

Graphische Spezifikation und Echtzeitverifikation von Produktionsautomatisierungssystemen (GRASP)

Prof. Dr.-Ing. Wilhelm Dangelmaier*, Carsten Darnedde*,
Stephan Flake**, Dr. Wolfgang Müller**, Ulrich Pape*

* Heinz Nixdorf Institut, Paderborn
** C-LAB, Universität Paderborn

Inhaltsverzeichnis

1. Das Projekt.....	2
1.1. Kurzbeschreibung der Thematik.....	2
1.2. Verwendete Spezifikationstechniken	2
1.3. Verwendete Werkzeuge	3
2. Modellierung eines Produktionsautomatisierungssystems	3
2.1. Der MFERT-Editor.....	3
2.1.1. Funktionsbeschreibung	4
2.2. MFERT-Modelle	5
2.2.1. Zweistufige Fertigung mit Paletten- und Werkzeugkreislauf	5
2.2.2. Holonischer Materialfluss	7
3. Anfragen an ein Produktionsautomatisierungssystem	10
3.1. Fragenpool	10
4. Ausblick	13
Literatur.....	14

1. Das Projekt

GRASP ist ein von der Deutsche Forschungsgemeinschaft (DFG) geförder-tes Projekt im DFG-Schwerpunktprogramm "Integration von Techniken der Softwarespezifikation für ingenieurwissenschaftliche Anwendungen".

1.1. Kurzbeschreibung der Thematik

Ziel dieses Projektes ist die Nutzbarmachung von formalen Verifikations-techniken im ingenieurmäßigen Entwurf von Produktionsautomatisie-rungsanlagen (PA-Anlagen). Die formale Verifikation von PA-Systemen dient dazu, bereits in frühen Entwurfsphasen und auf hohen Abstraktions-ebenen Entwurfsfehler aufzuspüren. Ein besonderer Schwerpunkt liegt hier auf der Verifikation und Modellierung von Zeiteigenschaften. Zu diesem Zweck wurden formale Spezifikationstechniken wie quantitative temporale Logiken oder zeitbehaftete endliche Automaten, die als Basis der formalen Verifikation dienen, mit Hilfe von grafischen und strukturiert-natürlichsprachlichen Methoden in den Entwurfsablauf integriert. Als Er-gebnis wird eine prototypische Entwurfsumgebung implementiert, die von der Eingabe über die Verifikation und Analyse bis hin zur Unterstützung bei der Fehlersuche den Entwurf von PA-Anlagen unterstützt.

Für die Modellierung von Produktionsaufgaben findet der Modellierungsan-satz MFERT (**Modell der Fertigung**) (Holtkamp 1999) nicht nur Anwendung in den internen Projekten der Arbeitsgruppe von Prof. Dangelmaier, son-dern er wird auch in Kooperationen mit der Industrie eingesetzt. Hierbei er-hebt MFERT über die Modellierung hinaus den Anspruch, ein operables Modell zu sein, d. h., die Durchführung der Planungs- und Steuerungsauf-gaben der modellierten Produktion zu ermöglichen.

1.2. Verwendete Spezifikationstechniken

Im Rahmen des Projekts werden Spezifikationstechniken aus folgenden Domänen integriert:

- MFERT (Modell der Fertigung) als pragmatische Spezifikations-technik der Produktionsautomatisierung (PA),
- zustandsorientierte SW-Spezifikationstechniken zur Unterstützung des Entwurfs von PA-Systemen,
- temporallogische Spezifikationstechniken zur formalen Verifikation und Analyse von PA-Systemen,
- alternative Ansätze zur Formulierung zu verifizierender (Echtzeit-) Eigenschaften,

- graphische Animationen, um eine nachvollziehbare Analyse der entworfenen PA-Systeme zu ermöglichen (Braatz/Flake/Müller/Westkämper 2000).

Die Integration basiert dabei auf der gemeinsamen Nutzung von erweiterten endlichen Automaten als Formalismus, der mit allen oben angegebenen Spezifikationstechniken verträglich ist.

1.3. Verwendete Werkzeuge

Die Spezifikation und Verifikation der Produktionsautomatisierungssystem wird durch folgende Software-Werkzeuge unterstützt:

- MFERT-Editor, Modellierungswerkzeug zur Erstellung von MFERT-Modellen
- OOPUS-DPS, Dynamic Production Scheduling - Produktionsmanagementsystem zur simultanen Planung von Materialeinsatz und Betriebsmittelbelegung (Hamady 2000)
- RAVEN, Real-Time Analyzing and Verification System for Process Networks (Ruf/Kropf 2000)

2. Modellierung eines Produktionsautomatisierungssystems

Der Verifizierung eines Produktionsautomatisierungssystems geht die Abbildung von MFERT in zeitannotierte Zustandsübergangssysteme voraus, die für ein bereits existierendes Werkzeug zur Modellprüfung als Eingabe einer Modellbeschreibung dienen. Bei der Modellprüfung wird diese Beschreibung auf die Einhaltung von Eigenschaften überprüft, die in einer temporalen Logik oder einer davon abstrahierten Form spezifiziert werden. Um nun zunächst auf einer möglichst einfachen Art und Weise zu einem geeigneten MFERT-Modell eines PA-System zu gelangen, wurde ein Editor zur Modellierung von MFERT entwickelt.

2.1. Der MFERT-Editor

In der aktuellen Entwicklungsphase eines Editors auf Basis der MFERT-Strukturbeschreibung wird derzeit ein grafischer Editor zur graphischen Spezifikation von Fertigungselement-Knoten (FE-Knoten, Dreiecke), Fertigungsvorgangs-Knoten (FV-Knoten, Vierecke) und ihren Verbindungskanten implementiert. Abbildung 1 zeigt die Bedienoberfläche der Applikation im aktuellen Stand der Implementierung. Zur Spezifikation von FV-Knoten wurde die Möglichkeit geschaffen, zeitbehaftete Zustandsübergangsregeln in Tabellen einzutragen, was der Spezifikation von zeitbehafteten endlichen Automaten entspricht. Zudem wurde bereits eine Simulationskomponente implementiert, die es ermöglicht den Ablauf des spezifizierten Modells zu simulieren und diesen anhand der Ausgabeinformation der einzelnen F-Vorgänge nachzuvollziehen.

