QUALITY ASSURANCE

Software-Engineering 2

Jan Philipps, Adil Khan, Can Bulut, Janine Galka, Serkan Celik

Brenan Keller
@brenankeller

A QA engineer walks into a bar.
Orders a beer. Orders 0 beers.
Orders 99999999999 beers.
Orders a lizard. Orders -1 beers.
Orders a ueicbksjdhd.

First real customer walks in and asks where the bathroom is. The bar bursts into flames, killing everyone.

1:21 PM · 30 Nov 18

GLIEDERUNG

- Einblick in die QA
- Waterfall vs Agile
- Use/User Error
- DAU
- Penetration Test
- Code Beispiel

GESCHICHTE UND EINFÜHRUNG

- Anfänge schon vor hunderten von Jahren
  - Gilden wollten Ruf schützen
  - Nur ausgewählte Handwerker wurden aufgenommen
- Zunehmende Relevanz mit der Industriellen Revolution
  - Zuvor wurde jedes Produkt vom Handwerker begutachtet
  - Maschinelle Fertigung macht das fast unmöglich

GESCHICHTE UND EINFÜHRUNG

- Erster Weltkrieg
  - Massenproduktion
  - Sinkende Qualität
  - Hauptberufliche Qualitätstester/Aufseher
- Zweiter Weltkrieg
  - Erneuter Anstieg von Produktionsumfang
  - Komplexere Maschinen
  - Große Mengen an Munition mussten überprüft werden
  - 1947: Gründung der ISO

GESCHICHTE UND EINFÜHRUNG

- Computersysteme
  - Unübersichtlich,Abstrakt
  - Praktisch eine Blackbox
  - Verschiedene Bereiche (Software, Hardware, logische Schichten)
  - Testen sehr aufwendig
  - Viele potenzielle Fehlerstellen

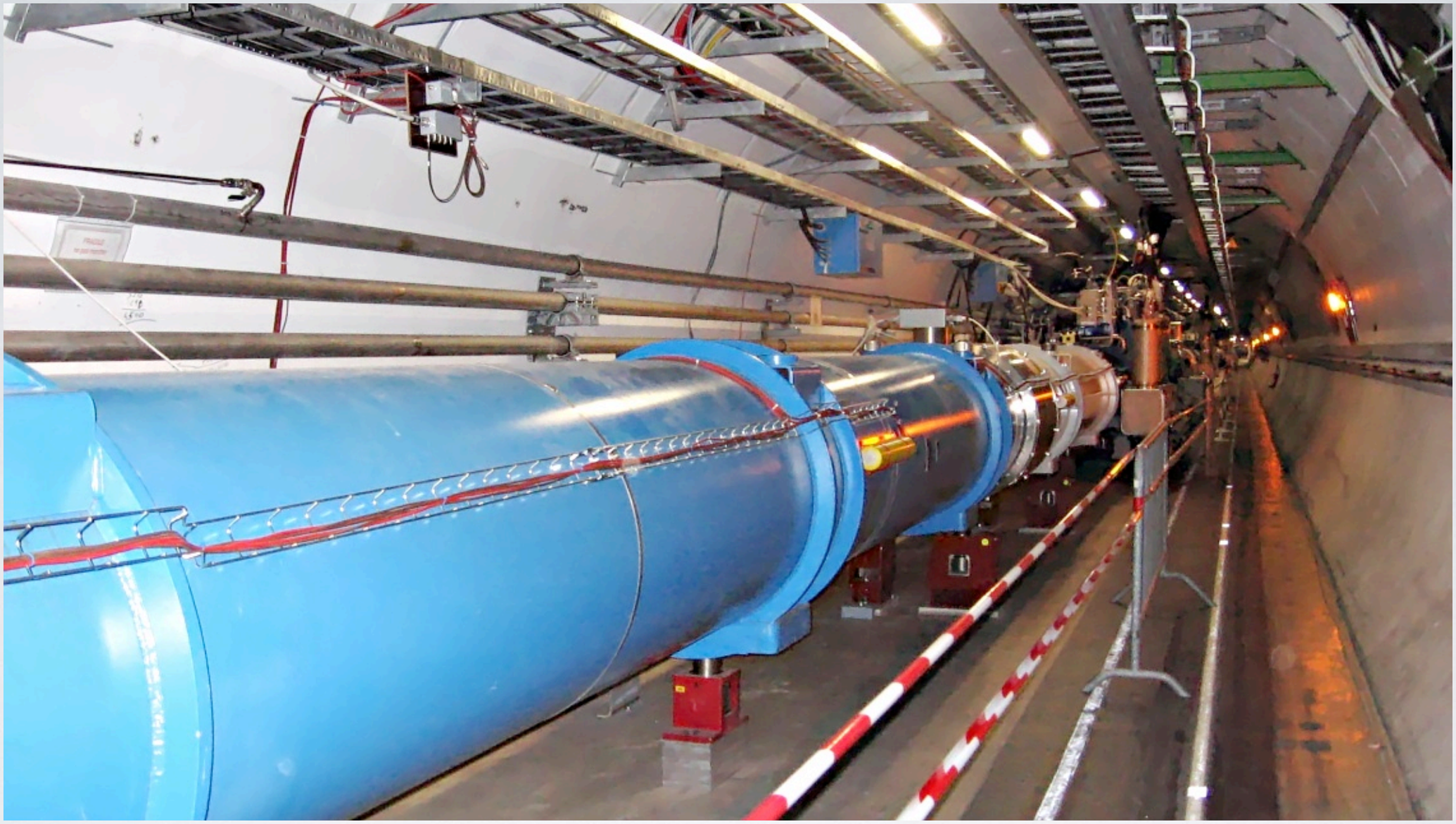
http://img.gawkerassets.com/img/17zls92f5eng3jpg/original.jpg

