Motor Mikroelektronik – Trends in der Flugzeugsystemtechnik

Henning Butz
Sen. Mgr. Information Management & Electronic Networks
Airbus Deutschland GmbH
Kreetslag 10, D-21129 Hamburg, Germany
Email: henning.butz@airbus.com
Tel: (+49) 40 743 73653

Einleitung

Die Flugzeugsystemtechnik hat in der vergangenen Dekade zwei entscheidende Fortschritte bei der Realisierung eingebetteter Funktionen hervorgebracht:

- mit der Integrierten Modularen Avionik (IMA) wurde ein standardisiertes Rechner-Plattformkonzept geschaffen, das es gestattet, Softwarefunktionen unterschiedlicher Kritikalität auf einer gemeinsamen Rechnerressource zu implementieren – eine gegenseitige Beeinflussung ist ausgeschlossen;
- der enorme Aufwuchs der Systemkomplexität im gleichen Zeitraum hat den Einsatz rechnerbasierter Entwicklungswerkzeuge und damit eine Neuorientierung bei den Entwicklungsprozessen vorangetrieben.

Beide Trends sind Bestandteil eines Paradigmenwechsels in der Systemtechnik, der bereits in den 80er Jahren des vorigen Jahrhunderts begann, in seinen Auswirkungen aber erst jetzt deutlich wird. Es handelt sich um die Virtualisierung von Funktionen. In der Vergangenheit dominierten elektro-mechanische oder hydro-mechanische Funktionskonzepte. Heute werden Funktionen - wesentlich flexibler und umfangreicher - nahezu ausschließlich mikro-elektronisch, algorithmisch realisiert. Die Beispiele reichen von der Flugsteuerung, deren alte Hebel-Seilrollenmechanik zur Steuerflächenkoordination - beispielsweise für den Kurvenflug - inzwischen mit erheblich erweitertem Funktionsumfang vollständig durch Mikroelektronik ersetzt wurde – bis hin zur Segregation der Funktionen durch Software-Partitionierung auf IMA Rechnermodulen. In der „klassischen“ Box-Avionik wurde dies „mechanisch“ durch Funktionstrennung in verschiedene Rechner oder Platinen, also mittels Aluminiumwänden oder Epoxyd-Boards erreicht. Parallel zur Virtualisierung der Funktionen und der Entwicklungswerkzeuge hat sich eine Veränderung der Prozesse zur Entwicklung und Qualifikation der Systeme vollzogen, die nachfolgend erörtert werden soll.

1 Integrierte, standardisierte Rechnerplattformen – modulare Avionik

Im „klassischen“ Geschäftsprozess wird die gesamte Entwicklung von Systemfunktionen als Auftrag an ausgewählte Systemhersteller vergeben. „Gesamt“ bedeutet, dass sowohl der mechanische Anteil wie auch die Rechnerelektronik und Funktionssoftware vom ausgewählten Hersteller entwickelt, integriert und qualifiziert werden muss. Der Liefergegenstand ist das integrierte und nachgewiesene System, das vom Flugzeughersteller ins Flugzeug eingebaut und bezüglich seiner Interoperabilität mit anderen Systemen sowie mit den Flugzeugkomponenten nachgewiesen wird, Bild 1.

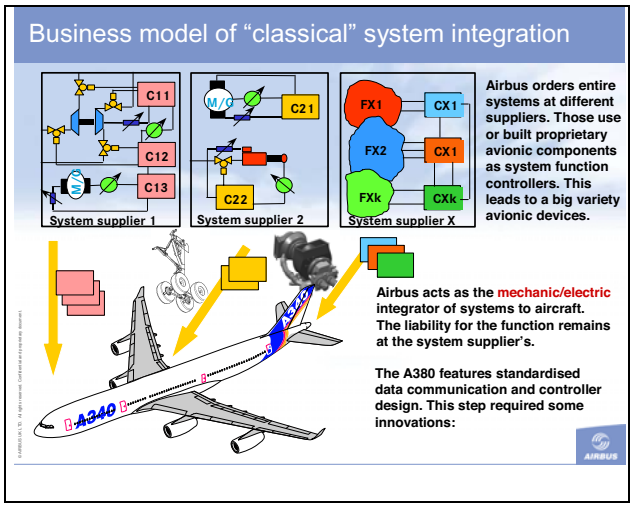

Bild 1 klassische Systemintegration

Auch nach dem Übergang auf die *Integrierte Modulare Avionik (IMA)* wird das oben beschriebene Geschäftsmodell der Systemfremdvergabe beibehalten. Im Unterschied