2.1.1. Funktionsbeschreibung

Der Arbeitsbereich der Benutzeroberfläche ist grob in vier Bereiche unterteilt. Dem Benutzer steht ein Werkzeugleiste zur Verfügung, in der der Benutzer die Komponenten zur Erstellung eines MFERT-Modells findet (Abbildung 1, Punkt 1). Zudem sind dort die Steuerungselemente für die Simulation eines erstellten Modells angeordnet. Links im Bild wird ein hierarchischer Baum des Modells zur Verfügung gestellt (Abbildung 1, Punkt 2), mit dessen Hilfe man sich zu jeder Komponente des Modells navigieren kann. Eventuell erstellte Untermodelle können dort der Übersichtlichkeit halber beliebig ein- oder ausgeblendet werden. Der in Abbildung 1 mit Punkt 3 gekennzeichnete Bereich ist der Bereich, in dem das jeweils angewählte Modell oder Untermodell dargestellt wird und bearbeitet werden kann. Die Ausgabe der Modellsimulationsinformationen erfolgt im unterem Bereich der Benutzeroberfläche (Abbildung 1, Punkt 4); die auszugebenden Informationen werden ausschließlich vom Benutzer festgelegt und in jedem Fertigungsvorgang einzeln definiert.

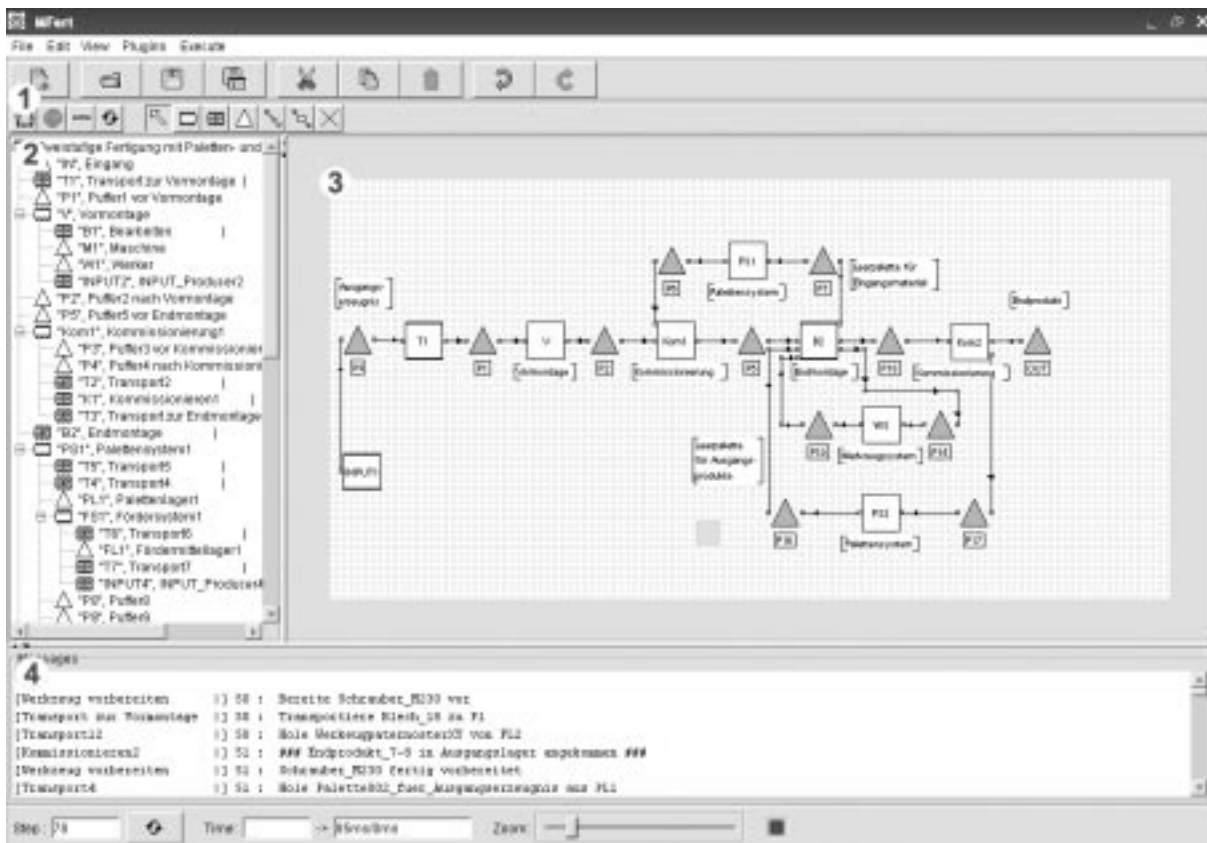


Abbildung 1: Die Benutzeroberfläche des MFERT-Editors

Die Spezifikation der einzelnen Fertigungsvorgänge werden in einer eigens dafür entwickelten Regelsprache definiert. Für die Definition stehen zwei Eingabealternativen zur Verfügung. Zum einen können die einzelnen Zustände der Fertigungsvorgänge tabellarisch angegeben werden (Abbildung 2, links) und zum anderen wird ein codebasierter Editor für die Eingabe angeboten (Abbildung 2, rechts).

