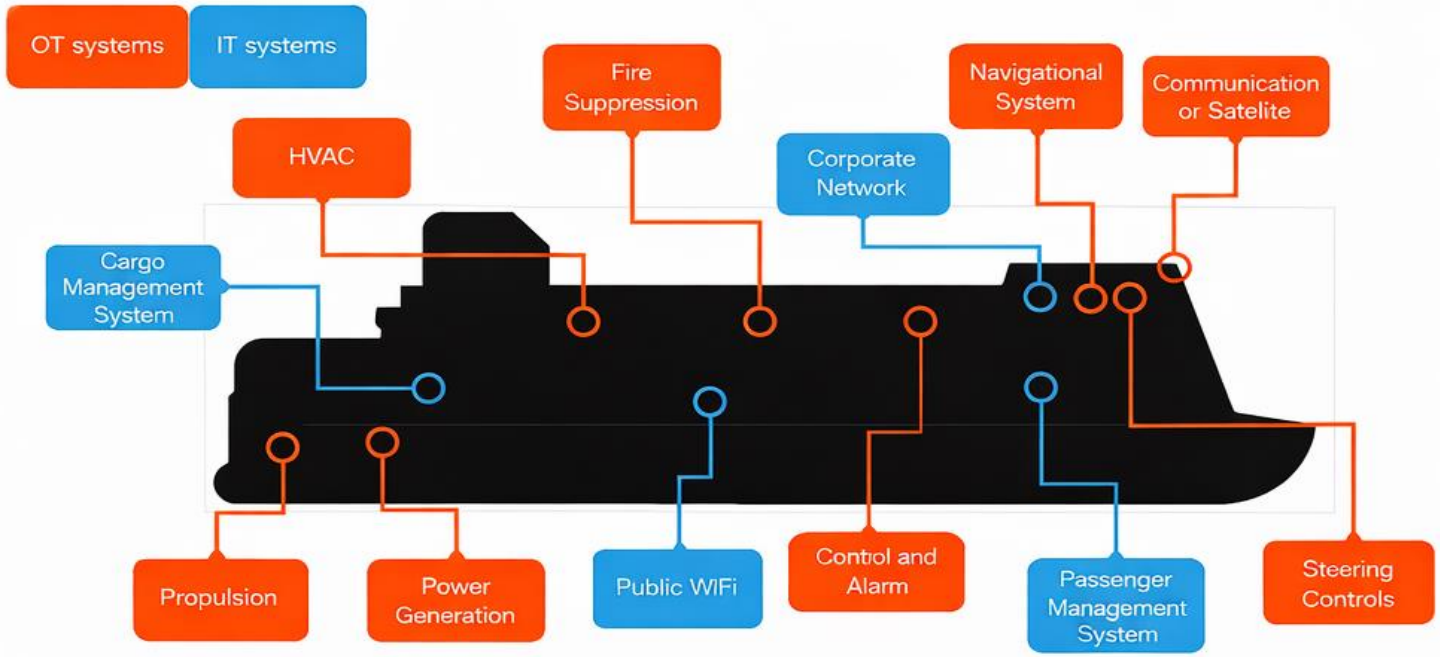
CyberMarSec fiziksel ve siber deniz güvenliği alanlarındaki çalışmaları risk değerlendirmesi, tehdit belirleme, güvenlik yönetimi, acil duruma hazırlık, kriz yanıtı, yeni teknolojiler, metodolojiler ve çözümler geliştirmeye yönelik araştırma konularını kapsayacaktır.

2023

İTÜ-DF-CYBERMARSEC LAB



GEMİ BİLGİ VE OPERASYONEL TEKNOLOJİLERİ



Gemi BT/OT'den Bazıları

Bligi Teknolojileri (BT)	Operasyonel Teknolojiler (OT)
• Yönetim, hesaplar, mürettebatl listeleri vb. • Planli bakim • Yedek parça yönetimi ve talepler • Elektronik kusurlar ve sertifikalar • Çalişma talimitlan • Charter parti, haziriik vb.	• PLC'ler, SCADA, • Gemideki Vehllesşik ölçüm ve kontrol sisteleï • ECDIS, GPS • Yeni kaydediciler • Makine ve kargo kontrol sistemleri

İTÜ

KAVRAM

GÜVENLİĞİN TEMEL İLKELERİ: CIA ÜÇLÜSÜ

GİZLİLİK

Bilgilere yalnizca yetkili kişilerin ulaşabilmesini saglamak. Yetkisiz ifşalari engellernek.

BÜTÜNLÜK

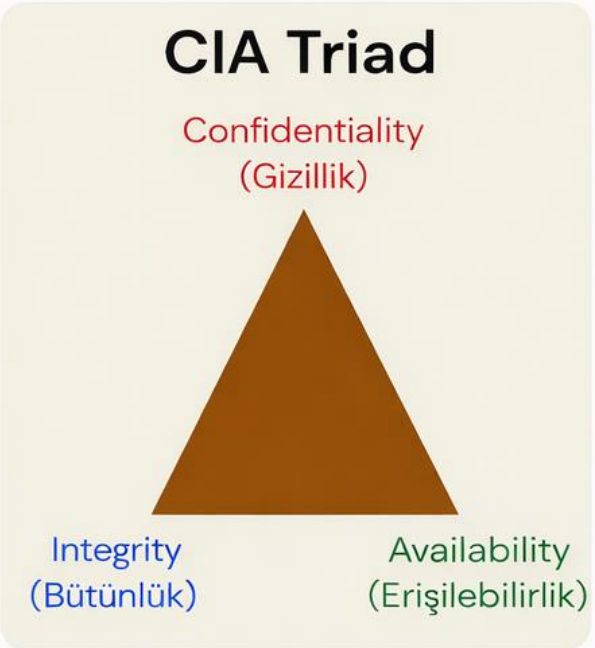
Sistemlerin ve bilgilerin yalnizca yetkili kişiler tarafından dégiştiniebilmesini saglamak.

ERİŞİLEBİLİRLİK

Yetkili erisimi ihtiyac duyuldugunda bilgilere ve sistemlere saglamak.

