# Paradigmenwechsel im Safety-Assessment – auf dem Weg zu stärkerem Einsatz physikalischer Modelle

Dr.-Ing. Burkhard Münker

burkhard.muenker@munker-consulting.de

www.munker-consulting.de

Icomod – Münker Consulting

Olper Straße 53, D-57258 Freudenberg

## Kurzfassung

Zeitgemäße Modellierungswerkzeuge ermöglichen eine hierarchische 1:1-Abbildung der physikalischen Einheiten des realen Systems. Intuitive, grafische Darstellungen der Komponenten und Subsysteme machen es auch nicht an der Modellerstellung Beteiligten leicht, die System-Zusammenhänge zu verstehen und ein Modell weiterzupflegen oder zu variieren. Diese Natürlichkeit ist seit einigen Jahren ein maßgeblicher Motivator, entsprechende Tools in den Entwicklungsprozess einzubinden.

Ein genauerer Blick zeigt aber, dass dieser Wechsel in Mentalität und Werkzeugen zwar sehr wohl bei der System- und Funktionsentwicklung stattgefunden hat, kaum jedoch im Bereich des Safety-Assessment, also den Analysen, welche die Untersuchung der funktionalen Sicherheit eines – oft komplexen – Systems zum Ziel haben. Eine Vielzahl von zwar seit Jahrzehnten etablierten, aber oft individuellen Analysearten mit proprietären Wissens- und Ergebnis-Repräsentationen wie Fault-Tree-Analyse oder FMEA prägen hier das Bild und die Denkmuster der Verantwortlichen.

Wie gezeigt wird, lassen sich zwar die im Safety-Prozess geforderten Analyse-Ergebnisse entlang des gesamten V-Prozesses direkt aus physikalischen Bauteil-Modellen toolgestützt ableiten. Ein sanfter Paradigmenwechsel ist aber nur durch parallele Unterstützung verschiedenartiger Wissensdarstellungen in derselben Umgebung zu gewährleisten. So kann der Safety-Ingenieur mittels einer FaultTree-Bibliothek die Ausfall-Logik des Systems wie gewohnt als Fehlerbaum darstellen und gleichzeitig – graduell zunehmend - für Teilumfänge zeitgemäße Komponenten-Bibliotheken zur physikalischen Beschreibung von Nominal- und Fehlerverhalten einsetzen.

Keywords: modellbasiert, Safety-Assessment, FMEA, Fehlerbaum, Komponentenbibliothek, Fehlermodell, Paradigmenwechsel, modellbasierte Diagnose, RODON

## 1 Einleitung

In den letzten 10 Jahren hat sich die Idee der komponentenorientierten Modellierung und Systemanalyse in vielen Bereichen der Produktentwicklung durchgesetzt. Wesentliche Gründe dafür waren und sind einerseits sicherlich die Standardisierung der Modellie-

rungssprache durch *Modelica*, die aus deren Offenheit resultierende Unterstützung durch eine breite Nutzer- und Entwicklergruppe aus den verschiedenartigsten Anwendungsdomänen sowie die Verfügbarkeit einer ganzen Palette von Tools.

Andererseits sind diese Faktoren strenggenommen nur als zweitrangig anzusehen hinter der Natürlichkeit des physikalischen Modellierungsansatzes als solchem. Erst durch die 1:1-Abbildung des jeweiligen Wissens von Bauteilen bzw. Systemeinheiten jeder beliebigen Hierarchiestufe ausschließlich in nur einer einzigen entsprechenden Einheit des Modells gemäß des Single-Source-Prinzips wird ein deutlicher Mehrwert gegenüber anderen Repräsentationsformen erreicht. Nicht nur ermöglicht sie eine deutlich bessere Wissens-Wiederverwertbarkeit durch Modell-Bibliotheken, die gemäß Struktur und Namensgebung ein exaktes Replikat des firmeninternen Teilekatalogs darstellen können, sondern macht – gerade bei Verwendung anschaulicher grafischer Symbole - komplexe Zusammenhänge deutlich besser verständlich, wartbar und für Außenstehende leichter zugänglich. So kann das im Rechner hinterlegte Systemmodell von einem ursprünglich nur notwendigen „Simulations-Vehikel“ letztlich entlang des gesamten V-Prozesses zu *der* zentralen Repräsentationsform für das Produktwissen werden, von Spezifikation und Konzeptentwurf über Design, Test, Produktion bis hin zu Training und Ausbildung.