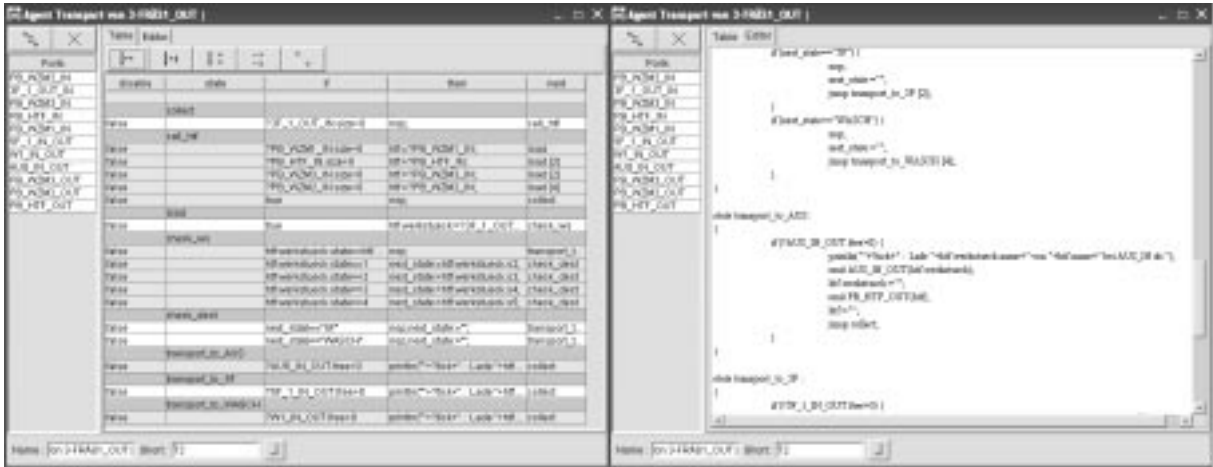


Abbildung 2: Eingabealternativen für die Spezifikation von Fertigungsvorgängen im MFERT-Editor

2.2. MFERT-Modelle

Im Zuge der Evaluierung des MFERT-Editors sind die Modelle zweier PA-Systeme entstanden. Zum einen ein MFERT-Modell für eine zweistufige Fertigung inklusive Paletten- und Werkzeugkreislauf und zum anderen der Modellierungsansatz eines holonischen Materialflusses in MFERT. Die beiden Modelle unterscheiden sich grundlegend darin, dass es sich beim ersten Modell um eine rein sequentielle Fertigung handelt und der Material- bzw. Markenfluss mit einem Blick nachzuvollziehen ist. Im zweiten Modell hingegen ist der Markenfluss abhängig von den jeweils anderen sich im Modell befindlichen Marken und variiert daher ständig. Somit lässt sich der genaue Ablauf des Modells nur Schritt für Schritt anhand der Ausgabeinformationen des Editors nachvollziehen.

2.2.1. Zweistufige Fertigung mit Paletten- und Werkzeugkreislauf

Als Modellierungstechnik für das in Abbildung 3 dargestellte Modell wurde die Top-Down-Methode verwendet, d.h. er wurde zunächst der grobe Ablauf des PA-Systems modelliert und dann durch das Hinzufügen von Untermodellen detailliert; drei von insgesamt sechs solcher Untermodelle sind in Abbildung 4 und Abbildung 5 zu sehen. Diese Methode eignet sich besonders gut für komplexe PA-Anlagen, da dadurch der nötige Überblick über das Gesamtsystem gewährleistet werden kann.

Die im Modell beschriebene zweistufige Fertigung zeigt die Vorbehandlung von Werkstücken, in diesem Fall Bleche, und das nachgelagerte Verschrauben von jeweils zwei Blechen in der Endmontage. Dazu werden die Bleche zunächst im Lager für Ausgangserzeugnisse bereitgestellt und anschließend zur Vormontage transportiert, wo die Bleche mit Bohrungen versehen werden. Es folgt die Kommissionierung von jeweils zwei Werkstücken auf eine Leerpallette. Die kommissionierten Bleche werden der Endmontage zusammen mit einer Leerplatte für das Ausgangsprodukt und einem Werkzeug bereitgestellt. Im Anschluss an die Montage werden die nun leere Palette des Eingangsmaterials und das benutzte Werkzeug wieder in ihren Kreislauf zurückgeführt und eine Palette mit montiertem Endprodukt ausgebracht. Das Endprodukt wird nun in einer weiteren Kommis-

sionierung entladen und ins Lager gebracht. Die entstandene Leerpallette wird wieder vom Palettensystem übernommen.

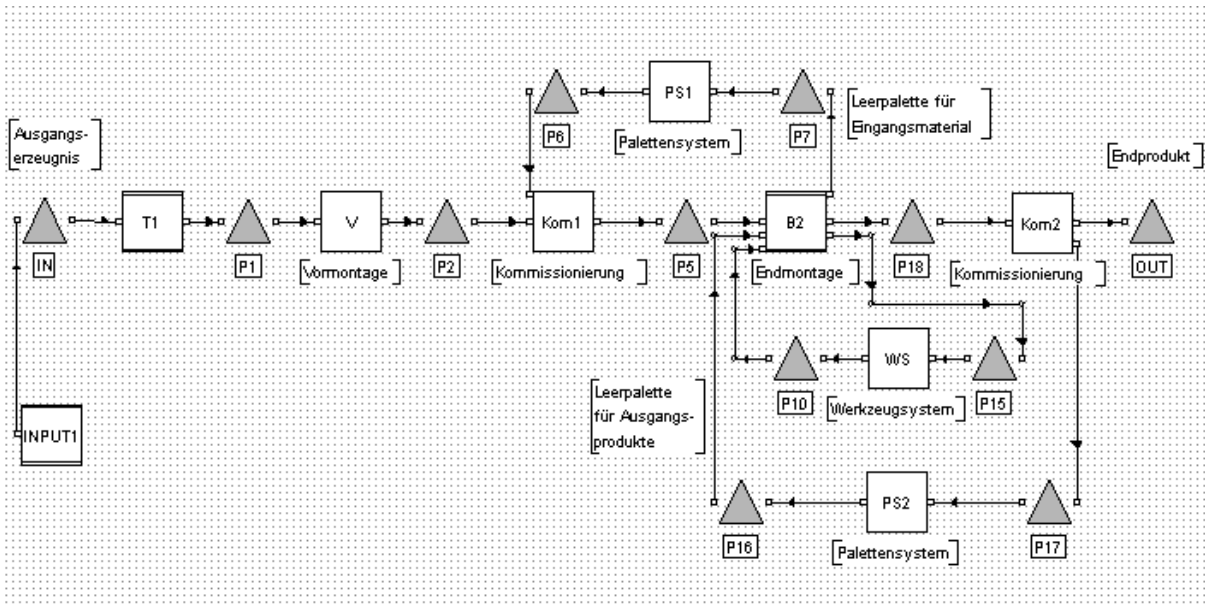


Abbildung 3: MFERT-Modell - Zweistufigen Fertigung mit Paletten- und Werkzeugkreislauf

