Proseminar

„Software Desaster und wie man sie verhindern kann“

# Stellwerk Hamburg Altona

# und

# Petri-Netze

Marc Hennes

18.Dezember 2002

# Gliederung:

# 1. Einführung

Am 12.März 1995 hat die Deutsche Bahn AG das Stellwerk in Hamburg Altona auf ein voll elektronisches Stellwerk umgestellt. Bei der Einführung dieser Technik kam es nach kurzer Zeit zu erheblichen Problemen. Im folgenden möchte ich auf diese Probleme genauer eingehen und Lösungsmöglichkeiten beschreiben.

# 2. Stellwerk Hamburg Altona

## 2.1. Stellwerk allgemein

Die allgemeine Definition eines Stellwerks aus dem Brockhaus lautet: „ Signale und Weichen sind von einander abhängig, sie werden vom Stellwerk gesteuert.“ Im Allgemeinen kann man sagen, dass Stellwerke die Aufgabe haben einen sicheren Betrieb zu gewährleisten und eine zuverlässige und fahrplangenaue Zuglenkung zu ermöglichen.

Es hat eine lange Entwicklung der Stellwerke gegeben, an deren Anfang die mechanischen Stellwerke stehen. Diese mussten von Hand bedient werden. Eine erhebliche Erleichterung der Arbeit bedeutete die Einführung der sogenannten Drucktastenstellwerke. Der nächste Schritt der Entwicklung sind die Relais-Stellwerke. Schließlich wurden die elektronischen Stellwerke (Estw) eingeführt. Diese benötigen 30% weniger Platz als Relais-Stellwerke, sind leichter zu warten, haben eine höhere Reichweite und sind leichter umzubauen.

Das erste elektronische Stellwerk wurde 1986 in Murnau in Betrieb genommen. Dies war eine Testanlage, bei der das Estw alte mechanische Anlagen abgelöst hat und parallel zu einem Stellwerk gelaufen ist, das auf Relais-Technik basierte. Da es sich in Murnau um einen sehr kleinen Bahnhof handelt, installierte man einen zusätzlichen Rechner, der weitere Betriebsabläufe simulierte. Weiterhin konnte man mit diesem Rechner Konfliktsituation simulieren, um das System Stresssituationen aussetzen zu können. Neben dieser Einrichtung sind sieben weitere Testinstallationen vorgenommen worden. Damit dieses System die Serienreife erlangen konnte, musste es sich über zwei Jahre hinweg als zuverlässig erweisen. Nachdem die erforderlichen Sicherheitsnachweise für die Hardware und für die Software erbracht wurden, wurde das Estw vom Bundesbahnzentralamt (BZA) endgültig abgenommen. Dieses elektronische Stellwerk wird immer weiter entwickelt, um den ständig wachsenden Anforderungen gerecht werden zu können.

