

Analysis and Synthesis of the Behavior of Complex Programmable Electronic Systems in Conditions of Failure

Y. Papadopoulos, J. McDermid,
R. Sasse, and G. Heiner

JUNBEOM YOO

Dependable Software Laboratory
KONKUK University

<http://dslab.konkuk.ac.kr>

Contents

- Introduction
 - Basic Concept
 - Classical Safety Analysis Techniques
 - Limitation of Classic Techniques
- Overview of the Proposed Method: HiP-HOPS
 - FFA+
 - Hierarchical Modeling
 - IF-FMEA
 - FTA
- Conclusions

Introduction

Safety

Safety is freedom from accidents or losses. (Leveson 1995)



Relative definition of safety

- All **hazard** cannot be eliminated.
- Often, hazard elimination requires sacrificing some other goals
- It makes sense, "It is absolutely safe from a particular hazard."

Introduction

Hazard

Hazard is a state or set of conditions of a system that together with other conditions in the environment, will lead inevitably to an accident.

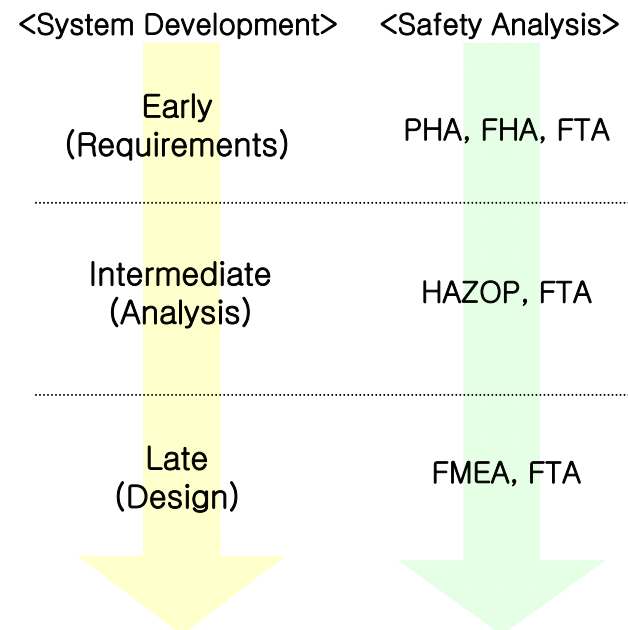
Hazard analysis investigates factors related to accidents.

- To identify and assess potential hazards
- To identify the conditions that can lead to hazard, so that the hazard can be eliminated or controlled.

Introduction

Classical Safety Analysis Techniques

1. Preliminary Hazard Analysis (PHA)
2. Functional Hazard Assessment (FHA)
3. Hazard and Operability study (HAZOP)
4. Failure Mode and Effects Analysis (FMEA)
5. Fault Tree Analysis (FTA)



Introduction

1. Preliminary Hazard Analysis (PHA)

Hazard	Effect (accident)	Severity	Co-effectors	Exposure to danger	Avoidance of danger
Loss of Braking	Death or serious injury to occupants of the vehicle, other vehicles or pedestrians	Critical	High speed travel and requirement to slow down or stop	Frequent = $1e-2$ [1/h]	Unlikely to avoid danger
Uneven Braking	Directional instability. Death or serious injury to occupants of the vehicle, other vehicles or pedestrians	Critical	Heavy traffic, Hazardous road condition	Frequent = $1e-2$ [1/h]	Likely to avoid danger

Table 2-5: Preliminary Hazard Analysis table

Introduction

2. Functional Hazard Assessment (FHA)

Function	Failure Condition (Hazard Description)	Phase	Effects of failure Condition on Aircraft/Crew	Classification	Reference to Supporting Model	Verification
Decelerate Aircraft on the Ground	<i>1. Loss of Deceleration Capability</i>	<i>Landing /Run to take off/ Taxi</i>	<i>See Below</i>			
	1.a. Unannuciated loss of deceleration capability	Landing/ Run to take off	Crew is unable to decelerate the aircraft, resulting in a high speed overrun	Catastrophic		Aircraft Fault Tree
	1.b. Annuciated loss of deceleration capability	Landing	Crew selects more suitable airport, notifies emergency ground support, and prepares occupants for landing overrun	Hazardous	Emergency landing procedures in case of loss of stopping capability	Aircraft Fault Tree
	1.c. Unannuciated loss of deceleration capability	Taxi	Crew is unable to stop the aircraft on the taxiway or gate resulting in low speed contact with terminal, aircraft, or vehicles	Major		

Introduction

3. Hazard and Operability study (HAZOP)

Guide Word	Deviation	Possible Causes	Consequences	Action Required
NONE	No flow	No hydrocarbon available from storage Transfer pump fails (motor fault, loss of power, impeller corroded etc.)	Loss of feed to reactor. Polymer formed in heat exchanger As above	1) Ensure good communication with storage area 2) Install low level alarm on settling tank Covered by 2)
MORE	More flow More Pressure More Temperature	Level control valve fails to open, or Level Control Valve bypassed in error Isolation valve or Level Control Valve closed when pump running High intermediate storage temperature	Settling tank overfills Line subjected to full pump pressure Higher pressure in transfer line and settling tank	3) Install high level alarm 4) Check size of overflow 5) Establish locking-off procedure for Level Control Valve bypass when not in use 6) Install kickback on pumps 7) Install warning of high temperature at intermediate storage
...	