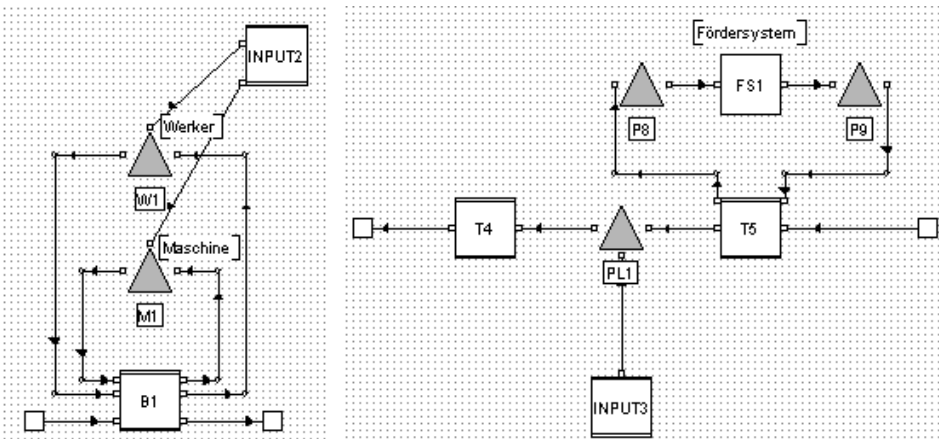


Abbildung 4: Untermodell „V“ Vormontage (links), Untermodell „PS1“ Palettensystem (rechts)

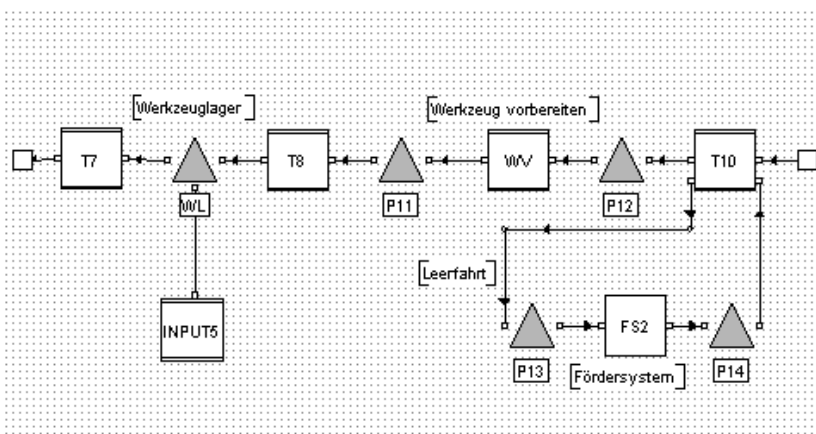
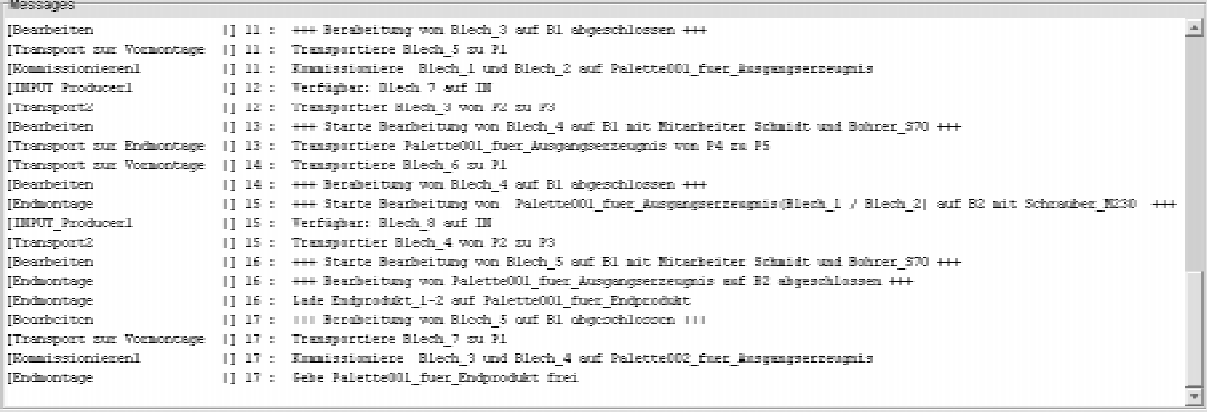


Abbildung 5: Untermodell „WS“ Werkzeugsystem

Die für diese Modell definierten Ausgabeinformationen sind in Abbildung 6 dargestellt. In jeder Zeile steht zunächst der Name des ausführenden Fertigungsvorgangs und darauf folgend der Zeitschritt in dem der jeweils beschriebene Vorgang ausgeführt wurde. Abschließend folgen die vom Benutzer definierten Ausgabertexte.



```
Messages
[Bearbeiten] [1] 11 : +++ Bearbeitung von Blech_3 auf B1 abgeschlossen +++
[Transport zur Vormontage] [1] 11 : Transportiere Blech_3 zu P1
[Kommissionieren] [1] 11 : Kommissioniere Blech_1 und Blech_2 auf PaLETTE001_fuer_Ausgangsergebnis
[INPUT_Producer1] [1] 12 : Verfügbar: Blech_7 auf I1
[Transport2] [1] 12 : Transportier Blech_3 von P2 zu P3
[Bearbeiten] [1] 13 : +++ Starte Bearbeitung von Blech_4 auf B1 mit Mitarbeiter Schmidt und Bohrer_570 +++
[Transport zur Endmontage] [1] 13 : Transportiere PaLETTE001_fuer_Ausgangsergebnis von P4 zu P5
[Transport zur Vormontage] [1] 14 : Transportiere Blech_5 zu P1
[Bearbeiten] [1] 14 : +++ Bearbeitung von Blech_4 auf B1 abgeschlossen +++
[Endmontage] [1] 15 : +++ Starte Bearbeitung von PaLETTE001_fuer_Ausgangsergebnis(Blech_1 / Blech_2) auf B2 mit Schrauber_M230 +++
[INPUT_Producer1] [1] 15 : Verfügbar: Blech_8 auf I1
[Transport2] [1] 15 : Transportier Blech_4 von P2 zu P3
[Bearbeiten] [1] 16 : +++ Starte Bearbeitung von Blech_5 auf B1 mit Mitarbeiter Schmidt und Bohrer_570 +++
[Endmontage] [1] 16 : +++ Bearbeitung von PaLETTE001_fuer_Ausgangsergebnis auf B2 abgeschlossen +++
[Endmontage] [1] 16 : Lade Endprodukt_1-2 auf PaLETTE001_fuer_Endprodukt
[Bearbeiten] [1] 17 : +++ Bearbeitung von Blech_5 auf B1 abgeschlossen +++
[Transport zur Vormontage] [1] 17 : Transportiere Blech_7 zu P1
[Kommissionieren] [1] 17 : Kommissioniere Blech_3 und Blech_4 auf PaLETTE002_fuer_Ausgangsergebnis
[Endmontage] [1] 17 : Gehe PaLETTE001_fuer_Endprodukt frei
```