zur klassischen Variante entfällt jetzt für den ausgewählten Systemhersteller die Entwicklung der Rechner für die Systemsteuerung. Von ihm wird erwartet, dass er das im Flugzeug vorinstallierte Basisrechnernetzwerk zur Ausführung seiner Softwarefunktionen benutzt. Als wesentlicher Faktor kommt hinzu, dass die gewählte Rechnerressource nicht einem Systemhersteller exklusiv zufällt. In der Regel wird ein IMA Rechner (Modul) von bis zu sieben verschiedenen Systemfunktionen gemeinsam genutzt, deren Sicherheitskritikalität durchaus sehr verschieden sein kann. Der Systemhersteller liefert nur noch den mechanischen Systemanteil sowie die Software für die Systemsteuerung. Die Steuerrechner werden getrennt von einem Avionik-Hersteller bezogen. Der Flugzeughersteller übernimmt wieder die mechanisch-elektrische Integration ins Flugzeug, inklusive der Interoperabilitätsnachweise. Zusätzlich muss er nun aber die Funktionssoftware in das vorinstallierte, zunächst leere Rechnernetz integrieren, Bild 2. Dazu sind vorangehende technische Maßnahmen und Prozeßschritte erforderlich, um die vom Systemhersteller zuvor erbrachte Produktqualifizierung nicht zu verlieren.

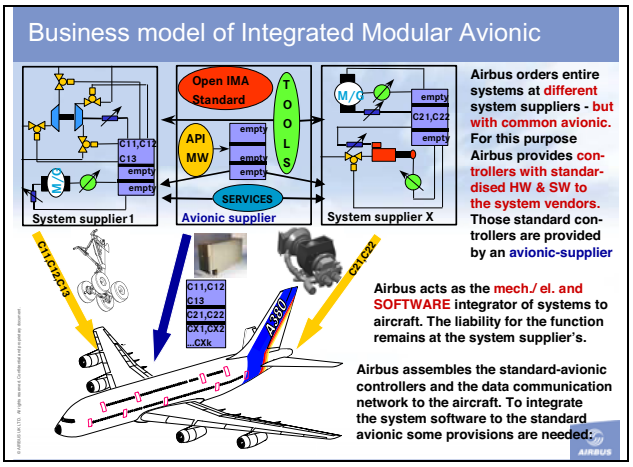

Bild 2 Systemintegration Modulare Avionik

Die vom Hersteller des Systems geführten Nachweise der Systemfunktionen gegenüber den Anforderungen der Sicherheit und Leistung erfolgt unter Verwendung von IMA Rechnermodulen, die dem im Flugzeug verbauten Standard entsprechen. Im Gegensatz zur finalen Integration, wo mehrere Funktionen verschiedener Hersteller in einem Modul implementiert sind, führt jeder einzelne Systemlieferant seine Systemqualifizierung jedoch ohne die Anwesenheit anderer Applikationen auf dem von ihm benutzten Rechner aus. Dieser Vorgang wird als „inkrementelle Qualifizierung“ bezeichnet. Die nachträgliche Integration weiterer Funktionssoftware neben den bereits nachgewiesenen Funktionen würde die Gültigkeit der Nachweise unmittelbar aufheben, wenn nicht zuvor unzweifelhaft bewiesen wird, dass alle Funktionspartitionen auf der Rechnerplattform vollständig voneinander entkoppelt sind. Dieser Nachweis bezieht sich auf die „strenge Partitionierbarkeit“ der IMA Rechnerplattform. Er ist getrennt und unabhängig von der Qualifizierung der Systemfunktionen generisch zu führen und ist Aufgabe des Avionik-Herstellers der IMA Rechnermodule. Am Endes dieses Prozesses steht der sog. „Zertifikationskredit“. Er besagt, dass eine gegenseitige Beeinflussung gemeinsam implementierter Funktionen auf einem IMA Rechner mit höchster Sicherheit (DAL-A = SIL4)* ausgeschlossen ist. Der Aufwand zahlt sich aus, da ohne ihn jede zusätzlich integrierte Funktion vom Integrator (dem Flugzeughersteller) nachqualifiziert werden müsste. Ein Vorgang, der bereits aus Kosten- und Zeitgründen, aber auch aufgrund fehlender Detailkenntnisse der Systemfunktionen nicht realisierbar ist.