Trotz dieser offensichtlichen Vorteile ist in der industriellen Praxis jedoch zu beobachten, dass sich die Bestrebungen für eine ganzheitlich-modellbasierte Methodik und integrierte Tool-Kette oft nur auf das nominale Produktverhalten beziehen. Das angesichts zunehmender System-Komplexität und gesetzlicher Vorgaben immer wichtigere Gebiet des Safety-Assessment (SA) - also der Analyse von Bauteilfehlern, deren Auswirkungen und der Diagnose – wird hingegen paradoxerweise häufig nur mit Hilfe proprietärer Lösungen abgedeckt, im Extremfall allein mit Standard-Office-Programmen. Methoden wie FMEA, FTA etc. und zugehörige Tools sind oftmals sehr freitext-basiert, was zwar einen schnellen Einstieg in die Methodik und die Eingabe von „viel Inhalt in kurzer Zeit“ erleichtert, eine automatische strukturierte Weiterverarbeitung aber sehr erschwert. Zudem sind Art und Strukturierung der Ergebnisse sehr stark von der persönlichen Erfahrung und Vorliebe des jeweiligen Autors geprägt, was die Nachvollziehbarkeit maßgeblich beeinflusst. Dadurch und wegen der generell nur begrenzten Wiederverwendbarkeit ist ein hoher Review- und Aktualisierungsaufwand im Falle späterer Systemänderungen die Folge.

So kommt es zu der eigenartigen Situation, dass derartige Analysen in den Augen vieler Systementwickler zwar ein „ungeliebtes Kind“ sind, dennoch aber Tools zur Unterstützung althergebrachter Standalone-Methoden attraktiv erscheinen und den Markt und damit auch die Denkweise der Safety-Ingenieure beherrschen. Angesichts erreichter Grenzen in der Anwendbarkeit klassischer Verfahren ist eine Unterstützung durch mehr modell- und simulationsbasierte Analysen - ähnlich wie in der Systementwicklung – aufgrund der Brisanz des Themas aber dringend geboten. Verfahren der physikalischen Modellierung von Komponentenfehlern, der darauf aufbauenden Ermittlung der notwendigen Analyse-Ergebnisse und der Integration in den V-Prozess sind seit Jahren bekannt, erfordern aber den Mut zu einer u.U. nachhaltigen Prozess-Änderung. Um hier einen sanften Paradigmenwechsel zu ermöglichen, sollten neben der reinen Komponentenorientierung daher auch Modellierungsansätze unterstützt werden, die den bisherigen Denkmustern der Zielgruppe entgegenkommen. Dies ist das Thema des vorliegenden Beitrags.

Abschnitt 2 des Aufsatzes beschreibt zunächst einige traditionelle Analysen des Safety-Assessments und zeigt, wie diese klassischerweise in den Produktentwicklungsprozeß eingebunden sind. Abschnitt 3 stellt dann einige Repräsentationsansätze vor, um mit einem einmal erstellten Systemmodell die diversen notwendigen Safety-Analysen zu unterstützen. Dabei kommt auch der Technologiewechsel als solcher zur Sprache. Abschnitt 5 fasst schließlich die Ergebnisse zusammen.

# 2 Klassische Analysen des Safety-Assessment

Die Durchführung der Safety-Analysen für komplexe, sicherheitskritische Anwendungen wird in verschiedenen Branchen sowohl durch übergreifende als auch domänen-spezifische Standards und Regularien geregelt, u.a. [1][2]. Auch wenn diese sich in einigen Ausdrücken und Ablauf-Details unterscheiden, so ist doch der generelle Ablauf der sicherheitstechnischen Prozeduren recht ähnlich. Daher sei hier die in der Luftfahrt übliche „Aircraft Recommended Practice“ ARP4761 herausgegriffen, um die wichtigsten Analysearten und Begriffe vorzustellen [3].

Bild 1 zeigt stilisiert die einzelnen in den jeweiligen Phasen der Produkt- und Systementwicklung empfohlenen Analysen anhand des V-Diagramms. Sie werden nachfolgend kurz beschrieben.