## 2.2. Der Bahnhof Hamburg Altona

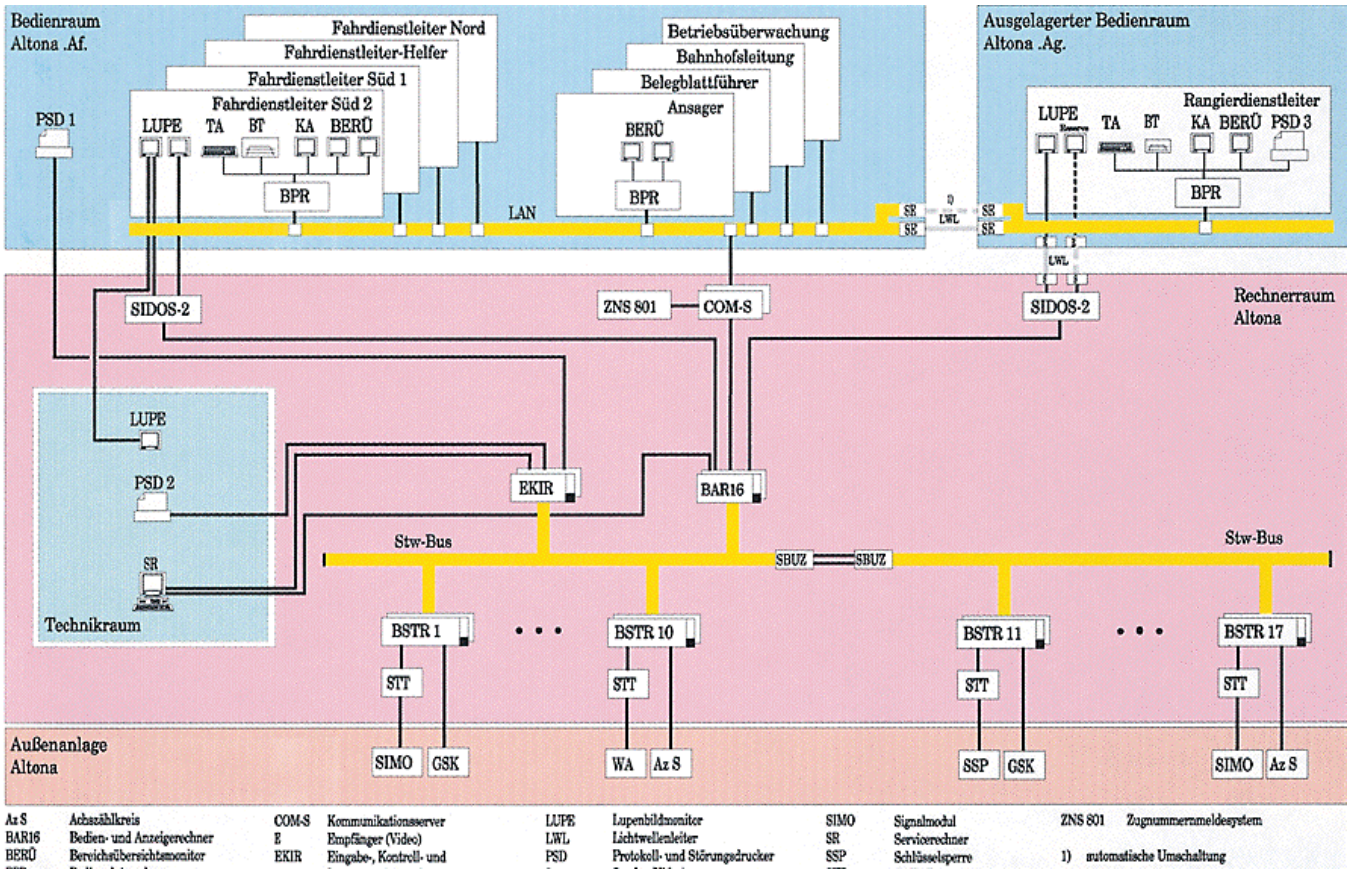
Bei dem Bahnhof in Hamburg Altona handelt es sich um einen Kopfbahnhof, d.h. alle Züge können den Bahnhof nur in der Richtung verlassen, aus der sie auch gekommen sind. Dies macht ein hohes Rangieraufkommen notwendig. Der Bahnhof Hamburg Altona ist ein nationaler und internationaler Verkehrsknoten. Täglich werden rund 130000 Reisende abgefertigt. Hamburg Altona ist außerdem ein Start- und Zielpunkt für viele innerdeutsche ICE Verbindungen.

## 2.3. Elektronisches Stellwerk von Siemens

Die gesamte zu überwachende Strecke wird in Teilabschnitte eingeteilt. Es muss immer die Bedingung gelten, dass nur ein Zug in einem Abschnitt ist. Die Aufgabe der Signale ist es, die Abschnitte rechtzeitig zu Sperren und zu sichern. Dies wird bei der Bahn unter dem Begriff signaltechnische Sicherheit zusammengefasst.
Weiterhin ist das Fahrstraßenkonzept ein wichtiges Instrument um die Sicherheit zu gewährleisten.
Durch das Stellen von Weichen wird eine Fahrstraße erstellt. Um diese schließt sich dann eine sogenannte Schutzzone, d.h. die entsprechenden Signale werden auf „Halt“ gestellt. Diese Zone wird dann auf die Einhaltung der Sicherheitsbedingungen überwacht, und erst dann wird das Einfahrtssignal auf „Fahrt“ gestellt. Nachdem die Fahrstraße benutzt wurde, wird diese automatisch wieder gelöscht.

Die Firma Siemens bedient sich bei ihren elektronischen Stellwerken dem sogenannten SIMIS-Konzept (SIMIS = Sicheres Mikrocomputersystem). Hierbei handelt es sich in der einfachsten Form um ein System, dass aus zwei identischen Computern besteht, die die gleiche Hardware und Software besitzen und die selben Signale empfangen. Weichen und Signale werden nur geschalten, wenn beide Computer zum selben Ergebnis kommen. Falls ein Rechner ausfallen sollte, wird dieser inaktiv geschaltet. Der inaktive Status wird immer als gefährdungsfreier Betriebszustand angesehen.

Bei dem Estw in Hamburg Altona handelt es sich um ein SIMIS-System, das aus drei Mikrocomputern besteht(Zwei-von-Drei-Konzept). Hierbei laufen immer zwei Rechner parallel. Sollte einer der beiden aktiven Rechner ausfallen, wird sofort auf den dritten Rechner umgeschaltet. Damit ist gewährleistet, dass schon nach wenigen Minuten die volle Betriebssicherheit wieder hergestellt ist. Weiterhin ermöglicht dies, den ausgefallen Computer bei laufendem Betrieb wieder instandzusetzen und ohne Störung den Rechner wieder in Betrieb zu nehmen.
Siemens baut diese Systeme sehr robust. Sie können Temperaturen von minus 40°C bis plus 80°C sowie Stöße bis zum fünffache der Erdbeschleunigung vertragen. Sogar Stromstöße bis 2000 Volt beeinflussen den laufenden Betrieb nicht.
Um die Sicherheit zu gewährleisten, gibt es zum einen Selbsttestprogramme, die etwaige unentdeckte Fehler selbstständig melden, zum anderen können bei einem Baugruppen Ausfall Ferndiagnosen durchgeführt werden. Weiterhin sind in allen wichtigen Komponenten Einschaltprüfprogramme installiert, deren Aufgabe es ist, die Aufhebung des inaktiven Zustands zu verhindern, bevor der Fehler behoben wurde.




