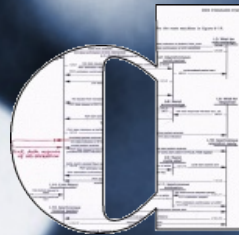




Validation and Analysis of Formal Methods using an Airbag Control Unit



10th Feb 2006



Universität des Saarlandes



Verification by
Simulation



Behavior Model
(MoDeST)

Safety Analysis
(Markov Chain)

Failure Analysis
(Fault Trees)

Interesting Point of Investigation

To which extent can
simulation be used
throughout the analysis
using Stochastic Timed
Automata



● Introduction

- ◆ The Airbag System
- ◆ MoDeST 
- ◆ Uppaal

● **Simulating the ECU** *(Modeling and Verification)*

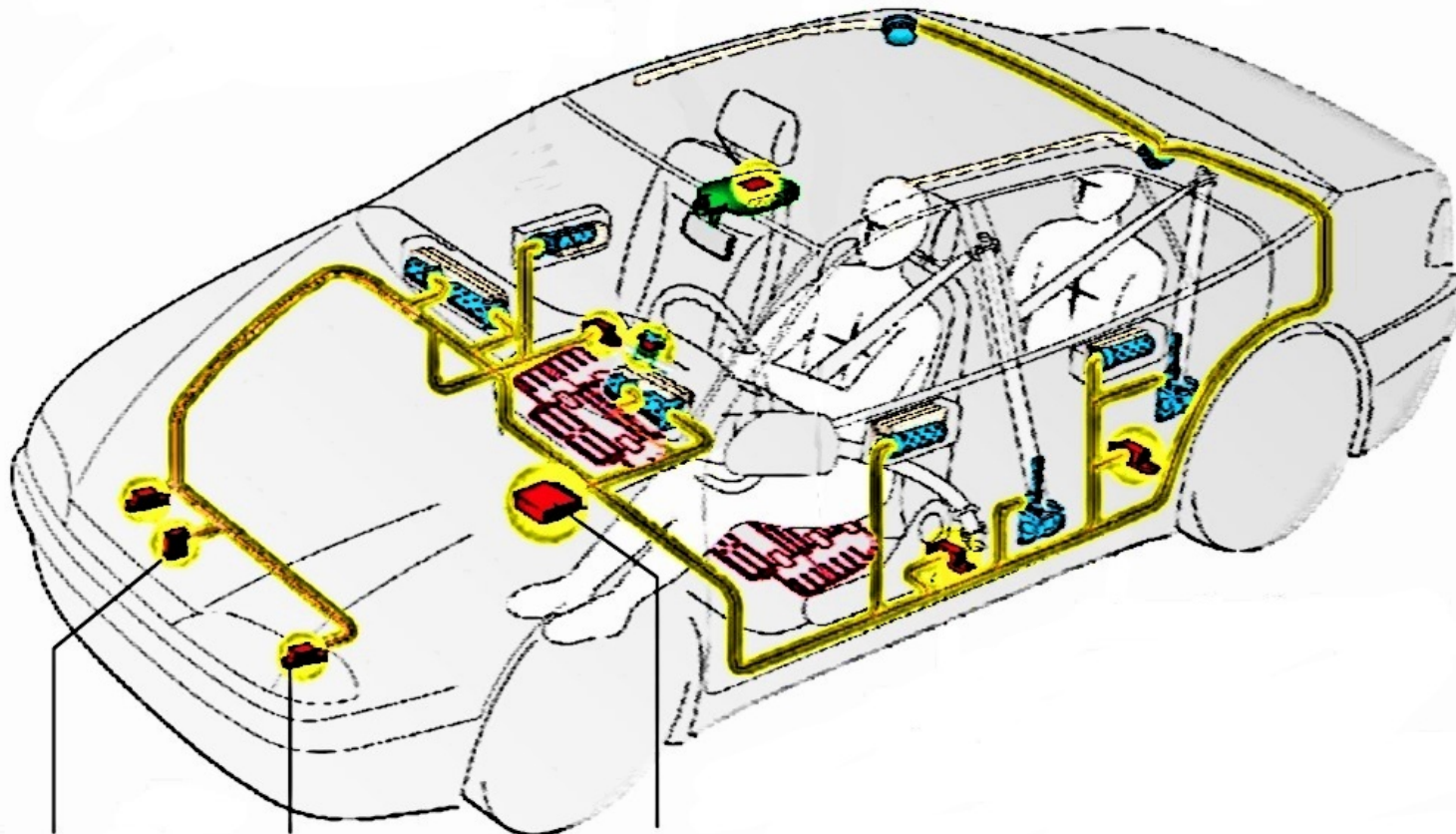
● **Safety Requirements** *(Markov Analysis)*