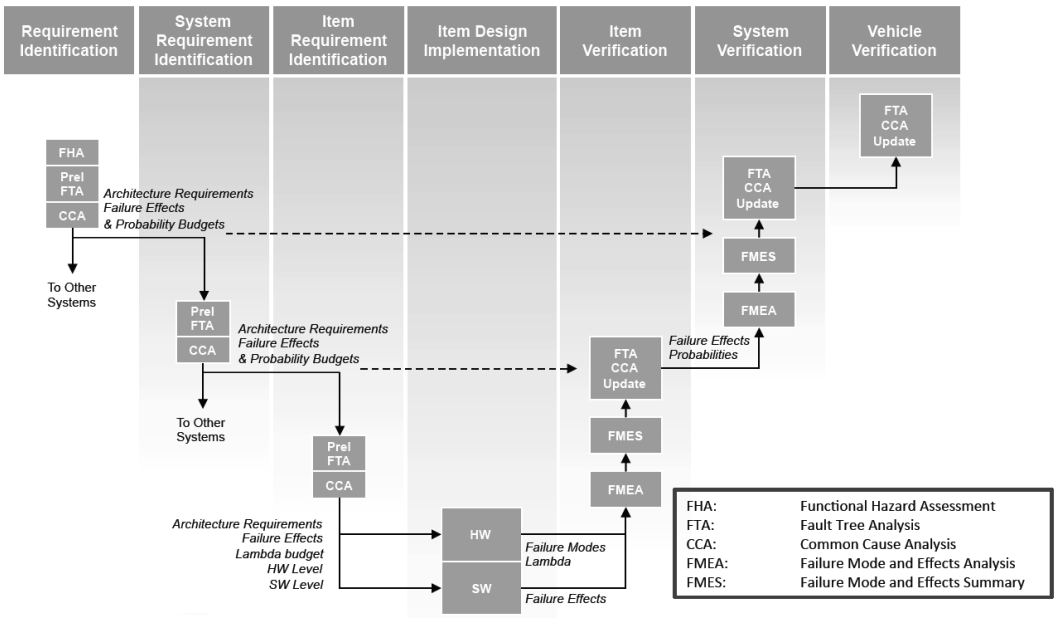



**Bild 1:** Safety-Assessment-Diagramm gemäß ARP4761

## 2.1 FHA (Functional Hazard Analysis)

Die Functional Hazard Analyse steht ganz zu Beginn des Systementwurfs, in der Phase, in der einerseits noch die Spezifikationen und Anforderungen detailliert werden, andererseits aber bereits erste Architektur-Konzepte erstellt werden. Sie hat zum Ziel, bereits früh die einzelnen Systemfunktionen unter Sicherheitsaspekten zu analysieren, bezüglich

ihrer Relevanz zu klassifizieren und mögliche Fehler oder Fehlerkombinationen zu erkennen, die eine kritische Funktion versagen lassen könnten.

Zunächst werden zur Erstellung der Liste der Systemfunktionen alle bereits verfügbaren Informationen u.a. aus Anforderungskatalog und gesetzlichen Regularien herangezogen. Für jede Funktion ermittelt man dann die möglichen „Failure conditions“ oder auch Hazards, für die dann auch eine systematische Namensgebung bzw. Indizierung eingeführt wird, z.B. „Haz100: Loss of all engines“. Eine Betrachtung unter diversen Nutzungs- bzw. Umgebungsbedingungen kann zu einer Hazard-Unterteilung führen, z.B. „Haz100.1: Loss of all engines during start“, „Haz100.2: ... during climb“ etc. In Zusammenarbeit mit den Domänen-Experten wird jeder dieser Hazards gemäß der möglichen Schwere (Auswirkungen auf Menschenleben, Umwelt, Sachschäden) bewertet, wobei die Werte beispielsweise „Minor, Major, Severe, Hazardous/Severe Major, Catastrophic“ lauten können [1]. Gemäß allgemeiner Grenzvorgaben des Risikos leiten sich aus dieser Klassifizierung unmittelbar Forderungen für die maximale Eintrittswahrscheinlichkeit eines Hazards ab („Extremely improbable“ für „Catastrophic“ Hazards bzw. $p<10^{-9}$). Vorschläge für Gegenmaßnahmen wie z.B. Systemänderungen oder Anweisungen sind ebenfalls Bestandteil der FHA. Die FHA ist von ihrer Natur her also eine eher qualitative Beurteilung, deren Ergebnisse häufig in Tabellenform zusammengetragen werden.

### 2.2 FTA (Fault Tree Analysis)

Um die Ursachen und Eintrittswahrscheinlichkeiten einzelner Hazards im Detail zu analysieren und quantitativ nachzuweisen, kommt allgemein die Fehlerbaum-Analyse zum Einsatz (siehe u.a. [3], Anhang D). Bei der FTA handelt es sich um eine deduktive Methode, bei man vom unerwünschten Ereignis (TOP-Event; hier: Hazard gemäß FHA) ausgehend die identifizierten möglichen Verursacher mittels UND- und ODER-Bedingungen grafisch verknüpft, diese Teilereignisse ihrerseits hinterfragt und diesen Vorgang rekursiv bis auf eine sinnvolle niedrigste Betrachtungsebene fortsetzt. Auf dieser „Blatt“-Ebene des Baumes beziehen sich die Elementar-Ereignisse häufig – aber nicht zwingend - auf individuelle Bauteil-Fehler, deren Eintrittswahrscheinlichkeiten bekannt sein oder aus separaten Quellen ermittelt werden müssen. Gemäß geltender Rechenregeln der Verzweigungen kann daraus dann die Wahrscheinlichkeit des TOP-Events ermittelt werden.