Die zentrale Einheit des Estw ist der BAR16 (= Bedien-und-Anzeige-Rechner, die 16 steht für die 16 Bit Bandbreite). Er ist für die Verbindung zwischen den Arbeitsplätzen der Fahrdienstleiter (FDL) und den Bereichsstellrechnern (BSTR) zuständig. Er koordiniert somit die gesamte Kommunikation zwischen den einzelnen Bereichen.
In den BSTR werden die erforderlichen Funktionsabläufe zum erstellen, sichern und auflösen der jeweiligen Fahrstraßen realisiert.
Die FDL haben im Bedienraum einen vollständigen Überblick über Zugstandorte, Zugbewegungen sowie über Signale und Weichen.

## 2.4. Gründe für die Einführung des elektronischen Stellwerks

Das Stellwerk in Hamburg Altona bestand aus acht verschiedenen Anlagen, die im Zeitraum von 1911 bis 1952 eingebaut wurden. Bei der ältesten Anlage handelt es sich um ein Hebelstellwerk. Diese alten Anlagen sollten nun durch ein neues elektronisches Stellwerk ersetzt werden. Weiterhin wollte man mit der Einführung der neuen Technik Arbeitsplätze einsparen, da für den Betrieb des neuen Stellwerks nur noch fünf Fahrdienstleiter notwendig waren, anstatt der bisher über 50.

Die Bahn AG gab bei Inbetriebnahme des Stellwerks bekannt: „Mit der Inbetriebnahme wird ein weiterer wichtiger Schritt zu einem modernen rationellen Betrieb der Deutschen Bahn AG vollzogen.“ Weiterhin: „Die neue Technik trägt zur Erhöhung der Betriebssicherheit bei“.

## 2.5. Problemfall

Nachdem am 12.3.1995 das Estw in Betrieb genommen wurde, kam es um 5:00 Uhr, 7:00 Uhr und 9:00 Uhr des folgenden Tages zu selbstständigen Sicherheitsabschaltungen des Systems. Es dauerte zwar immer nur ca. 10 Minuten, bis die Anlage wieder betriebsbereit war, aber die Bahn beschloss den Zugverkehr aus Sicherheitsgründen weitgehend einzustellen, bis der Fehler gefunden und behoben wurde. Dies kam einer Vollsperrung des gesamten Bahnhofs ziemlich nahe. Durch diese Sperrung kam es zu erheblichen Verspätungen im gesamten Bahnverkehr.
Die Fehleranalyse dauerte zwei Tage. Am 15.3.1995 konnte das Stellwerk den Betrieb wieder aufnehmen, doch es kam noch bis zum 19.3.1995 zu Unregelmäßigkeiten, die aber nicht auf die Technik zurückzuführen sind.

## 2.6. Fehlersuche

Als Ursache für den Fehler konnte ein Hardwareproblem auf Grund der Redundanz ausgeschlossen werden.
Es dauerte zwei Tage, bis feststand wo der Fehler liegt. Die Suche nach dem Fehler gestaltete sich so schwierig, da der Fehler so selten auftrat.
Das Problem lag im BAR16. Er ist die zentrale Einheit des Systems. Bei diesem Rechner handelt es sich um einen 80486 Prozessor von Intel mit einer Taktfrequenz von 25 MHz. Der BAR16 kontrolliert den gesamten Datenfluss zwischen den Bereichsstellrechnern und den Fahrdienstleitern. Weiterhin werden mit diesem Rechner die Handlungen der FDL auf Plausibilität überprüft. Außerdem ist er für die entgültige Fahrstraßenwahl zuständig. Eine weitere Aufgabe ist der Aufbau und der Abbau des Auftragsspeichers. In diesem Speicher werden alle Stellbefehle abgelegt.
Dieser Speicher hatte eine Größe von 3,5 Kbyte. Dies war aber für die große Anzahl von Stellaufträgen zu gering.
Unter bestimmten Bedingungen kam es hier zu einem Überlauf. Dies war schon der Fall beim normalen Berufsverkehr. Weiterhin wurde festgestellt, dass die Routine, die einen Überlauf abfangen sollte falsch programmiert wurde und in einer landete Endlosschleife.
Aufgrund dieser Probleme schaltete sich der BAR16 ab und somit das gesamte Stellwerk.

