06.04.2019

Sicherheit – Die Macht der Automatik

Was ist schlechter als eine Uhr die steht? Eine Uhr, die die Zeit falsch anzeigt.

Segelschiffe hatten früher drei großvolumige Zeitmesser an Bord – zur Berechnung des Breitengrades. Die Gangungenauigkeit der damaligen Schiffschronografen war nur ein Grund für die Dreifachredundanz. Die Kapitäne verließen sich nicht auf eine Uhr allein, sie richteten sich lieber nach dem Mittelwert. Der andere Grund war der mögliche Defekt eines dieser mechanischen Wunderwerke. Eine Missweisung von einer Viertelstunde hätte gereicht, und das Schiff wäre zum Fliegenden Holländer geworden. Nur mit drei Uhren war ein „Falschspieler" zu identifizieren.

Das Prinzip der Mehrfachredundanz spielt auch im Flugwesen, bei der Raumfahrt, in Kernkraftwerken und im Automobilbau eine große Rolle. Überall übernehmen zunehmend Elektroniken die Steuerung. Eine große Herausforderung für die Techniker, die Systeme nicht zu komplex und undurchsichtig zu gestalten.

Tschernobyl:

Extrem heikle Situationen entstehen immer dann, wenn in sicherheitskritischen Betriebszuständen Automaten die Kontrolle ausüben. Ein Kernkraftwerk befindet sich immer im kritischen Zustand. Man kann es mit einem Automobil vergleichen, dessen Motor immer auf Vollgas läuft und die Bremse den Vortrieb regelt. Bei Versagen der Bremse ist Panik angesagt. Man tut gut daran, die Bremse mehrfach redundant auszulegen, und alle Teile der Bremse sowie der verschiedenen Hilfsbremsvorrichtungen permanent zu überwachen, und für den Fall der Fälle einen manuellen Eingriff zu ermöglichen. Von Zeit zu Zeit sollte man die ordnungsgemäße Funktion der einzelnen Bauteile überprüfen. Zu diesem Zweck schaltet man die automatische Regelung ab, und prüft bei einem simulierten Notfall, ob die Systeme die vorgesehene Funktion erfüllen.

Diese Beschreibung eines sicherheitskritischen Systems trifft auf Kernkraftwerke zu. Zur Katastrophe kam es, weil bei einem Sicherheitscheck die Automatik teilweise abgeschaltet wurde, um einzelne Systemfunktionen manuell kontrollieren zu können. Automatik und Mensch arbeiteten anschließend gegeneinander, bis zur Katastrophe. Dass die Betreiber die drohende Kernschmelze nicht verhinderten, lag an der undurchschaubaren Komplexität, die durch eine unübersichtliche Vielzahl von Schaltern, Reglern und Anzeigen noch zusätzlich verschärft wurde.

Wir stellen fest, hohe Komplexität, undurchsichtige Automatismen, und eine Überfrachtung des Menschen mit Informationen sind eine extrem kritische Melange bei sicherheitskritischen Einrichtungen. Die Erkenntnisse aus Tschernobyl führten zu einer verbesserten Visualisierung der Vorgänge.

Space Shuttle Challenger 1986:

Eine billige Gummidichtung verursachte eine der größten Raumfahrtkatastrophen. Fielen die Astronauten dem Kostendenken zum Opfer? Vermutlich nicht. Schon eher der Sorglosigkeit, mit der man sich auf millionenfach produzierte Komponenten verlässt. Man weiß oft nicht, mit wieviel Sicherheitsspielraum man es zu tun hat. Insbesondere Kunststoffteile sind diesbezüglich grenzwertig, besonders, wenn sie in die Jahre kommen.

Je komplexer ein System aufgebaut ist, je mehr Komponenten es beinhaltet, desto anfälliger ist es rein rechnerisch. Auch dies ein Hinweis darauf, es mit der Systemkomplexität nicht zu übertreiben. Und auf vermeintlich billige Teile ganz besonders zu achten.

Airbus Flug 447 2009:

Ausfall der Geschwindigkeitssensoren wegen Vereisung war die Ursache für den Absturz. Die Piloten versuchten verzweifelt, das Flugzeug in eine stabile Position zu bringen. Dabei überzogen sie es mehrfach bis zum Strömungsabriss.

Den Automobilentwicklern wurde die Fliegerei in Sachen Sicherheit als leuchtendes Vorbild präsentiert. Die Rede war von Fünffach-Redundanzen. Von hydraulischen, mechanischen und elektrischen Backups. Die Praxis sieht anders aus. Im verunglückten Airbus vereisten zwei Geschwindigkeitssensoren gleichzeitig, weil sie beide identisch waren, und obendrein technisch unzureichend, dafür aber billig. Ohne Geschwindigkeitssignal und ohne Sicht in einer Unwetterwolke waren die Piloten überfordert.

Boeing 737 Max 8:

Der Kampf Mensch mit Automatik – so könnte man die jüngsten Abstürze der beiden Maschinen betiteln. Eine Automatik funktioniert nur auf Basis einwandfreier Signale. Die waren anscheinend in den Unglücksfliegern nicht gegeben. Die Automatik sollte einen zu steilen Steigflug verhindern, verursacht durch neue Triebwerke. Anscheinend wurden die Piloten nicht ausreichend informiert.