Es gibt Beispiele hoch integrierter Rechnerplattformen – insbesondere für militärische Anwendungen – die versucht haben, ohne den generischen Nachweis der strengen Partitionierung auszukommen. Sie sind entweder unmittelbar bei der Zulassung der Systeme gescheitert oder haben extrem hohe Kosten bei der Nachqualifikation erzeugt, die zudem bei jeder Modifikation irgendeiner Funktion in beachtlicher Höhe erneut entstehen.

2. Entwurfskriterien für die Architektur und Konfiguration von IMA Plattformen

Qualifikation und Zertifikation sind Prozessschritte, die weitgehend am Ende einer Entwicklung stehen. Die gemeinsame Nutzung eines vorinstallierten Rechnernetzwerks führt aber schon zu Beginn des Entwurfs zu Abweichungen von der klassischen Vorgehensweise, die im folgenden diskutiert werden sollen. Sie betreffen die Festlegung des Sicherheitsbudgets der IMA Plattform sowie die Verteilung ihrer Ressourcen an die Nutzer, mithin die Definition der Plattform Architektur, Konfiguration und Topologie, Bild 3.

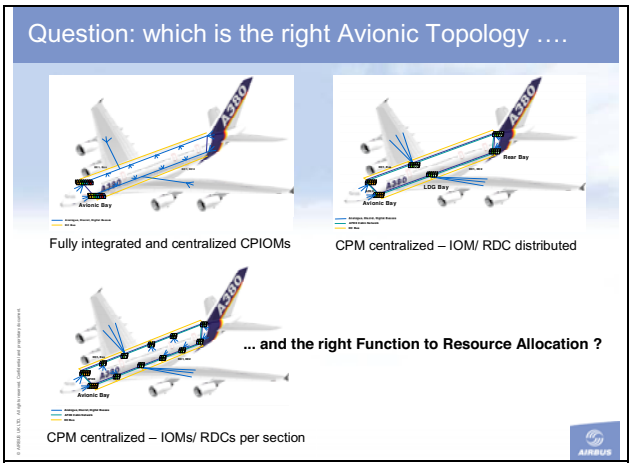

Bild 3 Topologie und Architektur modularer Avionik

* DAL: Design Assurance Level, SIL: System Integrity Level

Der Anwender (hier der Systemhersteller) einer von dritter Seite (hier der Flugzeughersteller) zur Verfügung gestellten Rechnerplattform muss wissen, welche Leistung und welche Sicherheitsreserve das Rechnernetzwerk für ihn bereitstellt. Die Leistung der zugewiesenen Partitionen wird auf der Basis der individuellen Systemanforderungen zwischen den Systemherstellen auf der einen und dem Flugzeughersteller auf der anderen Seite verhandelt. Gegenstand dieser Verhandlungen sind: Rechenleistung, Zykluszeiten, Speicherbedarfe und Signalschnittstellen nach Anzahl und Typ. Dies ist ein iterativer Vorgang, bei dem zunächst summarisch der gesamte Bedarf erhoben wird. Unter Zuschlägen erheblicher Reserven (ca. 50%) für alle zuvor genannten Parameter entsteht so die Basisspezifikation für das gesamte Rechnernetzwerk. Aus diesem – global definierten - Kontingent werden die geforderten Ressourcen den jeweiligen Systemlieferanten zugemessen und in einer Konfigurationsdatenbank verwaltet.