Table 2-7: HAZOP table

Introduction

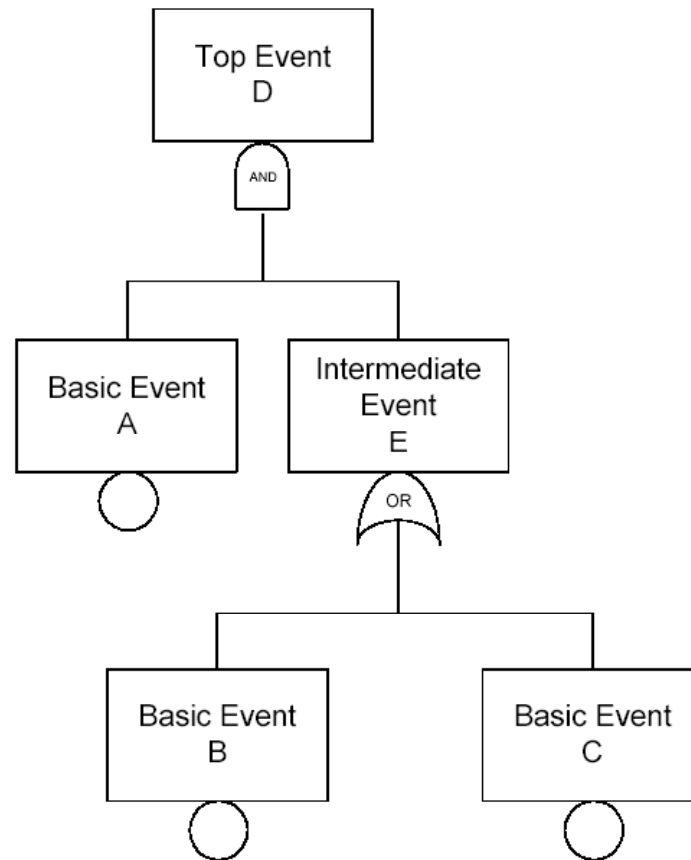
4. Failure Mode and Effects Analysis (FMEA)

<i>Component</i>	<i>Failure Mode</i>	<i>Subsystem Effects</i>	<i>Vehicle Effects</i>	<i>Haz</i>	<i>Failure rate [1/h]</i>	<i>Comments</i>
Vehicle Speed Sensor	No signal	Vehicle speed will always be calculated as zero	1.No speed indication 2.Mileometer not incremented 3.Electronic gearbox control may select too low gear, possibly resulting in wheel lockup or transmission damage	Min Min Maj	5E-5	Effect 3) requires simultaneous failure of engine load calculation and mechanical interlocks on gearbox
Vehicle Speed Sensor	Noisy (too Many edges)	Calculated vehicle speed will be too high. If edges arrive at higher rate than specified, they will be lost	4.Indicated speed greater than actual 5.Mileometer over-reads 6.Electronic gearbox control may select too high gear, possible resulting in stall	Min Min Min	3E-5	Effect 6) is hard to detect via engine load calculation, unless noise is extreme
Vehicle Speed Sensor	Intermittent	Calculated vehicle speed will be too low	7.Speed indicated lower than actual 8.Mileometer under-reads 9.As 3)	Min Min Maj	4E-5	See above

Table 2-8: Failure Mode and Effect Analysis table

Introduction

5. Fault Tree Analysis (FTA)



Introduction

Limitation of Classic Techniques

As the **complexity** of modern programmable electronic systems increases, the **applications of classical techniques** is becoming increasingly more problematic.

Problems issued:

- Inconsistent
- Untraceable
- Unmanageable

Introduction

Limitation of Classic Techniques

1. Inconsistent

- These techniques are based on different design notations as the development lifecycle.
- Updates are not kept well.

2. Untraceable

- These analysis remains fragmented, so the results are incomplete.
- HW / SW analysis are separated, so the relationship between HW and SW often remains vague and unsolved.

3. Unmanageable

- Fault tree analysis : consistent, traceable
- But, FTA is exert-dependent, laborious, non-systematic, error-prone, and voluminous

Overview of the Proposed Method: HiP-HOPS

HiP-HOPS

Hierarchically Performed Hazard Origin and Propagation Study

Characteristics:

- Integrated assessment of hierarchically described system.
- From functional level to lower HS/SW design level.
- Modify and incorporate classical techniques.

- Early: FFA+ (Extended FFA)
- Later: IF-FMEA (Interface Focused FMEA)
- Across: FTA (Mechanically generated)

- Tool supported.