Man stelle sich als Autofahrer vor, ein Fahrzeug ziehe konstruktionsbedingt immer nach rechts. Eine Automatik sorgt dafür, dass das Fahrzeug trotzdem geradeaus fährt. Meldet der Lenkungssensor fälschlicherweise eine Abweichung nach rechts, versucht die Automatik übereifrig den Wagen nach links zu steuern. Der Fahrer bemerkt dies, und hält verzweifelt dagegen. Die Automatik sitzt aber am längeren Hebel und überdrückt den Fahrer gnadenlos – bis das Fahrzeug günstigenfalls im Straßengraben landet. Ein Flugzeug landet auch im Gaben – höchst unsanft. Es ist noch keines oben geblieben.

Tesla Autopilot:

Der naive Herr Tesla, mit Namen Elon Musk, der gerne über die verschnarchte Automobilindustrie spottet, realisierte mit ein paar dürftigen Sensoren das Autonome Fahren. Es mussten erst einige Unfälle mit Todesfolge passieren, bis er eingestand: Hoppla, das haben wir gründlich unterschätzt. Das voll autonome Fahren reduzierte er anschließend auf teil-autonom, die Hände müssen am Lenkrad bleiben, der Fahrer muss in kritischen Situationen sofort manuell eingreifen. Wenn etwas passiert, ist er selber schuld. Damit zog der alerte Elon den Kopf aus der Schlinge.

Aber sein Ziel gab er deswegen noch lange nicht auf. Aus ein paar Sensoren wurden über Nacht ein paar Dutzend, unterstützt durch Kameras in alle Richtungen. Damit schickt er die verkauften Neufahrzeuge auf die Piste. Die Informationen sammelt er online, und aus diesem Datenwust, oder besser Datengebirge, destilliert er die Verbesserungen der Algorithmen, auf dass sie für alle Eventualitäten gerüstet sind – hoffentlich.

Hoffnungsträger KI:

Die Zukunft der Menschheit liegt in der Künstlichen Intelligenz. Oder anders ausgedrückt, ohne KI geht fast nichts mehr. Diesen Eindruck bekommt man unter dem Dauerfeuer der Medien. Wenn der Mensch nicht mehr in der Lage ist, komplexe Zusammenhänge programmtechnisch abzubilden, dann muss es die KI richten. Für das Autonome Fahren ist die KI ein absolutes Muss, heißt es.

Der Mensch lernt das Verhalten im Verkehr bereits von Kleinkind auf, die Fahrschule bildet nur den krönenden Abschluss. Das Verfahren nennt sich „Learning by Doing". In kritischen Situationen greift der Fahrlehrer ein. Wie jeder Mensch benötigt auch die KI ein Training. Stichwort „Deep Learning". Hoffentlich artet es nicht in „Learning by Crashing" aus, denn den Fahrlehrer ersetzt der Kunde.

Bis jetzt bestehen die Regelungs- und Steuerungsprogramme noch aus Algorithmen. Wenn dies - dann das. Wenn dieses Ereignis eintritt, dann passiert automatisch die entsprechende Reaktion. Das ist von den Programmierern durchschaubar, wenn sie es mit Verzweigungen und Sonderfällen nicht übertreiben. Treten Probleme auf, lässt sich der Fehler eingrenzen, je nach Komplexität mit mehr oder weniger hohem Aufwand. Die Softwareentwickler von Boeing sind also in der Lage, den oder die Fehler in ihrem Programm zu finden, wenn sie nur lange genug suchen.

Fehlersuche bei einer KI? Zwecklos. Eine KI, die den Namen verdient, ist in permanenter Veränderung begriffen. Sie lernt ständig dazu. Dieses Eigenleben ist von den Entwicklern nicht mehr zu durchschauen. Stellt sie irgendeinen Blödsinn an, der bei einem Autonomen Fahrzeug zu einem Unfall oder auch nur Beinahe-Unfall führt, kann niemand rekonstruieren, was es (oder sie?) dabei gedacht hat.

Mensch vs. KI:

Fast ständig antizipiert jeder Autofahrer das Verhalten der anderen Verkehrsteilnehmer und richtet sich danach. Eine KI sollte das auch können. Die menschlichen Verkehrsteilnehmer werden aber relativ schnell spitz kriegen, wenn im anderen Auto eine KI am Steuer sitzt, und ihre Reaktionen darauf ausrichten. Da zieht die KI den Kürzeren, denn sie muss vom dümmst-möglichen Verhalten aller Anderen ausgehen. Anders ist der hehre Anspruch der KI Protegés „Zero Accidents" oder „Vision Zero" wie es auch genannt wird, nicht zu halten. Ob es dem Fahrer des KI-Wagens gefällt oder nicht.

Man kann sich schon darauf freuen, wenn die ersten Autonomen Wagen in der Innenstadt unterwegs sind. Kommen sie überhaupt vorwärts?

Oder wird aus dem Autonomen Fahren ein Autonomes Stehen?

Jacob Jacobson