Industrial Control Systems Security

Lerneinheit 3: Schwachstellen

Prof. Dr. Christoph Karg

Studiengang Informatik
Hochschule Aalen

Wintersemester 2013/2014

Einleitung

Das Thema dieser Lerneinheit sind Schwachstellen von ICS.

Es werden folgende Punkte behandelt:

- Beispiele für Sicherheitsvorfälle
- Vergleich von ICS und IT-Systemen bezüglich Schwachstellen
- Kategorisierung von Schwachstellen

Ein großer Teil dieser Lerneinheit basiert auf [MS12, Kapitel 3].

Sicherheitsvorfälle

- In den letzten Jahren wurde eine Vielzahl von Sicherheitsvorfällen bei ICS publik
- Besonders hohe Wellen schlug das Bekanntwerden des Stuxnet Wurms
- Durch Schwachstellen sind ICS in verschiedensten Branchen gefährdet
- Schwachstellen in Heizungsanlagen betreffen auch private Haushalte

Stuxnet

- Stuxnet ist ein Computerwurm, der 2010 entdeckt wurde
- Angriffziel: Industrieanlagen mit Siemens SPS S7 Steuerungen
- Stuxnet sabotierte unter anderem Zentrifugen in einem iranischen Atomkraftwerk
- Aufgrund der Komplexität des Schadkodes vermuteten Experten, dass Stuxnet von Profis entwickelt wurde
- Später stellte sich heraus, dass Stuxnet von des USA und Israel entwickelt wurde

Quellen: [KL10; And12]

Schwachstelle in Embedded Servern

- Tridium, eine Tochterfirma von Honeywell, produziert Embedded Server, die in einer Vielzahl von ICS Verwendung finden
- Grundlage für die Programmierung ist der Niagara AX Framework
- Durch eine Schwachstelle erlangten Hacker Zugriff auf diese Server und waren in der Lage, die Anlage komplett zu steuern
- Es waren mehr als 21.000 über das Internet erreichbare Geräte betroffen
- Es sind mehr als 11 Millionen dieser Geräte in ICS in 52 Ländern im Einsatz

Quelle: [Goo13]

Sicherheitslecks in Heizungssteuerungen

- Die Vaillant-Anlage ecoPower 1.0 produziert im Eigenheim aus Erdgas Wärme und Strom
- Zwecks Wartung müssen im heimischen Router FTP, HTTP und SSH an die Steuerung der Anlage weitergeleitet werden
- Über einen Webzugang kann man die Heizung ein- oder ausschalten sowie die Temperaturvorgaben manipulieren
- Der eingebaute Webserver gibt durch eine spezielle Anfrage alle hinterlegten Passwörter im Klartext aus
- Der Bug kann nur durch einen Techniker vor Ort behoben werden

Quelle: [Sta13]

Zugriff auf ein Blockheizkraftwerk

- c't Redakteuren gelang der Zugriff auf die Steuerung eines Blockheizkraftwerks im Fernwärmenetz des Bioenergiedorfs St. Peter im Schwarzwald
- Es war möglich, die Fernalarmierung zu deaktivieren, beliebige Parameter zu verstellen oder die Anlage komplett zu deaktivieren
- Ist das Fernwärmenetz deaktiviert, dann lässt es sich nicht ohne weiteres wieder in Betrieb nehmen
- Es waren weitere Wärmenetze von dieser Sicherheitslücke betroffen
- Der Betreiber sperrte den Internetzugang der Geräte, als er von dem Vorfall erfuhr

Quelle: [Sta13]

Sicherheitslücken in medizinischen Geräten

- Im Juni 2013 warnt das ICS-CERT vor einer kritischen Sicherheitslücke in medizinischen Geräten
- Betroffen sind unter anderem Infusionspumpen, Defibrillatoren, Patientenüberwachungssysteme und Anästesiegeräte
- Die Schwachstelle ist ein Wartungsaccount mit einem voreingestellten Passwort
- Es sind mehr als 300 Geräte von über 40 Herstellern betroffen

Quelle: [ICS13]

Schwachstellen in ICS

- Die Bedrohungen von ICS stimmen in vielen Fällen mit denen von IT-Systemen überein
- ICS sind anfälliger für Lucky Strikes als IT-Systeme
- Eine gezielte Ausnutzung einer Schwachstelle bei ICS erfordert ein hohes Fachwissen
- Um Schwachstellen und die von ihnen ausgehenden Gefahren besser analysieren können, müssen sie kategorisiert werden
- Es gibt mehrere Ansätze zur Kategorisierung von Schwachstellen

Abgrenzung IT-/ICS-Schwachstellen

IT-Systeme:

- Gute Dokumentation von Schwachstellen und deren Analyse
- Client-Server-Modell vereinfacht die Analyse
- Vertraulichkeit, Datenintegrität und Authentizität als Primärziele

ICS:

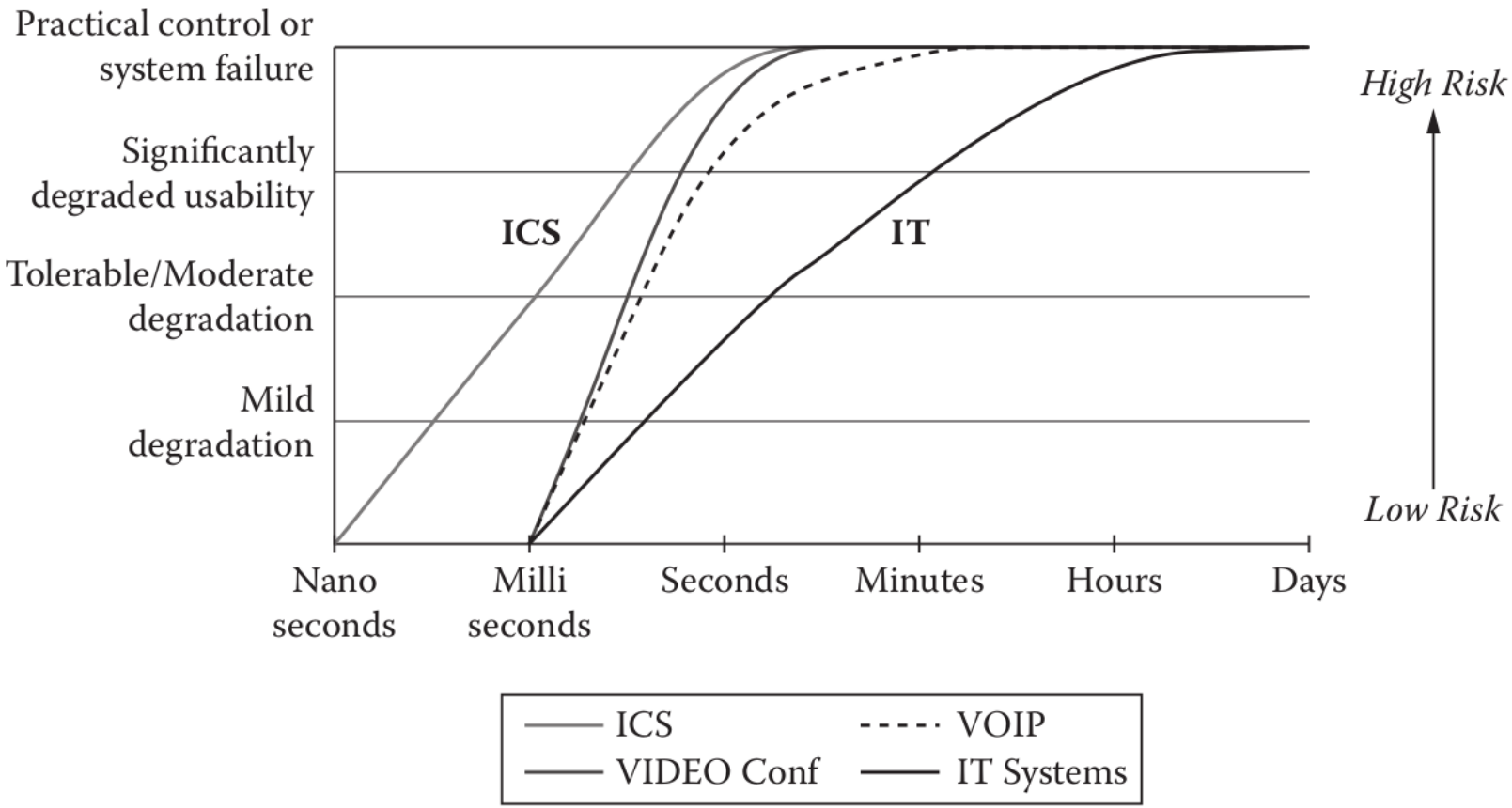
- Dokumentation der Schwachstellen und deren Auswirkungen oft knapp und unvollständig
- Kombination aus Peer-To-Peer Verbindungen und Client-Server Modell erschwert die Analyse
- Verfügbarkeit und Zuverlässigkeit als Primärziele

Frage: Inwieweit kann man Erkenntnisse von Schwachstellen von IT-Systemen auf ICS übertragen?

Vergleich von ICS und IT-Systemen

- Macaulay und Singer vergleichen ICS und klassische IT-Systeme hinsichtlich mehrerer Sicherheitsanforderungen [MS12]
- Folgende Systeme/Dienste wurden verglichen:
  - IT-System (Client-Server Modell)
  - Voice-over-IP
  - Videokonferenz
  - ICS
- Folgende Schutzziele werden hinsichtlich Störungen im Netzwerkverkehr untersucht:
  - Verfügbarkeit
  - Datenintegrität
  - Vertraulichkeit
- Die Unterschiede werden anhand von Grafiken dargestellt

Verfügbarkeit – Grafik

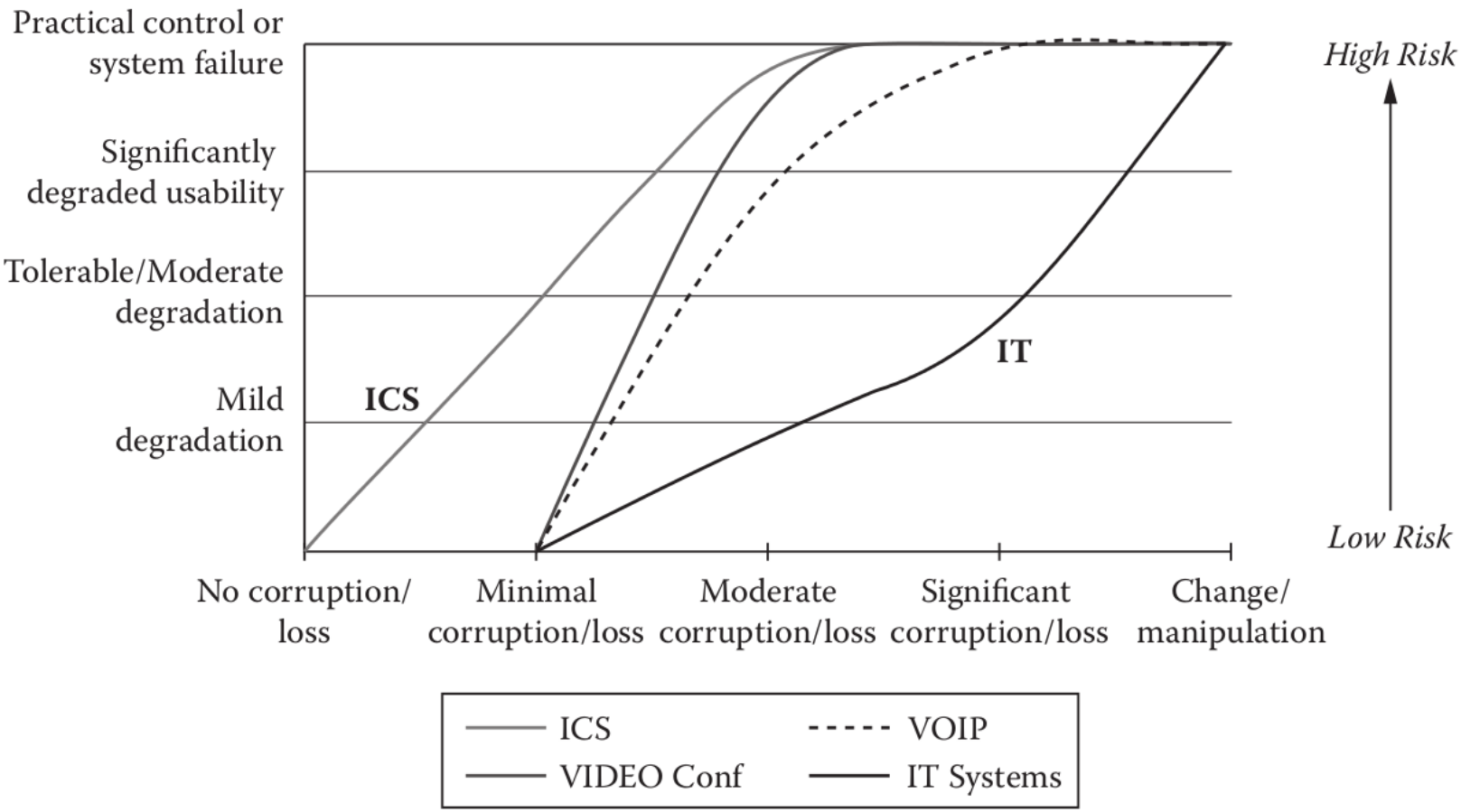


Quelle: [MS12, Seite 86]