Overview of the Proposed Method: HiP-HOPS

HiP-HOPS

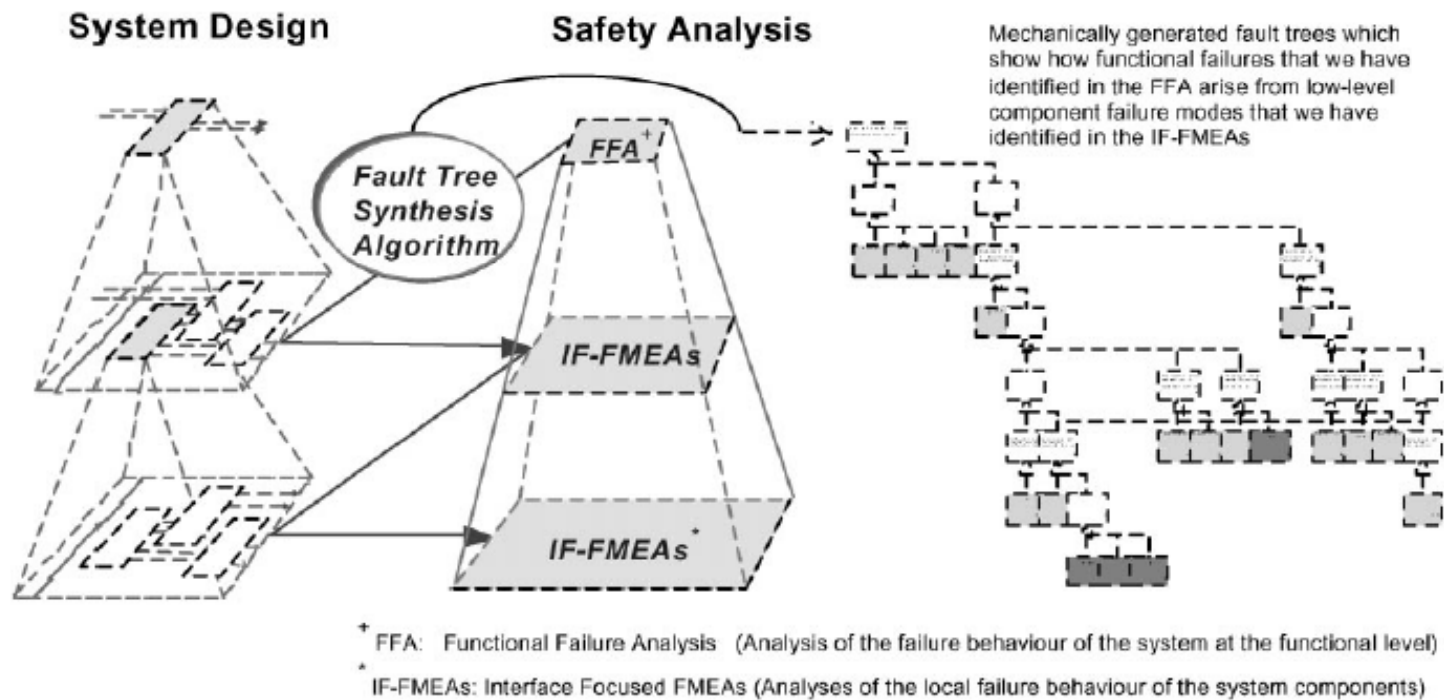


Fig. 2. Overview of design and safety analysis in HiP-HOPS.

Overview of the Proposed Method: HiP-HOPS

Early: FFA+

Standard FFA process (SAE ARP-4761, 1996)

1. Identification and listing of all system functions
2. Precise definition of purpose and behavior of each function
3. Examination of **each function** for potential **failure modes in three classes**:
 - Loss of function (omission)
 - Function provided when not required (commission)
 - Incorrect operation of function (malfunction)
4. Determine of the effects of each failures
5. Determination of the severity of each functional failures
6. Compilation of the results in tabular form
[function, failure mode, contributing factors, effects, severity]

Overview of the Proposed Method: HiP-HOPS

Early: FFA+

Proposed FFA+ process

1. Construct a **function block diagram**, which identifies system functions and their dependencies
2. Remove any avoidable dependencies between functions
3. Identify **single functional** failures examining each function:
 - Loss of function
 - Inadvertent delivery of function
 - malfunction
4. Assess single function failures
 - Determine any contributing factors (I.e. environmental factors)
 - Determine the effects and severity of failure
 - Determine potential mechanisms for **detection and recovery**
 - Compile the results in a tabular form
[failure mode, contributing factors, effect, severity, detection, recovery, recommendation]
5. Identify unique, plausible **combination of multiple functional failures**
 - Identify unique combinations by examining symmetries and exclusivity.
 - Examining by applying other plausibility criteria
6. Assess multiple functional failures in step 4.