SİBER RİSK

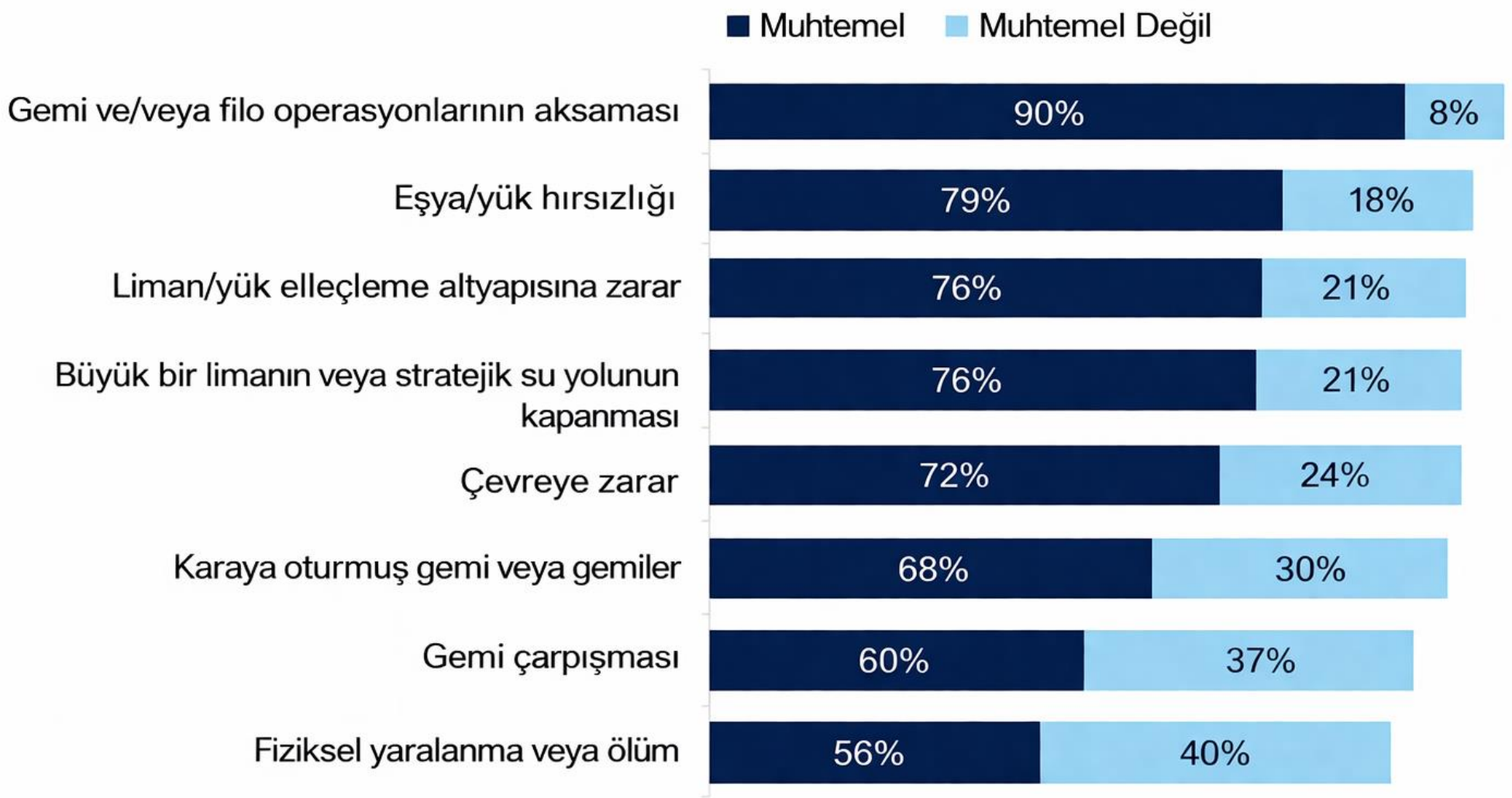
Siber güvenlik riskleri, BT ve OT bünyesindeki sistemlerin, bilgilerin, veya verilerin **gizliliğinin** (confidentiality), **bütünlüğünün** (integrity) veya **kullanılabilirliğinin** (availability) kaybıyla ilgilidir ve kurumsal operasyonalara (misyon, işlevler, imaj veya itibar) ve varliklara, bireylere, kişilere, diğer kuruluş ve çevreye potensiyel olumsuz etkileri yansıtır.



SİBER RİSK

Bilgi Teknolojileri (BT)	Risk: Temel olarak finans ve itibar
Operasyonel Teknolojiler (OT)	Risk: Can, mal ve çevre +finans ve itibar

Önümüzdeki Yıllarda Siber Güvenliğin Denizcilikteki Etkisi



İTÜ

KAVRAM

TEHDİT AKTÖRLERİNİN PROFİLİ

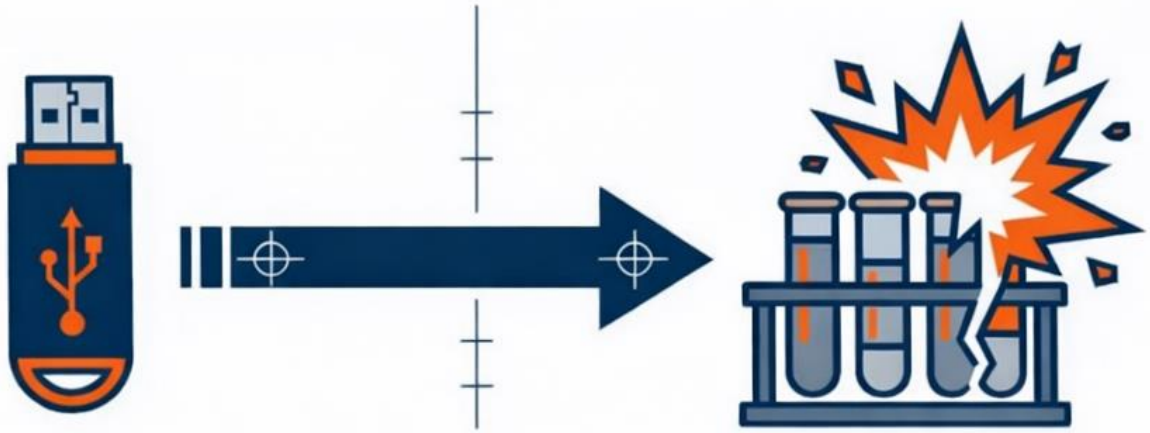
TEHDİT AKTÖRÜ	MOTİVASYON	HEDEF
 **Hacktivistler**	• Politik değişim, Ego • Meydan okuma	• Verilerin imhası • Medya ilgisi çekme • Hassas bilgilerin yayımlanması
 **Casuslar / Rakipler**	• Ticari casusluk • IP Hırsızlığı	• Veri çalmak • Sistemi fidye yazılımıyla işletilmez hale getirmek
 **Devlet Destekli**	• Politik kazanç • Casusluk • Savaş	• Bilgi elde etmek • Manipülasyon • Stratejik avantaj
 **Teröristler**	• İdeolojik hedefler • Korku	• Ekonomik ve kritik ulusal yapılarda aksaklıklara yol açmak
 **Suçlular**	• Maddi kazanç	• Sahte kargo taşımacılığı • Insan kaçakçılığı • Kaçakçilik

