Grußwort

zur Veranstaltung des „Arbeitskreises Sicherheit im VDI/VDE BV BB“
am 31.05.2016

bei der Bundesanstalt für Materialforschung und -prüfung (BAM)
in Berlin

Erste großtechnische Anwendungen sicherheitstechnischer Konzepte zur vorsorglichen Beherrschung von versagensbedingten Störungen und den daraus möglicherweise resultierenden Schadensfolgen finden sich bereits in der Frühzeit des Eisenbahnwesens. Das vielfach bewährte Konzept der Zwangsbremsung hat seinen Ursprung vor knapp eineinhalb Jahrhunderten. Das Prinzip stellt sich so dar, dass bei Auftreten einer Störung automatisch eine bedingungslose Zwangsbremsung ausgelöst wird oder manuell herbeigeführt werden kann. Das mit Druckluft betriebsbereit gehaltene Bremssystem eines Eisenbahnzugs wird entlüftet, wodurch der Zug konstruktionsbedingt bis zum Stillstand abgebremst wird. Dieses Prinzip ist unter dem Begriff „fail safe“ bekannt, – auf Deutsch heißt das etwa „versagens- oder störungssicher“, wobei der stehende Zug wird als „sicher“ definiert wird. Dieses sicherheitstechnische Konzept bedingt, dass bei dessen Anwendung der eigentliche Nutzungszweck – nämlich das Fahren des Zuges – unterbunden wird.

In einer schweizerischen Studie aus den 1970-er Jahren wird festgestellt, dass es bei der – (in Personalverantwortung) provisorischen – Weiterfahrt nach einer Zwangsbremsung relativ häufig doch noch zu einem Unfall kommt. Was ist also zu tun?

Uns allen ist bewusst, dass ein Verkehrsflugzeug sich beim Auftreten einer Störung nicht durch eine Zwangsbremsung in den so genannten sicheren Zustand überführen lässt. Statt des „fail safe“-Prinzips gilt hier das „fail operational“-Prinzip. Auch im Störfall muss das Flugzeug solange weiter fliegen können bis es wieder auf der Erdoberfläche aufgesetzt hat. Bis dahin muss die Flugfähigkeit aufrecht erhalten bleiben.

Optimieren wir die beiden Prinzipien!

Es ist durchaus vorstellbar, dass ein irreversibel zwangsgebremster Zug in einem Tunnel zum Stehen kommt, wo die Feuerwehr nur erschwert Zugang findet, – oder auf einer Brücken- und Rampenkonstruktion, wo nicht hinreichend schnell und sicher evakuiert werden kann. Bei den heute möglichen hohen Fahrgeschwindigkeiten müsste sich die bisher bedingungslos ablaufende Zwangsbremsung doch als Zielbremsung gestalten lassen, wodurch sich der gebremste Eisenbahnzug an einer Stelle zum Stillstand bringen ließe, an der Rettungsarbeiten und Evakuierungen optimal möglich sind. Die kinetische Energie der heutigen mit hoher Geschwindigkeit fahrenden Züge sowie die „fail operational“-Prinzipien des modernen Luftverkehrs ließen dies ohne weiteres zu. Zudem ließen sich so auch störungsbedingte Verspätungen und mögliche Folgeunfälle weitgehend einschränken. Aber auch ein Zugbrand wie 05.09.1983 bei der Münchener U-Bahn müsste nicht mehr zum Totalverlust des Zuges und zu Schäden am Tunnelgebäude führen.

Wohin das Beharren auf anwendungstypischen Sicherheitskonzepten führen kann, zeigt eine Begebenheit beim Kickoff-Meeting für die Entwicklung der Magnetbahn „Transrapid“: Dort erklärte ein von der Bundesregierung bestellter, projektbegleitender Sachverständiger die Anwendung der Digitaltechnik als *nicht sicherheitsfähig*. Im Verlauf der weiteren Entwicklung der Magnetbahntechnologie kam immer wieder die Forderung nach „fail safe“ auf – also die Forderung nach einer flugzeugähnlichen Bauchlandung aus 400 … 500 km/h. Ein Flugzeug landet in der Regel mit einer Geschwindigkeit von etwa 250 km/h; eine Bauchlandung mit 400 … 500 km/h würde zwangsläufig zum Totalschaden des Flugzeugs führen. Dass bei der Magnetbahn „Transrapid“ jeder Störungsfall das Risiko eines Totalschadens in sich bergen sollte, damit waren wir bei der zentralen Projektleitung selbstverständlich nicht einverstanden.