Die i.a. durch spezielle Programme unterstützte Methodik erlaubt – unabhängig von der System-Hierachie - die freie Partitionierung des Fehlerbaumes gemäß der Vorgaben des Autors, z.B. in die Haupt-Äste Hydraulikfehler/Elektrikfehler/Steuerungsfehler, oder auch catastrophic/hazardous/..., und die nachträgliche Einführung und Verknüpfung zusätzlicher Blocks. Das Ergebnis einer „Preliminary FTA“ (linker Ast in Bild 1) stellt oft die erste rechnergestützte Repräsentation der Ausfall-Logik des designierten Systems dar, mit Netto-Erstellungsaufwänden bis zu mehreren Personenwochen bei komplexeren Systemen. Ein Ausdruck des grafischen Baumes, der durchaus 3-stellige Seitenzahlen umfassen kann, bildet daher oft einen wesentlichen Teil von SA-Reports. Ganz am Ende der Systementwicklung (rechts oben in Bild 1) - bei größeren Systemen also u.U. Jahre später – wird diese Analyse dann gemäß der tatsächlichen Realisierung aktualisiert, oft durch andere Mitarbeiter als damals. Systeme mit Rekonfigurierbarkeit („self-repairing systems“) oder mit zeitlichen Abhängigkeiten lassen sich mit FTA nur schlecht bearbeiten.

## 2.3 CCA (Common Cause Analysis)

Eine CCA dient des Nachweises der hinreichenden Unabhägigkeit verschiedener Funktionen oder Teilsysteme und wird vor allem in sehr sicherheitssensiblen Branchen angewandt. Vom der Art her eine qualitative Analyse sollte sie gemäß Bild 1 den gesamten Entwicklungsprozess begleiten. Sie untersucht beispielsweise eine Abhängigkeit aufgrund der Bauteil-Anordnung in denselben Bereichen (Zonal Safety Analysis), durch bisher unentdeckte gemeinsame Anfälligkeiten wie den Herstellungsprozess, Software-Compiler oder Umgebungsbedingungen (Common Mode Analysis) oder durch sonstige individuelle Risiken wie Strahlung, Explosion oder Wechselwirkungen von Teilsystemen (Particular Risk Analysis).

## 2.4 FMEA (Failure Mode and Effect Analysis), FMECA und FMES

Ebenso wie die FTA ist auch die FMEA eine der verbreitetsten Analysen, sicherlich auch da sie im einfachsten Fall lediglich das Ausfüllen von elektronischen oder papiernen Tabellen-Formularen erfordert, also nur geringe technische Anforderungen stellt. In i.A. mehreren multidisziplinären Team-Sitzungen werden hierbei zunächst die möglichen Fehlermodi der Bauteile identifiziert und dann induktiv aus der Kenntnis von Systems-Arbeitsweise und Topologie deren Einzel-Auswirkungen auf die nächsthöhere Stufe(n) ermittelt (siehe u.a. [3], Anhang G). Zu den zu dokumentierenden Analyse-Ergebnissen gehören auch Methodenvorschläge zur Erkennung der jeweiligen Fehlermodi, was im Gesamtbild eine Aussage über die sogenannte „Diagnostic Coverage“ ermöglicht.

| Component | Function | Failure Mode | Probability in fpmh | Possible Causes | Effects | Higher Level Effects | Severity | Detection | Proposal to reduce risk | ... |
|---|---|---|---|---|---|---|---|---|---|---|
| ... | | | | | | | | | | |
| ValveX43 | Control Flow | Stuck closed | 20 | Corrosion, Bad Maintenance | Flow interrupted | Tanklevel becomes too low | minor | Install Valve Position Sensor/ Monitor | | ... |
| | | Stuck open | 12 | Corrosion, Bad Maintenance | Flow cannot be stopped | Tank overflow | major | Install Valve Position Sensor/ Monitor | Install 2nd valve in path | ... |
| | | | | | | | | | | |

**Bild 2:** Ergänzung einer FMEA zur FMECA

Werden in der Ergebnistabelle neben den eher qualitativen Aussagen auch numerische Angaben zur Fehlerwahrscheinlichkeit und deren Kritikalität auf höherer System-Ebene gemacht, spricht man von einer FMECA („C“ für „Criticality“). Die FMEA-Tabellen mehrerer Subsysteme können – umsortiert nach gemeinsamen Fehler-Auswirkungen – zu einer Failure Mode and Effect Summary (FMES) der nächsthöheren Ebene zusammengefasst werden. Obwohl die FMEA die anderen Safety-Analysen unterstützen soll, wird sie oft erst in den späteren Entwicklungsphasen (vgl. Bild 1) durchgeführt, zu einem Zeitpunkt also, zu dem es für strukturelle Design-Änderungen oft bereits zu spät ist.