İTÜ

KAVRAM

OLAY İNCELEMESİ: STUXNET (2010)

Fiziksel Tahribata Giden Yolu Aşmak



Bulaşma Vektörü

Hava Boşluğu
(Sistemin internete bağli değil)

Fiziksel Tahribat

Olay:
Iran'in Buşehr ve Natanz nükleer tesislerine saldiran hedefli bir solucandı.

Kilit Gelişme:
Stuxnet, siber kodun endüstriyel SCADA sistemlerini fiziksel olarak **tahrip edebileceğini** kanitladi.

Ders:
Kapal, sistemler güvenli değildir. Bir mühendisin dizustü bilgisayari ve USB bellek, hava bosluğunu aşmak için yeterli oldü.

İTÜ

MAERSK'İN UĞRADIĞI SİBER SALDIRI

MAERSK

NotPetya fidye yazılımı
milyonlarca dolar zarara yol açtı

2 hafta süren küresel operasyon durması

49 bin bilgisayar
1.200 uygulama
3.500 sunucu
etkisiz hale geldi

Maersk, yaklaşik 300 milyon dolar zarara ugradı

- Haziran 2017'de gerçekleşti.
- NotPetya, sahte bir yazılım güncellemesi aracılığıyla yayildi.
- Maersk'ün Ukrayna'daki bir ofisinde başlayan saldırı hizla dünya çapinda yayildi.
- Veriler şifrelendi, sistemler devre dşı bırakıldı, ciddi şekilde karışıklik ve büyük mali kayıplar yaşandı.

Siber güvenlik büyüyen bir iş ve önemli bir güvenlik riski, önümüzdeki on yılın belki de “en büyük riski”

Seyahat gemisi, OT sistemlerini **kaybettiği** ve **güvenlik** sorunları yaşadığı için **limana dönüyor.** Yedekler, operasyon maliyetleri 210 milyon dolara kadar ulaşiyor

ECDIS güncellemesi **yakit kontrolü ve balast suyu valfleri kontrolünün kaybı ile sonuçlanıyor**

GPS arızasına **güvenmenin “pervasızlığı”** nedeniyle deni- aracının **karaya oturması** ve bunun mürettebatın yol açtığı petrol sızintısı ile sonuçlanması

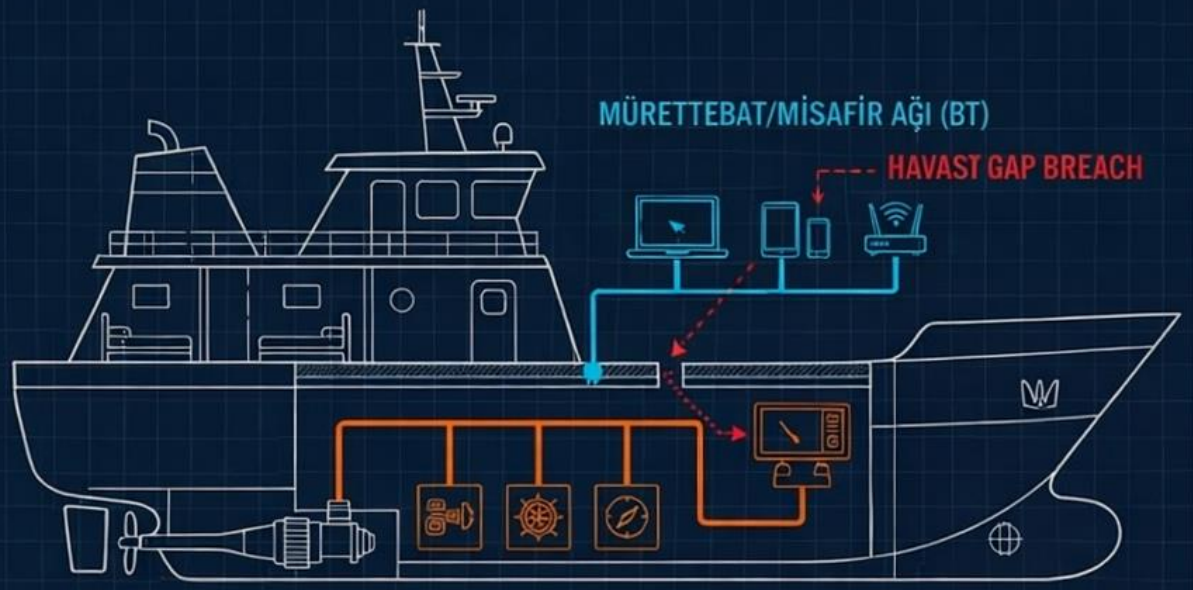
Uzaktan bağlantının servis mühendisi **tarafından** “yanlış” sondaja yapılması sebebiyle **petrol platformunun** acil durdurulması

Yolcu feribotu, sistem arızası ve müretebat eğitimi eksikliği nedeniyle ana tahrik sisteminı kaybediyor ve **karaya oturuyor**

İTÜ

MAVİ SULAR TEHDİTLER: SAVUNMASIZ GEMI

MAVİ SULAR TEHDİTLER: SAVUNMASIZ GEMİ



GİRİŞ NOKTASI: Kurumsal e-posta veya yasa dişi Wi-Fi köpruleri saldirganlarin kontrol ele geçirmesine imkän tänir.