Abbildung 6: Ausgabeinformationen des Modells „Zweistufige Fertigung mit Paletten- und Werkzeugkreislauf“

2.2.2. Holonischer Materialfluss

Das in diesem Abschnitt untersuchte Szenario basiert auf einem sog. holonischen Fertigungssystem, welches als Fallstudie im Zuge der IMS Initiative eingeführt (Westkämper/Höpf/Schaeffer 1994) und später im Rahmen dieses DFG-Projekts weiterentwickelt wurde (Braatz/Ritter 2001). In diesem Zusammenhang wurde die Idee eines holonischen Fertigungssystems basierend auf der Lehre der Holarchien entwickelt, welche sich mit der Organisation von Chaos und Komplexität befasst. Ein Holon wird als autonomer, kooperativer Teil eines komplexen Ganzen verstanden, welches nur in der Summe der Einzelteile bestehen kann. Holonische Systeme zeichnen sich durch die Selbstähnlichkeit und Selbstkonfigurationsfähigkeit ihrer Komponenten aus, was zu einer hohen Fehlertoleranz und Stabilität des Gesamtsystems führt.

Es wurde nun versucht, den Materialfluss und die Transportwege der holonischen Transportfahrzeuge (HTF) möglichst genau nach den Vorgaben der Referenzfallstudie in MFERT nachzubilden (Abbildung 7). Eine echte Autonomie der HTF, wie sie durch die Fallstudie vorgegeben wird, kann in der Nachbildung in MFERT nicht modelliert werden, da die HTF in MFERT als Marken modelliert werden, welche laut Definition keine Eigensteuerung zulassen. Die Steuerung der HTF erfolgt im Modell über sechs verschiedene Fertigungsvorgänge; die Verarbeitung des Materials erfolgt über 3 weitere – die Werkzeugmaschinen (WZM). Die sechs erstgenannten Fertigungsvorgänge können zusammenbetrachtet als ein in der Fallstudie vorhandenes funkgestütztes Broadcast-Kommunikationssystem interpretiert werden, welches der Kommunikation zwischen den HTF und den Werkzeugmaschinen dient.

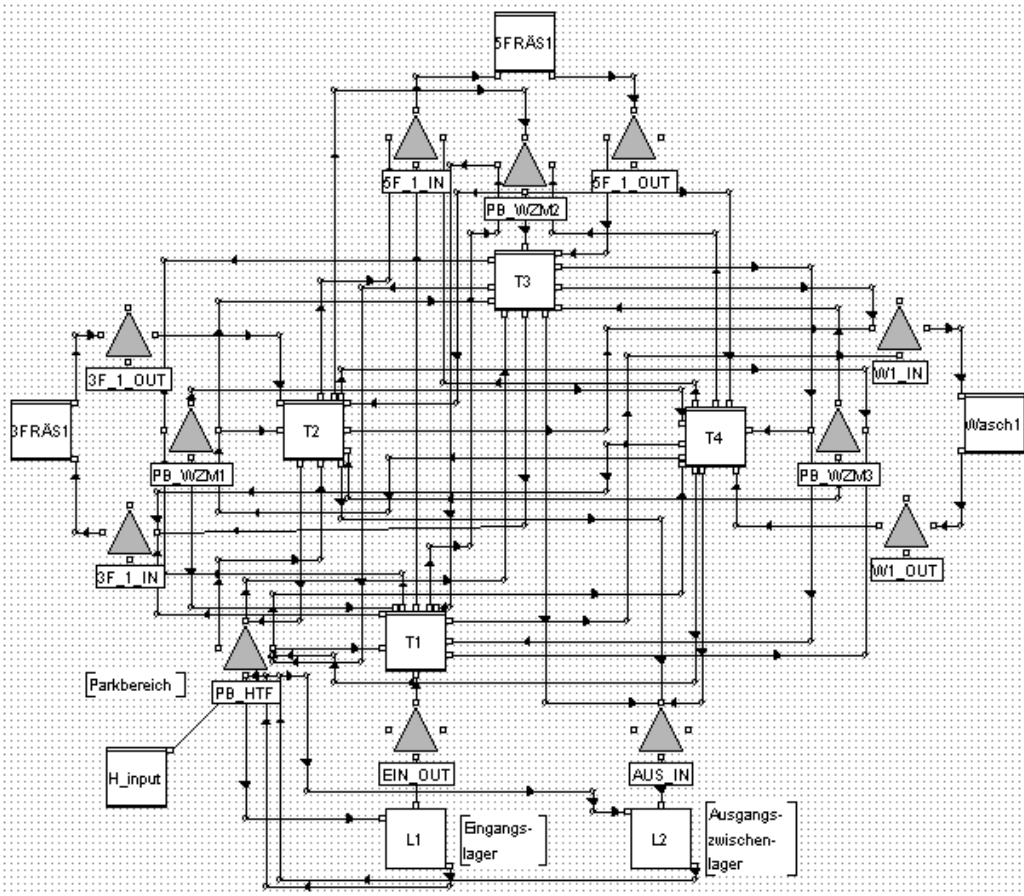


Abbildung 7: MFERT-Modell – Holonischer Materialfluss

Der Modellablauf ist wesentlich komplexer als der im zuvor vorgestellten Modell der zweistufigen Fertigung.