GESCHICHTE UND EINFÜHRUNG

- 1987: ISO 9000 Normreihe für QA Prozesse
- Verteilte Systeme/ Persönliche Computer
  - Mehr Angriffsfläche
  - Unerwartete Ereignisse
  - Unerfahrene Nutzer
  - Kleine Fehler führen zu großen Schäden
- Kritische Systeme
  - Komplexe (Computer) Systeme werden immer wichtiger (Medizin, Wirtschaft, Strom/Wasserversorgung, Militär)
  - Hohe Nutzerzahlen bei Computersystemen
  - Konsequenzen von Fehlern immer schlimmer

HEUTE

- QA ist aus modernen Softwareprojekten nicht mehr wegzudenken
- 25% des Budgets für QA genutzt
- ISO 9001:2015 regelt QA-Prozesse
    - Kunden im Fokus
    - Aktuell bleiben
    - Arbeitsabläufe für effiziente Fehlerfindung
- Verschiedene SQA Strategien
    - Water
    - Agile
    - Scrum



LARGE HADRON COLLIDER

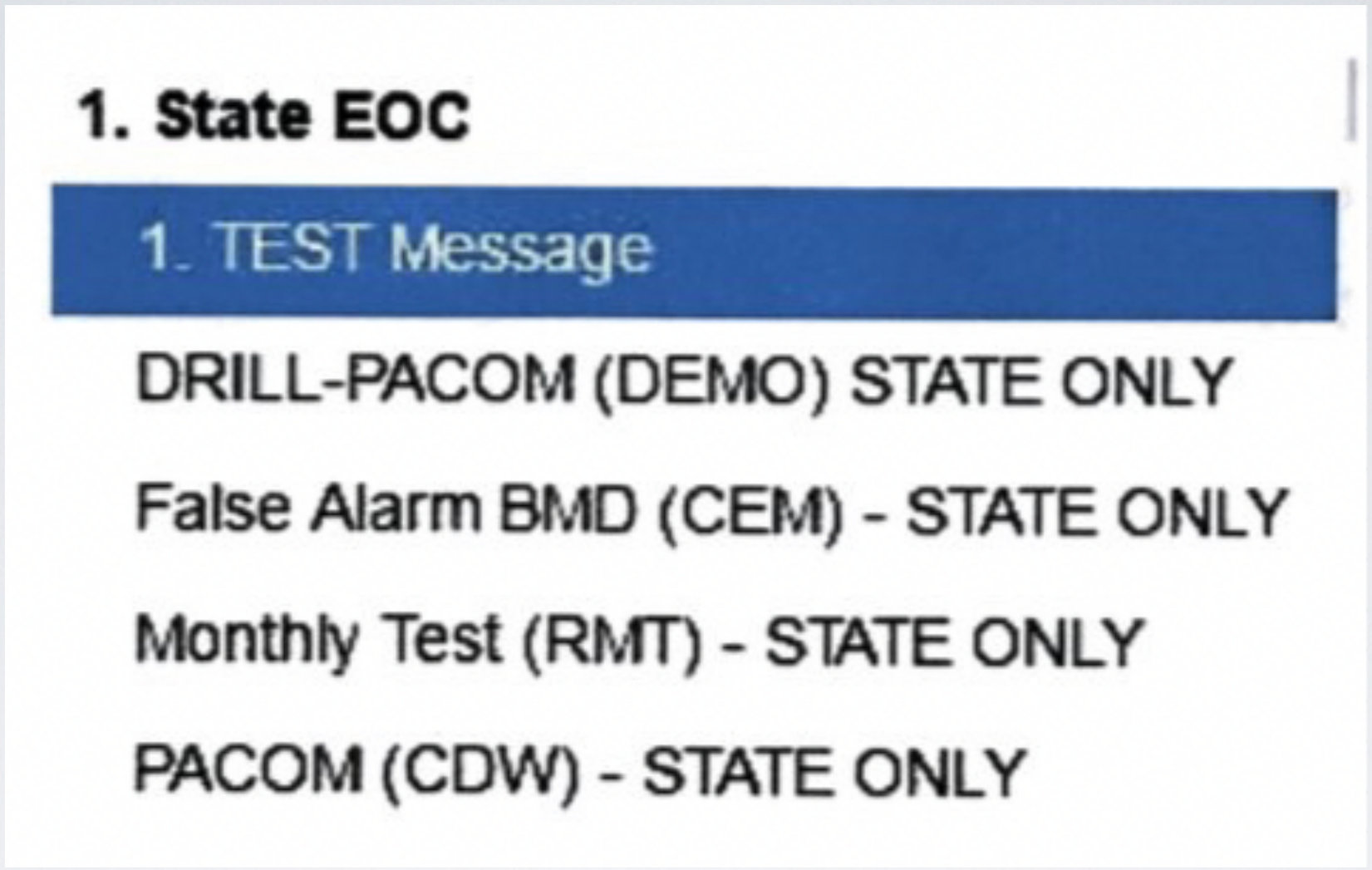
Komplexeste Maschine auf dem Planeten

Software-Engineering 2

Jan Philipps, Adil Khan, Can Bulut, Janine Galka, Serkan Celik

FALSCHER ALARM JANUAR 2018

Jan Philipps, Adil Khan, Can Bulut, Janine Galka, Serkan Celik



FALSCHER ALARM JANUAR 2018

Jan Philipps, Adil Khan, Can Bulut, Janine Galka, Serkan Celik

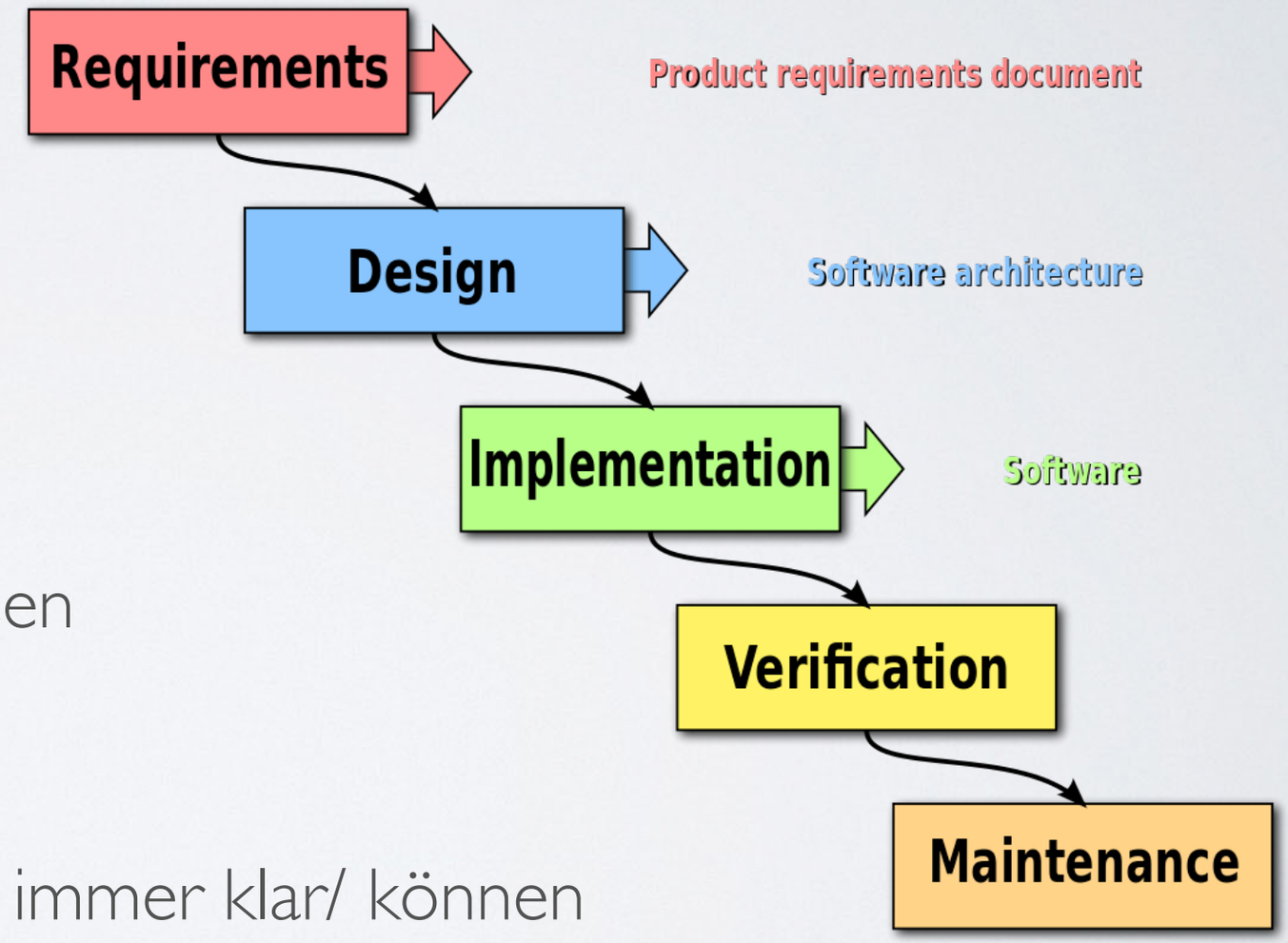
FALSCHER ALARM SEPTEMBER 1983

Frühwarnsystem hielt Wolken für nuklearen Erstschlag
Stanislov Petrov meldete den Alarm als falsch und verhinderte Vergeltungsschlag

Jan Philipps, Adil Khan, Can Bulut, Janine Galka, Serkan Celik

WATERFALL

- Sequentieller Ablauf von nach Unten (Wasserfall)
- Je früher das Problem gefunden desto billiger ist er zu beheben (50 - 200x)
- 20-40% in den ersten zwei Phasen
  30-40% fürs Coden
- Ersten beiden Phasen sind nicht immer klar/ können sich ändern



AGILE

- Iterative Vorgehensweise
- Bürokratischer aufwand und Regeln so gering wie möglich
- Schnell an Änderungen anpassen
- 4 Leitsätze
  - Individuen und Interaktion stehen über Prozessen und Werkzeugen
  - Funktionierende Software steht über einer umfassenden Dokumentation
  - Zusammenarbeit mit dem Kunden steht über der Vertragsverhandlung
  - Reagieren auf Veränderungen steht über dem Befolgen eines Plans