Verfügbarkeit – Bemerkungen

- Klassische IT-Systeme „verkraften“ einen Ausfall von mehreren Minuten
- Bei zeitkritischen Anwendungen wie Voice-over-IP wird die Nutzbarkeit bei Unterbrechungen im Sekundenbereich bereits eingeschränkt
- Die Funktionsfähigkeit von ICS bereits bei Unterbrechungen im Millisekundenbereich nicht mehr gegeben

Datenintegrität – Grafik

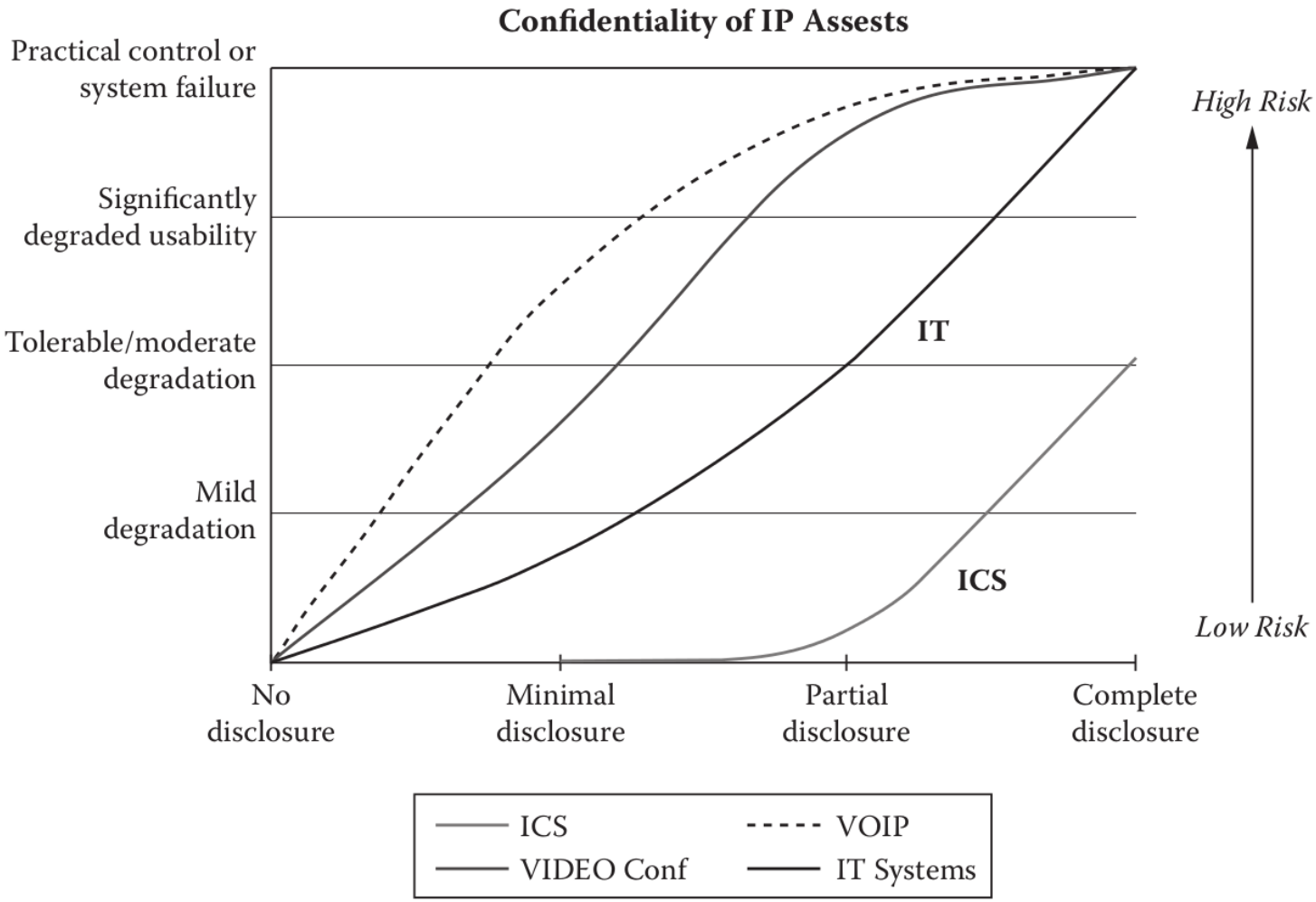


Quelle: [MS12, Seite 86]

Datenintegrität – Bemerkungen

- Es wird zwischen Datenverlust bzw. Verfälschungen durch Störungen und gezielter Manipulation der Daten unterschieden
- IT-Systeme sind auch bei moderatem Datenverlust/-verfälschung noch funktionsfähig
- Bei Sprach- und Videoübertragungen ist geringer Datenverlust tolerierbar
- ICS sind anfällig für geringen Datenverlust

Vertraulichkeit – Grafik



Quelle: [MS12, Seite 87]

Vertraulichkeit – Bemerkungen

- Sprach- und Videoübertragungen sind sehr anfällig gegen den Verlust von Vertraulichkeit, da man schon mit einem geringen Teil der abgefangenen Daten Informationen von Gesprächen rekonstruieren kann
- Bei IT-Systemen muss die komplette Übertragung einer Datei abgefangen und entschlüsselt werden, um an die entsprechenden Informationen zu gelangen
- Bei ICS spielt Vertraulichkeit eine untergeordnete Rolle, da selten Verschlüsselungstechniken zum Einsatz kommen