Damit derartigem Verlangen im Namen der Technischen Sicherheit von vornherein Einhalt geboten wird, beauftragten wir im Jahr 1980 ein internes Gremium, für die Magnetbahntechnologie das „verdeckte Gemeinsame“ aus allen Bereichen der

Sicherheitstechnik herauszuarbeiten und zu prüfen, inwieweit Erkenntnisse aus dieser Sammlung für die Zwecke der Magnetbahn nutzbar gemacht werden können. Im Jahr 1982 beauftragte mich dann auch der Wissenschaftliche Beirat des Vereins Deutscher Ingenieure, diese Themenstellung in einem dazu berufenen VDI-Ausschuss für weitere Anwendungen nutzbar zu machen. Nach berufsbedingter Unterbrechung konnte die Arbeit hierzu schließlich wieder aufgenommen werden. Als Ergebnis liegt jetzt die VDI-Publikation ‚Das Qualitätsmerkmal „Technische Sicherheit" – Denkansatz und Leitfaden' vor und wird nun auch hier der fachkundigen Öffentlichkeit vorgestellt.

Die Bedeutung, die einem interdisziplinären Vorgehen bei der Sicherheitstechnik zukommt, lässt sich an zwei aktuellen Begebenheit der jüngsten Zeit messen. Technische Sicherheit erfordert Vorkehrungen gegen

- zufälliges (d.h. vorstellbares, aber nicht terminierbares) Versagen von Baueinheiten,
- umgebungsbedingtes (umweltbedingtes) Versagen von Baueinheiten (wie z.B. Umgebungstemperatur, Sonnenstrahlung, mechanische Vibration, Wasser) und
- menschliches Versagen (bei der Bedienung im Mensch/Maschine-System).

Technische Sicherheit macht es erforderlich, dass technische Einrichtungen so konzipiert und gestaltet werden, dass sich keine Einzelstörung und kein Einzelversagen zu einem Schadenszustand oder -verlauf entwickelt, der sicherheitstechnisch nicht mehr beherrschbar ist und sich deshalb zur Katastrophe ausweiten könnte.

- Beim Tsunami-Ereignis in Fukushima am 11.03.2011

  wurde offenbar, dass die Aggregate zur Notstromversorgung zwar außerhalb der „wahrscheinlichen" Flutwelle angeordnet waren, nicht aber außerhalb der (als worst case) „maximal vorstellbaren" Flutwelle. Deshalb konnte die Notstromversorgung durch die so ermöglichte „common mode"-Wirkung ebenso versagen wie die eigentliche Stromversorgung. Die Katastrophe wurde somit zwangsläufig, – wäre allerdings zu verhindern gewesen, wenn die „maximal vorstellbare" Flutwelle bei der Konzipierung der Notstromversorgung als worst case beachtet worden wäre.

- Zum Eisenbahnunfall im Stellwerksbezirk „Bad Aibling" (zuständig für den Streckenabschnitt zwischen Bad Aibling und Kolbermoor) am 09.02.2016

  berichteten die Medien, dass der diensttuende Fahrdienstleiter dem Zug aus Richtung Holzkirchen mindestens einmal irrtümlich ein *Ersatzsignal* gegeben habe, was für den Triebfahrzeugführer bedeutet, dass er am Halt zeigenden (oder gestörten Hauptsignal) ohne schriftlichen Befehl vorbei fahren darf. Nachdem er seinen Irrtum erkannt habe, soll der Fahrdienstleiter zwei *Nothaltaufträge über Zugfunk* abgesetzt haben, die jedoch bei den beiden betroffenen Triebfahrzeugführern nicht angekommen seien. Da die Übermittlung der *Nothaltaufträge* versagte, führte das irrtümlich gegebene Ersatzsignal, also menschliches Versagen, zwangsläufig zur Katastrophe.

  Sollten diese Medienberichte stimmen, müsste im Verlauf der bereits eingeleiteten Strafverfolgung die Frage geklärt werden, wer hier deliktisch gehandelt hat: der irrtümlich handelnde Fahrdienstleiter, der sich eines Besseren besonnen hat, oder das Team, das für die sicherheitstechnische Gestaltung und Zulassung des Zugfunks für Nothaltaufträge zuständig war.

Ihnen wünsche interessante Anregungen, die Ihnen die Vorträge des heutigen Abends bieten. Mich persönlich wird auch weiterhin interessieren, wie in Japan zukünftig Notstromversorgungen ausgelegt werden, damit es dort nicht wieder zu umweltbedingtem *commen mode-Versagen* von Strom- und Notstromversorgung kommen kann. Ebenso interessiert werde ich beobachten, wie die tätigen Strafverfolgungsbehörden und die befassten Gerichte die Eisenbahnkatastrophe von Bad Aibling abhandeln werden.

Dipl.-Ing. Wolf-Dieter Pilz VDI

Vorsitzender des ehemaligen
VDI-Ausschusses „Technische Sicherheit"