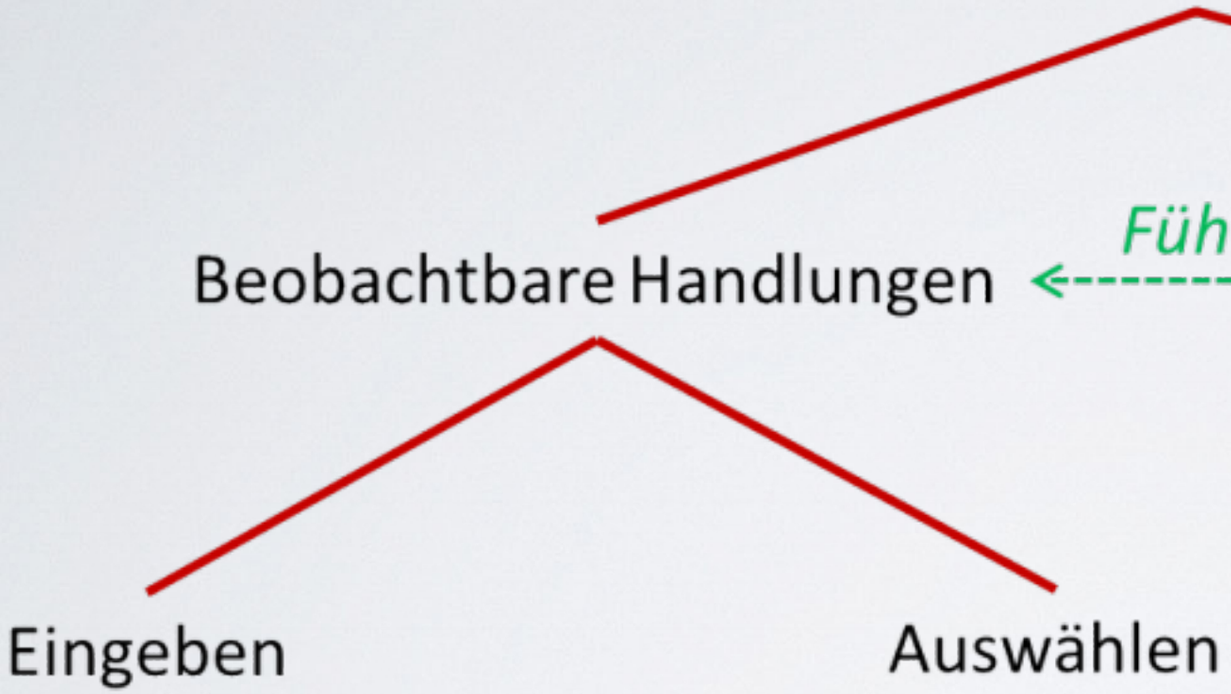
USE UND USER-ERROR

- Unterschied zwischen Use und User Error
- Gefährdung durch beobachtbare Handlungen
- Normaler sowie abnormaler Gebrauch
- Verschiedene Ursachen
- Kognitive Fehler können auftreten
- Error in Perception , Error in Cognition , Knowledge Based Error , Action Errors