BAŞLICA SALDIRI VEKTÖRLERİ

SAHTECILIK & SİNYAL BOĞMA (GPS/AIS)

Konum verilerini manipule etme. Ticar gemiler iskeledeyken konumlarini millerce otede

KARARTMA

Faal yatkrl gizlemek veya durumsal färkindaliği bözmak işin rakip sistemlerini devre dişi

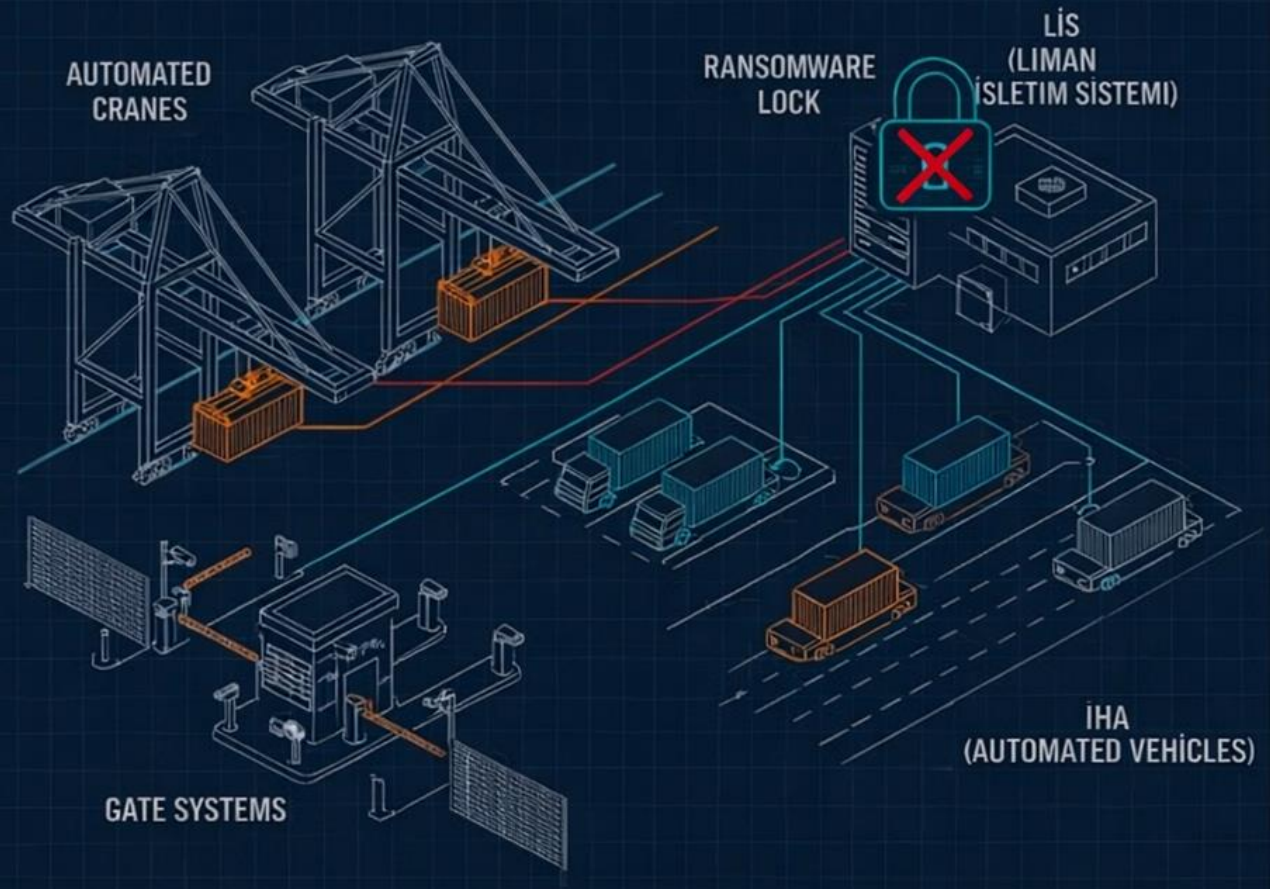
FİDYE YAZILIMI

Direct engoileme. Eğer yükleme kağrilarim e-posta yoluyia färhänläyamazsaniz. gemi yoa

İTÜ

KARA TARAFI TEHDİTLER: AKILLI LİMAN HEDEFLERİ

KARA TARAFI TEHDİTLER: AKILLI LİMAN HEDEFLERİ



BAŞLICA SALDIRI VEKTÖRLERİ

FİDYE YAZILIMI (Baskin Tehdit)

Yuksek operasyonel rnaliyet, durak, süresinde innanka jinedet alir form. Transnet, COSCO) Maliarm akisim burdurur.

LİS MANIPÚLASYONU

Lirnann 'fbcynt" Hacklenebilit Kontoynerleri yanlis vonlendirebilit Veya IHA laka carpabilir.

FİZİKSEL SONÚÇLAR

Elo optom nik UIS vincterin arrzalanmasina veya sinetarm cerbismasma neden diarak dogrudan guveniik riskleti yaratabilir.

İTÜ

TEMEL SEBEP: SİBER HİJYEN EKSİKLİĞİ

SİBER HİJYEN ÜÇGENİ

SİBER HİJYEN ÜÇGENİ

İNSAN FAKTÖRÜ

- Eğitim ve Farkindalik
- Guvenlik Kültürü
- Hata Türü: Kimlik Avina Duyarillik

ALTYAPI FAKTÖRÜ

- Donanim ve Varlik Yönetimi
- Güvenlik Duvarlari & Şifreleme
- Hata Türü: Yamasi Eksik Eski Sistemler

PROSEDÜR FAKTÖRÜ

- Yönetisim & Risk Yonetimi
- Olay Müdahale Planlari
- Hata Türü: Belge Eksikliği

Bu sütunlardan biri ya da daha fazlasi çöktüğünde bir ihlal meydana gelir.

İTÜ

OT GÜVENLİĞİ ZORLUKLARI: ERİŞİLEBİLİRLİK vs BÜTÜNLÜK

BT ORTAMI

Öncelik: Gizlilik ve Bütünlük

- **Eylem:** Yama yapmak standarttir.
- **Gerçek:** Sistemler yeniden başlatilabilir.

OT ORTAMI

- **Öncelik:** Erişilebilirlik ve Güvenlik
- **Eylem:** Yama yapmak tehilkelidir. ⚠
- **Gerçek:** Gemi seyir halindeyken navigasyon sistemi yeniden başlatilamaz. Zafiyet taramaşi akttl sistemieri devre dişi birakabilir.