Die Festlegung der Sicherheitsreserve des Rechnernetzwerks ist ein Faktor, der einerseits auf der berechneten Gesamtzuverlässigkeit des IMA Netzwerks beruht, gleichzeitig aber auch konservative Elemente enthält, die die Vorsicht des Flugzeugherstellers angesichts beschränkter Erfahrungshorizonte mit der neuen IMA Technologie widerspiegeln. Konkret wird festgelegt, dass der Ausfall einzelner Netzwerkkomponenten (EtherNet Knoten, IMA Rechnermodule) Auswirkungen der Kategorie „major“ nicht überschreiten dürfen. Als “major” bezeichnete Schadensereignisse treten äußerstenfalls alle 100.000 Flugstunden auf. Die Schadenseffekte sind definiert als „significant reduction in safety margins or functional capabilities, significant increase in crew workload or in conditions impairing crew efficiency, some discomfort to occupants”. Der Ausfall des gesamten IMA Systems darf zu Situationen der Kategorie “hazardous” führen, mit einer Eintrittswahrscheinlichkeit von höchstens 1/10.000.000 Flugstunden (10^{-7}/ fh), denn die zu erwartenden Schadenseffekte sind: “large reduction in safety margins or functional capabilities, higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely, adverse effects upon occupants”.

Systemfunktionen, deren Kritikalität eine Ausfallwahrscheinlichkeit von 10^{-5} (einkanalig), bzw. 10^{-7} (mehrkanalig) pro Flugstunde als Untergrenze vorschreibt, können demzufolge unter alleiniger Verwendung der IMA Rechnerressurcen realisiert werden. Systemfunktionen mit höherem Sicherheitsanspruch (z.B. „catastrophic“ mit einer geforderten Ausfallwahrscheinlichkeit von 10^{-9}/fh) müssen zusätzliche, eigene Maßnahmen, z.B. eine dissimilare, redundante Datenkommunikation oder dissimilare Rechner vorsehen. Die hier geschilderte konservative Bemessung der Sicherheitsreserve neuer Systeme ist charakteristisch für den Flugzeugbau. Beim Übergang von der mechanischen zur elektronischen Flugsteuerung („fly-by-wire“), Mitte der 80er Jahre, wurde die Begrenzung der Schadenseffekte bei Totalausfall der Flugsteuerungsrechner ebenso zu „hazardous“ vorgeschrieben. Das ist der Grund, warum bis zum Ende der 90er Jahre alle fly-by-wire Flugsteuerungen mit zusätzlichen mechanischen Funktionselementen (sog. „mechanical back-up“) für die Nick- und Giersteuerung (Quer- und Hochachse) ausgestattet waren. Die A340-600 war 1999 das erste Flugzeug, bei dem die Flugsteuerungsfunktionen ausschließlich elektronisch realisiert wurden. Die Erfahrung hatte bewiesen, dass mit der Mikroelektronik ausreichend sichere und zuverlässige Systemarchitekturen realisiert werden können. Heute verwenden so gut wie alle modernen fly-by-wire Flugzeuge elektronische Reservefunktionen anstelle eines mechanischen back-up in der Flugsteuerung. Der Totalausfall aller Rechner und der „Not-Elektronik“ wäre hier „catastrophic“ - aber das passiert nie!

Für die Konfiguration eines von vielen Anwendern integral genutzten Rechnernetzwerks sind die individuellen Ressourcenanforderungen sowie die Sicherheitsanalysen generell die wichtigsten Entwurfskriterien. Sie sind aber nicht die einzigen, wenn eine optimale Aufteilung der Netzwerkarchitektur erreicht werden soll, Bild 4. Weitere entscheidende *Entwurfsparameter* sind beispielsweise Gewichte (Avionikboxen, Kabel), Komplexität der Konfiguration und die dadurch bedingten Kosten aller Art (Geräte, Installation, Fehlerdiagnose, Logistik, Wartung, Modifikationen, Dokumentation, etc.), Fehlertoleranz (d.h. lange Wartungsintervalle) und auch rechtliche Aspekte, z.B. die Freigabe geistiger Eigentumsrechte an speziellen Funktions- oder Signalisierungstechnologien, die ggf. im IMA System implementiert werden müssen. Die genannten Kriterien treiben den Entwurf zum Teil in diametral entgegengesetzte Richtungen. Man denke nur an Sicherheit und Verfügbarkeit, die durch hohe Redundanz gewinnen, was aber kaum den damit verbundenen Kostenindizes unterstellt werden kann. Zur „Optimierung“ des Entwurfs einer IMA Plattform müssen diese Kriterien quantifiziert und parametrisiert werden, um sie mittels geeigneter Zielfunktionen innerhalb zulässiger Grenzen zu orientieren.