Overview of the Proposed Method: HiP-HOPS

Early: FFA+

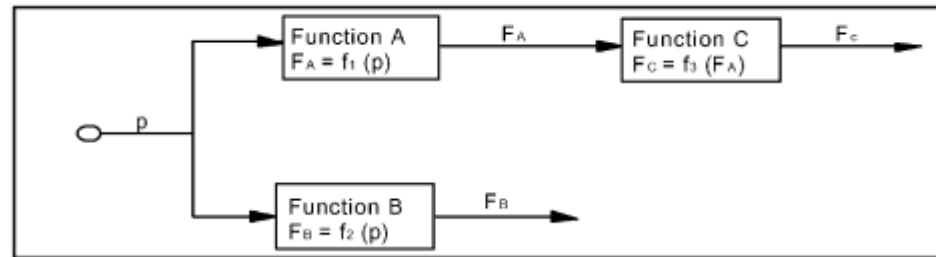


Fig. 4. Example functional model.

Dependencies found by FFA+:

1. Between A and B (common source P)
→ Duplication of input sensor P
2. Between A and C (functional input from A)
→ Range validation check of F_A

Overview of the Proposed Method: HiP-HOPS

Early: FFA+

Special features of FFA+:

1. Function block diagram
2. Removal of multiple dependencies
3. Failure detection and recovery recommendation
4. Reflected on a successive system design

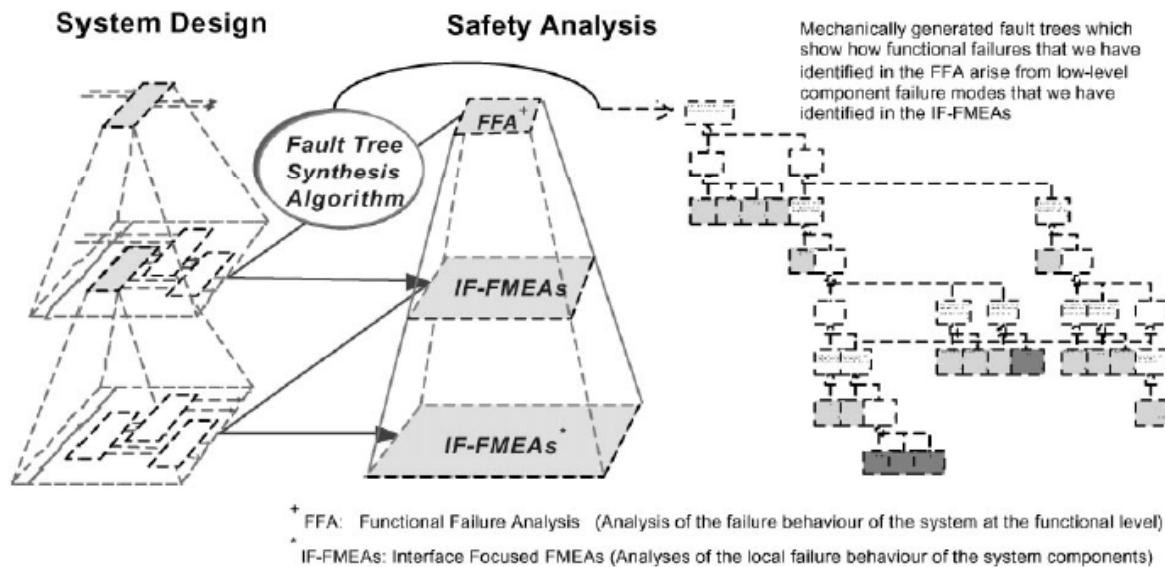


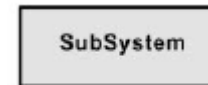
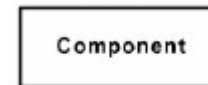
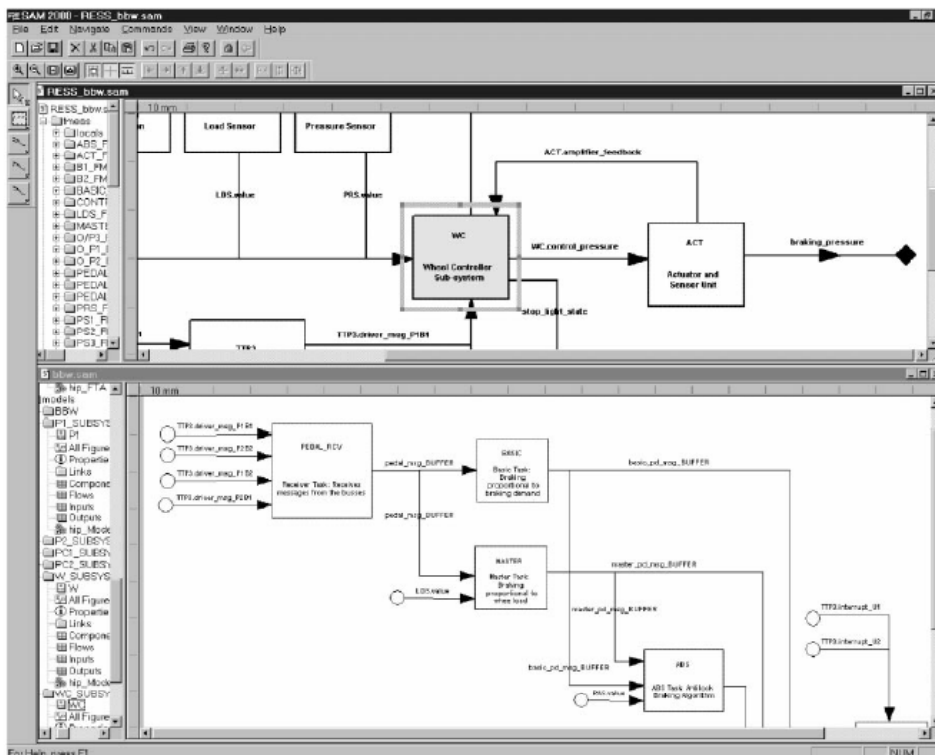
Fig. 2. Overview of design and safety analysis in HiP-HOPS.

