Vergleich DCCA mit FTA und FMEA

FTA

Minimal Cut Sets der FTA

```
{
    Zugbremsen versagen,
    Lichtsignalanlage defekt,
    Schranken defekt,
    BÜ-Sender defekt,
    Sicherheitszuschlag zu gering x {
        -- Punkte falsch berechnet
        Positionsbestimmung falsch durch defekten Hodometer,
        Zuggeschwindigkeit falsch gemessen durch Hodometer,
        Verwendete Zwangsbremsverzögerung zu gering,
        Fehler im Zentralregister
    }
} x {
    Lichtsignalanlage defekt,
    Schranken defekt,
    Zug braucht zu lange um BÜ zu erreichen,
    SP-Sensor meldet fälschlicherweise Zug-Durchfahrt,
    Zugsender defekt,
    BÜ-Empfänger defekt,
    Funksignal wird gestört,
    -- Punkte falsch berechnet
    Fehler im Zentralregister,
    Positionsbestimmung falsch durch defekten Hodometer,
    Zuggeschwindigkeit falsch gemessen durch defekten Hodometer,
    Schließzeit zu gering festgelegt,
    Sicherheitszuschlag zu gering für Fehlerausgleich,
    Kommunikationsverzögerung zu gering bestimmt,
    Verwendete Zwangsbremsverzögerung zu gering
}
```

Vergleich mit DCCA

- Sicherheitszuschlag, Kommunikationsverzögerung sind bei den Programmgraphen immer richtig gewählt für den fehlerfreien Fall -> gibt es in der DCCA nicht, in der FTA sinnvollerweise aber schon
- Lichtsignalanlage, Funkkanal und Zentralregister gibt es in der DCCA nicht mehr
- "Schranken defekt" ist in der FTA eine einelementige kritische Fehlermenge, das entspricht der Schrankensensor_Stoerung in der DCCA
- Die falsch berechneten Punkte sind beim FTA einelementige kritische Fehlermengen, analog zur DCCA
- Sensor_Stoerung ist in der DCCA eine einelementige kritische Fehlermenge; in der FTA haben wir nicht bedacht, dass das alleine schon zur Gefährdung führen kann (Bsp.: Zug fordert Sicherung an, BÜ sichert sich, BÜ sagt Zug, dass er gesichert ist, Sensor sagt Zug ist vorbei, BÜ öffnet sich wieder - Zug denkt aber, BÜ ist gesichert, Zug fährt über ungesicherten BÜ)
- Zugmotor_Ausfall ist in der DCCA eine einelementige kritische Fehlermenge, bei der FTA haben wir nicht bedacht, dass das aufgrund des timeouts alleine schon zur Gefährdung führen kann (Bsp.: Zug fordert Sicherung an, BÜ sichert sich, BÜ sagt Zug, dass er gesichert ist, Zugmotor fällt zeitweise aus, BÜ erhält timeout und entsichert, Zugmotor springt wieder an, Zug fährt über ungesicherten BÜ)
- {Funksignal wird gestört, Schranken defekt} in der FTA entspricht {BahnuebergangFunksender_Stoerung, Schrankenmotor_Ausfall} in der DCCA
- {BÜ-Sender defekt, Zugsender defekt} in der FTA entspricht

{BahnuebergangFunksender_Stoerung, ZugFunksender_Ausfall} in der DCCA

- {Zugbremsen versagen, Schranken defekt} in der FTA entspricht {Zugbremse_Ausfall, Schrankenmotor_Ausfall} in der DCCA
- {Zugbremsen versagen, Zugsender defekt} in der FTA entspricht {Zugbremse_Ausfall, ZugFunksender_Ausfall} in der DCCA

Generell ist beim FTA die Schwierigkeit, dass man über den Top-Down Ansatz zunächst zu abstrakt denkt und dabei vergisst, dass kleinere Fehlermengen schon zur Gefährdung führen können. Dies ließe sich beheben, indem man bei den letztendlichen minimal cut sets nochmal prüft, ob sie wirklich minimal sind.

Auch sind die Störungen in der FTA sehr vage formuliert, was unserem initial schlechten Verständnis des Systems geschuldet ist. Wir haben erst über die Programmgraphen komplett durchdacht, was hinter dem FFB steht.

FMEA

Die möglichen Fehlerursachen entsprechen Einzelfehlern (welche aber nicht kritisch sein müssen). Im Vergleich zur DCCA sollten die einelementigen kritischen Fehlermengen (*EKF*) eine möglichst hohe RPZ haben.

Zug

- Motorstörung/-ausfall bei BÜ-Anfahrt (RPZ 9) -> EKF in der DCCA (Zugmotor_Ausfall), aber zu geringe RPZ
- *Bremsen versagen*: Elektronik fällt aus (RPZ 160), Abnutzung der Bremsscheiben (RPZ 40) -> nur Element einer zweielementigen kritischen Fehlermenge, aber Ausfall der Bremsen im Allgemeinen schlecht für einen Zug
- Zentralregister meldet falsche Werte (RPZ 126) -> in DCCA nicht abgebildet
- Fehlerhafte Geschwindigkeits- / Positionsmessung durch defekten Hodometer (RPZ 216) -> EKF in der DCCA (ZugPunktpositionsbestimmung_Stoerung), entsprechend hohe RPZ in der FMEA
- Zugsender fällt aus (RPZ 24) -> Element einer zweielementigen kritischen Fehlermenge in der DCCA (zusammen mit Bremsen-Ausfall)
- Zugempfänger fällt aus (RPZ 24) -> Fehler in DCCA nicht modelliert

Bahnübergang

- Empfänger fällt aus (RPZ 32) -> Fehler in DCCA nicht modelliert (~ analog zu Fehler beim Zugsender)
- Sender fällt aus (RPZ 18) -> Teil einer zweielementigen kritischen Fehlermenge in DCCA (zusammen mit Schrankenmotor_Ausfall/ZugFunksender_Ausfall), dafür sollte die RPZ höher sein
- Schrankenmotor defekt (RPZ 96) -> Teil einer zweielementigen kritischen Fehlermenge in DCCA, angemessen hohe RPZ
- Lampe ausgefallen (RPZ 180) -> in DCCA nicht modelliert
- Verschmelzung der Kontakte im Sensor (RPZ 80) -> EKF Sensor_Stoerung in DCCA

Nur in DCCA: EKF Schrankensensor_Stoerung, in FMEA nur eine Entdeckungsmaßnahme für "Schrankenmotor defekt", aber noch nicht als eigene Komponente betrachtet.

Zusammenfassend sind (fast) alle Störungen der DCCA auch in der FMEA zu finden, allerdings in geringerer Genauigkeit und mit teilweise arbiträren RPZs. FMEA zeigt keine Kombinationen von Fehlern auf, über eine gut gewählte RPZ könnte man die Fehleranfälligkeit trotzdem minimieren.

DCCA

Eindeutig das genaueste Mittel, um Störungen und vor allem Kombinationen von Störungen zu finden.

Allerdings ist die State Explosion und die damit verbundene Laufzeit des Model-Checkers ein Problem, das man durch Abweichen von der Realität mit verringerten

Variablen-Ranges und viel Rumschrauberei bedingt lösen kann. Auch muss man viel über die LTL/CTL-Spezifikationen nachdenken, bis sie wirklich das ausdrücken, was man will.