Überwachung des Kontroll- und Datenflusses bei der Programmausführung

Echtzeit 2017

16. - 17.11.2017 in Boppard

Stefan Widmann

Aufbau des Vortrags

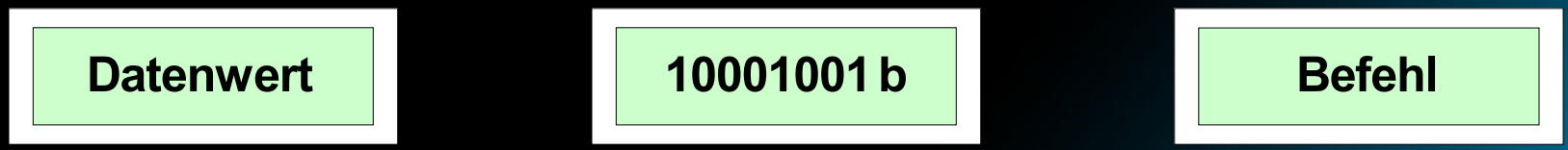
- Problemstellung mit Beispiel aus Praxis
- Stand von Wissenschaft und Technik
- Kontrollflussüberwachung (Gollub)
- Datenflussüberwachung (Widmann)

Problemstellung (1)

- Steigende Verantwortung von Systemen
- Steigende Komplexität
- Sinkende Strukturbreite von ICs
- Folge: höhere Fehlerwahrscheinlichkeit
  - Kontrollflussfehler
  - Datenflussfehler
- ggf. gefährliche Ausgaben

Problemstellung (2)

- Heutiger Ansatz:
  Fehlererkennung durch immer komplexere SW
- Daten- und Befehlsabbildung nur durch Datenwert bzw. Instruktion



- nur implizite Annahme von Eigenschaften durch Art des Zugriffs

Beispiel aus “Praxis”: Therac-25

- Medizinisches Bestrahlungsgerät (1983 - 1987)
- Vorgänger Therac-20 mit HW-Sicherheits-einrichtungen → bei Therac-25 unnötig, da SW
- Unzureichende Synchronisation
  → Parametervermischung (alt + neu)
  → teils massive Verstrahlung
- 6 (bekannte) schwere Unfälle, teils mit Todesfolge

Stand der Technik (1): Konventionelle Architekturen

- x86 und ARM millionenfach im Einsatz
- Wenige Fehlererkennungsmerkmale
- Maximaler Datendurchsatz ist Ziel
- Hochkomplexe Merkmale wie
  - Verdecktspeicher (Caches)
  - Tomasulo-Algorithmus

Stand der Technik (2): Datentyp-, -struktur- und Befähigungsarchitekturen

- 60er bis 80er Jahre,
  z.B. AEG TR4, Intel iAPX 432
- Datenwert mit Datentyp DT, Zugriffsrechten ZR, Integritätsprüfung IP

- Entsprechende Fehler durch HW erkennbar

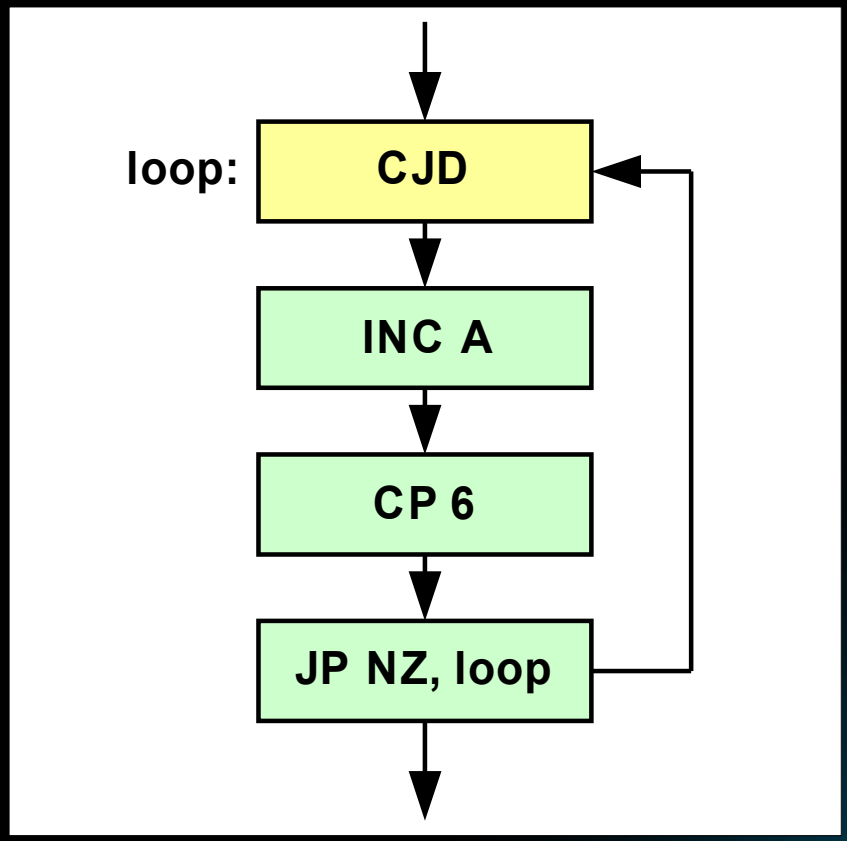
Kontrollflussüberwachung: Kontrollflussfehler und -anomalien

- Kontrollflussfehler:
  Abweichung von vorgesehenen Pfaden
- Kontrollflussanomalie:
  Pfade korrekt, aber Pfadauswahl nicht