Purdue Enterprise Reference Architecture

- Entwicklung der Purdue University in West Lafayette, Indiana, USA
- Bereitstellung von Werkzeugen zur Modellierung von Unternehmensarchitekturen, Geschäftsprozessen, ...
- Einteilung der Unternehmensbestandteile in Ebenen
- Zuordnung von Anforderungen an Verfügbarkeit für jede Ebene
- Weitere Informationen findet man unter `http://www.pera.net`

PERA Levels I

Enterprise Systems (Level 4 und 5)

- Geschäftsplanung, Logistik und Finanzen
- Vertraulichkeit hat Vorrang vor Verfügbarkeit

Operations Management (Level 3)

- Steuerung und Überwachung des Produktionsablaufs
- Verfügbarkeit hat Vorrang vor Vertraulichkeit

Supervisory Control (Level 2)

- Steuerung und Überwachung eines physikalischen Prozesses
- Zugriff auf HMI und Log-Daten
- Verfügbarkeit hat Vorrang vor Vertraulichkeit

PERA Levels II

Local or Basic Control (Level 1)

- Zugriff auf die Sensoren und Aktoren einer Maschine
- Sensordatenauswertung
- Oft in einem PLC angesiedelt
- Verfügbarkeit hat Vorrang vor Vertraulichkeit

Process (Level 0)

- Analoge Kommunikation zwischen Sensoren
- Verfügbarkeit hat Vorrang vor Vertraulichkeit

Zuordnung von Geräten und Bereichen

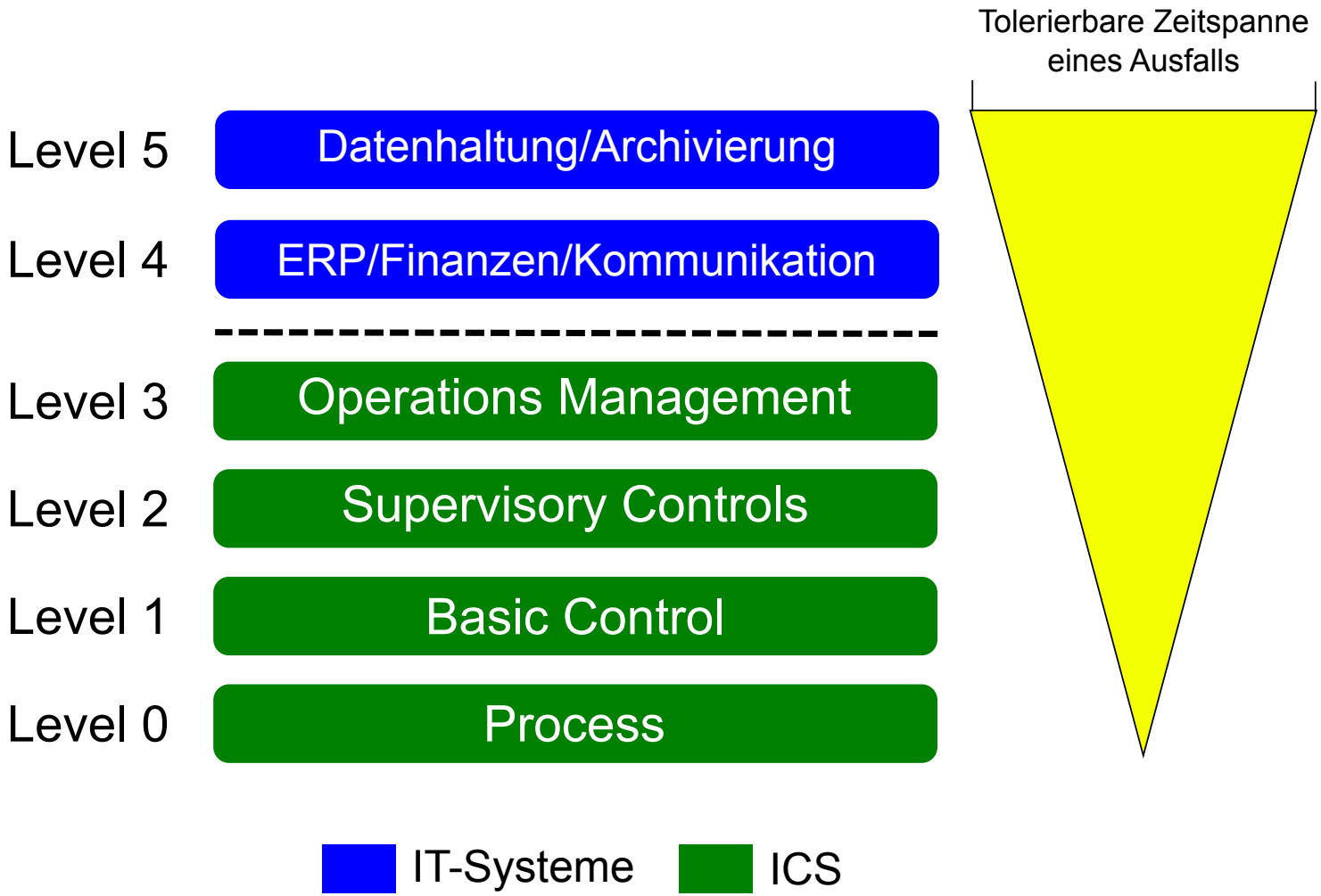
- Level 5 $\rightsquigarrow$ Produktionsplanung, Buchhaltung, Verwaltung von Zulieferungen, Entwicklung & Design
- Level 4 $\rightsquigarrow$ Produktionsablaufplanung, Planung von Wartungsarbeiten, Ressourcenplanung, Berichtswesen
- Level 3 $\rightsquigarrow$ Aufzeichnung von Produktionsdaten (Logging), Überwachung von Wartungsvorgängen
- Level 2 $\rightsquigarrow$ Echtzeitstatistiken, HMI-Zugriff
- Level 1 $\rightsquigarrow$ Lokale Steuerungseinheiten (PLCs)
- Level 0 $\rightsquigarrow$ Sensor und Aktor Input/Output

Anforderungen an Verfügbarkeit

Folgende Zeitspannen sind bei Systemausfällen tolerierbar:

- Level 5 $\rightsquigarrow$ Tage
- Level 4 $\rightsquigarrow$ Stunden
- Level 3 $\rightsquigarrow$ Minuten bis zu Stunden
- Level 2 $\rightsquigarrow$ Sekunden bis zu Minuten
- Level 1 $\rightsquigarrow$ Millisekunden bis Sekunden
- Level 0 $\rightsquigarrow$ kein Ausfall erlaubt

