LEHRSTUHL 14
SOFTWARE ENGINEERING

Willkommen zur Vorlesung

Methodische Grundlagen des Software-Engineering

im Sommersemester 2011

Prof. Dr. Jan Jürjens

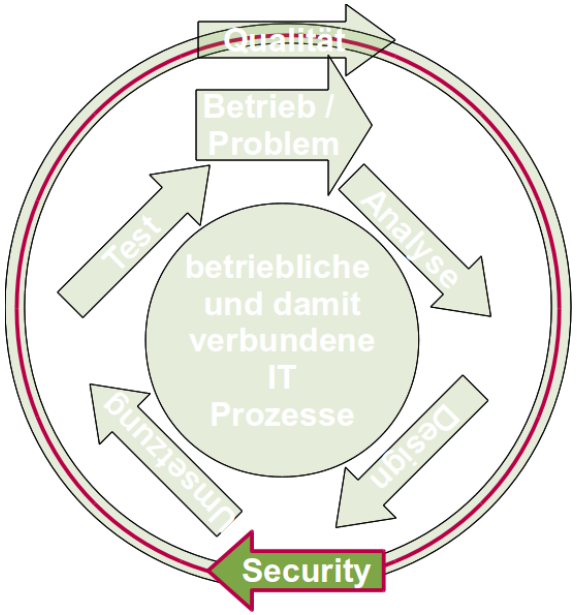
TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

15. Verlässlichkeit von Systemen

[inkl. Beiträge von Professor Summerville, St Andrews University]

Einordnung
Grundlagen Dependabilty & Security

- Was ist Dependabilty?
- Was ist Security?
- Wie hängen sie zusammen?



Einordnung
Grundlagen Qualität

- Business Prozesse
- Qualitätsmanagement
- Testen
- Sicherheit
  - Verlässlichkeit
  - IT Sicherheit
  - Netzwerksicherheit
- Sicheres Software Design

Die Themen

- Verlässlichkeits-Eigenschaften
  - Die System-Eigenschaften, die Verlässlichkeit (Dependability) herbeiführen.
- Verfügbarkeit (Availability) und Zuverlässigkeit (Reliability)
  - Das System sollte verfügbar sein und die Dienste wie erwartet zur Verfügung stellen.
- Safety (Unfallsicherheit)
  - Die Systeme sollten sich nicht in einer unsicheren Weise verhalten.
- Security (Angriffssicherheit)
  - Die Systeme sollten sich und ihre Daten vor externen Eingriffen schützen.

Verlässlichkeits-Eigenschaften

- Für viele IT-basierte Systeme ist Verlässlichkeit die wichtigste Systemeigenschaft.
- Die Verlässlichkeit eines Systems spiegelt das Maß an Vertrauen der Benutzer in das System wider. Es spiegelt das Ausmaß an Zuversicht wider, dass alles so funktioniert, wie der Benutzer es erwartet und nicht im Normalfall Fehler verursacht.
- Verlässlichkeit deckt die damit verbundenen Systemattribute der Zuverlässigkeit, Verfügbarkeit und Sicherheit ab. Diese sind alle voneinander abhängig.