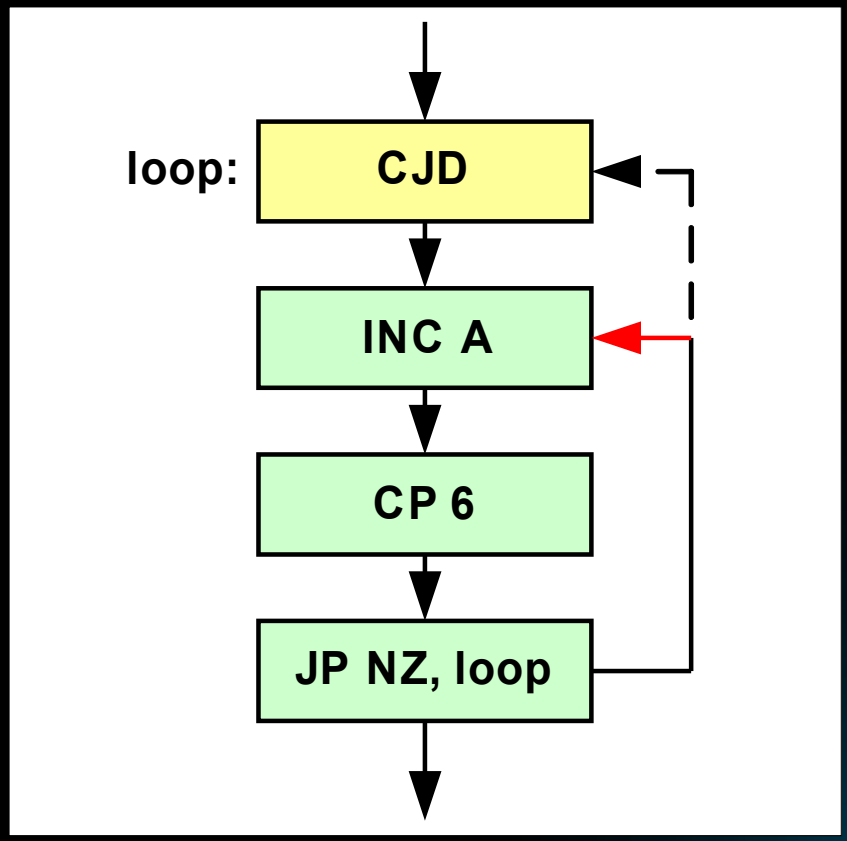
Kontrollflussüberwachung (1): Ansprungbefehle

- Sprungziele werden im Code identifiziert
- Ansprungbefehl am Ziel identifiziert Art des Ziels
- 10 verschiedene Zielarten
- Erlaubt HW die einfache Erkennung von fehlerhaften Sprüngen

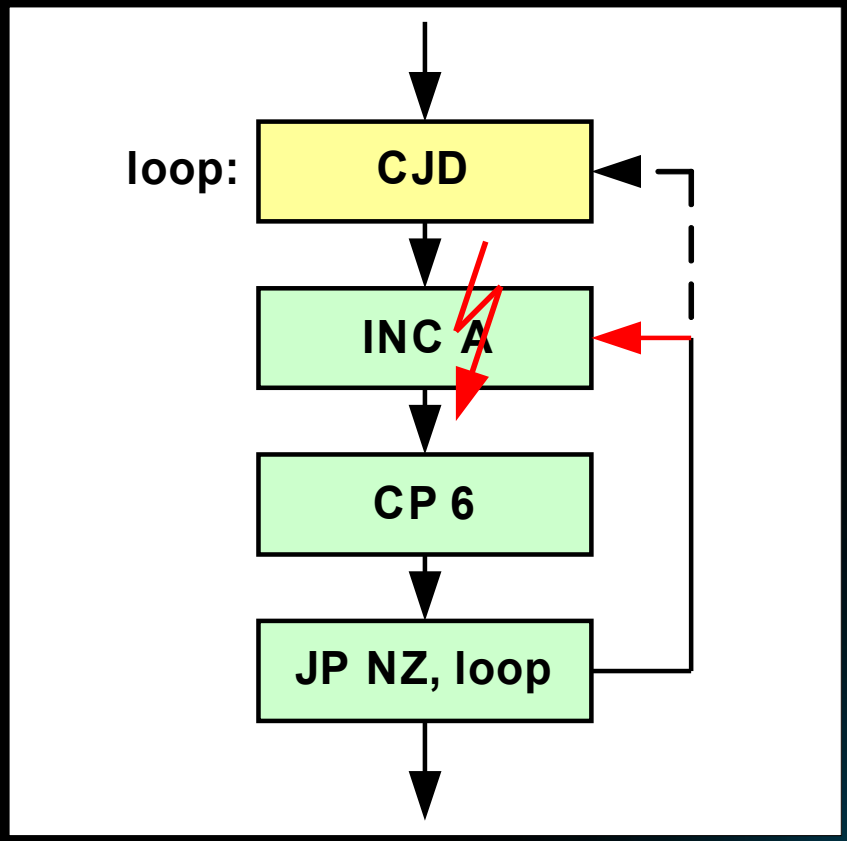
Kontrollflussüberwachung (1): Ansprungbefehle – Beispiel



Kontrollflussüberwachung (1): Ansprungbefehle – Beispiel



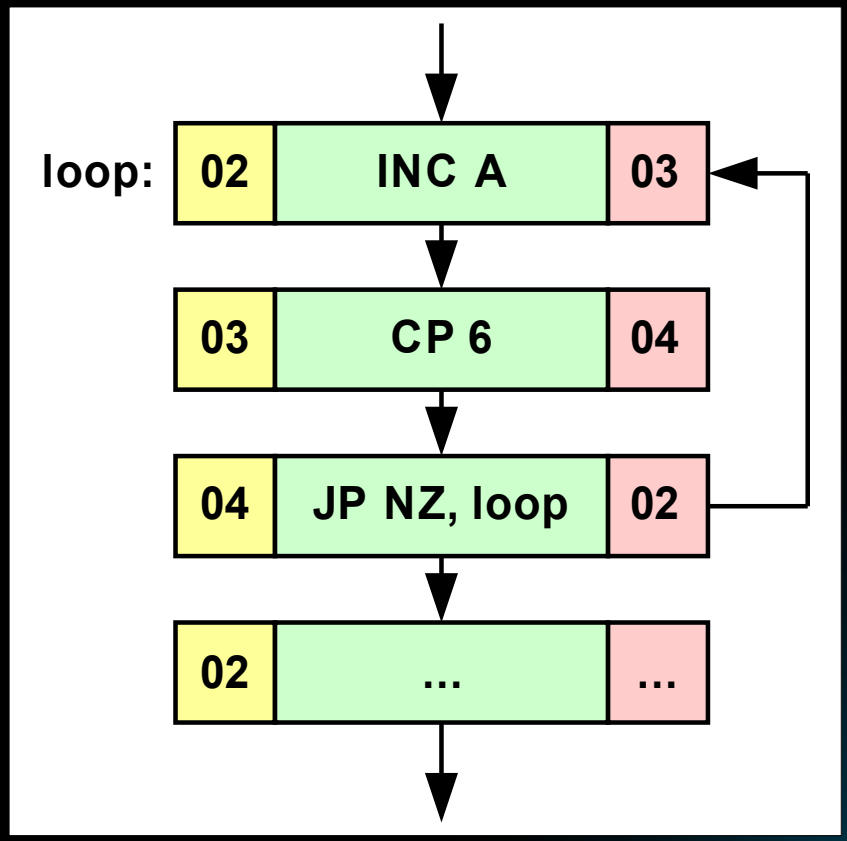
Kontrollflussüberwachung (1): Ansprungbefehle – Beispiel