- ◆ via Simulation in MoDeST
- ◆ Analytical Approach





Airbag and Belt Tensioner Deployment depend on configuration determined by

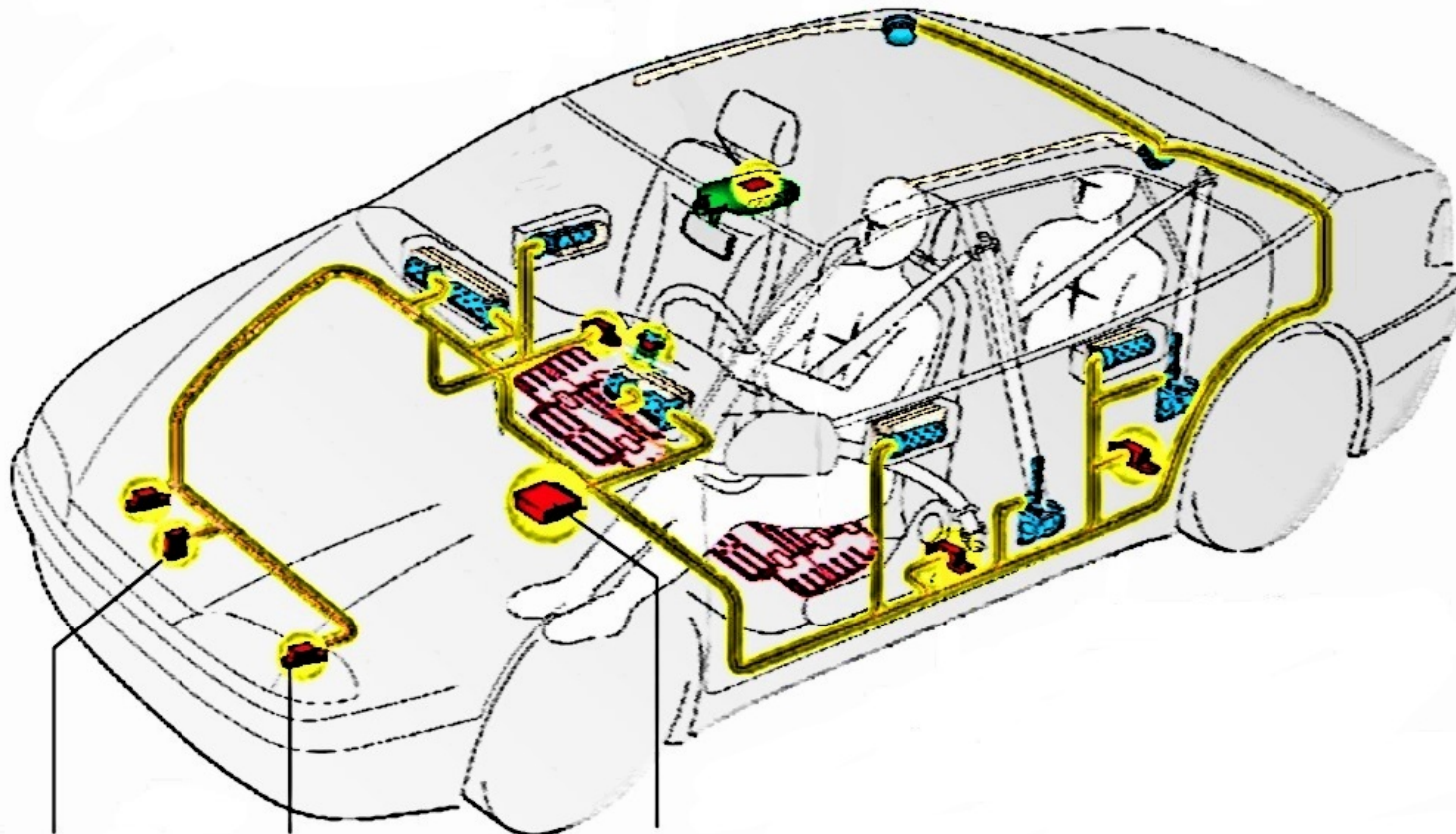


Pre-crash
Sensor

Up-Front
Sensor



Airbag and Belt Tensioner Deployment depend on configuration determined by



Pre-crash
Sensor

Up-Front
Sensor

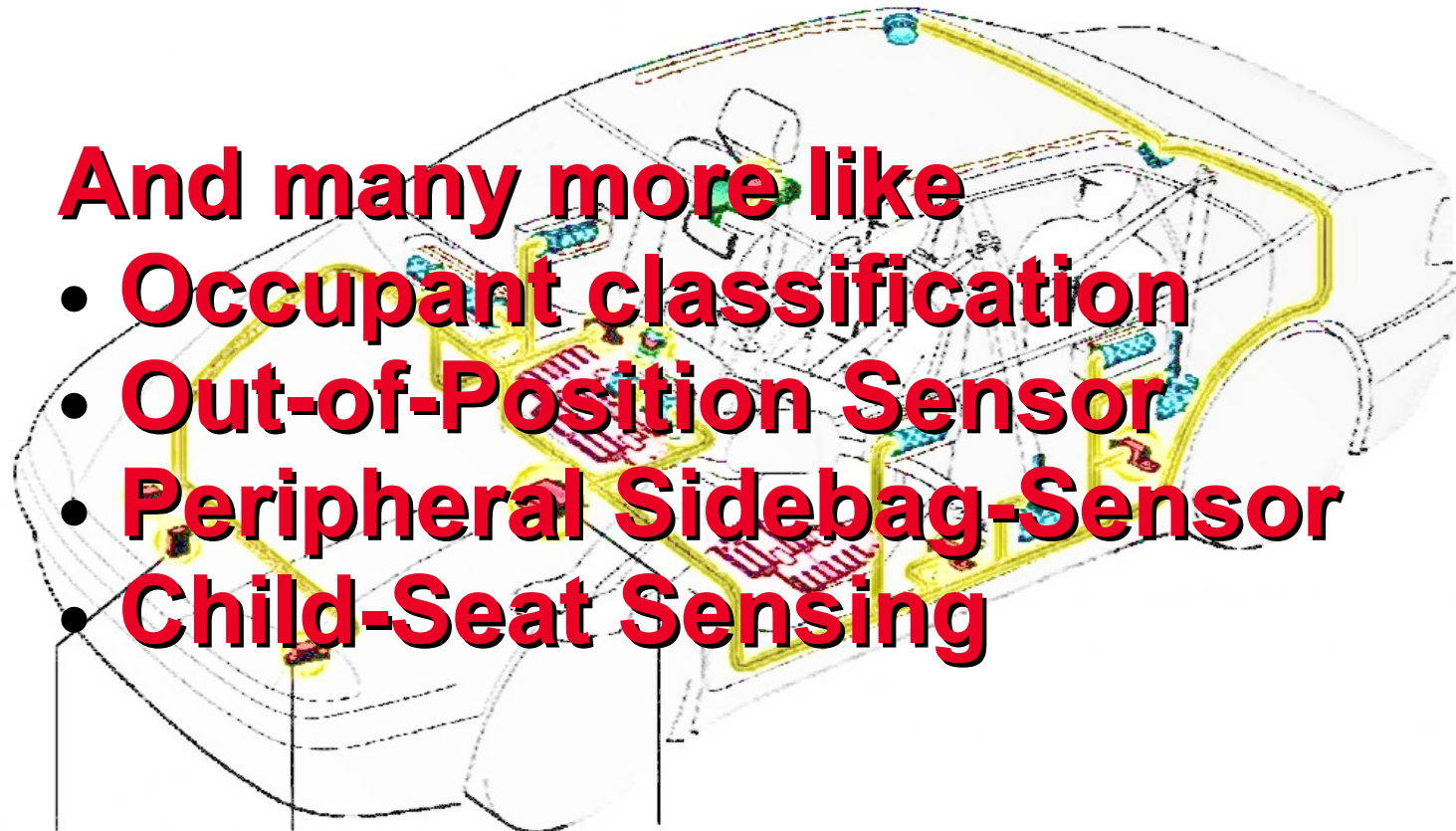
Central Control w/
over-roll sensing



Airbag and Belt Tensioner Deployment depend on configuration determined by