Anforderungen an Verfügbarkeit – Grafik



Arten von Daten

Ruhende Daten (Data at Rest)

- Daten, die sich auf einem sekundären Speichermedium befinden
- Es findet kein Zugriff auf die Daten statt

Daten in Bewegung (Data in Motion)

- Daten, die momentan über das Netzwerk übertragen werden
- Hierzu werden die Daten auf Pakete aufgeteilt und gegebenfalls verschlüsselt

Daten in Benutzung (Data in Use)

- Daten, auf die momentan über eine Software zugegriffen wird
- Die Daten befinden sich in der Regel im Hauptspeicher eines Rechners

Ruhende Daten

ICS:

- In der Regel sind dies Log-Dateien, Messungen, ...
- Mit zunehmendem Alter verlieren diese Daten schnell an Bedeutung

IT-Systeme:

- Die Daten sind über eine längere Zeitspanne wichtig
- Die Relevanz der Daten ist oft unabhängig von deren Alter
- Die Daten sind Bedrohungen hinsichtlich der Vertraulichkeit ausgesetzt

Daten in Bewegung

ICS:

- Die Manipulation von über das Netzwerk übertragenen Steuerungsdaten stellt eine große Gefahr dar
- Eine Verschlüsselung der Daten ist oft wegen der leistungsschwachen Geräte nicht möglich

IT-Systeme:

- Es existieren zahlreiche Standards, um Daten während der Übertragung zu verschlüsseln
- Um die Daten zu entschlüsseln, muss die komplette Übertragung abgefangen werden

Daten in Benutzung

ICS:

- Der Zugriff auf die Daten erfolgt über HMI-Komponenten
- In der Regel sind diese Komponenten zu leistungsschwach, um eine gezielte Manipulation zu ermöglichen
- Beim Abschalten des Geräts gehen die Daten verloren

IT-Systeme:

- Der Zugriff erfolgt über leistungsfähige Geräte
- Der Verlust der Vertraulichkeit der Daten stellt eine große Gefahr dar

Sicherheitsaspekte im Zusammenhang mit ICS

Geschäftliche Aspekte

- Standard Compliance und gesetzliche Vorgaben
- Service Levels
- Geschäftsstrategien und Sicherheitsrichtlinien

Betriebliche Aspekte

- Organisation betrieblicher Abläufe
- Qualitätskontrollen
- Betriebshandbücher

Technische Aspekte

- Sicherheitsrelevante Hard- und Software
- Mechanismen zu deren Verwaltung auf betrieblicher und geschäftlicher Ebene

Geschäftliche Aspekte

- Nachträgliche Investitionen in die Sicherheit einer Produktionsanlage können selten durch Preiserhöhungen finanziert werden

  Gründe:

  - Betreiber von ICS unterliegen oft gesetzlichen Vorgaben oder Preisregulierungen, die kurzfristige Preiserhöhungen ausschließen
  - Eine nachträgliche Kostensteigerung hat Auswirkungen auf Amortisierungszeitraum einer Industrieanlage
- Sicherheitsvorfälle haben direkte Auswirkungen auf dem Kapitalmarkt z.B. Aktienkurs des Unternehmens

Betriebliche Aspekte

- Für ICS zuständiges Personal ist wenig vertraut mit Sicherheitsaspekten
- Das Fehlen von Testumgebungen erschwert die Planung von Wartungsarbeiten sowie das Ausrollen von Sicherheitspatches
- Kosten für IT-Sicherheitsmaßnahmen wurden in der ursprünglichen Kalkulation nicht berücksichtigt
- Es gelten andere Voraussetzungen für das Design von Sicherheitsmechanismen. Beispiele:
  - Durch die geringe Anzahl bekannter Sicherheitslücken existieren mehr unbekannte Risiken
  - Systeme können während Updates nicht offline geschaltet werden
  - Systeme können nicht durch Zusatzsoftware vor Angriffen geschützt werden

Technische Aspekte

- Das Update von veralteten Systemen gestaltet sich schwierig
- Wegen der räumlichen Distanz zwischen den Steuerungskomponenten eines ICS ist die Fernwartung zwingend erforderlich
- Technische Modifikationen führen zu Garantieverlust
- Sicherheitsvorfälle können zu Verletzungen von Menschen führen und zu hohen finanziellen Schäden führen

Schwachstellen von ICS

- Verglichen mit klassischen IT-Systemen ist der Kenntnisstand bei Schwachstellen von ICS gering
- Eine systematische Klassifizierung von Schwachstellen ist erforderlich
- Ansatz: Einsatz von drei Klassen
  - Management Schwachstellen
  - Organisatorische Schwachstellen
  - Technische Schwachstellen

Management Schwachstellen I

- Fehlendes Risikomanagement
  - Potentielle durch ICS-Schwachstellen verursachte Schäden fließen oft nicht in das Risikomanagement ein
  - Konsequenz: Keine Berücksichtigung in strategischen Entscheidungen
- Unzureichende Richtlinien
  - Zuständigkeiten sind oft nicht in ausreichendem Maße geregelt
  - Konsequenz: Verantwortlichkeit des Managements ist nicht klar definiert

Management Schwachstellen II

- Unzureichende Finanzplanung
  - ICS-Sicherheit ist ein fortlaufender Prozess und keine einmalige Investition
  - Unzureichende Finanzplanung verhindert die Weiterentwicklung von Sicherheitsmaßnahmen
- Mangelndes Engagement des Managements
  - Oft fehlen von Seiten der Geschäftsleitung klare Leitlinien im Umgang mit ICS-Sicherheit
  - Es sollten elementare Anweisungen vorhanden sein z.B. NIST 800-82

Organisatorische Schwachstellen I

- Keine Trennung von ICS- und Office-Datenverkehr
  - ICS ist auch von Arbeitsplatzrechnern erreichbar
  - Office-Datenverkehr behindert die Kommunikation mit dem ICS
  - Malware kann sich über Office-Systeme auf das ICS ausbreiten
- Gemeinsam benutzte Administrationszugänge
  - Durchgeführte Aktivitäten sind nur schwer Personen zuordenbar
  - Berechtigungen orientieren sich nicht am Aufgabengebiet