### 2.5 Zusammenfassende Bewertung

Trotz des heute in mehreren Standards definierten und gemäß Bild 1 vermeintlich durchgängigen Prozesses ist das SA in vielen Unternehmen noch durch viele Einzel-Lösungen geprägt. Eine Ausnutzung der Ergebnisse früherer in späteren Analysen ist oft nur durch manuelle – und damit ihrerseits konsistenzfehleranfällige - Handarbeit möglich. Die Bandbreite der Anwender-Einschätzungen reicht vom stolzen Eindruck, nach der Anschaffung z.B. eines speziellen FMEA-Programms technologisch auf der Höhe der Zeit zu sein bis zur Erkenntnis, dass es der herkömmlichen FMEA, angewandt z.B. auf integrierte Schaltungen, an Automatismus und Vollständigkeit mangelt [4].

## 3 Ansätze modellbasierter Unterstützung der Fehler-Analysen

Es liegt nahe, sich auf dem Weg zu einer höheren Vollständigkeit, Qualität und Automatisierung der SA-Analysen analog zur Systementwicklung für einen modellbasierten Ansatz zu entscheiden. Zwar prägt die Idee der physikalischen Modellierung vor allem den aktuellen Trend, wurde aber bereits vor 10 Jahren erfolgreich zur Berechnung der Ursache-Effekt-Zusammenhänge bzw. automatischen FMEA-Generierung direkt aus komponentenorientierten Systemmodellen eingesetzt [5]. Dieser Abschnitt beschreibt kurz einige Möglichkeiten und Beispiele, die dank seiner flexiblen Modellierungs- und Analyse-Umgebung im modellbasierten Reasoning-Tools RODON realisiert wurden.

### 3.1 Physikalische Verhaltens- und Fehlermodellierung in RODON

Will man durch Simulation nicht nur das Nenn-, sondern auch das nicht-nominale Verhalten von System-Bauteilen analysieren, so sind zunächst auch deren jeweils mögliche Fehlerarten im Modell zu erfassen. Durch einen komponentenorientierten Ansatz wird dies' sehr erleichtert, da ja gemäß des Single-Source-Prinzips die bereits bestehenden Bauteil-Modellklassen nur um die Beschreibungen der jeweils möglichen Fehlerarten zu erweitern sind. Ebenso wie beim Nominalmodell werden die physikalischen Gesetzmäßigkeiten nur bezüglich der lokalen Schnittstellen, aber keiner externer Größen, angegeben. Im Systemmodell ergeben sich im Idealfall keine Änderungen, da ja auch die durch lokale Fehler ggf. „verstimmten" Variablenwerte nur durch die auch im Nominalfall geltenden realen Schnittstellen mit ihrer Umgebung interagieren. Allerdings sind aufgrund ihrer Fehler-Relevanz sonst als ideal angenommene Übertragungselemente wie Leitungen oder Rohre nun u.U. neu in das Modell aufzunehmen.

Da somit eine einzelne Bauteilklasse nicht mehr nur ein einziges, sondern mehrere alternative Verhaltensmodelle enthält, wird eine Kennung zur Adressierung der jeweiligen Varianten während der Evaluation erforderlich. Das kommerzielle modellbasierte Analyse-Tool RODON [6] nutzt dazu eine einfache diskrete Schalter-Variable `FailureMode`, an deren bestimmte Werte die Modellvarianten gebunden werden. Das folgende Code-Segment in *Rodelica* – einem tool-spezifisch ergänzten Derivat von *Modelica* – zeigt beispielhaft das physikalische Modell einer elektrischen Leitung:

```
model Wire // ===== Model class of Wire with 2 physical failuremode models ==========
  Pin p1, p2;
  FailureMode fm  (min=0, max=2, mapping="ok, disconnected, short_to_ground");
```

```
behavior
  if (fm == 0)       // Constraints valid for nominal mode
  {  p1.i + p2.i = 0;    // current balance
     p1.u = p2.u;}       // identical voltage on pins
  if (fm == 1)       // Constraints for failure mode "disconnected"
  {  p1.i + p2.i = 0;    // current balance
     p1.i = 0;}          // no current on p1 --> no current on p2
  if (fm == 2)       // Constraints for failure mode "short to ground"
  {  p1.u = p2.u;        // identical voltage on pins
     p1.u = 0;}          // ground voltage on p1 --> ground voltage on p2
end Wire; // ============================================================
```

Im Fall einer Leitungsunterbrechnung gilt demnach weiterhin die Strom-Bilanz zwischen den beiden Pins, nun allerdings mit verschwindendem Stromfluss. Im Kurzschluss-Fall hingegen verschwindet die Spannung an beiden Pins. Den einzelnen Modi lassen sich auch individuelle Auftretenswahrscheinlichkeiten λ zuordnen (hier nicht dargestellt).