## 2.7. Problemlösung

Obwohl der Stackspeicher nur um wenige Bytes übergelaufen ist, hat man den Speicher um 0,5 Kbyte auf 4,0 Kbyte erhöht. Weiterhin hat man die Routine zur Überlaufprüfung neu programmiert. Außerdem musste sich das Bedienpersonal intensiven Schulungen unterziehen, um in kritischen Situation besser reagieren zu können.

## 2.8. Fazit

Abschließend kann man sagen, dass es erforderlich gewesen wäre das System besser zu testen. Ein paralleler Probebetrieb vom alten und vom neuen Stellwerk wäre wohl durchaus sinnvoll gewesen, um im Falle eines Versagens auf das alte System zurück schalten zu

können. Dies war aber dadurch nicht möglich, das die alte und die neue Technik nicht mit einander kompatibel waren.
Weiterhin zeigt sich an diesem Beispiel, dass Hardwareredundanz alleine nicht ausreicht, wenn die Software Fehler aufweist.

Während des gesamten Stellwerksausfalls war jedoch die Sicherheit im Sinne von „keine Gefahr für Person und Güter“ niemals gefährdet.

# 3. Petri-Netze

## 3.1. Definition

Petri-Netze sind eines der ersten Konzepte, die für die Beschreibung von verteilten Systemen und Prozessen vorgeschlagen wurden. Sie dienen der graphischen Darstellung von verteilten Systemen.
Ihren Namen verdanken sie C.A. Petri, der sie in seiner Dissertation 1962 zur Beschreibung von Kommunikation in Automaten eingeführt hat.
Ein Petri-Netz ist ein gerichteter Graph, der aus zwei verschiedenen Arten von Knoten besteht. Den Transitionen (oder Hürden) und den Stellen (oder Plätzen). Die Kanten verlaufen dabei jeweils von Transitionen (T) zu Stellen (S) oder von Stellen zu Transitionen. Der Zustand eines Netzes definiert sich über die Belegung der Stellen. In einem gegebenen Zustand sind bestimmte Mengen von Transitionen schaltbereit. Durch das Schalten der Transitionen ändert sich die Belegung des Netzes.

## 3.2. Notation

Zur Beschreibung von Petri-Netzen ist es, nötig eine algebraische Notation einzuführen.

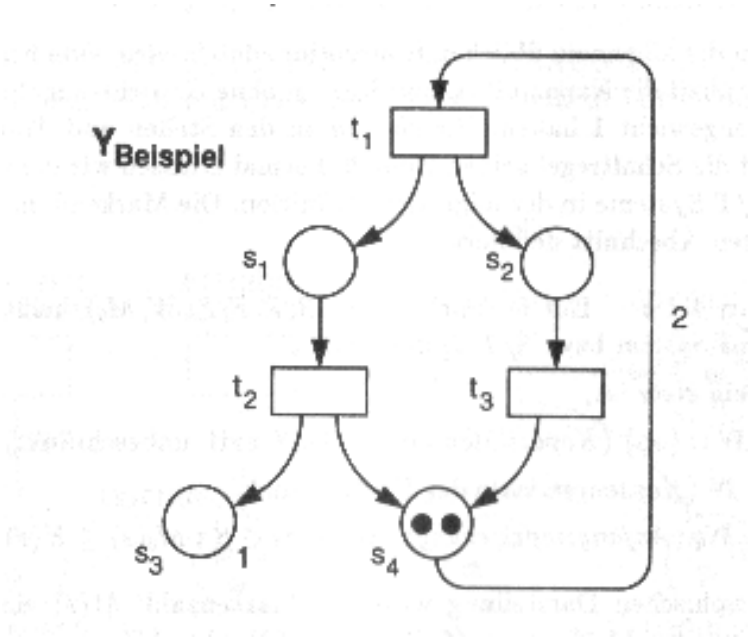
### 3.2.1. Formale Definition eines Petri-Netzes

Ein 6-Tupel $Y=(S,T,F,K,W,M_0)$ heißt Stellen-Transitions-System bzw. S/T-System falls:

- (S,T,F) ein Netz ist (d.h. die Schnittmenge der Stellen mit den Transitionen muss leer sein, und die Flussrelation F ist eine Teilmenge von $(S \times T) \cup (T \times S)$)
- $K: S \rightarrow \mathbb{N} \cup \{\infty\}$ (die *Kapazitäten* der Stellen sind evtl. beschränkt) ($\mathbb{N}$ = natürliche Zahlen)
- $W: F \rightarrow \mathbb{N}$ (*Kantengewichte* der Kanten)
- $M_0: S \rightarrow \mathbb{N}_0$ (*Anfangsmarkierungen*)

Hierbei wird davon ausgegangen, dass Stellen ohne Kapazitätsangabe immer die Kapazität $\infty$ besitzen und Kanten ohne Gewichtsangabe immer das Kantengewicht 1 haben.
Kapazitäs- bzw. Gewichtsangaben werden an die entsprechenden Stellen bzw. Kanten geschrieben.