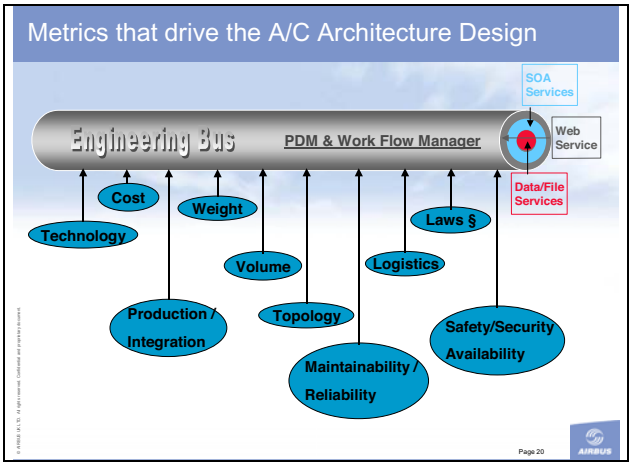

Bild 4 Avionik Entwurfsparameter / -metriken

3. Entwurf und Optimierung von IMA Plattformen

Die zuvor umrissenen Beispiele lassen bereits die Komplexität der Aufgabe erahnen, eine „optimale“ Konfiguration und Topologie der Avionik-Plattform zu bestimmen, die als offene Ressource von sehr vielen verschiedenen Anwendern genutzt werden soll. Grundvoraussetzung für einen optimierten Entwurf ist die Umwandlung der oben aufgeführten „*Entwurfsparameter*“ in *Metriken*, die als *Optimierungskriterien* alternative Architekturen und Topologien unterscheiden und bewerten. Bisher existierte dieser Prozess geschlossen nur im Rahmen der Sicherheitsanalysen. Die anderen Kriterien wurden zwar auch ermittelt, allerdings an verschiedenen Stellen im und außerhalb des Unternehmens, unter Zuhilfenahme unterschiedlichster Modelle und Werkzeuge und zumeist auch asynchron zu weit auseinander liegenden Zeitpunkten. Dadurch war die Korrespondenz der Kriterien kaum sicherzustellen. Designentscheidungen blieben deshalb zumeist funktionsbezogen und konnten globale Optima auf der Ebene des Gesamtflugzeuges nur eingeschränkt erreichen.

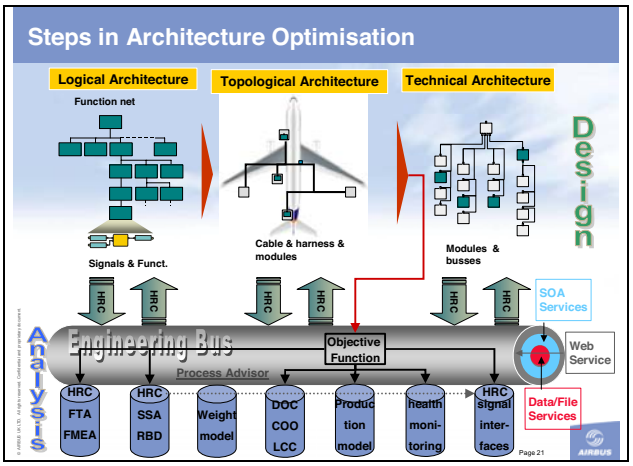

Bild 5 Modellbasierte Optimierung der Avionik

Diese Vorgehensweise war bei verteilten, systemspezifischen Rechnerentwicklungen vertretbar. Bei hochintegrierten Rechnernetzwerken dagegen ist sie unangemessen langsam, unvollständig, unkoordiniert und damit ungeeignet für die notwendige globale Optimierung querschnittlich genutzten Avionikplattformen. Hier kommt es gerade am Beginn einer Entwicklung auf hohe Iterationsgeschwindigkeit und Transparenz an, wenn viele Anwender mit ihren verschiedenen Anforderungen synchron berücksichtigt und mit den Avionik-Plattformvarianten koordiniert werden müssen. Deshalb werden beim Entwurf integraler Avioniksysteme die Entwurfsparameter und -artefakte auf einer gemeinsamen *PDM (Product Data Management)* Entwicklungsplattform (*Engineering Bus*) verwaltet. Die verschiedenen Aspekte des Avioniksystems (Performance, Funktion, Kosten, Sicherheit etc.) sind in individuellen, aber korrespondierenden Modellen und/oder Metriken des Systems repräsentiert. Übertragungsfehler und Datenverluste – etwa aufgrund unterschiedlicher Modellsemantik und –syntax dürfen dabei keinesfalls auftreten. Konkret: die Kongruenz eines Engineering Modells in „MatlabSimulink“ und seines Pendants als RBD (Reliability Block Diagram) für die Zuverlässigkeitsanalyse mit z.B. „SyRelAn“ muss durch die PDM Entwicklungsplattform in höchster Qualität gewährleistet sein. Das gleiche gilt für die Integrität und Konsistenz der Parameter, die zwischen den einzelnen Entwurfsschritten vermittelt werden, Bild 5.