Overview of the Proposed Method: HiP-HOPS

Hierarchical Modeling

Use a kind of **Flow Diagram** derived from **original design notation**.

- Engineering schematics
- Piping/instrumentation diagram
- Data-flow diagram
- MASCOT diagram



Flow



Input



Output



Overview of the Proposed Method: HiP-HOPS

Hierarchical Modeling

Special features of Hierarchical Modeling:

1. Precise relationship between original design and proposed flow diagram
2. Static structural model/analysis only

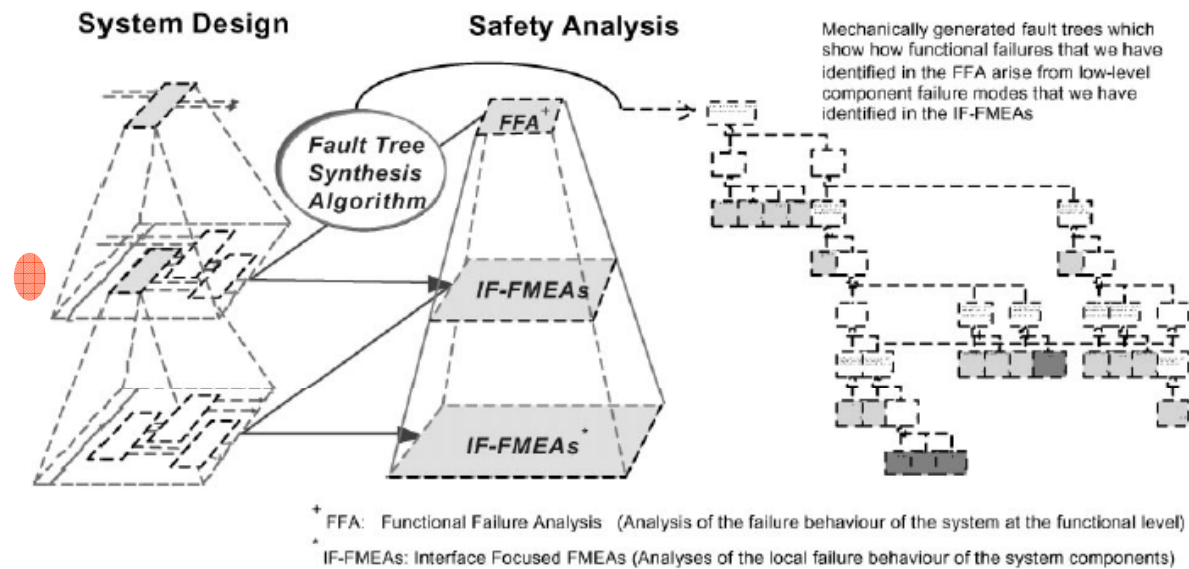
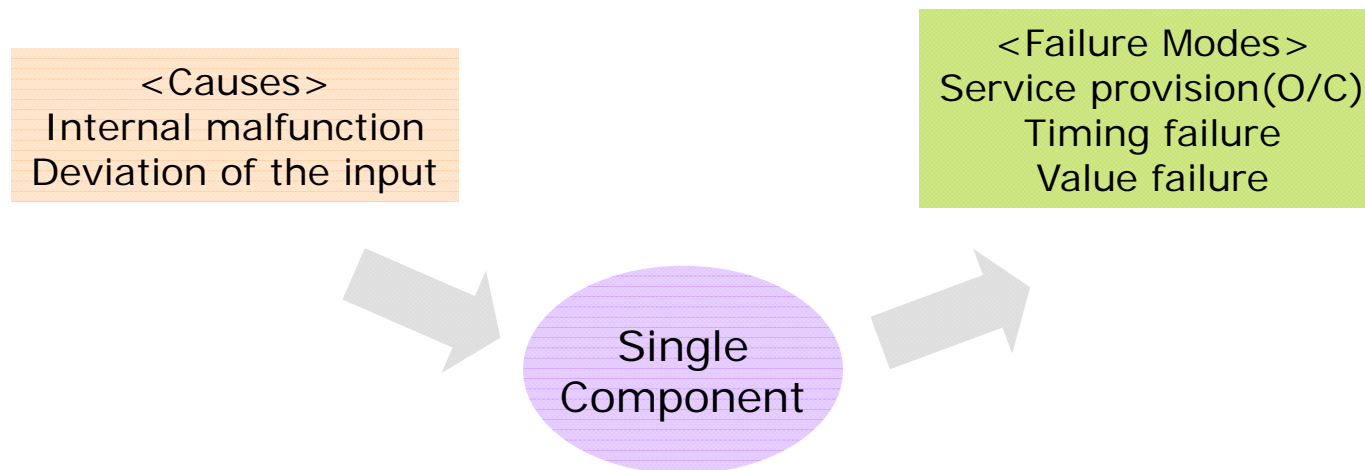