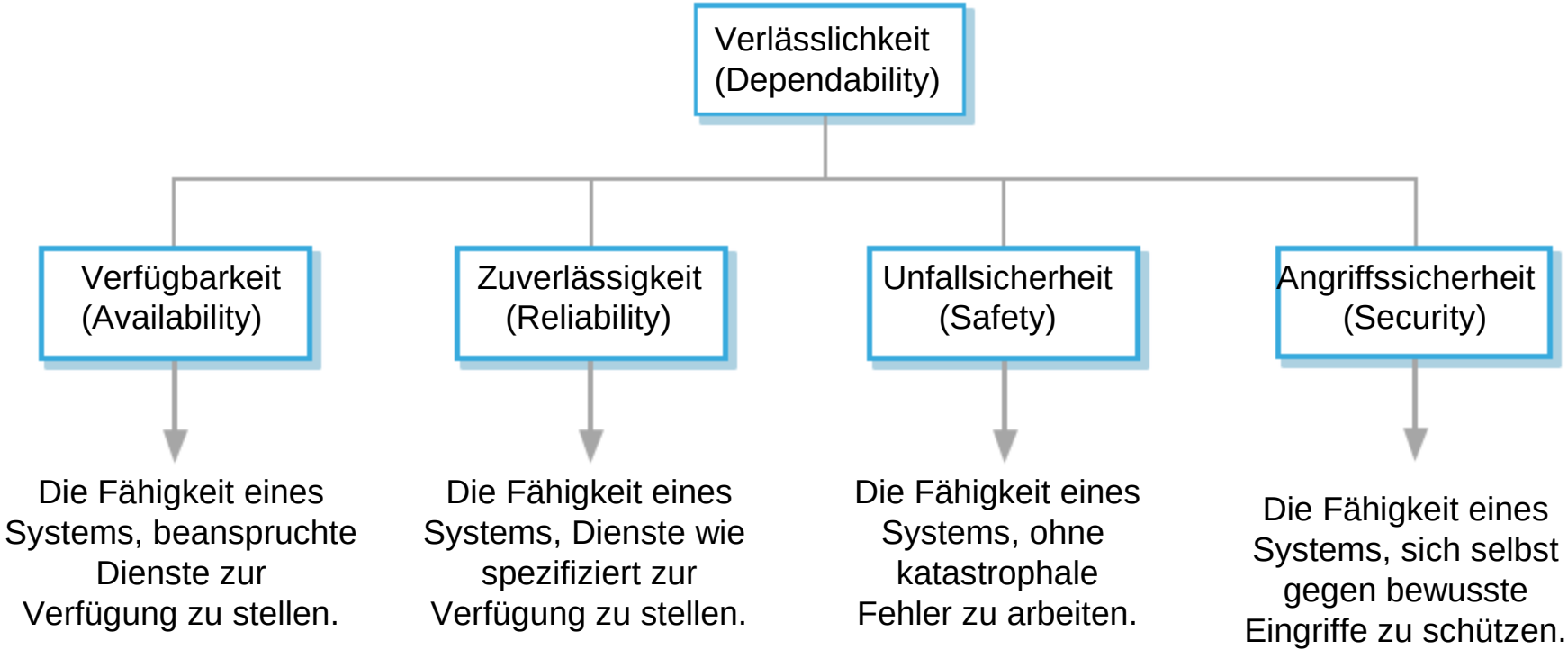
Wichtigkeit der Verlässlichkeit

- Systemausfälle können weitreichende Wirkungen haben, durch die eine große Zahl von Menschen durch den Ausfall betroffen sein können.
- Systeme, die nicht verlässlich und unzuverlässig, oder unsicher (i.S.v. Safety und Security) sind, können von ihren Nutzern abgelehnt werden.
- Die Kosten eines Systemausfalls können sehr hoch sein, wenn das Versäumnis zu wirtschaftlichen Verlusten führt oder physikalische Schäden verursacht werden.
- Unzuverlässige Systeme können Informationsverlust mit großen Reparaturkosten verursachen.

Ursachen des Scheiterns

- Hardware-Fehler
  - Hardware schlägt fehl, weil die Entwicklung und Fertigung Fehler aufweisen oder weil Komponenten das Ende ihrer Lebensdauer erreicht haben.
- Software-Fehler
  - Software ist fehlerhaft aufgrund von Fehlern in der Spezifikation, Design oder Umsetzung.
- Betriebsausfall
  - Benutzer machen Fehler. Heutzutage vielleicht die größte einzelne Ursache für Ausfälle in sozio-technischen Systemen.

Hauptsächliche Verlässlichkeitseigenschaften



Haupteigenschaften

- Verfügbarkeit (Availability)
  - Die Wahrscheinlichkeit, dass das System in Betrieb genommen werden kann und in der Lage ist, nützliche Dienste für die Nutzer zu liefern.
- Zuverlässigkeit (Reliability)
  - Die Wahrscheinlichkeit, dass das System Dienste wie vom Benutzer erwartet liefert.
- Unfallsicherheit (Safety)
  - Ein Urteil darüber, wie wahrscheinlich es ist, dass das System Schaden an Menschen oder seiner Umgebung verursacht.
- Angriffssicherheit (Security)
  - Ein Urteil darüber, wie wahrscheinlich es ist, dass das System zufällige oder vorsätzliche Angriffe abwehren kann.

Andere Verlässlichkeitseigenschaften

- Reparierbarkeit (Repairability)
  - Reflektiert das Ausmaß, in dem das System im Falle eines Ausfalls repariert werden kann.
- Wartbarkeit (Maintainability)
  - Reflektiert das Ausmaß, in dem das System an neue Anforderungen angepasst werden kann.
- Überlebensfähigkeit (Survivability)
  - Reflektiert das Ausmaß, in dem das System die Dienste während feindlicher Angriffe liefern kann.
- Fehlertoleranz (Error tolerance / fault tolerance)
  - Reflektiert das Ausmaß, inwieweit Eingabefehler durch den Benutzer oder Fehler durch die Hard- oder Software vermieden und toleriert werden können.

Reparierbarkeit

- Störung durch Systemausfällen kann minimiert werden, wenn das System schnell repariert werden kann.
- Dies erfordert Problemdiagnose, Zugang zu der ausgefallenen Komponente(n) um Änderungen vorzunehmen, um die Probleme zu beheben.
- Reparierbarkeit ist ein Urteil darüber, wie einfach es ist, die Fehler in der Software zu beheben, die zu einem Systemausfall führen könnten.
- Die Reparatur wird von der Betriebsumgebung beeinflusst; so ist es schwer abzuschätzen, wann diese abgeschlossen ist.

Wartbarkeit

- Ist ein Urteil darüber, wie leicht das System nach einem entdeckten Systemausfall oder Änderungen durch Hinzufügen von neuen Funktionen repariert werden kann.
- Abgrenzung:
  - Reparaturfreundlichkeit - kurzfristige Perspektive, das System zurück in Dienstbereitschaft zu setzen
  - Wartbarkeit - langfristige Perspektive.
- Sehr wichtig für kritische Systeme sind Fehler, die wegen Problemen bei Wartungsarbeiten in das System eingeführt werden. Wenn ein System wartbar ist, gibt es eine geringere Wahrscheinlichkeit, dass diese Fehler eingeführt werden oder unerkannt bleiben.

Überlebensfähigkeit

- Die Fähigkeit eines Systems, im Angesicht eines absichtlichen oder zufälligen Angriffs weiterhin seine Dienste für die Nutzer zu liefern.
- Dies ist eine zunehmend wichtige Eigenschaft für verteilte Systeme, deren Sicherheit kompromittiert werden kann.
- Ausfallsicherheit beinhaltet den Begriff der Resilienz - die Fähigkeit eines Systems, trotz Ausfall von Bauteilen weiter in Betrieb zu bleiben.