Durch seinen ursprünglichen Fokus auf modellbasierte Diagnose und dem Umgang mit unscharfem Wissen motiviert, interpretiert RODON die Modellvorgaben als Constraints, was auch die Analyse von unter- oder überbestimmten Systemen ermöglicht. Die systematische Ansteuerung und Simulation aller in einem Systemmodell durch die Komponentenmodelle implizit eingebrachten Fehlerarten sowie Module zur Nachverarbeitung der in einer Datenbank abgelegten Simulationsergebnisse erlauben die detaillierte Bearbeitung vieler der oben erwähnten SA-Aufgaben. Klassische Beispiele sind die bereits in der frühen Entwicklungsphase mögliche Aufdeckung versteckter Fehler [7] oder die Analyse der zu erwartenden Diagnose-Qualität und des Fehlersuch-Aufwands bei gegebenem Sensor-Konzept [8][9]. Die Erstellung der notwendigen Modell-Bibliotheken fällt Safety-Ingenieuren aber - nicht nur wegen des Zeitaufwand - oft schwer.

### 3.2 Komponentenorientierte qualitative Funktionsmodelle

Neben dieser detaillierten physikalischen Modellierungsart lassen sich in *Rodelica* auch beliebige andere Modellierungsformen realisieren und in Bibliotheken strukturieren. Initiiert aus der realen Problemstellung, die frühe Architekturfindung und –optimierung bei gegebenen Toplevel-Systemfunktionen und deren Safety- und Reliability-Forderungen zu unterstützen, entstand eine Bibliothek rein qualitativer Modellbausteine, mit denen sich generisch sowohl Komponenten als auch Funktionen darstellen lassen.

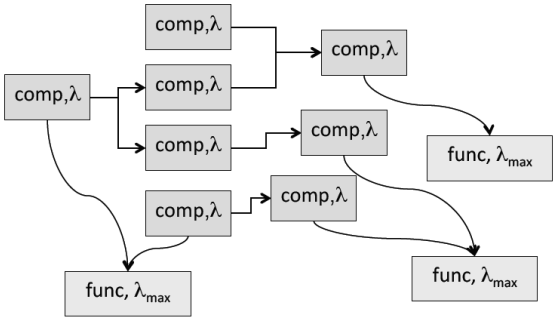


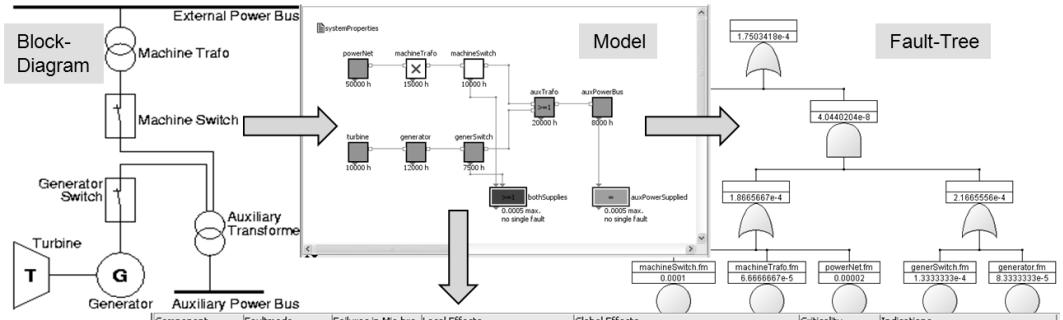

**Bild 3: Orthogonaler Zusammenhang von System-Funktionen und -Komponenten**

Ihr liegt der Gedanke zugrunde, dass alle durch die System-Spezifikation ausgedrückten Funktionen durch eine definierte Gesamtanzahl von Bauteilen implementiert werden. Gemäß Bild 3 benötigt jede einzelne Funktion eine spezifische Untermenge intakter Bauteile, um korrekt zu arbeiten. Funktionen- und Komponentenorientierung sind orthogonale Sichten. Jeder Ausfall einer Funktion stellt ein unerwünschtes Ereignis dar. Umgekehrt läßt sich jeder in der FHA identifizierte Hazard in einem Modell als - ausgefallene - Funktion repräsentieren, der nur mit einer Maximal-Wahrscheinlichkeit $\lambda_{max}$ eintreten darf und topologisch von den Bauteilen und deren Qualität $\lambda$ abhängt.

Da in einer frühen Phase detaillierte Komponentendaten weder vorhanden noch notwendig sind, ist eine rein qualitative bzw. Boole'sche Modellierung möglich: Ein Bauteil erfüllt seine eigene Funktion, wenn es selbst intakt ist *und* seine hinreichende Versorgung sichergestellt ist. Das folgende *Rodelica*-Segment beschreibt ein Bauteil mit zwei Versorgungs-Eingängen `in1` und `in2` und einem Ausgang `out1`. Es dient in dieser Form zur Beschreibung von Bauteilen, die zur korrekten Funktion nur einen der beiden Eingänge benötigen, z.B. einen elektrisch und hydraulisch betriebenen Aktuator.

```
model DiAltSo // ========= Model class for components with2 alternative inputs ==========
  extends DoubleInput;
  extends SingleOutput;
behavior
  // dependence of out.signal on failure mode and in.signal, described as implicit equation:
  out1.signal  :=  (fm==0) & (in1.signal | in2.signal);
end DiAltSo; // ================================================================
```