STRATEJİK DEĞİŞİM: OT yamalanamayacağından ayrı tutulmalıdır.

İTÜ

DENİZ SİBER DAYANIKLILIK

IACS UR E26 & E27'YE NAVİGASYON

- **DURUM:** YENİ İNŞALAR İÇİN ZORUNLU
- **YÜRÜRLÜK TARİHİ:** 1 OCAK 2024
- **KAPSAM:** KLASLAMA KOŞULU

MARITIME TECH INNOVATIONS

İTÜ

DENİZ SİBER GÜVENLİĞİ DÜZENLEMELERİ

Yeni Standart: IACS UR E26 & E27

1 Temmuz 2024 veya sonrasında imzalanan sözleşmeler için geçerlidir.

IACS UR E26
(Gemilerin Siber Dayanıklılığı)

Tüm geminin siber dayanıklılığını sağlamaya yönelik gereklilikler

Uygulama Kapsamı: Gemiler, sistemler, ekipmanlar

Sorumlu Taraflar ve Roller:
Gemi Sahibi/Şirket, Entegratör, Tedarikçi, Sınıflandırma Kuruluşu

IACS UR E27
(Gemideki Sistemlerin Siber Dayanıklılığı)

Bireysel sistem ve ekipmanların siber dayanıklılığına yönelik özel teknik gereklilikler

Uygulama Kapsamı: E26 kapsamında yer alan bilgisayar sistemleri

Sorumlu Taraflar ve Roller:
Tedarikçi

E26 Açıklaması

- **Kapsam:** Tüm gemi ağının siber dayanıklılığı.
- **Amaç:** OT (Operasyonel Teknoloji) ve IT (Bilgi Teknolojisi) sistemlerinin **güvenli entegrasyonu.**
- **Sorumluluk:** Gemi Sahibi, Şirket ve **Entegratör (Tersane).**

E27 Açıklaması

- **Kapsam:** Bireysel ekipmanların siber dayanıklılığı.
- **Amaç:** **Belirli bileşenlerin güçlendirilmesi** (ör. ECDIS, Makine Kontrol Sistemleri).
- **Sorumluluk:** **Tedarikçi (Vendor).**

İTÜ

İSTANBUL TEKNİK ÜNİVERSİTESİ 1773

DENİZ SİBER GÜVENLİĞİ DÜZENLEMELERİ

DÜZENLEYİCİ PARADİGMA DEĞİŞİMİ

Deniz siber riski artık yalnızca bir BT güvenliği sorunu değil;
ISM Kodu ve SOLAS tarafından yönetilen kritik bir emniyet ve seyre elverişlilik sorunudur.

2017–2021: FARKINDALIK DÖNEMİ

- Gönüllü Rehberler (MSC.428(98))
- Prosedürel Hijyene Odak

2021–2024: UYUM DÖNEMİ

- Zorunlu SMS Entegrasyonu
- İlk Yıllık Doğrulamalar
- Fidye Yazılımlarının Artışı

2025+: DAYANIKLILIK DÖNEMİ

- Zorunlu Siber Dayanıklılık (IACS UR E26/E27)
- Sigorta Kapsamı Dışında Kalma
- Cezai Sorumluluk

UYUMSUZLUK RİSKİ: GEMİ BAĞLATMA ve SİGORTA GEÇERSİZ KALMA

DERİNLEMESİNE İNCELEME: UR E26 (GEMİ)

Hedef: "Sistemler Sistemi". Gemi, ilk cizim tahtasindan nihai teslimata kadar siber dayaniklilik ile tasarlanmalidir. Bu, tersane ve entegratörün sorumluluğun adadir.

KURTAR:	MÜDAHALE ET:	MÜDAHALE ET:	KORU:
Yedekleme	Olay Müdahale	Olay Müdahale Mekanizmaiarı	Bölümlendirme

UR E26 Gemilerin Siber Direnci

UR E26'nın 17 Gereksinimi

Belirle
- CBS'lerin ve ağların envanteri

Koruma
- Güvenlik bölgesi
- Ağ koruma önlemleri
- Antivirüs, antimalware, antispam ve diğer kotü amäcli yazilimlara karşi koruma
- Erişim kontrolü
- Kablosuz iletişim
- Güvenilmeyen ağlarla uzaktan erişim kontrolü ve iletişim
- Mobil ve taşınabilr cihazların kullanımı

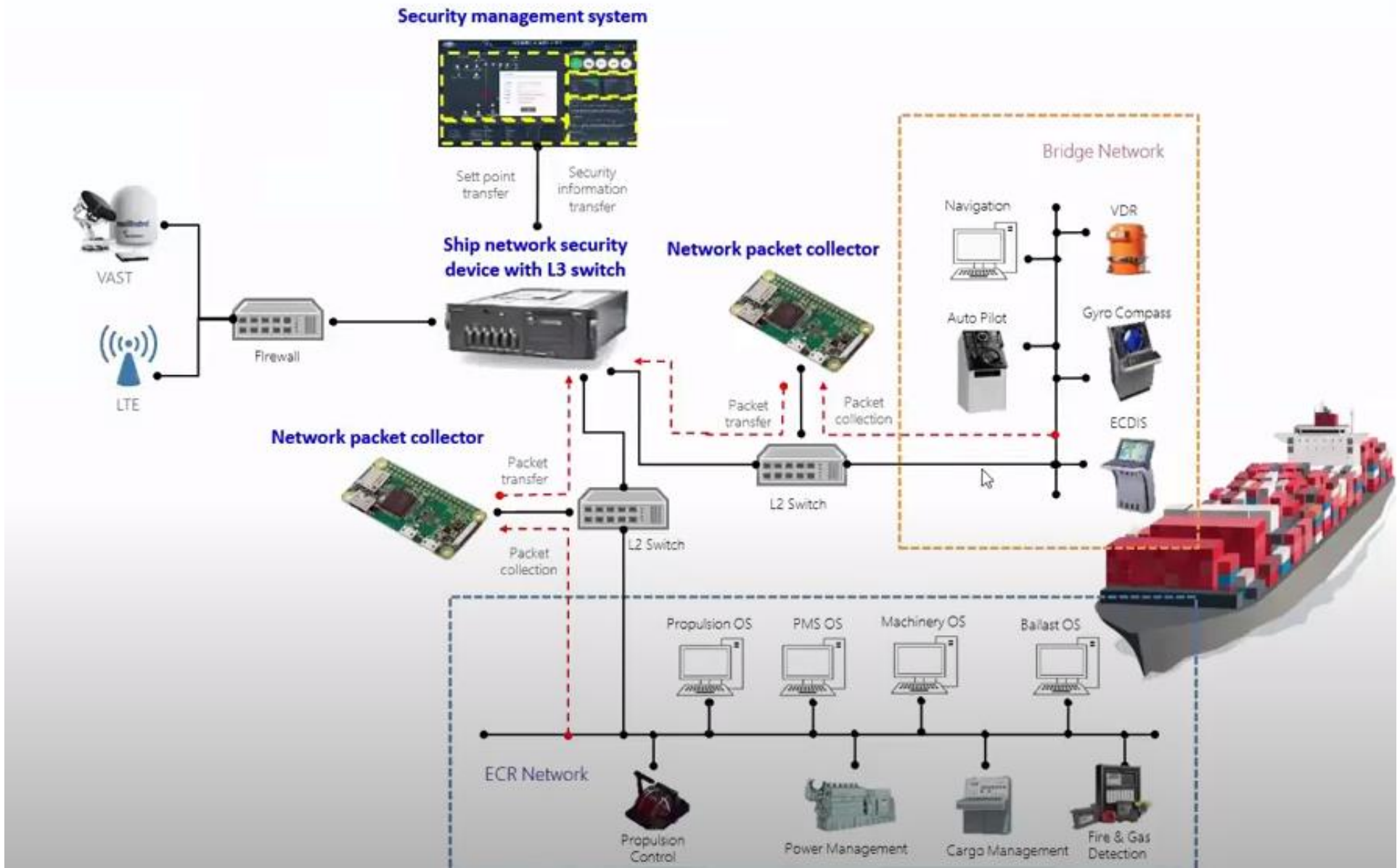
Tespit
- **Ağ operasyonu izleme**
- CBS'ler ve ağların **teşhis** işlevleri