Zu Beginn werden einmalig mittels des Fertigungsvorgangs H_input drei HTF erzeugt und in PB_HTF bereitgestellt – der Fertigungsvorgang wird im weiter Modelablauf nicht weiter benötigt. Die Produktion von Werkstücken erfolgt im Fertigungsvorgang INPUT innerhalb des Untermodells L1. Von dort fließen durchgängig Werkstückmarken vom Typ „Kurbelwelle“ und „V6-Motor“ in das Modell ein, und zwar so, dass immer 10 Werkstückmarken im Eingangslager bereitliegen. Die beiden Markentypen besitzen jeweils eine unterschiedliche Bearbeitungsreihenfolge durch die WZM.

Sobald ein Platz im Ausgangspuffer (EIN_OUT) vom Eingangslager frei ist, wird dort die nächste Werkstückmarke aus dem Eingangslager mit Hilfe eines HTF platziert; hierbei wird nur auf verfügbare HTF aus dem Parkbereich PB_HTF zurückgegriffen. Die Anzahl der benötigten Zeitschritte für diesen Vorgang ist variabel und abhängig vom Lagerplatz des Werkstücks; es werden zwischen 5 und 10 Zeitschritte benötigt.

Wartet ein Werkstück in EIN_OUT auf seine Bearbeitung, wird ein HTF zum Transport gerufen. Dabei werden die vier Parkbereiche der HTF nacheinander auf die Verfügbarkeit von freien HTF überprüft. Und zwar wird zunächst der am dichtesten liegende Parkbereich befragt, welches von EIN_OUT aus gesehen PB_HTF wäre. Danach werden in aufsteigender Reihenfolge alle andern Parkbereiche befragt bis hin zum am weitesten

entfernten Parkbereich, also PB_WZM2. Allen Entfernungen liegt eine vorgegebene Entfernungsmatrix zugrunde.

Ist ein HTF gefunden braucht es der Entfernung entsprechend viele Zeitschritte um zu EIN_OUT zu gelangen. Anschließend wird anhand der Werkstückattribute der nächste Bearbeitungsort der Werkstückmarke ermittelt und diese dann mittels angefordertem HTF in entsprechend vielen Zeitschritten zum Bearbeitungsort transportiert. Ist der Eingangspuffer der betreffenden Bearbeitungsmaschine belegt, wartet das HTF beladen vor dem Puffer. Ist ein Platz frei, wird das Werkstück entladen und das HTF im Parkbereich des angefahrenen Bearbeitungsortes positioniert. Jedes Werkstück muss mindestens einen Bearbeitungsschritt aufweisen; ein Transport von EIN_OUT zu AUS_IN ist somit nicht möglich.

Von den WZM werden die Werkstücke aus dem jeweiligen Eingangspuffer entnommen, innerhalb von zwei Zeitschritten zur Bearbeitung positioniert, in maschinenabhängiger Zeit bearbeitet und schließlich ebenfalls innerhalb von zwei Zeitschritten auf dem Ausgangspuffer verbracht. Der Weitertransport zum nächsten Bearbeitungsort erfolgt analog zum Transport aus EIN_OUT; nun ist allerdings ein Transport zu AUS_IN möglich, wenn nämlich der letzte Bearbeitungsschritt des Werkstückes abgeschlossen wurde. Nach dem Entladen eines Werkstückes auf AUS_IN wird das HTF immer auf PB_HTF abgestellt.

Von AUS_IN wird das Werkstück schließlich mittels eines freien HTF aus PB_HTF im Ausgangszwischenlager positioniert; dieser Vorgang dauert abhängig von zugewiesenen Lagerplatz zwischen 5 und 10 Zeiteinheiten.

Ist der vorgegebene Tagesoll erfüllt, läuft das System weiter bis ein Transport aus Platzmangel nicht mehr ausgeführt werden kann, da kein Platz auf AUS_IN mehr frei geräumt wird.

In Abbildung 8 wird die durch eine Simulation des Modells generierte Ausgabe der Fertigungsvorgangsinformationen gezeigt. Der Detaillierungsgrad der Informationen wird dabei durch den Benutzer festgelegt.

```

Messages
[Transport von EIN_OUT ] 325 : Lade W6-Motor_4 von HTF3 bei 3-FRÄSI_IN ab.
[Transport von WASCHL_OUT ] 326 : Nehme W6-Motor_2 mit HTF1 bei WASCHL_OUT auf.
[Drei-Achsen-Fräsmaschine 1] 327 : Positioniere W6-Motor_4 auf 3-FRÄSI.
[Waschmaschine 1 ] 328 : Positioniere Kurberleville_3 auf WASCHL.
[Drei-Achsen-Fräsmaschine 1] 330 : Starte Bearbeitung von W6-Motor_4 auf 3-FRÄSI.
[Waschmaschine 1 ] 331 : Starte Bearbeitung von Kurberleville_3 auf WASCHL.
[Transport von WASCHL_OUT ] 332 : Lade W6-Motor_3 von HTF1 bei AUS_IN ab.
[Transport von EIN ] 335 : Nehme Kurberleville_4 mit HTF1 bei EIN auf.
[Fünf-Achsen-Fräsmaschine 1] 343 : Bearbeitung von Kurberleville_3 auf 5-FRÄSI beendet. Entlade Kurberleville_3 ...
[Transport von EIN ] 345 : Lade Kurberleville_4 von HTF1 bei EIN_OUT ab.
[Fünf-Achsen-Fräsmaschine 1] 345 : Kurberleville_3 von 3-FRÄSI entladen und auf SPU_OUT verbracht.
[Transport von 5-FRÄSI_OUT ] 345 : Nehme Kurberleville_3 mit HTF2 bei 5-FRÄSI_OUT auf.
[Transport von HTF_IN ] 351 : Positioniere W6-Motor_3 mit HTF1 in AUS.
[Transport von EIN_OUT ] 351 : Nehme Kurberleville_4 mit HTF3 bei EIN_OUT auf.
[Drei-Achsen-Fräsmaschine 1] 351 : Bearbeitung von W6-Motor_4 auf 3-FRÄSI beendet. Entlade W6-Motor_4 ...
[Fünf-Achsen-Fräsmaschine 1] 351 : Positioniere W6-Motor_3 auf 3-FRÄSI.
[Transport von 5-FRÄSI_OUT ] 354 : Lade Kurberleville_3 von HTF2 bei WASCHL_IN ab.
[Drei-Achsen-Fräsmaschine 1] 354 : W6-Motor_4 von 3-FRÄSI entladen und auf SPU_OUT verbracht.
[Fünf-Achsen-Fräsmaschine 1] 354 : Starte Bearbeitung von W6-Motor_3 auf 5-FRÄSI.
[Transport von EIN_OUT ] 357 : Lade Kurberleville_4 von HTF3 bei 5-FRÄSI_IN ab.
[Transport von 3-FRÄSI_OUT ] 359 : Nehme W6-Motor_4 mit HTF2 bei 3-FRÄSI_OUT auf.
[Transport von HTF_IN ] 360 : #3 von 5 Werkstücke in Ausgangszwischenlager.#
[Transport von EIN ] 363 : Nehme W6-Motor_5 mit HTF1 bei EIN auf.
    
```