Es zeigte sich, dass diese Darstellung bereits nach kurzer Einweisung eine zügige Modellierung anhand des Blockschaltbildes erlaubt. Farbige Codierungen des Komponentenzustands ermöglichen nach der Simulation einen sofortigen Überblick der von einer Störung betroffenen System-Bereiche und -Funktionen, siehe das Kraftwerk-Beispiel in Bild 4.




| Component | Faultmode | Failures in Mio hrs | Local Effects | Global Effects | Criticality | Indications |
|---|---|---|---|---|---|---|
| auxPowerBus | failed | 125 | | Hazard: Loss of Auxiliary Power | Catastrophic | |
| auxTrafo | failed | 50 | | Hazard: Loss of Auxiliary Power | Catastrophic | |
| battery | noPower | 66.667 | Loss of internal Power Supply | Hazard: Loss of Auxiliary Power | Catastrophic | |
| | | | | Hazard: Loss of Power Supply Control System | Critical | |
| ecu | controlFailure | 40 | Loss of internal Power Supply | Hazard: Loss of Auxiliary Power | Catastrophic | |
| | | | | Hazard: Loss of Power Supply Control System | Critical | |
| generSwitch | stuck_open | 133.33 | Loss of internal Power Supply | Hazard: Loss of Auxiliary Power | Catastrophic | |
| generator | failed | 83.333 | Loss of internal Power Supply | | | Failure of internal supply detected |
| machineSwitch | stuck_open | 100 | | | | |
| machineTrafo | failed | 66.667 | | | | Failure of external supply detected |
| powerNet | powerLoss | 20 | | | | Failure of external supply detected |

**Bild 4: Vom Blockschaltbild über Systemmodell zum Fehlerbaum und FMEA**

Aus dieser Darstellung lassen sich zum einen durch Batch-Simulationen und Prädikaten-Definitionen automatisiert FMEA-Tabellen – auch für Doppelfehler - generieren, zum

anderen mittels besonderer Rechenverfahren die Fehlerbäume und damit die Ist-Ausfallwahrscheinlichkeiten der modellierten System-Funktionen ableiten. Dank des *Modelica*-Konzepts `inner-outer` können hierbei auch bauteilart-bezogene Common Causes automatisch mit erfasst werden. Im Modell belassene Freiheitsgrade ermöglichen zudem eine automatische Architektur-Optimierung unter Einhaltung der o.g. $\lambda_{max}$–Forderungen.

### 3.3 Einstieg via direkter Fehlerbaum-Modellierung

Beide soeben beschriebenen Ansätze erlauben die top-down- oder bottom-up-Analyse des Zusammenhangs zwischen Bauteil-Fehlern und Versagen von System-Funktionen. Ein komponentenorientiertes System-Modell löst dabei den klassischen Fehlerbaum oder die FMEA-Tabelle als initiale Repräsentationsform ab. Letztere sind nun *Output* der Analyse.

Dennoch kann es Sinn machen, auch innerhalb einer modellbasierten Tool-Umgebung eine Fehlerbaum-Erstellung auf klassische Weise zu ermöglichen, da sich so ein noch allmählicherer Paradigmenwechsel erreichen lässt. Der designierte Nutzer kann einerseits gemäß seiner gewohnten Denkweise die Ausfall-Logik des Systems beschreiben, dabei aber unmittelbar von einer größeren Flexibilität sowie weiteren Vorteilen profitieren. So konnten nach Nachbau eines in einem klassischen Tool vorliegenden Fehlerbaums in RODON allein durch das striktere Klassenkonzept mehrere Inkonsistenzen entdeckt werden. Je nach Bedarf lassen sich dann – praktisch auf ganz natürliche Weise und ohne Lernaufwand – auch gemäß anderer Paradigmen dargestellte Modellteile hinzufügen und kombinieren. In Bild 6 wurde beispielhaft das aus Bild 4 bekannte Kraftwerk-Energieversorgungssystem als Fehlerbaum modelliert (links) und das Top-Event an das gemäß Abschnitt 3.2 erstellte exemplarische Modell der Notfall-Prozeduren angebunden (oben).