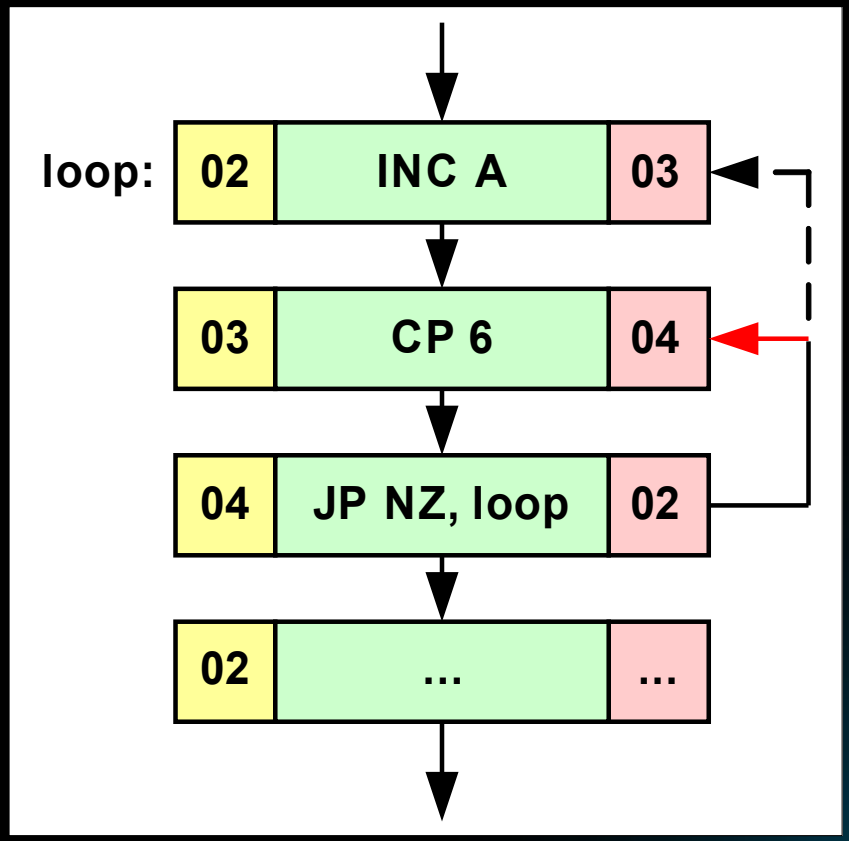
Kontrollflussüberwachung (2): Befehlsverkettung

- Befehle erhalten Eigen- und Folgekennungen
- Eigenkennung Befehl = Folgekennung Vorgänger
- Erlaubt HW die einfache Erkennung von Sequenzfehlern bei Befehlsausführung

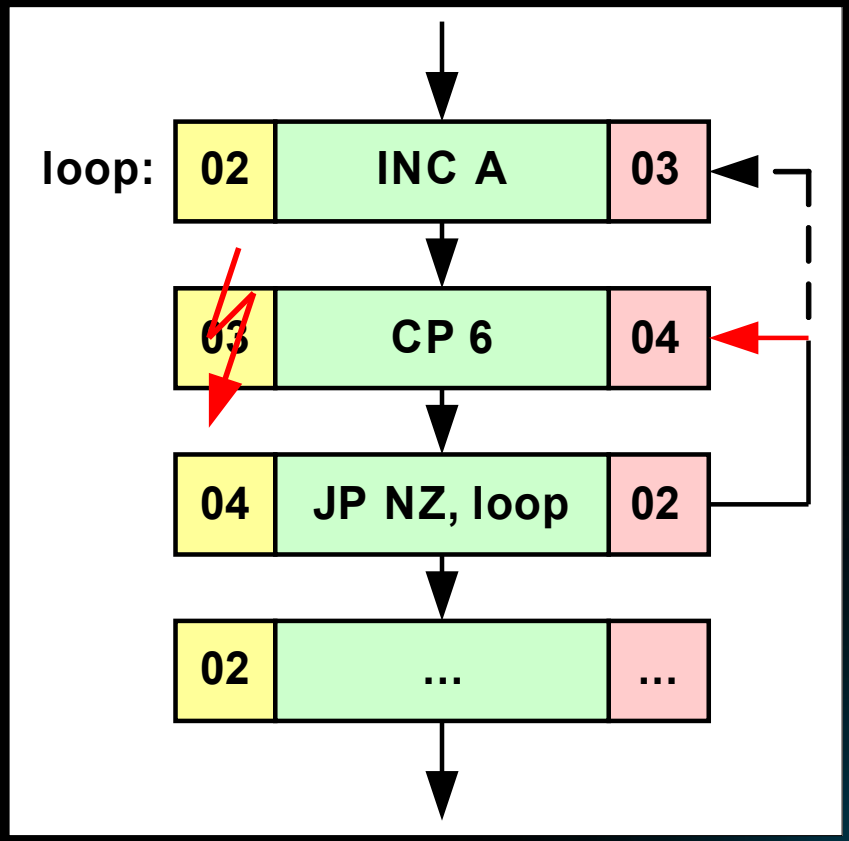
Kontrollflussüberwachung (2): Befehlsverkettung – Beispiel