Beispiel 1:




Diesem Beispiel liegt das Netz N=(S,T,F) zugrunde mit :

S={s1,s2,s3,s4}
T={t1,t2,t3}
F={(t1,s1),(t1,s2),(s1,t2),(s2,t3),(t2,s3),(t2,s4),(t3,s4),(s4,t1)}

Die einzelnen Tupel in F beschreiben die Kanten des Petri-Netzes.

Daraus wird ein S/T-Netz N=(S,T,F,K,W) unter Einbeziehung der Kapazitäten

K={(s1,∞),(s2,∞),(s3,1),(s4,∞)}

und der Kantengewichte oder genauer der Gewichtsabbildung

G={[(t1,s1),1],[(t1,s2),1],[(s1,t2),1],[(s2,t3),1],
[(t2,s3),1],[(t2,s4),1],[(t3,s4),1],[(s4,t1),2]}

Da N mit der Anfangsbelegung

$M_0$={(s1,0),(s2,0),(s3,0),(s4,2)}

belegt ist, erhalten wir nun das S/T-System $Y_{Beispiel}$=(S,T,F,K,W,$M_0$) bzw. (N,$M_0$).

## 3.2.2. Markierungen

Eine Abbildung M: S → $N_0$ mit ∀s ∈ S : M(s) ≤ K(s) heißt *Markierung* von N.
***M*** (N) bezeichnet die Menge aller Markierungen auf N.

Eine Transition t∈T heißt *aktiviert* unter M, geschrieben M[t⟩, wenn

∀s ∈ •t : M(s) ≥ W(s,t), *(1.)*
∀s ∈ t• : M(s) ≤ K(s) - W(t,s) *(2.)*

wobei mit •t die sogenannten Eingangsknoten bezeichnet sind und mit t• die Ausgangsknoten.

Diese Definition sagt aus, dass t nur dann schalten kann, wenn (1.) mindestens so viele Markierungen auf s vorhanden sind, wie die Wertigkeit der Kante, die t und s verbindet. Und weiterhin (2.), dass die Anzahl der Markierungen auf der Zielstelle höchstens so hoch sein darf, wie die Differenz zwischen der Kapazität der Stelle und der Wertigkeit der Kante.

Man sagt, t schaltet von M nach M' und schreibt M[t⟩M', wenn t unter M aktiviert ist und M' aus M entsteht, indem von den Eingangsstellen Marken entnommen werden und dann Marken auf die Ausgangsstellen gelegt werden. Die Anzahl der Marken, die auf die Ausgangsstellen abgelegt werden hängt von den Kantengewichten ab.

$$M'(s) = \begin{cases} M(s) - W(s,t), & \text{falls } s \in {\bullet t} \setminus t^{\bullet}, \\ M(s) + W(t,s), & \text{falls } s \in t^{\bullet} \setminus {\bullet t}, \\ M(s) - W(s,t) + W(t,s), & \text{falls } s \in t^{\bullet} \cap {\bullet t}, \\ M(s), & \text{sonst} \end{cases}$$

M' heißt unmittelbare Folgemarkierung von M unter t und wird auch als Mt geschrieben.

Beispiel:

Abbildung s.o.

In Beispiel 1 ist t1 aktiviert, denn $\bullet t1 = \{s4\}$ und mit $M_0(s4) = 2 = W(s4,t1)$ ist die Bedingung (1.) erfüllt.
Weiterhin ist $t1^{\bullet} = \{s1,s2\}$ und mit $M_0(s1) = 0 = K(s1) - W(t1,s1)$ und $M_0(s2) = 0 = K(s2) - W(t1,s2)$.
Schaltet t1, so erhalten wir als neue Markierung von N:

$M_0t1 = \{(s1,1),(s2,2),(s3,0),(s4,0)\}$

## 3.2.3. Inzidenzmatrix

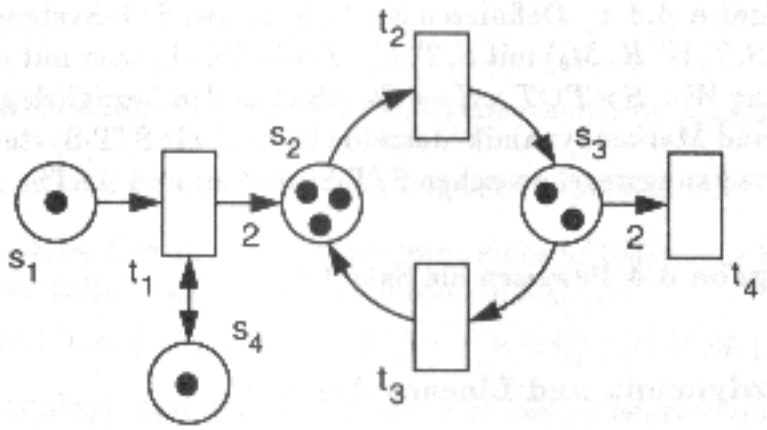
Die Inzidenzmatrix C zu einem Netz N ist definiert durch:

$$\forall\ 1 \le i \le m,\ 1 \le j \le n$$

$$C_{ij} := \begin{cases} W(t_j,s_i) & \text{wenn } (t_j,s_i) \in F \setminus F^{-1} \\ -W(s_i,t_j) & \text{wenn } (s_i,t_j) \in F \setminus F^{-1} \\ W(t_j,s_i) - W(s_i,t_j) & \text{wenn } (t_j,s_i) \in F \cap F^{-1} \\ 0 & \text{sonst} \end{cases}$$

$C_{ij}$ zeigt jeweils an, wie sich die Anzahl der Markenzahl von $s_i$ ändert, wenn $t_j$ schaltet.

Beispiel 2:




Die Inzidenzmatrix des Netzes lautet:

$$C = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 2 & -1 & 1 & 0 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

An diesem Beispiel kann man sehr gut erkennen, wie die Inzidenzmatrix aufgebaut ist.
In der ersten Zeile sieht man die Einträge für s1, in der zweiten für s2 usw.

Mit Hilfe dieser Matrix kann man schlingenfreie Petri-Netze eindeutig beschreiben, da über die Einträge in der Matrix der Aufbau des Petri-Netzes genau beschrieben wird. Dies gilt nur für schlingenfreie Netze, da Schlingen in der Matrix nur als Differenz ihrer Kantengewichte auftauchen. Bei Gleichheit also mit 0. Damit kann in diesem Fall das Netz nicht eindeutig aus der Matrix hergeleitet werden.
So auch im obigen Beispiel, da es sich bei der Stelle s4 um eine Schlinge handelt. Ein Netz hat eine Schlinge, wenn es eine Stelle besitzt, die eine Transition hat, die sowohl Eingangs- als auch Ausknoten ist.

Da $C_{i\,j}$ angibt, um wieviel sich die Markenzahl von $s_i$ bei einer Schaltung von $t_j$ ändert, entspricht $C_{\bullet j}$, also die j-te Spalte der Inzidenzmatrix, gerade der Veränderung der Markierung bei Schaltung von $t_j$:

$$M[t_j\rangle M' \Rightarrow M' = M + C_{\bullet j} \qquad \textit{(A)}$$

Angewandt auf unser Beispiel, für den Fall, dass t2 schaltet:

$$\begin{pmatrix} 1 \\ 2 \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \\ 2 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}$$

### 3.2.4. Häufigkeitsvektor

Jeder Schaltfolge w kann ein Häufigkeitsvektor h zugeordnet werden. Dieser gibt die Anzahl der Vorkommen der $t_j$ in w an.

Beispiel: im Fall n=4

$$w= t_1\ t_2\ t_1\ t_4\ t_1 \quad \Rightarrow \quad h= \begin{pmatrix} 3 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

w gibt an, in welcher Reihenfolge die $t_j$ geschalten werden. In h wird angegeben, wie oft die jeweiligen Transitionen geschaltet haben.

Wenn man nun einen Häufigkeitsvektor für eine Transition $t_j$ erzeugt, erhält man einen Vektor n, der bis auf die j-te Stelle aus Nullen besteht. An der j-ten Stelle steht eine 1.
Wenn man die Inzidenzmatrix C mit dem Vektor n multipliziert erhält man die j-te Spalte der Matrix, also:

$$C\ n = C_{\bullet j}$$

Durch die Mehrfachanwendung der Gleichung ***(A)*** erhält man den grundlegenden linearen Zusammenhang zwischen einer Markierung und ihren Folgemarkierungen:

Wenn w eine Schaltfolge eines S/T-Systems (N, $M_0$) ist, gilt:

$$M_0[w\rangle \Rightarrow M_0w = M_0 + C\ h \qquad \textbf{(B)}$$

Dies läßt sich durch Induktion über die Länge von w beweisen.

Für |w|=0 ist $M_0w = M_0 = M_0 + C\ h$, da h=0 (Nullvektor)
Sei nun w'=$wt_j$ , $M_0\ [wt\rangle$, und die obige lineare Gleichung ***(B)*** gelte für w, dann ist

$$\begin{aligned} M_0w' &= M_0w + C_{\bullet j} = M_0 + C\ h + C\ n \\ &= M_0 + C\ (h + n) = M_0 + C(hn) \\ &= M_0 + C\ h' \end{aligned}$$

Unter *hn* ist hier der Häufigkeitsvektor von $wt_j$ zu verstehen.