Fig. 2. Overview of design and safety analysis in HiP-HOPS.

Overview of the Proposed Method: HiP-HOPS

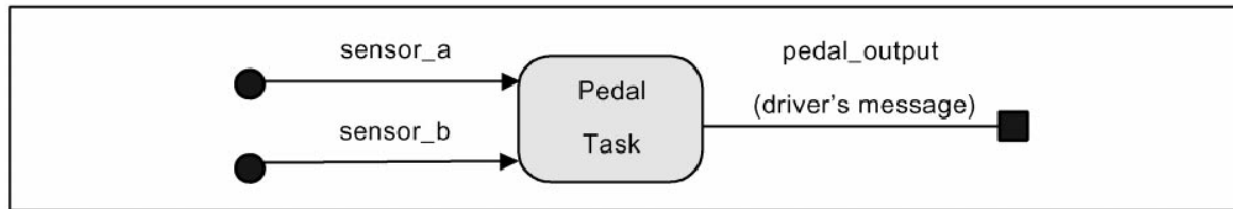
Later: IF-FMEA

Interface Focused FMEA on a single component.



Overview of the Proposed Method: HiP-HOPS

Later: IF-FMEA

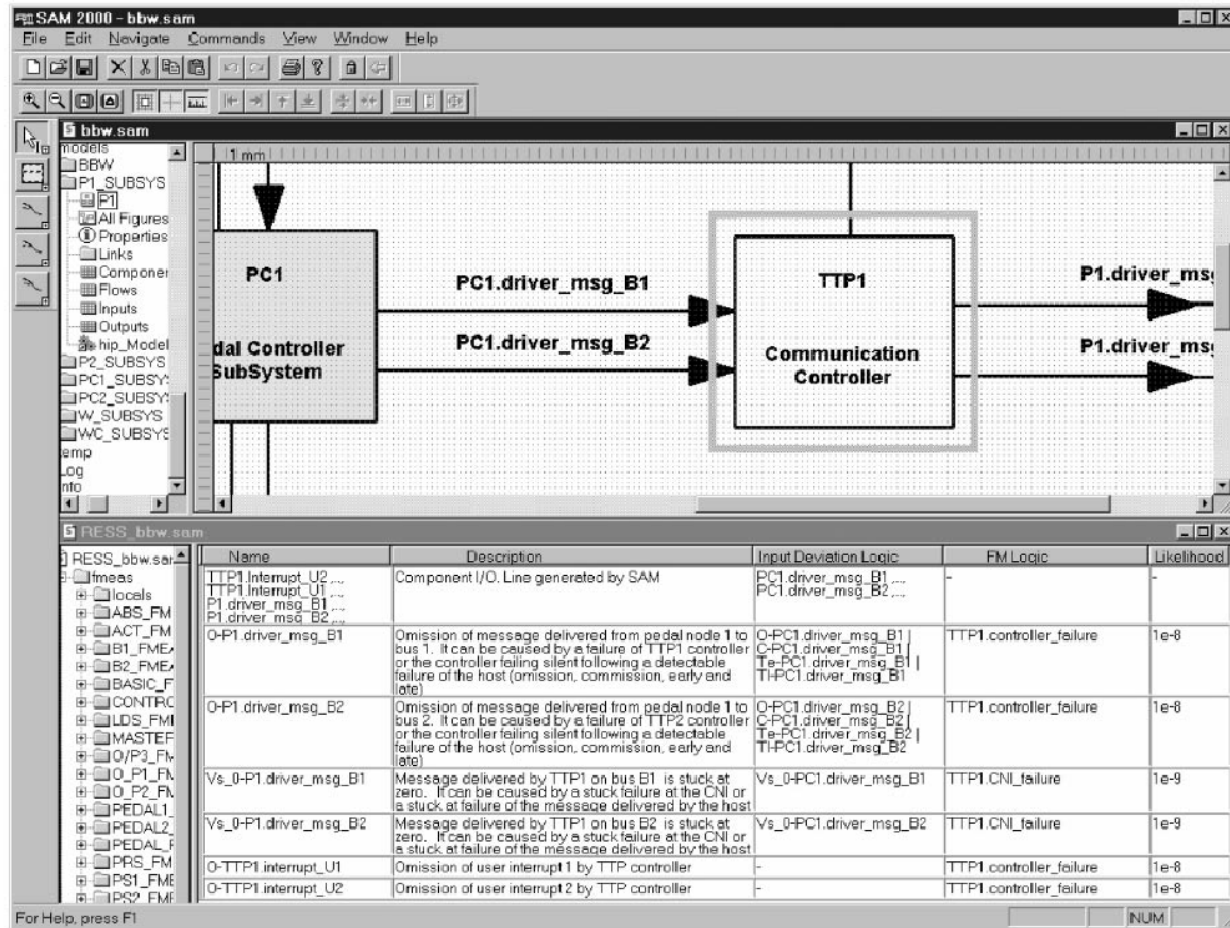


Output Failure Mode	Description	Input Deviation Logic	Component Malfunction Logic	+ (f/h)
O-pedal_output	Omission of <i>Pedal</i> output (driver's message). It can be caused by task malfunction or out of range failures of both pedal sensors.	(V>max-sensor_a V<min-sensor_a) & (V>max-sensor_b V<min-sensor_b)	processor_ failure operating_ system_ failure	1.00E-07 9.00E-07