Kontrollflussüberwachung (2): Befehlsverkettung – Beispiel



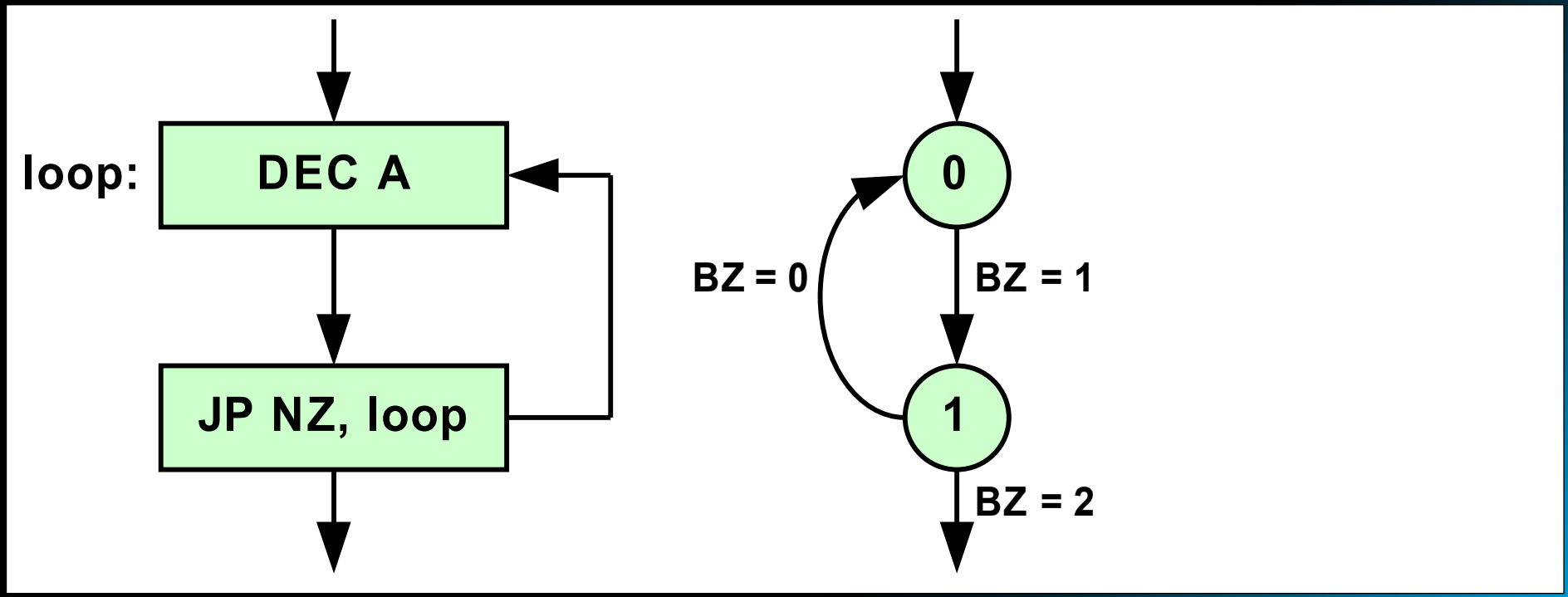
Kontrollflussüberwachung (2): Befehlsverkettung – Beispiel



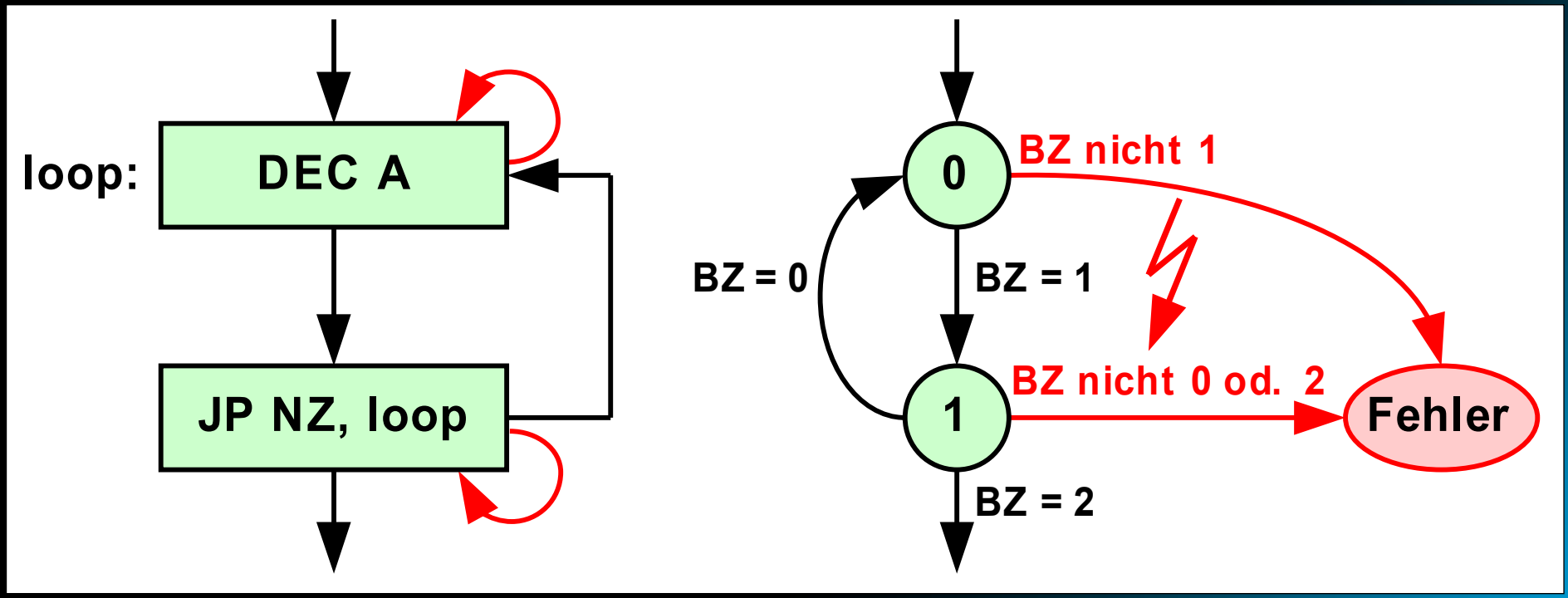
Kontrollflussüberwachung (3): Befehlszählerüberwachung

- Abbildung der Programmstruktur in endlichem Automaten
- Prozessor führt Programm aus, prüft Transitionen des Befehlszählers anhand Automat
- Leistungsfähigste Variante: Einbeziehung von Prozessgrößen in Automat
- HW kann Kontrollflussfehler und -anomalien aufdecken