Fehlertoleranz

Fehlertoleranz gegenüber:

- Hardware- oder Softwarefehlern (fault tolerance)
- Benutzerfehlern (error tolerance)
  - Ist Teil der allgemeineren Eigenschaft „Benutzbarkeit“ (usability) und spiegelt den Umfang wider, in dem Benutzerfehler vermieden, erkannt oder toleriert werden. Benutzerfehler sollten so weit wie möglich erkannt und automatisch korrigiert werden und nicht zu Ausfällen des Systems führen.

Abhängigkeiten der Verlässlichkeitseigenschaft

- Sicherer Systembetrieb hängt davon ab, dass das System zur Verfügung steht und den Betrieb zuverlässig leistet.
- Ein System kann unzuverlässig sein, da seine Daten durch einen externen Angriff beschädigt worden sein könnten.
- Denial of Service-Angriffe auf ein System können es unverfügbar machen.
- Wenn ein System mit einem Virus infiziert ist, kann man nicht sicher sein, dass es zuverlässig oder sicher arbeitet.

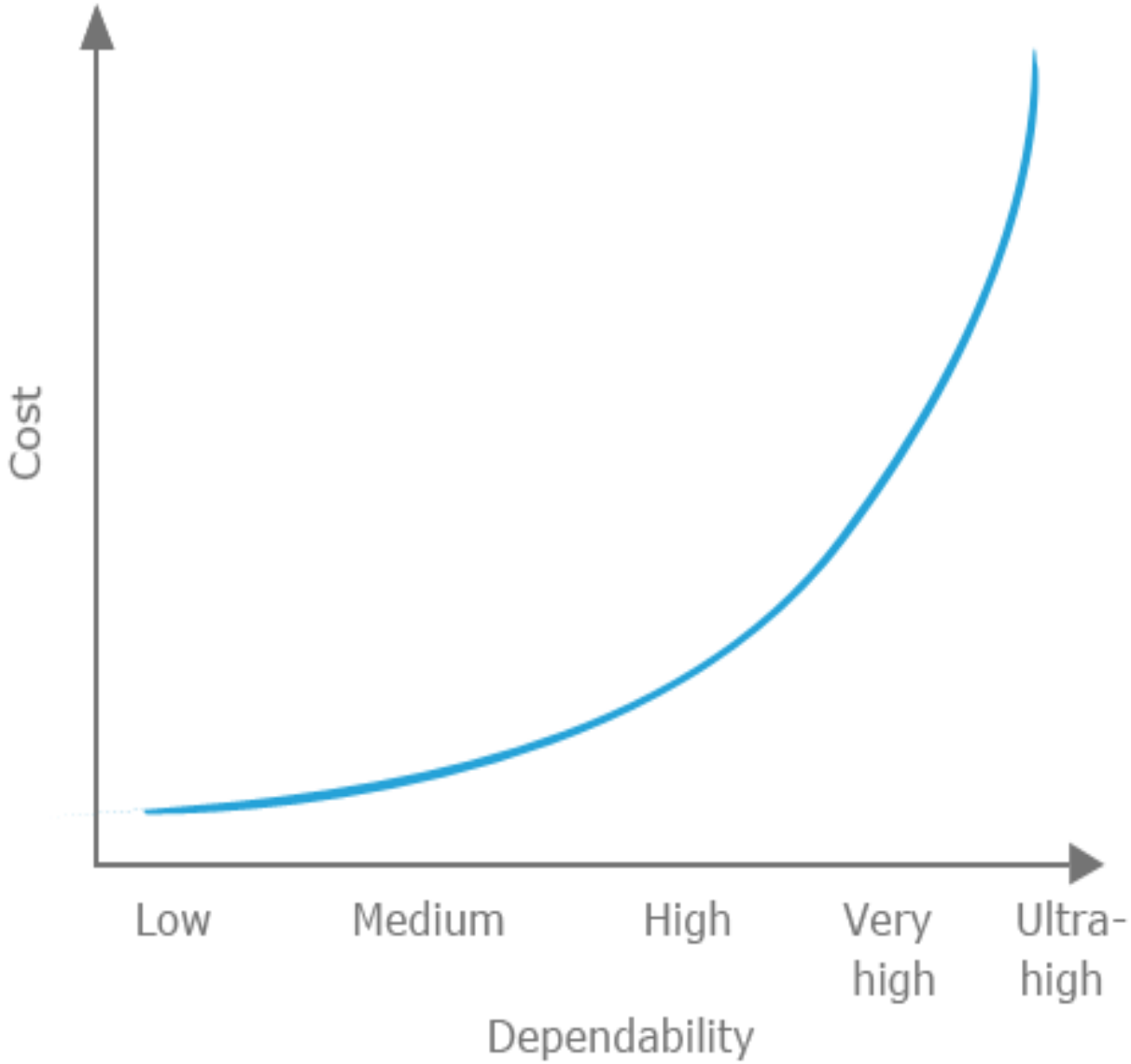
Erreichung der Verlässlichkeit

- Vermeidung von zufälligen Fehlern bei der Entwicklung des Systems.
- Prozesse für die Validierung und Verifikation des Entwurfs, die wirksam sind bei der Entdeckung von verbleibenden Fehlern im System.
- Design von Schutzmechanismen, die externe Angriffen abwehren.
- Ordnungsgemäße Konfiguration für die Betriebsumgebung.
- Recovery-Mechanismen zur Wiederherstellung des normalen Systembetriebs-Dienstes nach einem Ausfall.

Kosten der Verlässlichkeit

- Die Kosten der Verlässlichkeit neigen exponentiell mit dem erforderlichen Grad an Verlässlichkeit anzusteigen.
- Zwei Gründe:
  - Die Verwendung von teureren Entwicklungs-Techniken und Hardware, die erforderlich sind, um die höheren Ebenen der Verlässlichkeit zu erreichen.
  - Die erhöhte Prüfung und Validierung von Systemen, die erforderlich ist, um Kunden und Behörden von der geforderten Verlässlichkeit zu überzeugen.