USE UND USER-ERROR

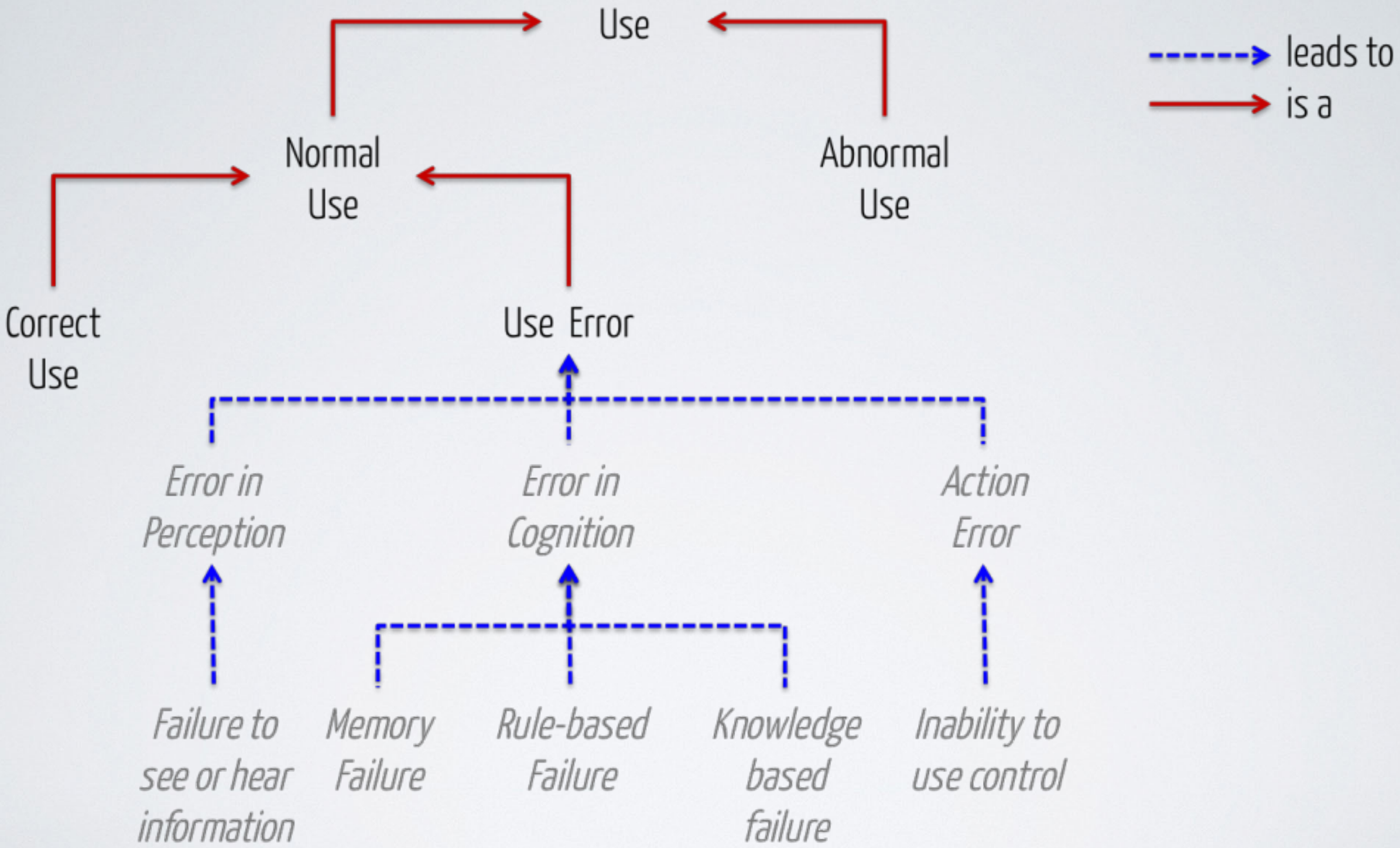
Use error and user error are terms for a mistake that a user makes in using a technology. In many cases, such "mistakes" aren't due to any fault on the part of the user as a technology may be poorly designed such that errors are likely.

Use Error vs User Error		
	Use Error	**User Error**
Definition	A mistake that occurs as a person uses technology.	A mistake that occurs as a person uses technology.
Implies	A poorly designed technology or human error.	Human error



Kognitive Leistungen

- Erkennen
- Sehen
- Verstehen
- Unterscheiden


Use
leads to
is a
Normal Use
Abnormal Use
Correct Use
Use Error
Error in Perception
Error in Cognition
Action Error
Failure to see or hear information
Memory Failure
Rule-based Failure
Knowledge based failure
Inability to use control

DAU

- Dümmster anzunehmender User
- Ausdruck für Nutzer einer Software / Computers
- Erstellung von Hard/Software (Usability)
- Durch DAU gefährdete Programme sind schlecht (Exception-Handling)
- Abgeleitet von GAU (Größter anzunehmender Unfall)
- Gebrauch im Projektmanagements und IT
- BDU / EIFOK / ERROR - 40 / FSVG / OSI - LAYER 8 / PICNIC