Kontrollflussüberwachung (3): Befehlszählerüberwachung – Beispiel



Kontrollflussüberwachung (3): Befehlszählerüberwachung – Beispiel



Datenflussüberwachung: Identifizierte Fehler- und Angriffsarten

Identifiziert wurden:

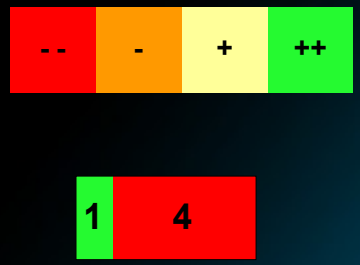
- 18 datenflussbezogene Fehlerarten
- 2 datenflussbezogene Angriffsarten

Fehlerkategorie	Anzahl
Inkompatibilität von Operanden	2
Wertebereichs- und Genauigkeitsprobleme	2
Fehlerhafte Operationen	3
Verletzung von Echtzeitbedingungen	3
Allgemeine Datenflussfehler	5
Datenverfälschung durch Störungen	1
Fehlerhafter Datenzugriff	2

Angriffe	Anzahl
Hackerangriffe	2

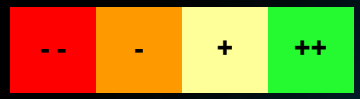
Datenflussüberwachung: Bewertung des Stands der Technik

Fehlerkategorie	Anzahl	x86 / ARM	DT, DS, BA
Inkompatibilität von Operanden	2		
Wertebereichs- und Genauigkeitsprobleme	2		
Fehlerhafte Operationen	3		
Verletzung von Echtzeitbedingungen	3		
Allgemeine Datenflussfehler	5		
Datenverfälschung durch Störungen	1		
Fehlerhafter Datenzugriff	2		
Angriffe	**Anzahl**		
Hackerangriffe	2		



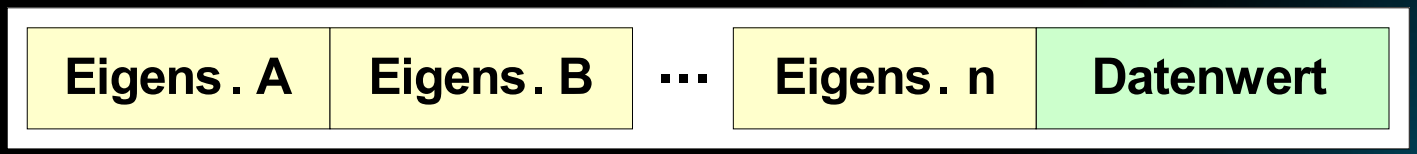
Datenflussüberwachung: Bewertung des Stands der Technik

Fehlerkategorie	Anzahl	x86 / ARM	DT, DS, BA
Inkompatibilität von Operanden	2		
Wertebereichs- und Genauigkeitsprobleme	2		
Fehlerhafte Operationen	3		
Verletzung von Echtzeitbedingungen	3		
Allgemeine Datenflussfehler	5		
Datenverfälschung durch Störungen	1		
Fehlerhafter Datenzugriff	2		
Angriffe	**Anzahl**		
Hackerangriffe	2		
		16 3 1 0	14 2 0 4



Datenflussüberwachung: Eine Datenspezifikationsarchitektur

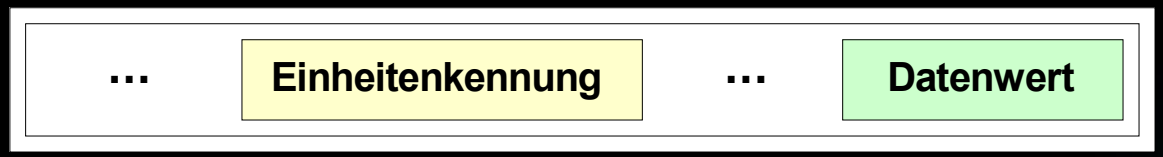
- Eine neue Architekturart: Datenspezifikationsarchitektur DSA
- Umfassende, HW-lesbare Beschreibung von Dateneigenschaften in 8 neuen Kennungen



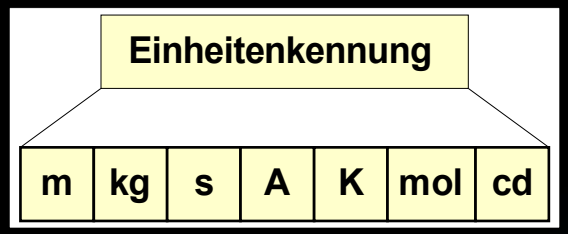
- Kennungen werden übertragen, gespeichert und verarbeitet mit Datenwert
  → einfache Fehlererkennung durch HW

Datenflussüberwachung (1): Einheitenkennung

- Physikalische Einheit in Einheitenkennung



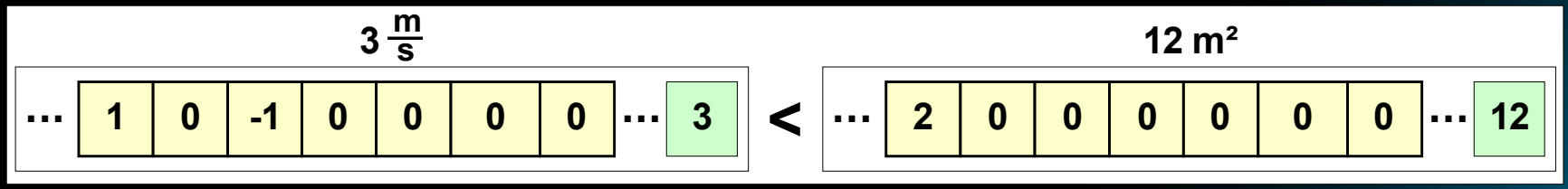
- Enthält Potenzen der sieben SI-Basiseinheiten