## 3.3. Lebendigkeit

Man unterscheidet zwei Arten von Lebendigkeit. Zum einen schwache Lebendigkeit und zum anderen starke Lebendigkeit.

Ein Netz heißt schwach lebendig oder verklemmungsfrei, wenn es unter keiner Folgemarkierung tot ist.
Formal ausgedrückt: $\forall M_1 \in [M_0\rangle : \exists t \in T : M_1[t\rangle$

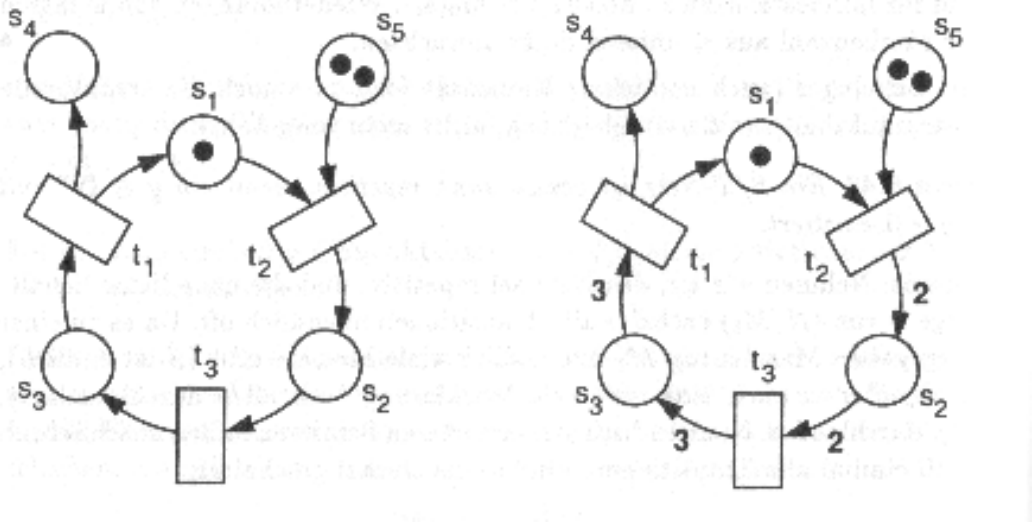
Ein Netz heißt tot, wenn alle seine Transitionen nicht schaltbereit sind.
Formal: $\forall t \in T : \neg M_0[t\rangle$

Ein Netz heißt stark lebendig, wenn alle Transitionen lebendig sind, d.h. schalten können.
Formal: $\forall t \in T, M_1 \in [M_0\rangle : \exists M_2 \in [M_1\rangle : M_2[t\rangle$

# 3.4. Lineare Invarianten

Lineare Invarianten sind einer der wichtigsten Begriffe der linear-algebraischen Netzanalyse. Mit den linearen Invarianten werden spezifische dynamisch definierte Netzeigenschaften charakterisierbar und berechenbar.

Beispiel 3:




Kommen wir zuerst zu einem w-konservativen Beispielsystem, bei dem also die Gesamtmarkenzahl auf gewissen Stellenmengen unter geeigneter Gewichtung konstant bleibt. Bei einfach gewichteten Kanten tragen die Stellen von Zyklen immer die gleiche Gesamtmarkenzahl. So z.B. {s1,s2,s3} im obigen Beispiel links.

Wenn man eine geeignete größere Kantengewichtung vornimmt, bleibt im Zyklus ein mit entsprechender Stellengewichtung ermitteltes Gesamtmarkengewicht konstant.
So z.B. $6M(s1) + 3M(s2) + 2M(s3) = 6$ für das obige Beispiel rechts.

Solche Eigenschaften lassen sich sehr leicht mit Hilfe von Invarianten zeigen.

**Definition S-Invariante:**
Sei N ein S/T-Netz mit der Inzidenzmatrix C. Eine S-Invariante von N ist ein m-Tupel $x \in Z^m$ mit $C^T x=0$

Ein m-Tupel x ist genau dann eine S-Invariante eines S/T-Netzes N, wenn für beliebige Anfangsmarkierungen $M \in \boldsymbol{M}(N)$ gilt:

$$\forall M' \in [M\rangle : M' * x = M * x$$

Beweis: Es gelte M[w⟩M'. Dann folgt

$$(M'-M) * x = x^T(M' - M)$$
$$= x^T C h \quad \text{(wegen } \mathbf{(B)} \text{)}$$
$$= (C^T x)^T h$$
$$= 0 \quad \text{(Definition der S-Invarianten)}$$