Kosten/Verlässlichkeitskurve



Wirtschaftlichkeit der Verlässlichkeit

- Aufgrund der sehr hohen Kosten die Verlässlichkeit zu verwirklichen, kann es kostengünstiger sein, unzuverlässige Systeme anzunehmen und die Ausfallkosten zu bezahlen.
- Allerdings hängt dies von sozialen und politischen Faktoren ab. Nicht vertrauenswürdige Produkte haben negativen Einfluss auf die Reputation und damit das zukünftige Geschäftsergebnis.
- Abhängig von Systemtyp - insbesondere für unkritische Geschäftsanwendungen können bescheidene Niveaus von Verlässlichkeit ausreichend sein.

Verfügbarkeit und Zuverlässigkeit

- Zuverlässigkeit
  - Die Wahrscheinlichkeit eines störungsfreien Betriebs der Anlage über eine bestimmte Zeit in einem gegebenen Umfeld für einen bestimmten Zweck.
- Verfügbarkeit
  - Die Wahrscheinlichkeit, dass ein System zu einem gegebenen Zeitpunkt einsatzfähig sein wird und in der Lage ist, die geforderten Leistungen zu liefern.
- Beide Attribute können quantitativ ausgedrückt werden, z.B. Verfügbarkeit von 0,999 bedeutet, dass das System für 99,9% der Zeit in Betrieb ist.

Verfügbarkeit und Zuverlässigkeit

- Es ist manchmal möglich, Systemverfügbarkeit unter der Systemzuverlässigkeit zu subsumieren.
  - Wenn ein System nicht verfügbar ist, dann kann es seine Dienste natürlich auch nicht bereitstellen.
- Allerdings kann es Sinn machen, Systeme mit geringer Zuverlässigkeit aber hoher Verfügbarkeit zu haben.
  - Solange Systemfehler schnell repariert und Daten nicht beschädigt werden können, stellen einige Systemfehler kein Problem dar.
- Die Verfügbarkeit ist daher am besten als separate Eigenschaft zu definieren, ob das System seine Dienste liefern kann.
- Verfügbarkeit berücksichtigt Reparaturzeit (wenn das System zur Reparatur der Störungen außer Betrieb gebracht werden muss).

Die Wahrnehmung der Zuverlässigkeit

- Die formale Definition der Zuverlässigkeit spiegelt nicht immer die Wahrnehmung der Zuverlässigkeit durch die Anwender eines Systems wider.
  - Die Annahmen, die über die Umwelt getroffen werden, wie ein System verwendet werden kann, könnten falsch sein.
    - Die Nutzung eines Systems in einer Büroumgebung ist wahrscheinlich ganz anders als die Nutzung des gleichen Systems in einem universitären Umfeld.
  - Die Folgen von Systemausfällen beeinflussen die Wahrnehmung der Zuverlässigkeit.
    - Unzuverlässige Scheibenwischer in einem Auto können in einem trockenen Klima irrelevant sein.
    - Störungen, die schwerwiegende Folgen (z.B. ein Motorschaden im Auto) haben können, werden von den Benutzern höhergewichtiger eingeschätzt, als Fehler, die nur die Bequemlichkeit beeinträchtigen.

Zuverlässigkeit und Spezifikationen

- Zuverlässigkeit kann nur in Bezug auf eine System-Spezifikation formal definiert werden, d.h. ein Fehler ist eine Abweichung von einer Spezifikation.
- Allerdings sind viele Spezifikationen unvollständig oder unrichtig - d.h. ein System, das sich nach der Spezifikation richtet, kann aus der Sicht der Nutzer als "nicht bestanden" angesehen werden.
- Außerdem lesen Benutzer die Spezifikationen nicht und wissen damit nicht, wie sich das System verhalten soll.
- Daher ist die wahrgenommene Zuverlässigkeit in der Praxis wichtiger.

Die Wahrnehmung der Verfügbarkeit

- Die Verfügbarkeit ist in der Regel als Prozentsatz der Zeit definiert, die angibt, wie lange das System seine Dienste zur Verfügung stellt, z.B. ausgedrückt 99,95%.
- Allerdings werden zwei Faktoren nicht berücksichtigt:
  - Die Zahl der Nutzer, die vom Dienst-Ausfall betroffen sind. Dienstverlust mitten in der Nacht ist für viele Systeme weniger wichtig, als Verlust des Dienstes während der Spitzen-Nutzungszeiten.
  - Die Länge des Ausfalls. Je länger der Ausfall, desto größer die Störung. Mehrere kurze Ausfälle sind wahrscheinlich weniger störend, als ein langer Ausfall. Lange Reparaturzeiten sind ein besonderes Problem.

Wichtige Punkte

- Die Verlässlichkeit eines Systems spiegelt das Vertrauen der Anwender in dieses System wider.
- Verlässlichkeit ist ein Begriff, der verwendet wird, um eine Reihe von verwandten, nicht-funktionalen System-Attributen zu beschreiben - Verfügbarkeit, Zuverlässigkeit, Unfallsicherheit und Angriffsicherheit.
- Die Verfügbarkeit eines Systems ist die Wahrscheinlichkeit, dass es verfügbar sein wird, wenn seine Dienste beansprucht werden.
- Die Zuverlässigkeit eines Systems ist die Wahrscheinlichkeit, dass System-Dienste wie spezifiziert geliefert werden.