- HW kann “Vergleich von Äpfeln mit Birnen” erkennen

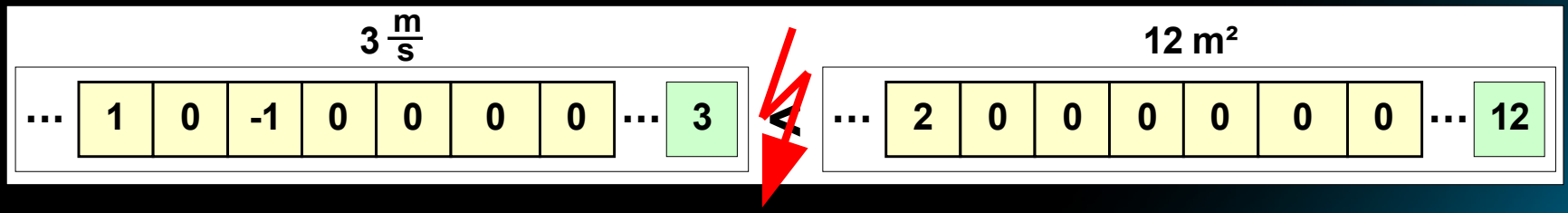
Datenflussüberwachung (1): Einheitenkennung – Beispiel

- Vergleiche, Subtraktionen, Additionen: HW prüft Gleichheit der Einheiten



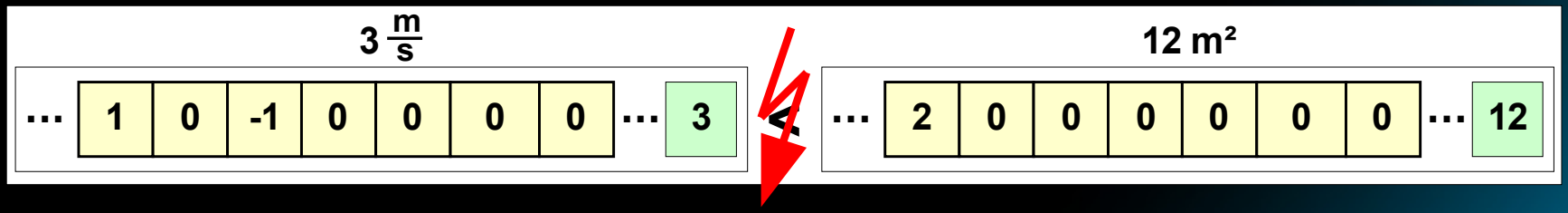
Datenflussüberwachung (1): Einheitenkennung – Beispiel

- Vergleiche, Subtraktionen, Additionen: HW prüft Gleichheit der Einheiten

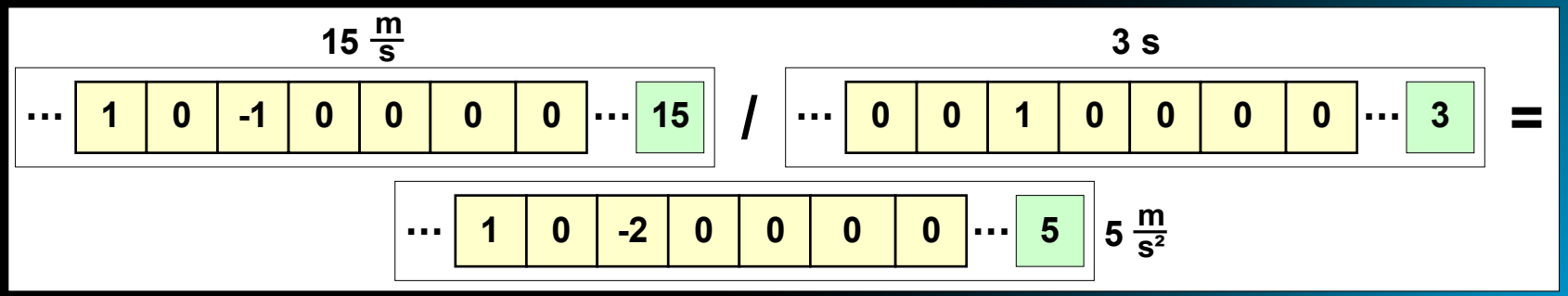


Datenflussüberwachung (1): Einheitenkennung – Beispiel

- Vergleiche, Subtraktionen, Additionen:
  HW prüft Gleichheit der Einheiten

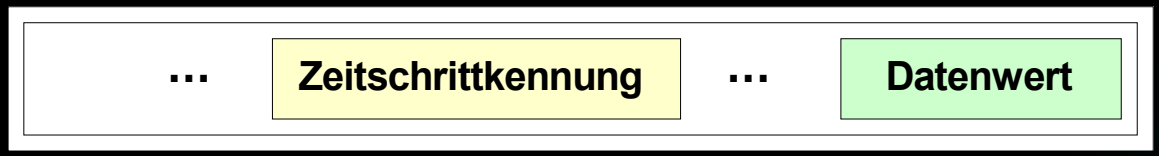


- Multiplikationen, Divisionen:
  HW berechnet Einheiten des Ergebnisses



Datenflussüberwachung (2): Zeitschrittkennung

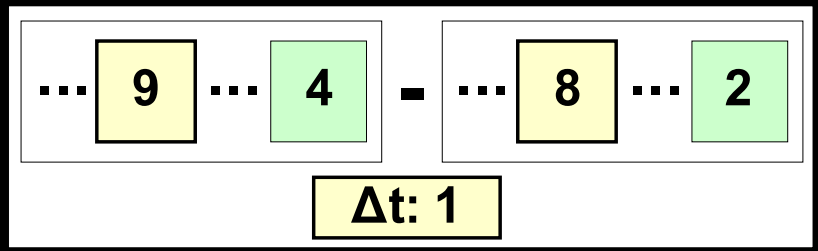
- Diskreter Zeitschritt in Zeitschrittkennung



- Temporale Beziehung von Operanden wird in Befehl kodiert und durch HW geprüft
- HW kann Duplikate von Datenwerten, verlorengegangene Aktualisierungen und Synchronisationsfehler erkennen

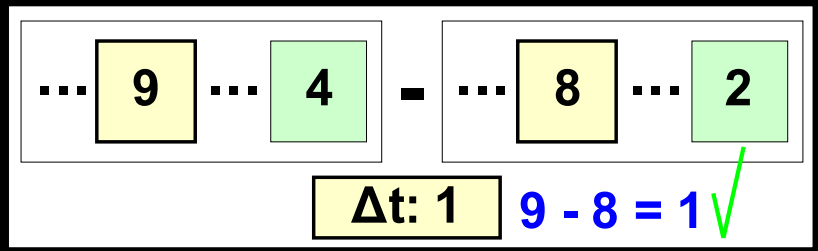
Datenflussüberwachung (2): Zeitschrittkennung – Beispiel