Die Bedeutung der zu Metriken kondensierten Entwurfskriterien besteht in ihrem Nutzen für die Bewertung der Entwürfe durch die Entscheidungsträger. Um das Optimum auf der Ebene der Gesamtavionik identifizieren zu können, ist die synoptische Betrachtung der Metriken erforderlich. So können bereits sehr früh – und insbesondere sehr schnell – Verletzungen von Grenzwerten (constraints) und die Empfindlichkeit eines Entwurfs hinsichtlich kritischer Kriterien bei Variation von Entwurfsparametern erkannt und beeinflusst werden. Die Bewertung eines Entwurfs durch schlichte Gegenüberstellung von Metriken in einer scorecard ist nicht notwendigerweise zielführend. - Wie bewertet man „Sicherheit“ gegen Kosten oder Gewicht? - Solche Ansätze funktionieren nur, wenn eine Lösung gefunden wird, bei der alle, bzw. die wichtigsten Kriterien gleichzeitig ihr Optimum erreichen. In der Regel wird aber die Verbesserung einer Eigenschaft zur Verschlechterung der anderen führen. Problemstellungen dieser Art sind seit langem z.B. aus der Ökonomie als „Pareto“ Probleme bekannt und es existieren einschlägige Methoden zum Auffinden einer Lösung. Weniger abstrakt und besser für das Vertrauen in die Entscheidung ist es, die Entwurfsalternativen (zusätzlich) durch ein Geschäftsmodell zu validieren. Auch dazu gibt es heute einschlägige Methoden und Werkzeuge (z.B. ISD-Scheer ARIS, GFU IPPL), die entweder den zum Produkt notwendigen Geschäftsprozess simulieren und/oder adäquate Kennzahlen für die Produktlebenszyklen liefern, anhand derer die Aufwände und Risiken bei Realisierung und Betrieb ermittelt werden.

4. Werkzeuge im IMA Plattform Entwicklungsprozess

Allen bisher beschriebenen Prozessschritten ist gemeinsam, dass zu ihrer Durchführung umfangreiche Produktdaten bearbeitet, geprüft und vermittelt werden müssen. Diese Arbeit ist „manuell“ oder auch unter Zuhilfenahme klassischer Datenverwaltungsmittel wie Tabellenkalkulation o.ä. nicht mehr zu bewältigen. Es werden dazu CAx basierte Entwurfswerkzeuge verwendet, die weitgehend autonom umfangreiche Prozessschritte mittels algorithmischer Methoden bearbeiten. Werkzeuge, die dies leisten, sind nicht mehr transparent und ihre Resultate lassen sich i.d.R. auch nicht mehr plausibel überprüfen. Das liegt einerseits an der umfangreichen Menge der verarbeiteten

Daten und zum anderen an der Komplexität und Abstraktheit der verwendeten Algorithmen. Dadurch entsteht die paradoxe Situation, dass ein auf diese Weise erzeugtes Entwicklungsergebnis beliebig unzuverlässig sein kann. Wenn das Zustandekommen eines Resultats intransparent ist, verlieren alle nachfolgenden Entwicklungsschritte die Evidenz der Korrektheit. Das ist für den Entwurf und die Qualifikation sicherheitskritischer Systeme unakzeptabel – die Vorschriften verlangen lückenlos nachweisbare Entwurfsschritte . Um diese zu erlangen gibt es i.w. drei verschiedene Wege:

1. das Werkzeug und die darin enthaltene Methode (Algorithmus) wird qualifiziert
2. zwischen den Eingangsparametern und den Ergebnissen wird durch ein zusätzliches Werkzeug (sog. Checker) eine Plausibilitätsprüfung durchgeführt
3. der intransparente Prozessschritt wird redundant mittels unterschiedlicher Methoden durchgeführt (diversitäre Bearbeitung). Freigabe nur bei Übereinstimmung der redundanten Ergebnisse.