Organisatorische Schwachstellen II

- Fernzugriff für Drittfirmen
  - Umfangreiche Steuerungsmöglichkeiten durch Wartungspersonal
  - Intransparenz durch fehlendes Identity and Access Management (IAM)
- Einsatz von drahtlosen Netzwerken
  - Wireless LANs sind einfach zu entdecken
  - Bei schlechter Konfiguration ist der Zugriff auf das Netzwerk einfach durchführbar

Organisatorische Schwachstellen III

- Schlechte Absicherung der Zugangspunkte im Internet
  - Einsatz von Komponenten in der Auslieferungskonfiguration
  - Unzureichende Wartung und Härtung der Zugangspunkte
- Umgang mit Sicherheitsvorfällen
  - Es gibt keinen Prozess, um einen Sicherheitsvorfall zu melden
  - Es findet keine automatisierte Überwachung hinsichtlich Sicherheitsvorfällen statt

Organisatorische Schwachstellen IV

- Nicht vorhandenes Change Management
  - Es gibt kein System zur Verwaltung von Software Patches und Updates
  - Konfigurationsmängel und Schwachstellen bleiben unentdeckt
- Fehlende Testverfahren und -umgebungen
  - Es stehen keine Testumgebungen zur Verfügung, um neue Komponenten und Software Updates vor dem produktiven Einsatz zu testen
  - Die Simulation von ICS ist aufwändig und teuer

Technische Schwachstellen

- Technische Schwachstellen stellen die größte Gefahrenquelle dar
- Diese Art von Schwachstellen beinhaltet Fehler in Hardware, Software und Netzwerken
- Die Recherche von Schwachstellen-Datenbanken offenbart, dass der Anteil ICS-spezifischer Schwachstellen sehr gering ist
- Ziel: Kategorisierung der technischen Schwachstellen

Kommunikationsarten eines PLCs

Internet-basierte Kommunikation

- Abruf von Daten über ein HMI oder einen SCADA Server
- Übertragungsweg für Exploits von außen
- Anfällig für Portscans und Denial-of-Service Angriffe

Input/Output (I/O) Kommunikation

- Steuerung der physikalischen Funktionen einer Anlage
- Ansprechen der Aktoren/Auslesen der Sensoren
- Störungen haben eventuell gravierende Auswirkungen

ICS-Schwachstellen

- PLCs und RTUs sind leistungsschwache Geräte, die keine aufwändigen Exploits ermöglichen
- PLCs und RTUs verfügen in der Regel über keine Benutzerverwaltung, d.h., gelingt der Zugriff auf das Gerät, dann hat man Administratorrechte
- Kommunikationsbeeinträchtigung:
  - Störung der Internet-Kommunikation $\rightsquigarrow$ Beeinträchtigung der Überwachung (degradation of view)
  - Störung der I/O-Kommunikation $\rightsquigarrow$ Beeinträchtigung der Steuerung (degradation of control)
- Einteilung:
  - Temporäre Störung
  - Permanente Störung
  - Gezielte Manipulation

Kategorien von technischen Schwachstellen

Unterteilung anhand der verursachten Störung:

- Denial of View
- Loss of View
- Manipulation of View
- Denial of Control
- Loss of Control
- Manipulation of Control

Beachte: Eine Schwachstelle kann mehreren Kategorien zugeordnet werden

Denial of View (DoV)

- Temporärer Ausfall der IP-Verbindung
- Das Netzwerkinterface erholt sich im Laufe der Zeit
- Die Funktion des PLC/RTU wird nicht beeinträchtigt
- Verlust von Produktionsdaten kann sich auf den kompletten Fertigungsablauf auswirken
- Fehlende Informationen können zu falschen Entscheidungen seitens des Bedienpersonals führen

Loss of View (LoV)

- Permanenter Ausfall der IP-Verbindung
- Ausfall kann nur durch Wartungspersonal behoben werden z.B. durch Neustart des Systems
- Die Funktion des PLC/RTU wird nicht beeinträchtigt
- Der Verlust von Produktionsdaten führt zu Beeinträchtigung des Fertigungsablaufs
- Es besteht die Gefahr von Fehlentscheidungen des Bedienpersonals durch fehlende Informationen

Manipulation of View (MoV)

- Es findet keine Beeinträchtigung der IP-Kommunikation statt
- Durch Einspielen gefälschter Daten werden Fehlentscheidungen des Bedienpersonals provoziert
- Das Berichtswesen des Unternehmens kann gezielt mit falschen Daten verunreinigt werden

Denial of Control (DoC)

- Temporärer Ausfall der I/O-Kommunikation
- Unbeabsichtigte Störungen:
  - Hardware Ausfälle
  - Fehlbedienung
  - Auswirkungen von DoV
- Beabsichtigte Störungen:
  - Angriff, der die I/O-Kommunikation des PLCs deaktiviert
  - „Nebenwirkungen“ eines DoV
- Störung ist automatisch behoben, wenn die Bedrohung nicht mehr existiert

Loss of Control (LoC)

- Permanente Störung, die zum kompletten Verlust der Kontrolle über das PLC führen kann
- Störung kann unbeabsichtigt oder absichtlich hervorgerufen werden
- Zur Behebung der Störung ist ein Eingriff des Wartungspersonals erforderlich

Manipulation of Control (MoC)

- Gezielte Manipulation des Codes eines PLC/RTU
- Keine Beeinträchtigung der I/O-Kommunikation
- Ausführung von Man-In-The-Middle Angriffen
- Risiko der kompletten Übernahme der Produktionsanlage durch Dritte
- Gefahr von gravierenden Schäden für den Produktionsbetrieb oder die Infrastruktur einer Stadt

Gefährdungsstufen

Stufe 1:

- DoV, aber kein DoC
- Risiko existiert nur, wenn die Beeinträchtigung über längere Zeit unentdeckt bleibt