Yanitla
- **Olay müdahale planı**
- Yerel, bağımsız ve/veya manuel operasyon
- Ağ izolasyonu
- Minimum risk koşuluna geri düşüş

Kurtarma
- Kurtarma planı
- Yedekleme ve geri yükleme yeteneği
- Kontrollü kapatma, yeniden başlatma eve geri yükleme

UR E26 Cyber Resilience of Ships

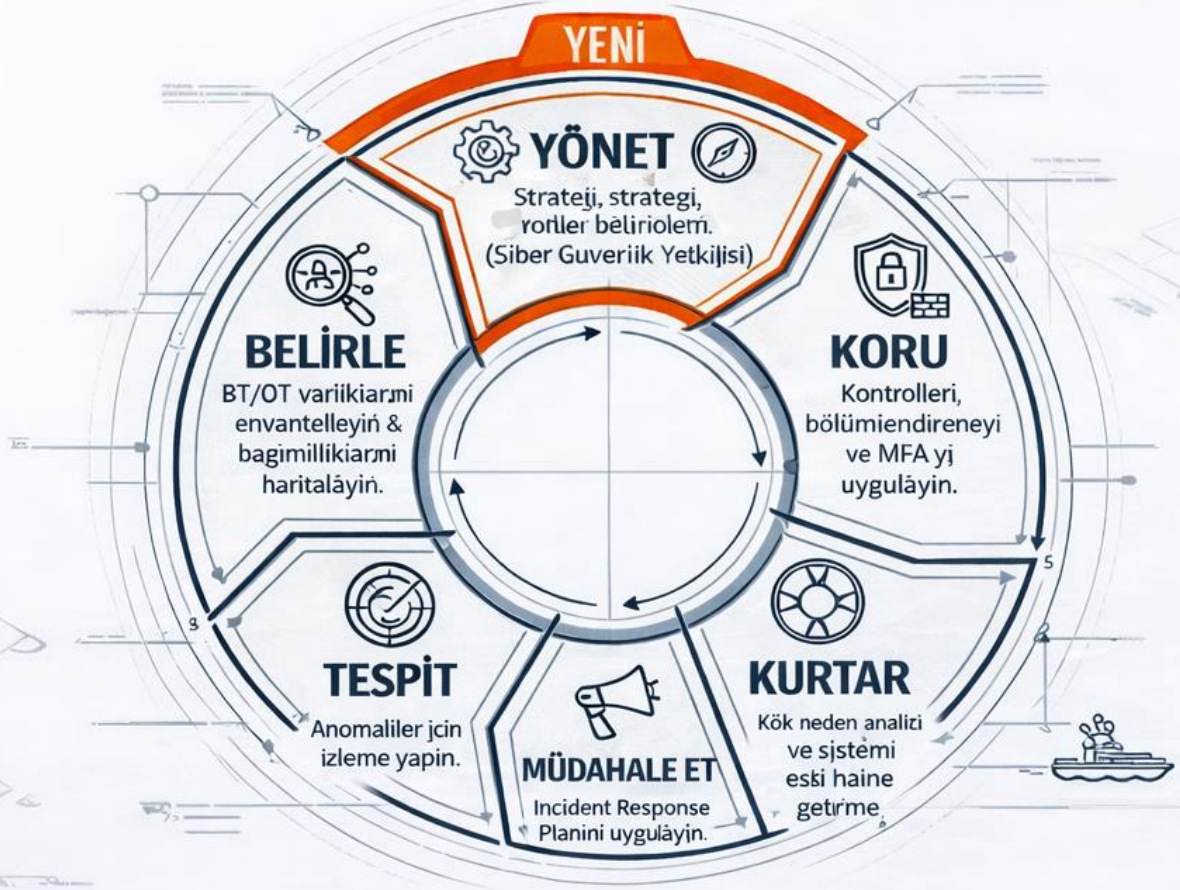
Example of Network Monitoring System



İTÜ

2025 STANDARTI: MSC-FAL.1/CIRC.3/REV.3

4 Nisan 2025'de Onaylandı - Yeni Fonksiyonel Çerçeve

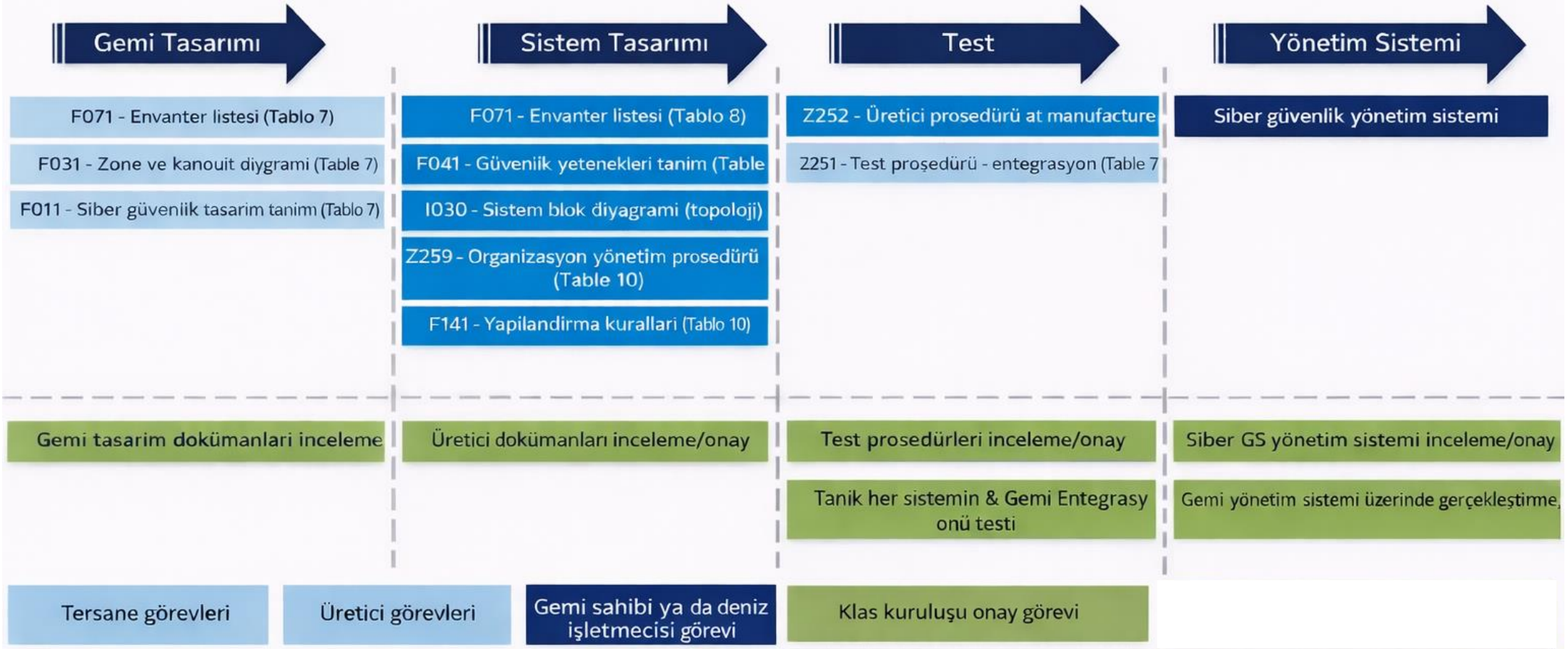


"Etkili siber risk yönetimi üst yönetim seviyesinden başlamalıdır."

ROLLER & SORUMLULUKLAR MATRİSİ

Önemli Ayrım: E27 belgesi satin alabilirsiniz, ancak kôtü bir kurulum (E26'ya aykırilik) varsa, gemi uyumlu değildir.

Süreç ve Dökümanlar - Siber Güvenli Sınıflandırma



DNV Cyber secure class levels for ships & offshore units

Cyber Secure Class Notation
(DNV-RU-SHIPS Pt.6 Ch.5 Sec.21)

Cyber Secure Type Approval
(DNV-CP-0231)

Different levels

IACS UR 2024

Entry-level for all merchant vessels 	Cyber secure <no qualifier>	Security Profile 0
Newbuildings & high-end vessels 	Cyber secure Essential	Security Profile 1
Advanced newbuildings with very high security 	Cyber secure Advanced	Security Profile 3

İNSAN FAKTÖRÜ: PERSONEL ZAFİYETİ

TESPİT 4: EKSİKLİKLER

- Siber güvenlik farkındalığı eksikliği.
- Tanıdık olmama nedeniyle yanlış işlem yapma.
- Gemi ve Kara arasındaki sorumluluklar tanımlı değil.