Vs_0-pedal_output	<i>Pedal</i> output (driver's message) stuck at 0. It can be caused by memory stuck at 0 failures, or by stuck at minimum failures of both pedal sensors.	Vs_min-sensor_a & Vs_min-sensor_b	Memory_ stuck_at_0	2.00E-06

Fig. 8. Model and fragment of the IF-FMEA of the pedal task.

Overview of the Proposed Method: HiP-HOPS


Later: IF-FMEA



Overview of the Proposed Method: HiP-HOPS

Later: IF-FMEA

Special features of IF-FMEA:

1. Obscure relationships marked 
2. No concern about updating of IF-FMEAs and the effects

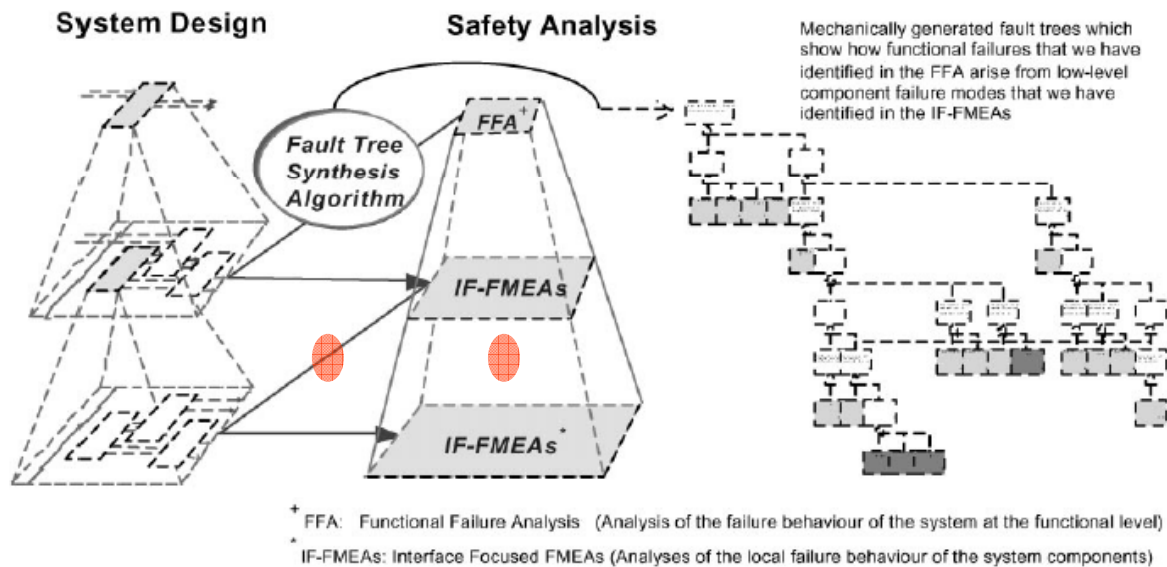
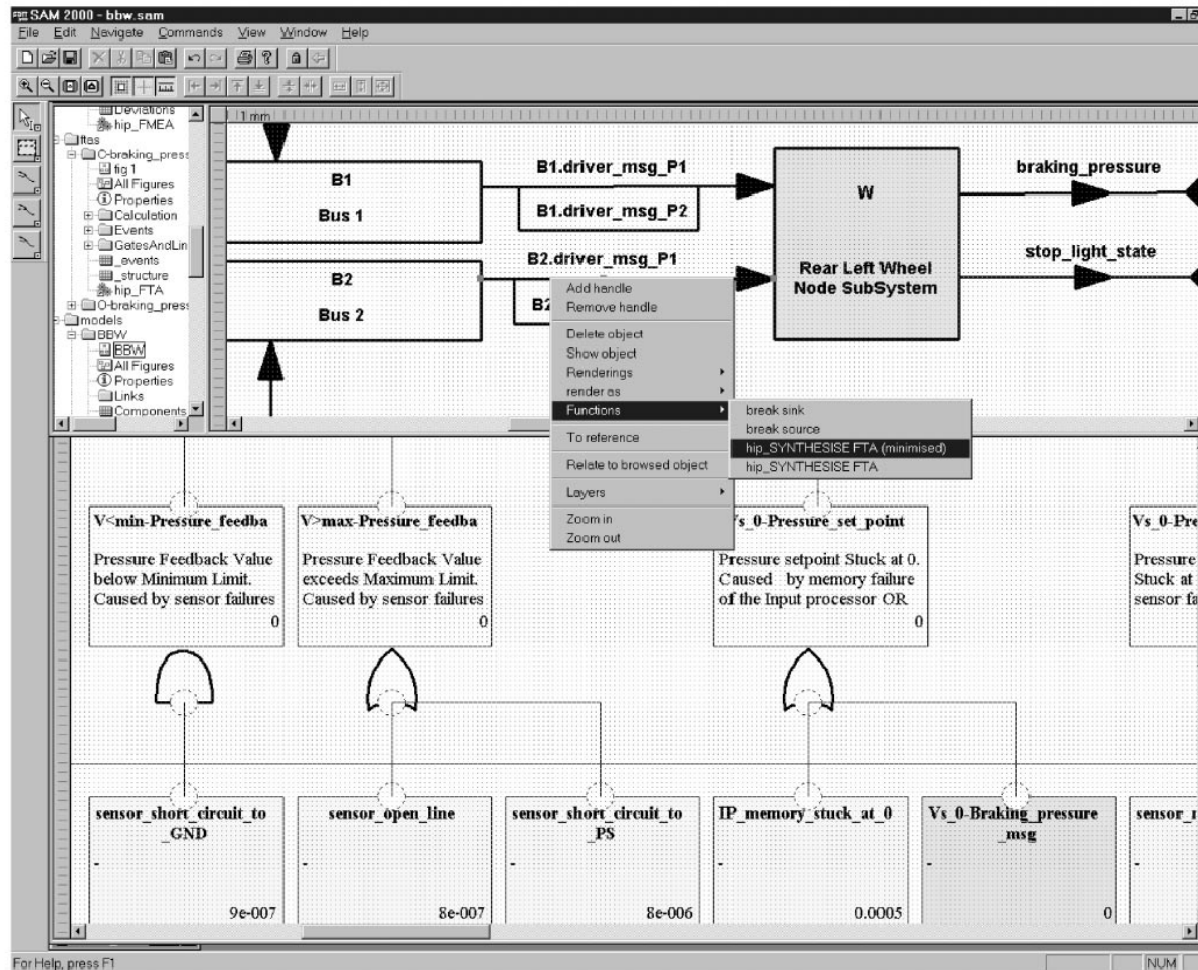