PENETRATION TESTS - ETHICAL HACKING

- Allgemein
- Ablauf
- Rechtliche Aspekte

ALLGEMEIN

- Ausgeführt von externen Firmen
- Während des Testings Ansprechpartner der zu testenden Organisation
- Methoden und Techniken, die auch tatsächliche Hacker nutzen würden
- Meist als Whitebox-Test, weil effizienter
- Blackbox ist auch möglich, allerdings Gefahr, unbeteiligte Dritte zu treffen

4 PHASEN DES ABLAUFS

- Als Zyklus im Kreislauf wiederholt

    1. Reconnaissance - “Aufklärung” : Informationsbeschaffung vor einem Angriff
    2. Enumeration: Identifikation von möglichen Angriffsvektoren
    3. Exploitation: Ausnutzen der gefundenen Schwachstellen
    4. Documentation: genaues Protokoll des Tests mit abschließendem Bericht

! Beseitigen der Schwachstellen ist NICHT Teil des Pentest

VERFAHREN/TECHNIKEN BEI EINEM ANGRIFF

Physisch	Technisch
Beobachten Zugang in der Firma/Organisation Social Engineering	Öffentlich zugängliche Informationen SQL oder Code Injection Session HiJacking Firewall Traversal ARP-Poisoning Man-in-the-Middle Buffer Overflow Fuzzing WLAN DLOS

Durch Einschleusen in einen Teil eröffnet sich meist auch Zugriff zu anderen Teilen!

RECHTLICHE ASPEKTE

Bezüglich des Test:

- Generell: Einverständnis der zu testenden Organisation
- Test nur innerhalb von Objekten, die der Organisation gehören, bzw was erlaubt wurde -kein Eindringen in Systeme/Netze Dritter
- Problem: einem echten Hacker ist das egal
- Non-Disclosure Agreement seitens des Testers

Gesetzlichkeiten:

- International anerkannte IT-Sicherheitsstandards für Pentests
- Vom Gesetzgeber nicht explizit vorgeschrieben, aber Datensicherheit wird gefordert

```
// Nach dem empfangen einer Nachricht soll diese angezeigt werden
socket.onmessage = function(msg) {

    message(msg.data);
    // HTML INJECTION
   document.getElementById("Chat").innerHTML(msg.data);
   document.write(msg.data);

}
// SENDEN
function send(){
    var content = $('#text').val();
    var empfaenger = $("#empfaenger").val();
    let date = new Date();
    let text = {
    "@context": "http://schema.org",
    "@type": "Message",
    "@id": "http://localhost:3000/messages/"+Date.now(),
        "sender":{
            "@type":"Person",
```

QUELLEN

https://www.qualityengineersguide.com/history-of-quality

https://www.qualityengineersguide.com/the-6-important-guide-on-what-a-quality-engineer-should-do-when-the-project-is-just-starting-out

https://www.business-wissen.de/hb/qualitaetsmanagementsystem-nach-din-en-iso-9001-2015/

https://www.weka.de/qualitaetsmanagement/die-normenreihe-iso-9000-ff/

https://cmmiinstitute.com/

http://www.testingreferences.com/testinghistory.php

https://edition.cnn.com/2018/01/13/politics/hawaii-missile-threat-false-alarm/index.html

https://www.extremetech.com/extreme/262166-hawaiis-missile-scare-driven-terrible-ui-fcc-launches-investigation

https://metro.co.uk/2017/09/18/stanislav-petrov-the-man-who-quietly-saved-the-world-has-died-aged-77-6937015/

https://bigsciencenews.blogspot.com/2008/09/accident-cripples-lhc.html

http://lhc-closer.es/taking_a_closer_look_at_lhc/0.lhc_cost

https://searchsoftwarequality.techtarget.com/definition/quality-assurance

https://de.wikipedia.org/wiki/Qualitätssicherung

https://www.johner-institut.de/blog/iec-62366-usability/user-errors-use-errors/

https://searchsoftwarequality.techtarget.com/definition/quality-assurance

Viele Dank für ihre Aufmerksamkeit

Jan Philipps, Adil Khan, Can Bulut, Janine Galka, Serkan Celik