- Aktueller Wert minus Vorgängerwert, HW prüft temporale Beziehung



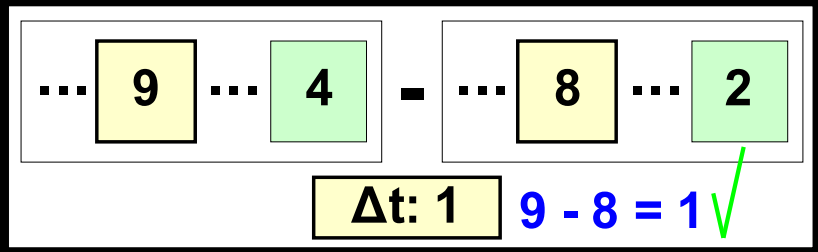
Datenflussüberwachung (2): Zeitschrittkennung – Beispiel

- Aktueller Wert minus Vorgängerwert, HW prüft temporale Beziehung

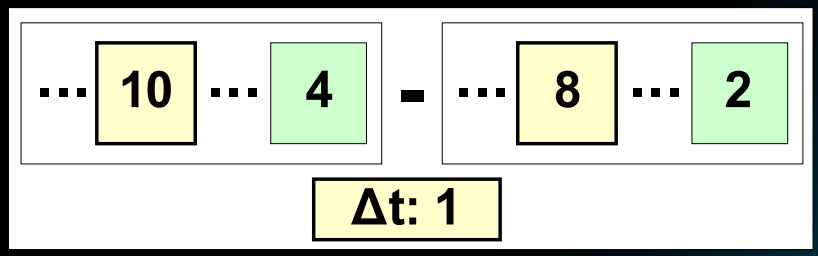


Datenflussüberwachung (2): Zeitschrittkennung – Beispiel

- Aktueller Wert minus Vorgängerwert, HW prüft temporale Beziehung

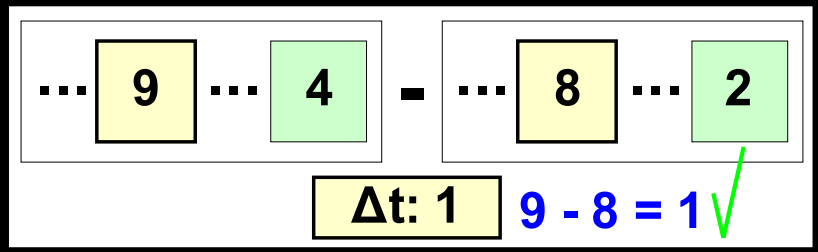


- Durch Fehler geht ein Wert verloren

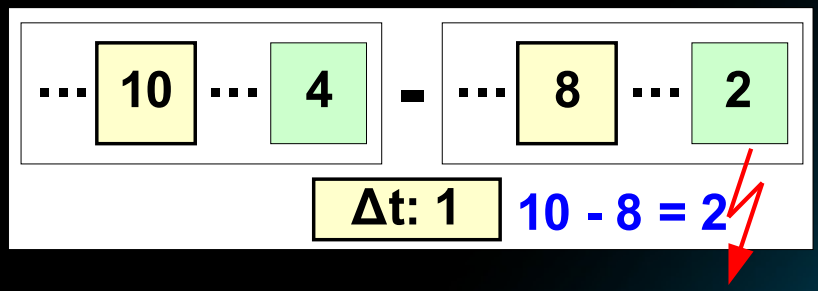


Datenflussüberwachung (2): Zeitschrittkennung – Beispiel

- Aktueller Wert minus Vorgängerwert, HW prüft temporale Beziehung

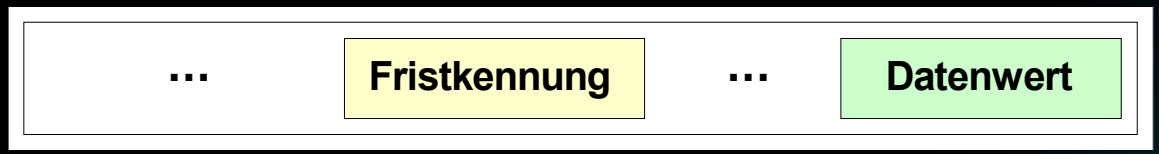


- Durch Fehler geht ein Wert verloren



Datenflussüberwachung (3): Fristkennung

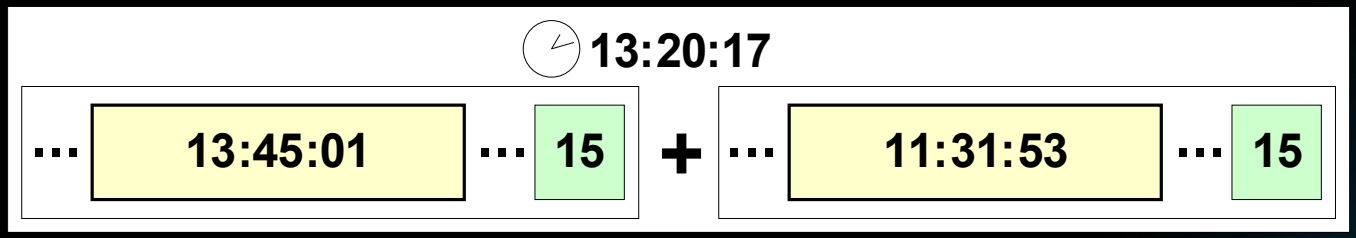
- In Echtzeitsystemen muss Verarbeitung von Daten bis zu bestimmtem Zeitpunkt erfolgt sein
- Frist in Fristkennung = Gültigkeitszeitraum



- Festlegung spezifisch für jeden Datenwert möglich
- HW prüft, ob Operanden noch gültig sind
  → kann Verletzungen von Echtzeitbedingungen sofort erkennen