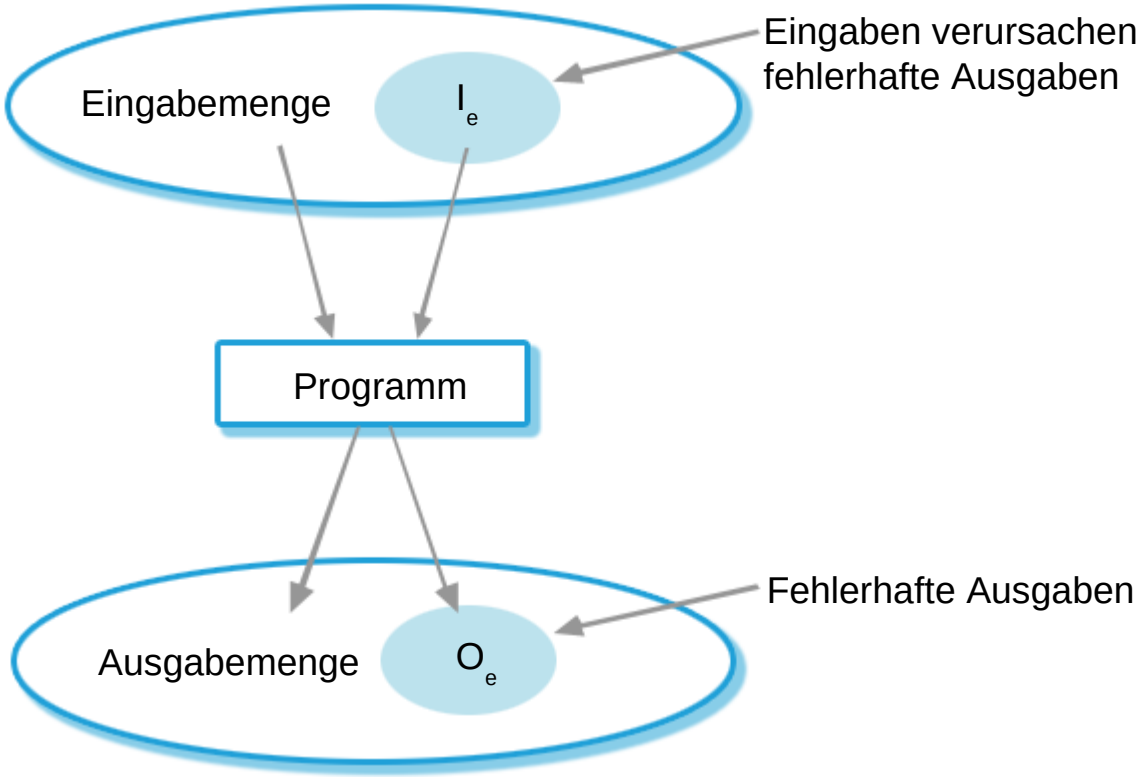
Terminologie der Zuverlässigkeit

Term	Description
Menschlicher Fehler	Menschliches Verhalten, dass Fehler in ein System einführt. Zum Beispiel könnte ein Programmierer in einem Wettervorhersagesystem entscheiden, dass die Zeit zur nächsten Übertragung berechnet wird, indem 1 Stunde auf die aktuelle Uhrzeit addiert wird. Dies funktioniert allerdings nicht zwischen 23.00 Uhr und Mitternacht.
Systemdefekt	Eine Eigenschaft eines Software-Systems, die zu einem Systemfehler führen kann. Der Fehler ist die Einbeziehung des Codes, eine Stunde auf die aktuelle Zeit zu addieren, um mit der nächsten Übertragung fortzufahren, ohne zu überprüfen, ob die Zeit größer oder gleich 23.00 Uhr ist.
Systemfehler	Ein fehlerhafter Systemzustand kann zu Verhalten führen, das vom Nutzer unerwartet ist. Der Wert der Sendezeit ist falsch (auf 24.XX anstatt 00.XX) gesetzt, wenn der fehlerhafte Code ausgeführt wird.
Systemausfall	Ein Ereignis, das irgendwann zu einem Zeitpunkt eintrifft, wenn das System seine Dienstleistung nicht, wie im Sinne von den Nutzern erwartet, liefern kann. Es werden keine Wetterbericht-Daten übertragen, weil die Zeit ungültig gesetzt wurde.