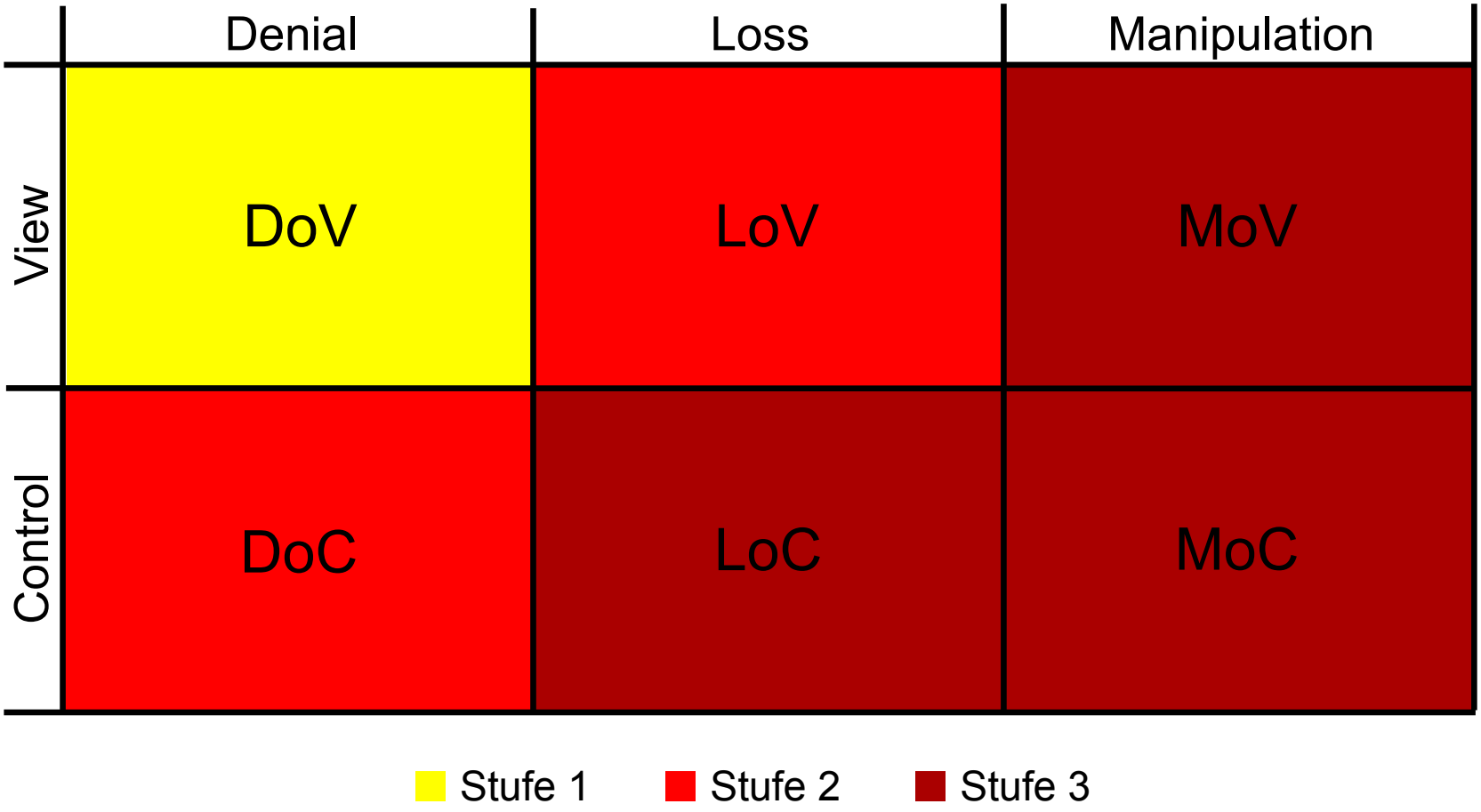
Stufe 2:

- LoV oder/und DoC
- Oft wechselseitige Beeinträchtigungen der Kommunikation
- Risiken hängen stark von der Art der Anlage ab

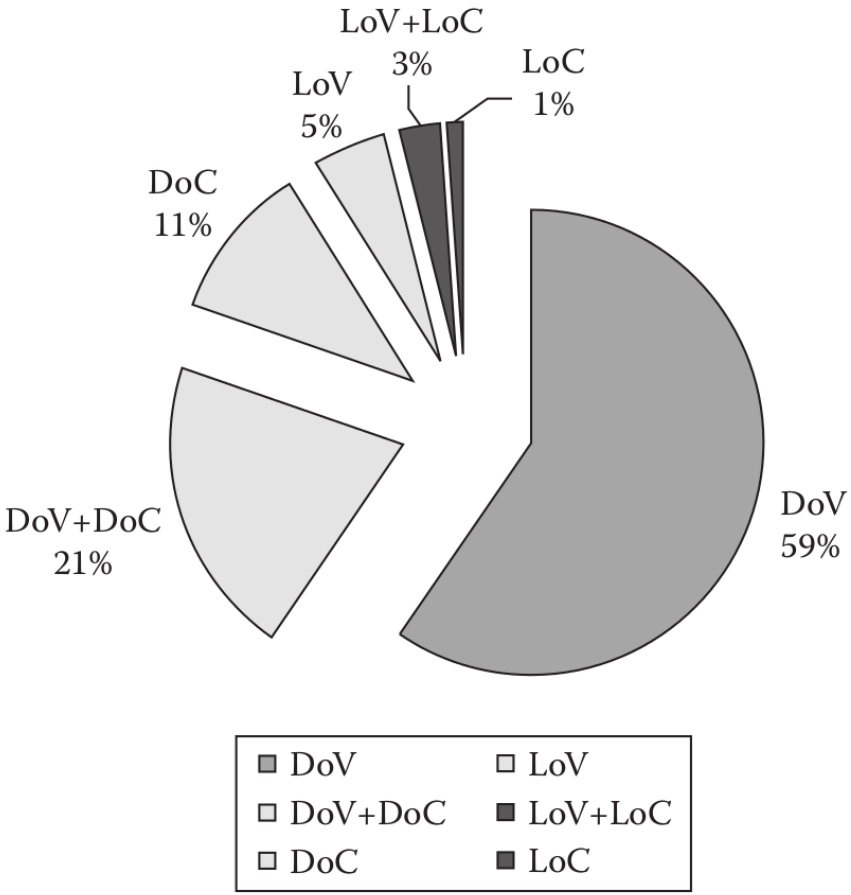
Stufe 3:

- MoV, LoC, MoC
- Regelbetrieb kann nur durch manuellen Eingriff wieder hergestellt werden
- Je nach Art der Anlage ist das Risiko schwer kalkulierbar z.B. wegen Dominoeffekten

Gefährdungspotential



Verteilung der Schwachstellen



Quelle: [MS12]

Typische Angriffsvektoren

- IT-Systeme im ICS-Netzwerk
- Wechselwirkungen mit IT-Systemen
- Unausgereifte Netzwerk-Stacks
- Trägheit bei der Entwicklung geeigneter Protokolle
- Leistungsschwache ICS-Hardware
- Denial-of-Service Attacken
- Fuzzing
- Man-in-The-Middle Attacken
- Packet Injection