Abbildung 8: Ausgabeinformationen des Modells „Holonischer Materialfluss“

Während der Simulation konnte keine Deadlock-Situation festgestellt werden. Dieser Sachverhalt lässt sich aber nur mit einer gewissen Wahr-

scheinlichkeit auf das reale PA-System übertragen. Die Wahrscheinlichkeit steigt mit der Anzahl an durchgeführten Simulation bzw. mit der Simulationsdauer. Eine vollständige Deadlock-Sicherheit wird auf diesem Wege nie bestätigt werden können. Daher soll das Modell in einem weiteren Schritt auf ein zeitannotiertes Zustandsübergangssystem abgebildet werden und diese Abbildung dann mittels des Modelchecker RAVEN verifiziert werden.

3. Anfragen an ein Produktionsautomatisierungssystem

Mit der Modellierung von MFERT als zeitbehaftete, endliche Automaten ist ein direkter Bezug zu dem im Modelchecker RAVEN benutzten Modell der E/A-Intervallstrukturen gegeben. Ein integriertes formales Modell für die Generierung von MFERT-Beschreibungen in die RAVEN Input Language (RIL) wird derzeit ausgearbeitet.

Um von den in RAVEN zur Spezifikation von Systemeigenschaften benutzten temporallogischen Formeln zu einer benutzerfreundlicheren Darstellung zu gelangen, wurde ein erstes Konzept zur Formulierung solcher Eigenschaften mittels strukturierter-natürlichsprachlicher Sätze erarbeitet. Das Konzept basiert auf existierenden Studien, in denen wiederkehrende Muster anhand von mehreren hundert vorhandenen Spezifikationen aus Industrie und Forschung identifiziert und kategorisiert wurden. Die in unserem Konzept vorgeschlagenen Sätze können aus einer Reihe von Satzfragmenten in englischer Sprache zusammengesetzt werden. Sie behandeln Aussagen über die Abfolge oder das gleichzeitige bzw. exklusive Auftreten von (Teil-)Modellkonfigurationen sowie Kausalzusammenhänge zwischen Modellkonfigurationen. Als wesentliche Neuerung ist hier die Einbeziehung von Zeitintervallen an verschiedenen Stellen innerhalb der Sätze zu nennen. Zur Formulierung der Sätze wurde interaktive Formulare erstellt, die auch in einem Web-Frontend Verwendung finden können.

Neben Korrektheitseigenschaften ist auch eine Menge von Sätzen zu Analyseabfragen über Zeitbedingungen zwischen verschiedenen Modellkonfigurationen konzipiert worden. Auch hier werden Satzfragmente zu vollständigen Sätzen zusammengesetzt.

Um die Satzmenge und die Abfragetypen der Analyseabfragen im produktionstechnisch sinnvollen Rahmen zu erweitern, wurde ein kategorisierter Fragenpool mit für die Entwurfphase von PA-Systemen relevanten Anfragen erstellt.

3.1. Fragenpool

Im Folgenden wird ein Auszug an Anfragen, die während des Entwurfs von PA-Systemen aufschlussreich hinsichtlich deren Durchsatz, Sicherheit und Zuverlässigkeit sind, aus dem kategorisierten Fragenpool dargestellt.

Die Buchstabenkennzeichnungen der Fertigungsvorgänge und -elemente bestimmen nicht deren Anordnungsreihenfolge, d.h. F-Vorgang/F-Element B muss nicht direkt auf F-Vorgang/F-Element A folgen.

- Kategorie: Zeit

- Kategorie: Zeitpunkte

Wann stehen im Fertigungs-Element A erstmals x Einheiten zur Verfügung?

Wann startet Fertigungsvorgang A zum x. Mal?

- Kategorie: Zeiträume

Wie lange verweilt eine Einheit mindestens im Fertigungselement A?

Wie lange verweilt eine Einheit höchstens im Fertigungselement A?

Wie lang ist der Zeitraum mindestens, in dem im Fertigungselement A jeweils auf die nächste Einheit gewartet wird?

Wie lang ist der Zeitraum höchstens, in dem im Fertigungselement A jeweils auf die nächste Einheit gewartet wird?

Wie lang ist der Zeitraum mindestens, in dem im Fertigungsvorgang A jeweils auf die nächste Einheit gewartet wird?

Wie lang ist der Zeitraum höchstens, in dem im Fertigungsvorgang A jeweils auf die nächste Einheit gewartet wird?

Wie lange darf die Instandsetzung von Fertigungsvorgang A nach dessen Ausfall zum Zeitpunkt t_1 dauern, damit zum Zeitpunkt t_2 x Einheiten im Fertigungselement B verfügbar sind?

Wie lang ist der Zeitraum von der Entnahme von Einheiten aus Fertigungselement A bis zum Eintreffen von Einheiten in Fertigungselement B?

- Kategorie: Menge

- Kategorie: Menge INPUT

Wie viele Einheiten müssen im Fertigungselement A verfügbar sein, damit in Fertigungselement B x Einheiten entstehen?

Wie viele Einheiten müssen im Fertigungselement A verfügbar sein, damit im Fertigungselement B x Einheiten entstehen, wenn Fertigungsvorgang A in der Zeit von t_1 bis t_2 ausfällt?

- Kategorie: Menge OUTPUT

Wie viele Einheiten entstehen im Fertigungselement A in der Zeit von t_1 bis t_2 ?

Wie viele Einheiten produziert Fertigungsvorgang A in der Zeit von t_1 bis t_2 ?

Wie viele Einheiten entstehen im Fertigungselement A in der Zeit von t_1 bis t_2 , wenn Fertigungsvorgang A in der Zeit von t_1 bis t_2 ausfällt?