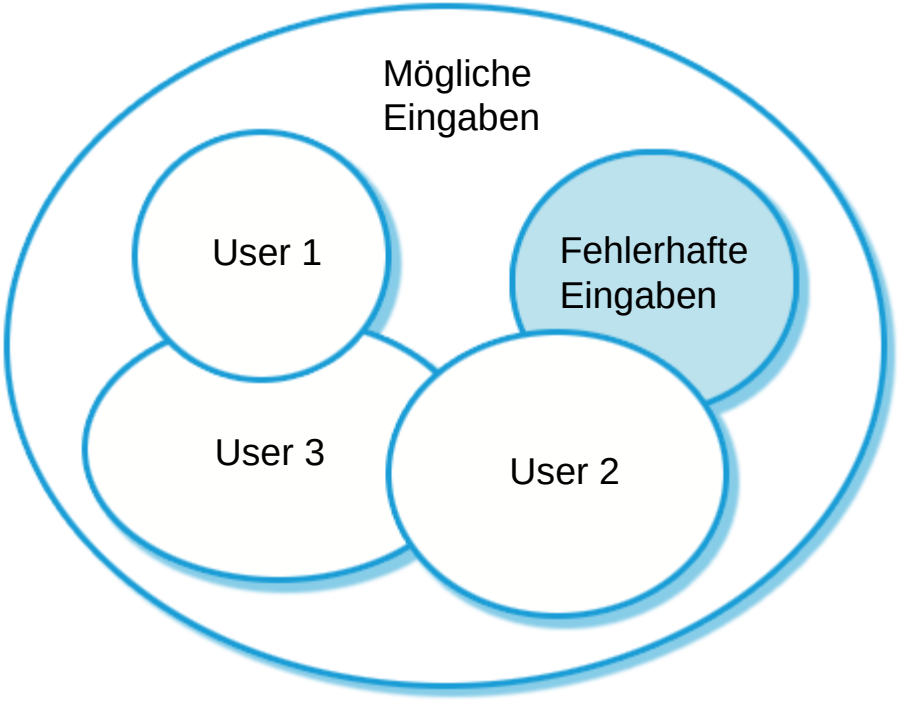
Störungen und Ausfälle

- Ausfälle sind in der Regel das Ergebnis von Systemfehlern, die aus Defekten im System abgeleitet werden.
- Allerdings führen Defekte nicht unbedingt zu Systemfehlern.
  - Die fehlerhafte Systemzustand, der aus der Störung resultiert, kann vorübergehend sein und "korrigiert" werden, bevor ein Fehler auftritt.
  - Der fehlerhafte Code wird ggf. nie ausgeführt.
- Fehler führen nicht unbedingt zu Systemausfällen.
  - Der Fehler kann durch eine integrierte Fehlererkennung und Wiederherstellung korrigiert werden.
  - Der Ausfall kann durch eingebaute Schutzeinrichtungen vermieden werden. Diese können zum Beispiel Systemressourcen vor Systemfehlern schützen.

Ein System als Input / Output-Diagramm



Software-Nutzungsmuster



Zuverlässigkeit vs. Fehler

- Entfernen von X% der Fehler in einem System führt nicht unbedingt zur Verbesserung der Zuverlässigkeit von X%. Eine Studie von IBM zeigt, dass die Entfernung von 60% der Mängel am Produkt in eine 3%ige Verbesserung der Zuverlässigkeit resultiert.
- Programmdefekte können in selten ausgeführten Teilen des Codes liegen, die niemals von den Benutzern bemerkt werden. Das Entfernen dieser Fehler hat keinen Einfluss auf die wahrgenommene Ausfallsicherheit.
- Benutzer passen ihr Verhalten an, um Systemfunktionalität zu vermeiden, die ausfallen kann.
- Ein Programm mit bekannten Fehlern kann daher noch immer als zuverlässig von den Nutzern wahrgenommen werden.

Verwirklichung der Zuverlässigkeit

- Fehlervermeidung
  - Es werden Entwicklungstechniken eingesetzt, die Fehler verringern oder vermeiden, bevor sie zu Systemdefekten führen.
- Fehlererkennung und Beseitigung
  - Verifikations- und Validierungs-Techniken, die die Wahrscheinlichkeit der Aufdeckung und Korrektur von Fehlern erhöhen, bevor das System in Betrieb genommen wird.
- Fehlertoleranz
  - Run-time Techniken, die eingesetzt werden, um sicherzustellen, dass Systemdefekte nicht zu Systemfehlern und/oder Systemausfällen führen.

Unfallsicherheit (Safety)

- Ist eine Eigenschaft eines Systems, welche die Fähigkeit des Systems darstellt (unter normalen oder unnormalen Umständen) ohne Gefahr, also ohne Verletzungen von Menschen und ohne Schäden der Systemumgebung zu arbeiten.
- Es ist wichtig, dabei die Sicherheit der Software zu betrachten, da die meisten Geräte, deren Ausfall kritisch ist, jetzt in Kontrolle von softwarebasierten Steuerungssystemen liegen.
- Sicherheitstechnische Anforderungen sind oft exklusive Anforderungen, d.h. sie schließen unerwünschte Situationen aus, anstatt die benötigten Systemdienste zu gewährleisten. Sie erzeugen funktionale Sicherheitsanforderungen.

Sicherheitskritikalität

- Primäre sicherheitskritische Systeme
  - Eingebettete Software-Systeme, deren Ausfall zum Scheitern der zugehörigen Hardware führen kann und direkt Menschen bedroht werden. Als Beispiel sei die Steuerung der Insulinpumpe genannt.
- Sekundäre sicherheitskritische Systeme
  - Systeme, deren Versagen zu Störungen in anderen (sozio-technischen) Systemen führen, die dann Sicherheits-Konsequenzen mit sich bringen. Zum Beispiel ist eine Datenbank mit Patientendaten sicherheitskritisch, da ein Versagen zu unsachgemäßer Behandlung führen kann.

Unfallsicherheit und Zuverlässigkeit

- Unfallsicherheit und Zuverlässigkeit sind verwandt aber unterschiedlich.
  - Im Allgemeinen sind die Zuverlässigkeit und Verfügbarkeit notwendige, aber nicht hinreichende Bedingungen für Unfallsicherheit.
- Zuverlässigkeit betrifft Übereinstimmung einer gegebenen Spezifikation und Lieferung des Dienstes.
- Unfallsicherheit stellt sicher, dass das betroffene System keinen Schaden anrichten kann, unabhängig davon, ob es der Spezifikation entspricht oder nicht.

Unsichere (i.S.v. Unfallsicherheit) aber zuverlässige Systeme

- Es können versteckte Fehler in einem System sein, die seit vielen Jahren unentdeckt sind und nur selten auftreten.
- Spezifikations-Fehler
  - Wenn die System-Spezifikation falsch ist, dann kann sich das System wie angegeben verhalten, aber immer noch einen Unfall verursachen.
- Hardware-Ausfälle erzeugen falsche Eingaben.
  - Schwer in der Spezifikation zu antizipieren.
- Kontext-sensitive Befehle, d.h. den richtigen Befehl zum falschen Zeitpunkt erteilen.
  - Häufig die Folge von Fehlbedienungen.