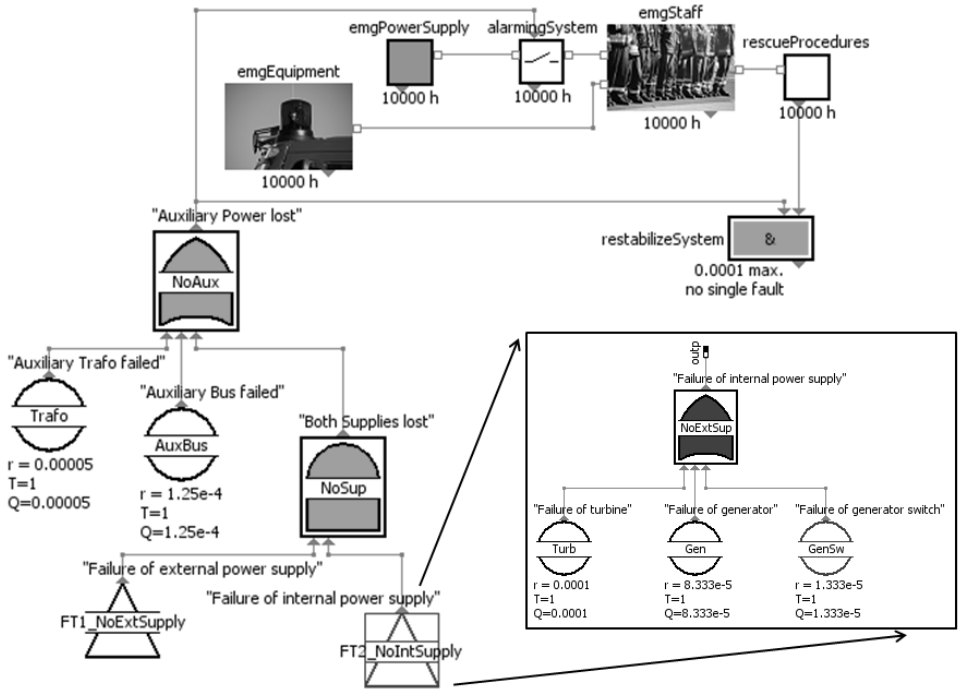



**Bild 5: Integrierte Verwendung verschiedener Modellierungsansätze**

# 4 Zusammenfassung

Dieser Beitrag beschreibt mögliche Ansätze zur Lösung der klassischen Aufgaben des Safety-Assessments mit Hilfe modellbasierter Methoden. Die besondere Herausforderung wird hier darin gesehen, einen anderswo bereits vollzogenen Paradigmenwechsel möglichst sanft zu gestalten, da die Affinität der designierten Zielgruppe zu mathematisch-physikalischen Modellen oft deutlich geringer ist als beispielsweise in der Systementwicklung. Dazu werden diverse, exemplarisch im Tool RODON realisierte Modellierungsansätze vorgestellt. In einer integrierten Tool-Umgebung lassen sich gemäß Anwender-Präferenzen Bibliotheken unterschiedlicher Granularität beliebig kombinieren und zur strukturierten Wissenserfassung bereits ab der FHA nutzen. Wie in etlichen Projekten erfolgreich praktiziert, erlaubt der modellbasierte Ansatz durch Simulation und automatisierte Ergebnisaufbereitung so eine deutlich systematischere, vollständigere und hochwertigere Generierung der im Safety-Assessment benötigten Ergebnisse sowie eine effiziente und frühzeitige Verkopplung mit der System-Entwicklung.

# 5 Literatur


[1] *MIL-STD-882D, Standard Practice for System Safety*, Department of Defence, 2000

[2] *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1 to 7*, CENELEC, 1998-2000

[3] *SAE ARP4761 (Society of Automotive Engineers Aerospace Recommended Practice)*: Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems, 1996

[4] *Riccardo Mariani*: Applying IEC 61508 to Integrated Circuits. Automotive Infomation Quarterly, Volume 6, Number 2, 2007

[5] *Edward J. Zampino, Dr. Dirk Burow*: The Application of RODON to the FMEA of a Microgravity Facility Subsystem. In Proceedings of Annual Reliability and Maintainability Symposium, Seattle, WA, USA, 28-31 Jan 2002

[6] *Karin Lunde*: Ensuring System Safety Is More Efficient. Aircraft Engineering and Aerospace Technology, vol: 75, issue: 5. pg 477 - 484, 2003

[7] *Jörg Krüger, Bernhard Meyer, Jürgen Zoller, Werner Seibold*: A380 Smoke Detection System (SDS) - Analyzed with RODON. Poster-Kurzvortrag DGLR-2005-272, Deutscher Luft- und Raumfahrt-Kongress, DLRK, 2005

[8] *Peter Bunus, Olle Isaksson, Beate Frey, Burkhard Münker*: Model-based Diagnostics Techniques for Avionics Applications with RODON. In Proceedings of the 2nd International Workshop on Aircraft System Technologies (AST 2009), Hamburg, Germany, 26-27 March, 2009

[9] *Peter Bunus, Olle Isaksson, Beate Frey, Burkhard Münker*: RODON - A Model-Based Diagnosis Approach for the DX Diagnostic Competition. In Proceedings of the 20th International Workshop on Principles of Diagnosis, Stockholm, Sweden, 14-17 June, 2009