Die 1. Vorgehensweise ist – insbesondere bei komplexen und entwurfskritischen Werkzeugen – sehr aufwändig und damit teuer. Genaugenommen muß für das Werkzeug der gleiche Qualifikationsaufwand betrieben werden, wie für eine äquivalent qualifizierte Betriebssoftware. Bei jeder Modifikation (z.B. eines Compilers) muß dieser Aufwand wiederholt werden.

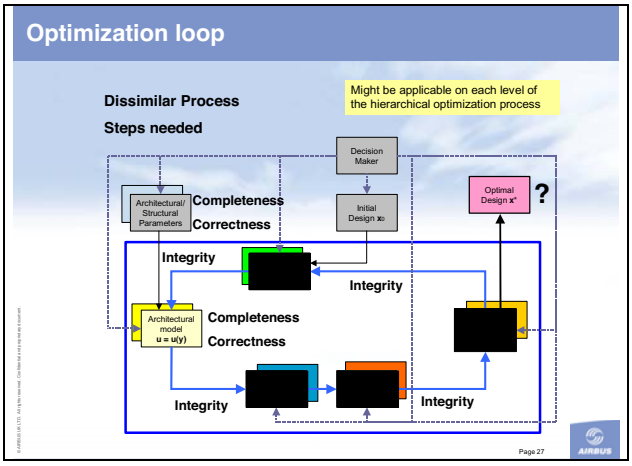

Bild 6 Ergebnissicherung “automatischer” Toolketten

In vielen Fällen ist es möglich, Kriterien aufzustellen, die das Ergebnis eines automatisierten Entwicklungsschrittes bei Vorliegen bekannter Eingangsparameter erfüllen muß. Die Überprüfung kann ebenso automatisch mittels eines „Checkers“ erfolgen. Der Vorteil ist, dass i.d.R. nur der Checker qualifiziert werden muß. Er ist zumeist deutlich einfacher strukturiert als das „ge-checkte“ Werkzeug. Außerdem ist eine Neuqualifikation nur sehr selten nötig, da die Plausibilitätsregeln („laws of nature“) so gut wie nie modifiziert werden.

Die „Checker-Lösung“ ist genau genommen eine spezielle Variante der redundanten, dissimilaren Durchführung eines, bzw. aller automatisierten Entwicklungsschritte. Jeder Entwicklungsschritt wird mindestens zweimal mit unterschiedlichen Methoden bearbeitet und die erhaltenen Resultate auf Übereinstimmung überprüft, Bild 6. Diese Vorgehensweise ist die Zuverlässigste, insbesondere bei sehr sicherheitskritischen Entwürfen. Sie ist definitiv auch empfehlenswert bei Verwendung „qualifizierter“ Werkzeuge, die auch nie 100%ig fehlerfrei sind, wie einschlägige Erfahrungen aus der Praxis belegen. Die vermeintlich höheren Investitionskosten amortisieren sich sehr schnell gegen Einsparungen bei der Werkzeugqualifikation und besonders wenn kritische Entwurfsfehler auf diese Weise vor der Produktfreigabe erkannt und zuverlässig beseitigt werden.

5. Zusammenfassung

Die „Virtualisierung“ von Funktionen sowie ihre Integration in Form komplexer Software Algorithmen auf integrierten Rechnerplattformen erfordert neue Herangehensweisen beim Entwurf und bei der Qualifikation der beteiligten Systeme. Der Vorgang der „generischen“ Qualifikation der Avionk-Ressourcen durch Festlegung von Sicherheitsbudgets und Zertifikationskrediten, die den Nutzern für ihre Funktionsnachweise zur Verfügung stehen, wurde erörtert. Sodann wurde diskutiert, wie die Entwurfsparameter und –anforderungen in Metriken und „constraints“ übersetzt und zur Bewertung durch die Entscheidungsträger verwendet werden. Die abschließenden Betrachtungen befassen sich mit dem Problem „automatisierter“ Entwurfsschritte mittels komplexer algorithmischer Werkzeuge, deren „Intransparenz“ die Notwendigkeit zusätzlicher und ggf. parallelisierter Engineering Prozesse nahe legen.