Unfallsicherheit (Safety): Terminologie

Begriff	Definition
Unfall (oder Unglück)	Ein ungeplantes Ereignis oder eine Folge von Ereignissen, die als Ergebnis den Tod, Körperverletzung oder Sach- oder Umweltschäden ergeben. Eine Überdosierung von Insulin ist ein Beispiel für einen Unfall.
Gefahr	Eine Bedingung mit dem Potenzial für die Verursachung oder Beitragung zu einem Unfall. Ein Ausfall des Sensors für die Blutzucker-Messung ist ein Beispiel für eine Gefahr.
Schäden	Ein Maß für die Verluste durch ein Missgeschick. Der Schaden als Ergebnis eines Unfalls kann zu geringfügigen Verletzungen oder Sachschäden bis hin zum Verlust von vielen Menschen reichen. Schäden durch eine Überdosis Insulin können zu ernsthaften Verletzungen oder dem Tod des Anwenders der Insulinpumpe führen.
Schwere der Gefahr	Eine Bewertung der schlimmstmöglichen Schäden, die sich aus einer bestimmten Gefahr ergeben. Die Schwere der Gefahr reicht von katastrophal (viele Menschen werden getötet), zu klein (nur kleinere Schäden werden verursacht). Wenn auch nur ein einzelner Tod möglich ist, so ist eine angemessene Beurteilung der Schwere der Gefahr als "sehr hoch" anzusehen.
Gefahr-Wahrscheinlichkeit	Die Wahrscheinlichkeit der Ereignisse, die eine Gefahr darstellen können. Wahrscheinlichkeitswerte sind eher willkürlich, reichen aber von "wahrscheinlich" (z.B. 1/100 Chance dass eine Gefährdung auftritt) zu "unglaubwürdig" (keine denkbaren Situationen sind wahrscheinlich, in denen Gefahr besteht). Die Wahrscheinlichkeit eines Ausfall des Sensors der Insulinpumpe, die zu einer Überdosierung führt ist wahrscheinlich gering.
Risiko	Dies ist ein Maß für die Wahrscheinlichkeit, dass das System einen Unfall verursacht. Das Risiko wird unter Berücksichtigung der Gefahr-Wahrscheinlichkeit, der Schwere der Gefahr und der Wahrscheinlichkeit, dass die Gefahr zu einem Unfall führt, bewertet. Das Risiko einer Überdosierung von Insulin ist wahrscheinlich mittel bis niedrig.

Verwirklichung der Unfallsicherheit (Safety)

- Gefahrenabwehr
  - Das System ist so konzipiert, dass sich einige Arten der Gefahr einfach nicht ergeben.
- Gefahr-Erkennung und -Entfernung
  - Das System ist so konzipiert, dass Gefahren erkannt und beseitigt werden, bevor sie zu einem Unfall führen.
- Schadensbegrenzung
  - Das System umfasst Schutz-Funktionen, die die Schäden minimieren, die aus einem Unfall entstehen können.

Normale Unfälle

- Unfälle in komplexen Systemen haben selten eine einzelne Ursache, da diese Systeme dazu entworfen sind, Einzelausfälle kompensieren zu können.
  - Systeme so zu entfernen, dass ein einzelner Ausfall nicht zu einem Unfall führt, ist grundlegendes Prinzip des sicheren System-Entwurfs.
- Fast alle Unfälle sind das Ergebnis einer Kombination von Störungen, anstatt einzelner Ausfälle.
- Es ist wahrscheinlich der Fall, dass ist die Analyse des Problems in alle Kombinationen, vor allem im software-gesteuerten Systemen nicht möglich ist, sodass die Erreichung absoluter Sicherheit unmöglich ist. Unfälle sind unvermeidlich.

Vorteile der Verwendung von Software in sicherheitskritschen Systemen

- Obwohl Software-Fehler sicherheitskritisch sein können, trägt die Verwendung von Software-Steuerungen zur erhöhte Systemsicherheit bei.
  - Software-Überwachung und -Steuerung ermöglicht ein breiteres Spektrum von Bedingungen, die überwacht und gesteuert werden können, als dies mit Hilfe elektromechanischer Sicherheitssysteme möglich wäre.
  - Software-Steuerung ermöglicht Sicherheitsstrategien die angenommen werden können, sodass die verbrachte Zeit in gefährdeten Bereichen minimiert wird.
  - Software kann sicherheitskritische Bedienfehler erkennen und korrigieren.

Angriffsicherheit (Security)

- Die Angriffsicherheit eines Systems ist eine Systemeigenschaft, die die Fähigkeit des Systems widerspiegelt, sich gegen zufällige oder vorsätzliche Angriffe von außen schützen.
- Angriffsicherheit ist wichtig, da die meisten Systeme so vernetzt sind, dass der externe Zugriff auf das System über das Internet möglich ist.
- Angriffsicherheit ist eine wesentliche Voraussetzung für die Verfügbarkeit, Zuverlässigkeit und Unfallsicherheit (Safety).

Angriffsicherheit vs. Zuverlässigkeit

- Wenn ein System ein vernetztes, unsicheres System ist, dann sind die Aussagen über seine Zuverlässigkeit und Unfallsicherheit unzuverlässig.
- Diese Aussagen sind abhängig davon, dass das ausführende System und das entwickelte System die gleichen sind. Allerdings kann Intrusion das ausführende System und/oder seine Daten verändern.
- Daher sind die Zuverlässigkeits- und Unfallsicherheits-Zusicherungen nicht mehr gültig.