Beispiel: Abbildung s.o. das Netz hat folgende Inzidenzmatrix

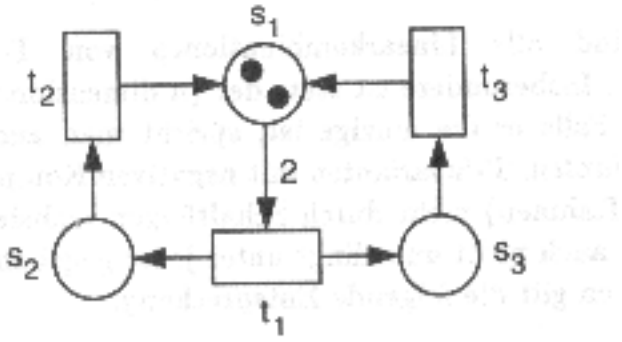
$$C = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 2 & -2 \\ -3 & 0 & 3 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix} \quad \text{und} \quad x = \begin{pmatrix} 6 \\ 3 \\ 2 \\ 0 \\ 0 \end{pmatrix}$$

ist eine Lösung des homogenen Gleichungssystems $C^T x = 0$. Somit kann man sehen, dass die konstant gewichtete Markensumme nicht zufällig ist.

Man kann somit einfach nachprüfen, ob ein m-Vektor eine S-Invariante ist. Die Bestimmung einer S-Invarianten ist aber wesentlich schwieriger.

S-Invarianten sind an der Gewichtung von Stellen und der Erzeugung eines invarianten Gesamtgewichts von Markierungen orientiert. Eine andere Art der linearen Invarianten bezieht sich mehr auf die Gewichtung von Transitionen und die Erzeugung von markierungs-wiederholenden Schaltfolgen.

Beispiel 3:




Die Inzidenzmatrix dieses Netzes lautet

$$C = \begin{pmatrix} -2 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix}$$

Die Markierung $M_0$, die im Netz eingezeichnet ist, wiederholt sich nach der Schaltung von t1, t2 und t3:

$$M_0 [t1t2t3\rangle M_0$$

Dies lässt sich darstellen durch

$$M_0 + C \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = M_0$$

Der Häufigkeitsvektor h der Schaltfolge t1, t2, t3 ist also eine Lösung des homogenen linearen Gleichungssystems Ch=0.

**Definition T-Invariante:**

Sei C die Inzidenzmatrix des S/T-Netzes N. Ein n-Tupel $y \in Z^n$, das das Gleichungssystem Cy=0 löst, heißt T-Invariante von N.

Ein $y \in \boldsymbol{N}^m{}_0$ ist genau dann eine T-Invariante eines S/T-Netzes n mit $K=\infty$, wenn es eine Markierung $M \in \boldsymbol{M}(N)$ gibt, die durch eine Schaltfolge mit Häufigkeitsvektor y reproduziert wird.

Mit Hilfe der Invarianten kann man nun nachweisen, ob ein Netz lebendig ist.
Dies kann man an den obigen Beispielen erkennen. Im Beispiel 3 ist der Vektor x die Invariante. Da die Anzahl der Markierungen konstant gehalten wird, ist immer mindestens eine der Transitionen schaltbereit. Somit ist das Netz schwach lebendig.
In Beispiel 4 ist der Häufigkeitsvektor h die Invariante. Da man nach schalten aller drei Tansitionen wieder zur Anfangsbelegung zurückkehrt, ist das Netz ebenfalls lebendig.

# 4. Quellenangabe

1. Baumgarten, Bern
Petri-Netze: Grundlagen und Anwendungen
BI Wissenschaftsverlag, 1990

2. c't vom Mai 1995, Artikel „Alle Räder stehen still",
Verfasser: Frank Möcke

3. Giese, Ingolf
„Warum explodierten Mariner 1, Ariane 5, ... oder: Was kümmern mich die Probleme der Datenverarbeitung? Softwarezuverlässigkeit gestern, heute und morgen"
http://www-aix.gsi.de/~giese/swr/fehler21.html

4. „The Risks Digest"
http://catless.ncl.ac.uk/Risks/17.02.html

5. Huckle, Thomas
„Kleine BUGs, große GAUs, Softwarefehler und ihre Folgen"
http://wwwzenger.informatik.tu-muenchen.de/persons/huckle/bugs.html

6.http://www.siemens.com/index.jsp?sdc_p=l0o23008t4u18mcn23008sfp&sdc_sid=32050174714&

7. http://www.google.de/search?q=cache:u8iH85jGqI4C:rcswww.urz.tu-dresden.de/~umaschek/estw/ESTW.pdf+simis-3216&hl=de&ie=UTF-8
bzw.
http://rcswww.urz.tu-dresden.de/~umaschek/estw/ESTW.pdf

8. „Sichere (PC-)Technik für die Deutsche Bahn? – Teil 1"
http://userpage.fu-berlin.de/~dittbern/Archiv/PC_and_Railways.html

9. Mehl, Walter
„Deutsche Bahn erwägt, Schadensersatz zu fordern, Siemens-Rechner legt Stellwerk in Hamburg für zwei Tage lahm"
Computerwoche Nr. 12 vom 24.03.1995, Seite 27
http://www.computerwoche.de/heftarchiv/1995/19950324/a16000.html