- Personel ayrıldığında erişim iptal prosedürü yok.

GEREKLİ ÖNLEMLER

- Düzenli Siber Güvenlik Tatbikatlari (Gemi & Birleşik Gemi-Arazi).
- Temiz Masa / Temiz Ekran Politikalari.
- Farkindalik Malzemeleri: Kilavuzlar, Afişler, Ekran Koruyucular.

"Teknoloji (E27), Prosedür (SMS) olmadan başarisiz olur."

TEKNOLOJİ, DENİZCİLİK DÜZENLEMELERİNİ GERİDE BIRAKTI

Yönerge

IMO MSC.428 güvenlik yönetim sistemlerinde siber risk yönetimini gerektirir.

Açık

Siber güvenlik yetkinliği için belirli bir STCW kursu yok.

Sonuç

Denizciler tehditleri tanıma ve önlemede **'Siber Hijyen'** eksikliğine sahip.

"Mevcut DİM programları, denizcilere mevcut siber tehdit senaryosunu tanıyıp önleyebilecek yeterli siber güvenlik bilgisini sunmuyor."

Fiziksel Varlık vs. Dijital Dayanıklılık

ISPS Kodu (Mevcut Durum)

Odak: Yetkisiz fiziksel erişimi caydırmak ve sabote etmeyi önlemek.

Araçlar: Citler, aydınlatma, kimlik kontrolleri, Devriyeler.

Yöntem: Statik prosedürler ve fiziksel denetimler.

Siber Risk (Veni Gereklilik)

Odak: BT/OT sistemlerinin koruması, veri bütünlüğü ve dijital sabotajı önlernek.

Araçlar: Ağ segmentasyonu, güvenlik duvarları, yazium yamaları.

Yöntem: Dinamik 'Bilgisayar Tabanlı Sistemler' (CBS) yönetimi ve sürekii izleme.

Bir ağı güvenceye almak için bir iskeleyi **korumakla** aynı zihniyeti kullanamazsınız.

Eğitmen Açığı: Eğitmenleri Kim Eğitecek?