Fig. 2. Overview of design and safety analysis in HiP-HOPS.

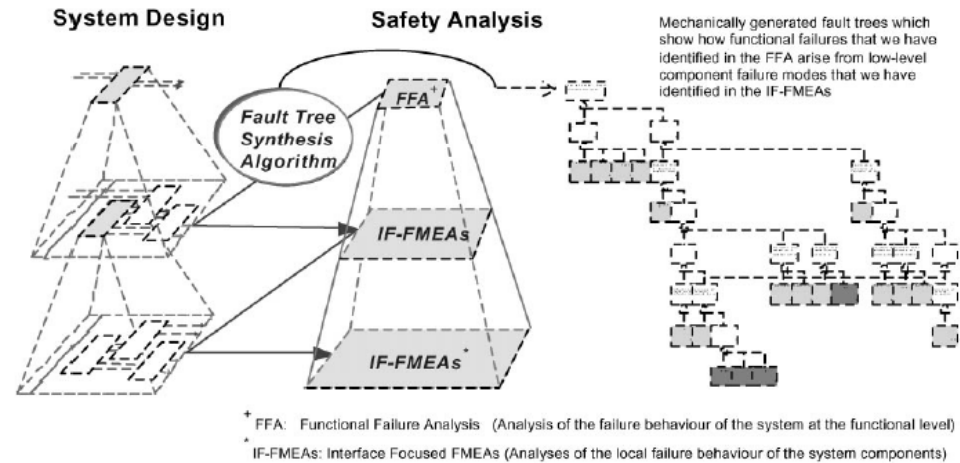
Overview of the Proposed Method: HiP-HOPS

Across: FTA (mechanically generated)



Overview of the Proposed Method: HiP-HOPS

Characteristic of HiP-HOPS



1. Consistent

- Based on one design notation: Flow diagram
- Updates are kept well.

2. Traceable

- Uses complete design model. (No fragments)
- HW / SW analysis are integrated

3. Manageable

- Mechanically generated fault tree analysis
- Selective generation

Conclusion and Future Work

HiP-HOPS:

- Provides consistent, traceable, and manageable safety analysis model
- Some limitations
- Can help safety analysts systematically with tool-support.

Future Work:

- Extends to interactive and dynamic system