Wie viele Einheiten produziert Fertigungsvorgang A in der Zeit von t_1 bis t_2 , wenn Fertigungsvorgang B in der Zeit von t_1 bis t_2 ausfällt?

Wie viele Einheiten entstehen in Fertigungselement A, wenn im Fertigungselement B x Einheiten zur Verfügung stehen?

Wie viele Einheiten entstehen in Fertigungselement A, wenn im Fertigungselement B x Einheiten zur Verfügung stehen und Fertigungsvorgang A in der Zeit von t_1 bis t_2 ausfällt?

- Kategorie: Kapazität

Wie hoch muss die Kapazität von Fertigungselement A sein, wenn Fertigungsvorgang A in der Zeit von t_1 bis t_2 ausfällt?

Wie hoch muss die Kapazität von Fertigungselement A sein, wenn Fertigungsvorgang A x Einheiten in der Zeit von t_1 bis t_2 produziert?

Wie hoch muss die Kapazität von Fertigungselement A sein, wenn in Fertigungselement B x Einheiten zur Verfügung stehen?

Wird die Kapazitätsgrenze k in Fertigungselement A jemals erreicht/überschritten?

- Kategorie: Ablauf

In welchem Fertigungselement entstehen die ersten Einheiten?

Welcher Fertigungsvorgang produziert die ersten Einheiten?

Entstehen im Fertigungselement A weiterhin Einheiten, wenn Fertigungsvorgang A in der Zeit von t_1 bis t_2 ausfällt?

Produziert Fertigungsvorgang A weiterhin Einheiten, wenn Fertigungsvorgang B in der Zeit von t_1 bis t_2 ausfällt?

Entstehen im Fertigungselement A weiterhin Einheiten, wenn im Fertigungselement B die Maximalkapazität bereits erreicht ist?

Produziert Fertigungsvorgang A weiterhin Einheiten, wenn im Fertigungselement A die Maximalkapazität bereits erreicht ist?

Wird der Ablauf des Modells unterbrochen, wenn Fertigungsvorgang A in der Zeit von t_1 bis t_2 ausfällt?

Wie oft muss Fertigungsvorgang A durchlaufen werden, bis in Fertigungselement A x Einheiten zur Verfügung stehen?

4. Ausblick

Bis zum Abschluss des Projekts soll eine Methodik zur Integration formaler Verifikation als Qualitätssicherung im ingenieurbasierten Entwurfsprozeß basierend auf dem formalem MFERT Ablaufmodell erarbeitet werden und der wohldokumentierte und qualitätsorientierte Entwurf von PA-Systemen für die industrielle Praxis ermöglicht werden.

Außerdem sollen neue temporallogische Verifikations- und Analyseverfahren entwickelt werden, die für den Einsatz im Bereich PA optimiert sind. Neben den in der nächsten Projektphase geplanten Entwicklung von Echtzeitverifikationsalgorithmen sind auch Untersuchungen von neuen Verfahren zur Abstraktion und Komposition geplant. Ebenfalls sollen auch Arbeiten auf der Basis von linearen Ungleichungssystemen oder Termersetzungssystemen untersucht werden. Auch die kombinierten Simulations-/Verifikationstechniken werden in der nächsten Phase untersucht, um sie dann bis zum Ende des Projektes auszubauen und in den Validationsprozess zu integrieren.

Es soll eine Integration von formalen Verifikationsverfahren in PA-Laufzeitsysteme stattfinden. Durch Generierung von Laufzeitüberprüfung als Verifikationsproblem werden erstmalig diese Methoden nicht nur zum Entwurf sondern zur Überwachung laufender Produktionsprozesse verwendet. Es ist dadurch möglich sich anbahnende Fehler bereits vor deren Eintreten zu erkennen und geeignete Gegenmaßnahmen zu ergreifen.

Weiterhin soll es neue Methoden und Schnittstellen zur Eingabe von CCTL-basierter Spezifikation und der Darstellung der Analyseergebnisse geben. Geplant sind Techniken, Mittel und methodische Unterstützung zur Spezifikation und Analyse von Agenten in verteilten Systemen.

Im Ganzen soll eine Erweiterung des Ansatzes zur agenten-basierten Spezifikation und Analyse von PA-Systemen geschaffen werden und die vollständige Integration der angegebenen visuellen formalen Spezifikations- und Analysetechniken in ein PA-System vollzogen werden.

Abschließend soll die Spezifikation und Verifikation größerer PA-Praxisbeispiele vorgenommen werden.

Literatur

- Holtkamp, Ralf (Holtkamp 1999):** Ein objektorientiertes Rahmenwerk zur Erstellung individueller, verteilter Fertigungslenkungssysteme. Dissertation, Heinz Nixdorf Institut, HNI-Verlagsschriftenreihe, Band 51, März 1999.
- Braatz, Arnulf; Flake, Stephan; Müller, Wolfgang; Westkämper, Engelbert (Braatz/Flake/Müller/ Westkämper 2000):** Prototyping einer Fahrzeugsteuerung in virtueller 3D-Umgebung, in: *Simulation und Visualisierung 2000*, Magdeburg, Deutschland, März 2000.
- Hamady, Mohamed (Hamady 2000):** OOPUS-DPS - "Dynamic Production Scheduling", <http://www.whni.uni-paderborn.de/cim/projekte/oopus-dps.php3>, Dezember 2000.
- Ruf, Jürgen; Kropf, Thomas (Ruf/Kropf 2000):** Analyzing Real-Time Systems, in: Design, Automation and Test in Europe (DATE), Paris, Frankreich, März 2000. IEEE Computer Society Press.
- Westkämper, Engelbert; Höpf, Michael; Schaeffer, Christoph (Westkämper/Höpf/Schaeffer 1994):** Holonic Manufacturing Systems (HMS) - Test Case 5, in: Proceedings of Holonic Manufacturing Systems, Lake Tahoe, CA, USA, Februar 1994.
- Braatz, Arnulf; Ritter Arno (Braatz/Ritter 2001):** Referenzfallstudie Produktionstechnik v2.0: Holonischer Materialfluss, <http://tfs.cs.tu-berlin.de/projekte/indspec/SPP/RefPAv2.doc>, Oktober 2001.