Mevcut Uzmanlık (ISPS)

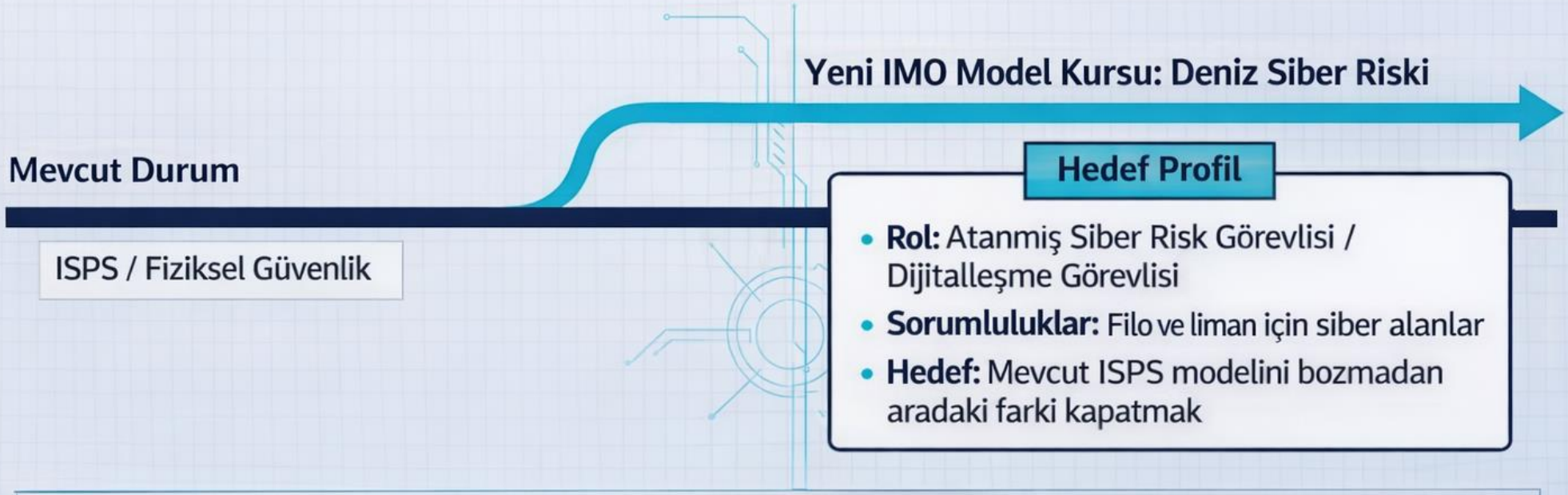
- SOLAS Bölüm XI-2
- Fiziksel Güvenlik Tatbikatları
- Eğitim Yöntemleri

Beceri Açığı

- Tehdit Modelleme
- Sizma Testleri
- NIST & ISO/IEC 27001 Çerçeveleri

Tüm deniz güvenliği eğitmenlerini bir gecede siber uzmanlara ‘yetkinleştiremeyiz’.
Aradaki fark çok büyük.

İleriye Dönük Adım: Uzmanlaşmış, Bağımsız Eğitim

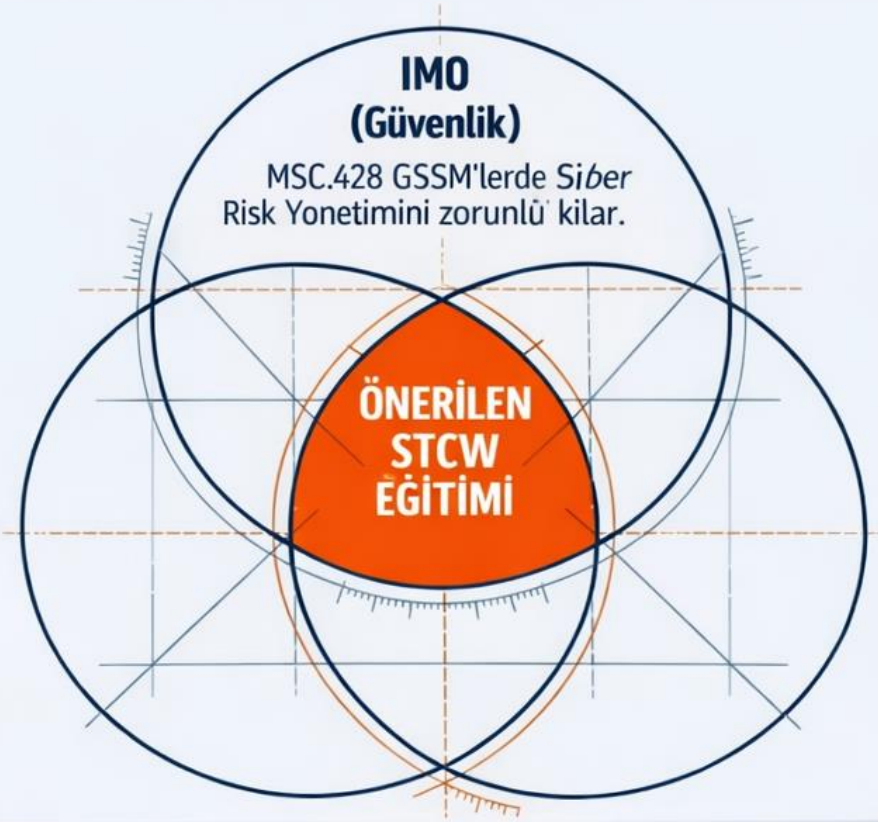


Öneri: Deniz Siber Risk Yönetimi için özgün IMO Model Kurslarının geliştirilmesi.

İTÜ

DÜZENLEYİCİ ÜÇGEN

Uyum Yapisaldir, Sadece İdari Değil



Müfredat, Güvenlik (IMO), Teknik Standartlar (IACS) ve En İyi Uygulamalar (NIST) arasindaki boşluğu köprüler.

IACS (Dayanıklılık)

UR E26 & E27 Gemi entegrasyonu' ve sistem sertlestirmesi icin ortak gereklilikleri belirler.

NIST (Metodoloji)

Kimlik, Koru, Tespit, Müdahale, Kurtar standardini sağlar.

Dinlediğiniz için Teşekkür Ederim

İTÜ Denizcilik Fakültesi
Deniz Güvenliği ve Siber Tehditler Araştırma Laboratuvarı
(CyberMarSec Lab)