Terminologie der Angriffsicherheit

Begriff	Definition
Vermögenswert	Etwas von Wert muss geschützt werden. Der Vermögenswert kann die Software selbst oder Daten sein, die von diesem System verwendet werden.
Exposition	Möglicher Verlust oder Schaden an einem Computersystem. Dies kann der Verlust oder die Beschädigung von Daten sein oder einen Verlust von Zeit und Aufwand bedeuten, wenn eine Wiederherstellung nach einer Sicherheitsverletzung notwendig ist.
Verwundbarkeit	Eine Schwäche in einem computer-basierten System, die genutzt wird, um Verlust oder Schaden anzurichten.
Angriff	Die Ausnutzung einer Systemschwachstelle. Im Allgemeinen findet dies von außerhalb des Systems statt und ist ein gezielter Versuch, Schaden anzurichten.
Bedrohungen	Umstände, die das Potenzial haben, Verlust oder Schaden zu verursachen (d.h. eine Systemschwachstelle, die einem Angriff ausgesetzt ist).
Kontrolle	Eine Schutzmaßnahme, welche die Anfälligkeit eines Systems verringert. Die Verschlüsselung ist ein Beispiel für ein Steuerelement, das eine Schwachstelle von einem schwachen Zutrittskontrollsystem reduziert.

Beispiele für Angriffsicherheits-Terminologie: Patienten-Datenbank

Begriff	Beispiel
Vermögenswert	Die Aufzeichnungen über jeden Patienten, der eine Behandlung erhalten wird oder erhalten hat.
Exposition	Mögliche finanzielle Verluste aus zukünftigen Patienten, die sich nicht behandeln lassen, weil sie kein Vertrauen in die Klinik haben, um ihre Daten zu pflegen. Finanzieller Verlust durch Klagen z.B. von Prominenten. Verlust der Reputation.
Verwundbarkeit	Ein schwaches Passwortsystem, welches es den Nutzern leicht macht, sein Passwort so zu wählen, dass man es erraten kann. Benutzername identisch mit Name des Benutzers.
Angriff	Einloggen des Angreifers als ein autorisierter Benutzer.
Bedrohung	Ein nicht autorisierte Benutzer erlangt Zugriff auf das System durch Erraten der Zugangsdaten (Benutzername und Passwort) von einem autorisierten Benutzer.
Kontrolle	Ein Passwortüberprüfungssystem, das Eigennamen oder Wörter, die normalerweise in einem Wörterbuch enthalten sind, verbietet.

Bedrohungsklassen

- Bedrohungen für die Vertraulichkeit des Systems und seiner Daten.
  - Kann Informationen an Personen oder Programme preisgeben, die keinen berechtigten Zugang zu diesen Informationen haben.
- Bedrohungen für die Integrität des Systems und seiner Daten.
  - Kann der Software schaden oder deren Daten manipulieren.
- Bedrohungen für die Verfügbarkeit des Systems und seiner Daten.
  - Können den Zugriff auf das System und die Daten für autorisierte Benutzer einschränken.

Schäden durch mangelnde Angriffssicherheit

- Denial of Service
  - Das System wird in einen Zustand gezwungen, in dem normale Dienste nicht verfügbar sind oder die Leistung deutlich abgebaut hat.
- Verfälschung von Programmen oder Daten
  - Die Programme oder Daten im System könnten auf nicht genehmigte Weise verändert worden sein.
- Offenlegung von vertraulichen Informationen
  - Informationen, die vom System verwaltet werden, könnten für Menschen, die nicht berechtigt sind diese zu lesen oder zu nutzen, offenbart werden.

Erreichung von Angriffsicherheit

- Vermeidung von Sicherheitslücken
  - Das System ist so konzipiert, dass Schwachstellen nicht auftreten. Zum Beispiel: wenn es keine externe Netzwerkverbindung gibt, dann sind externe Angriffe unmöglich.
- Angriffserkennung und -beseitigung
  - Das System ist so entworfen, dass Angriffe auf Schwachstellen erkannt und neutralisiert werden, bevor sie ein Risiko darstellen. Zum Beispiel finden und entfernen Virenscanner Viren, bevor sie ein System infizieren.
- Risikobegrenzung und Datenwiederherstellung
  - Das System ist so konzipiert, dass die negativen Folgen eines erfolgreichen Angriffs minimiert werden. Zum Beispiel ermöglicht ein Backup, die beschädigten Daten wiederherzustellen.

Wichtige Punkte

- Zuverlässigkeit hängt mit der Wahrscheinlichkeit zusammen, dass ein Fehler im operativen Einsatz auftritt. Ein System mit bekannten Defekten kann trotzdem zuverlässig sein.
- Unfallsicherheit (Safety) ist eine Systemeigenschaft, die die Fähigkeit des Systems widerspiegelt, ohne Gefahr für Mensch und Umwelt betreiben zu werden.
- Angriffsicherheit (Security) ist eine Systemeigenschaft, die die Fähigkeit des Systems widerspiegelt, sich vor Angriffen von außen zu schützen.
- Die Verlässlichkeit ist gefährdet, wenn ein System unsicher ist und der Code oder Daten beschädigt werden können.

Zusammenfassung

- Lesson Learned
  - Verlässlichkeit und seine Eigenschaften
    - Verfügbarkeit
    - Zuverlässigkeit
    - Unfallsicherheit
    - Angriffssicherheit
    - Reparierbarkeit
    - Wartbarkeit
    - Überlebensfähigkeit
    - Fehlertoleranz