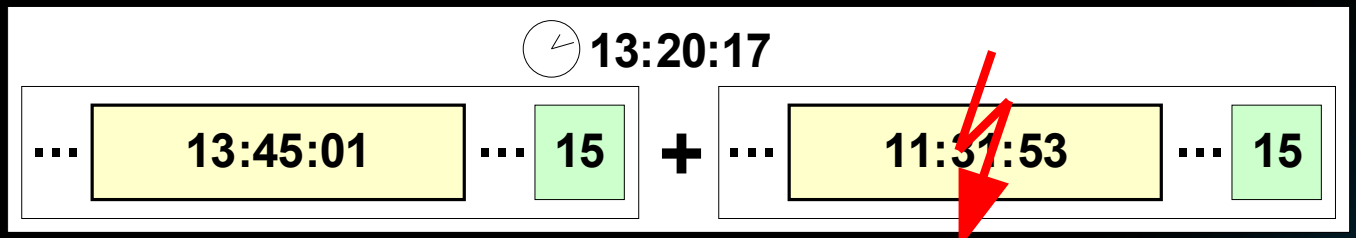
Datenflussüberwachung (3): Fristkennung – Beispiel

- Prüfung der Fristen der Operanden durch HW



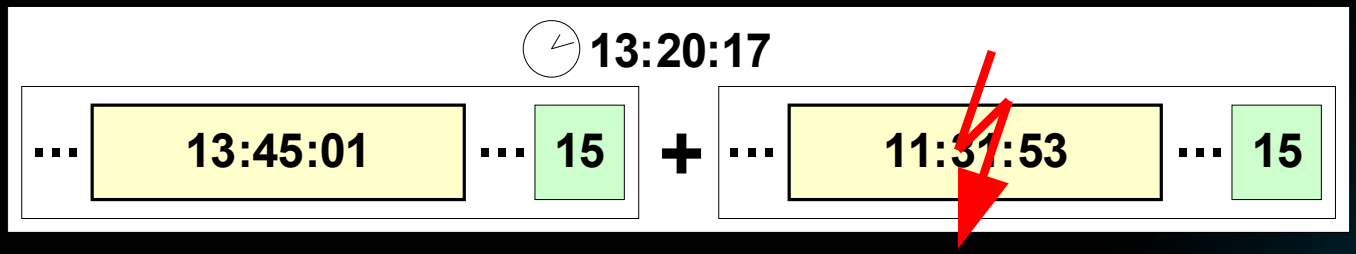
Datenflussüberwachung (3): Fristkennung – Beispiel

- Prüfung der Fristen der Operanden durch HW

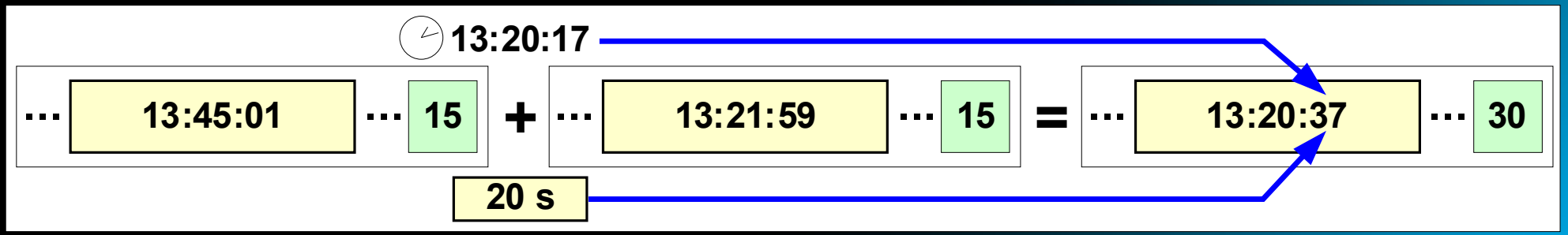


Datenflussüberwachung (3): Fristkennung – Beispiel

- Prüfung der Fristen der Operanden durch HW



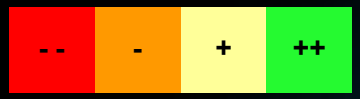
- Frist des Ergebnisses = kürzere Frist der Operanden oder neue relative Frist im Befehl kodiert



Datenflussüberwachung (Ergebnisse 1): Aufbau eines Datenelements

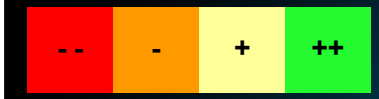
Datenflussüberwachung (Ergebnisse 2): Bewertung anhand Fehlererkennung

Fehlerkategorie	Anzahl	x86 / ARM	DT, DS, BA
Inkompatibilität von Operanden	2	--	+, --
Wertebereichs- und Genauigkeitsprobleme	2	-, --	--
Fehlerhafte Operationen	3	--	--
Verletzung von Echtzeitbedingungen	3	--	--
Allgemeine Datenflussfehler	5	+, --	+, -, --
Datenverfälschung durch Störungen	1	-	+
Fehlerhafter Datenzugriff	2	-, -	+, -
Angriffe	**Anzahl**		
Hackerangriffe	2	--	--
		16 3 1 0	14 2 0 4



Datenflussüberwachung (Ergebnisse 2): Bewertung anhand Fehlererkennung

Fehlerkategorie	Anzahl	x86 / ARM	DT, DS, BA	DSA
Inkompatibilität von Operanden	2			
Wertebereichs- und Genauigkeitsprobleme	2			
Fehlerhafte Operationen	3			
Verletzung von Echtzeitbedingungen	3			
Allgemeine Datenflussfehler	5			
Datenverfälschung durch Störungen	1			
Fehlerhafter Datenzugriff	2			
Angriffe	**Anzahl**			
Hackerangriffe	2			
		16 3 1 0	14 2 0 4	0 0 0 20



Datenflussüberwachung (Ergebnisse 3): Bewertung am Beispiel Therac-25

- Vermischung alter und neuer Parameter hätte durch eine DSA erkannt werden können:
  - Begrenzung der zeitlichen Gültigkeit der Parameter auf eine Behandlungssitzung
    → Fristkennung
  - Parameter müssen denselben Zeitschritt = Sitzungsnummer aufweisen
    → Zeitschrittkennung
- Programmabbruch als Folge, daher kein Unfall

Zusatzfolie: Speicherausnutzung der DSA

Bitbreite Datenwert	Speicherausnutzung Integritätsprüfungskennung (640 Bit)	Speicherausnutzung Signaturkennung (1664 Bit)
128 Bit	20,00 %	7,69 %
. . .	. . .	. . .
32 Bit	5,00 %	1,92 %
. . .	. . .	. . .
1 Bit	0,16 %	0,06 %