IT-Systeme im ICS-Netzwerk

- Im mehr IT-Systeme werden innerhalb eines ICS-Netzwerk angesiedelt
- Für diese Systeme existieren zahlreiche Schwachstellen
- Die Systeme können als Ausgangspunkt für Angriffe auf die ICS-Komponenten dienen
- Ein infiziertes IT-System kann die Netzlast deutlich erhöhen und so die Arbeit der ICS-Komponenten beeinträchtigen

Wechselwirkungen mit IT-Systemen

- ICS werden zunehmend an die Unternehmens-IT angebunden
- Ein wesentlicher Vorteil dieser Anbindung ist Real-Time Verarbeitung der Produktionsdaten
- Oft wird die Anbindung nachträglich vorgenommen und ist besonders für Störungen anfällig
- Auch vom Internet separierte ICS können z.B. über Wartungsnotebooks mit den Gefahren des Internets in Berührung kommen

Unausgereifte Netzwerk-Stacks

- Viele ICS-Komponenten besitzen Eigenentwicklungen des TCP/IP-Stacks
- Oft sind die Implementierungen unausgereift oder unvollständig
- Die Implementierungen sind im Hinblick auf ein spezielles Einsatzgebiet entwickelt worden
- Durch „geschickt“ gewählte Pakete kann die Arbeitsweise des Stacks negativ beeinflusst werden
- Oft wird die Implementierung nicht unter Extrembedingungen (z.B. hohe Netzlast) getestet

Trägheit bei der Protokollentwicklung

- Protokolle mit Kinderkrankheiten oder Fehler im Design werden über eine lange Zeit eingesetzt
- Durch den langen Lebenszyklus von ICS-Komponenten kann ein schlechtes Protokoll nicht einfach ausgetauscht werden
- Protokolle mit nachgewiesenen Schwächen werden weiterhin verwendet z.B. Open Process Control (OPC)
- Sicherheitsmechanismen werden trotz Empfehlung des Herstellers nicht aktiviert, da es eine komplexe IT-Infrastruktur voraussetzt

Leistungsschwache ICS-Hardware

- Die Rechenleistung von ICS-Komponenten ist vergleichsweise gering
- ICS-Komponenten verfügen über wenig Hauptspeicher
- Vorteile:
  - Robustes Design für einen langen Lebenszyklus
  - Geringere Kosten für Beschaffung und Wartung
  - Geringere Anfälligkeit gegen Konfigurations- und Bedienungsfehler
  - Für viele Angriffe ein ungeeignetes Ziel
- Nachteile:
  - Keine Flexibilität in Hardware und Software
  - Aufwändiges Patch- und Update-Management

Denial-of-Service Attacken

- Flooding Angriffe haben das Ziel, ein System durch Auslastung des Netzwerks lahmzulegen
- Distributed Denial of Service (DDOS) Angriffe sind über Jahre hinweg eine der häufigsten Angriffsarten
- Eine Denial-of-Service Attacke kann die Funktionsfähigkeit von ICS-Komponenten stark beeinträchtigen

Fuzzing

- Unter Fuzzing versteht man das Versenden von nahezu zufälligen Datenpaketen an Geräte, um zu sehen wie diese sich verhalten
- In der Regel werden Pakete versendet, die nicht standardkonform sind
- Es gibt eine Vielzahl von Varianten, wie ein Paket und dessen Inhalt erzeugt wird
- Fuzzing kann sowohl absichtlich als auch unbeabsichtigt erfolgen
- Auch Umwelteinflüsse wie z.B. elektromagnetische Felder können zu Fuzzing führen

Man-in-The-Middle Attacken

- Man-In-The-Middle Angriffe treten bei klassischen IT-Systemen an vielen Stellen auf
- Im Umfeld von ICS stellen Man-In-The-Middle Angriffe ein geringes Risiko dar
- Gründe:
  - ICS-Komponenten sind leistungsschwach
  - Es ist eine umfangreiche Rekonfiguration des Netzwerks notwendig
- Man-In-The-Middle Angriffe auf die Unternehmens-IT können sich auch auf das ICS auswirken

Packet Injection

- Unter Packet Injection versteht man das wiederholte Senden von (evtl. veränderten) Paketen an ein IT-System
- Packet Injection kann bei ICS-Komponenten sehr effektiv sein
- Als Nebeneffekt ist ein DoS-Angriff möglich
- Der Sender kann ein kompromittiertes System oder ein extra eingeschleustes Gerät sein

Zusammenfassung

- ICS sind zunehmend Bedrohungen aus dem Internet ausgesetzt
- Viele Schwachstellen von IT-Systemen existieren auch bei ICS
- Die Auswirkungen eines Angriffs sind für IT-Systeme und ICS unterschiedlich
- Zum besseren Verständnis der Auswirkungen von Schwachstellen für ICS müssen diese kategorisiert werden
- Man unterscheidet zwischen geschäftlichen, betrieblichen und technischen Aspekten

Literatur I

Nate Anderson. *Confirmed: US and Israel created Stuxnet, lost control of it*. Ars Technica. 1. Juni 2012. URL: http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/ (besucht am 18. 06. 2013).

Dan Goodin. *We're going to blow up your boiler: Critical bug threatens hospital systems*. 7. Feb. 2013. URL: http://arstechnica.com/security/2013/02/were-going-to-blow-up-your-boiler-critical-bug-threatens-hospital-systems/ (besucht am 18. 06. 2013).

ICS-CERT, Hrsg. *Medical Devices Hard-Coded Passwords. Alert (ICS-ALERT-13-164-01)*. 13. Juni 2013. URL: http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01 (besucht am 18. 06. 2013).

Literatur II

Matthias Krempp und Konrad Lischka. *Computervirus Stuxnet: Der Wurm, der aus dem Nichts kam*. Spiegel Online. 22. Sep. 2010. URL: http://www.spiegel.de/netzwelt/web/computervirus-stuxnet-der-wurm-der-aus-dem-nichts-kam-a-718927.html (besucht am 18. 06. 2013).

Tyson Macaulay und Bryan Singer. *Cybersecurity for Industrial Control Systems — SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2012.

Louis-F. Stahl. "Gefahr im Netzwerk". In: *c't Magazin für Computertechnik* 11 (2013), S. 78–83.