And many more like

- **Occupant classification**
- **Out-of-Position Sensor**
- **Peripheral Sidebag-Sensor**
- **Child-Seat Sensing**



Pre-crash
Sensor

Up-Front
Sensor

Central Control w/
over-roll sensing



MoDeST (**M**odeling and **D**escription language for **S**tochastic **T**imed systems)

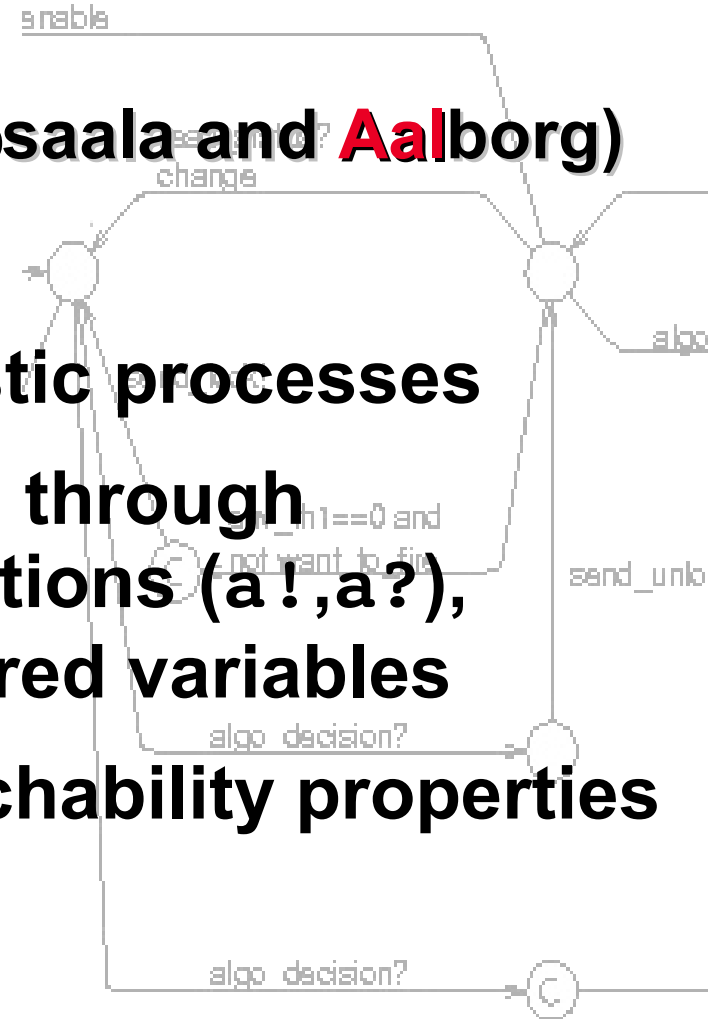
- **Definition actions (symmetric), variables, data structures**
- **Stochastic Distributions**
- **Probabilistic branching (pa1t)**
- **Non-deterministic branching (a1t)**
- **Local C1ock variables**
- **Parallelize Processes (par)**



```
PROCESS sender() {  
  clock t;  
  do {  
    :: { = t=0, sample=Exponential(lambda) = };  
    when (t==sample) urgent(true) sync  
  }  
}  
  
PROCESS receiver() {  
  do {  
    :: sync { = counter+=1 = }  
  }  
}  
  
PAR {  
  :: sender()  
  :: receiver()  
}
```

Uppaal (by Universities in Uppsala and Aalborg)

- Based on Timed Automata
- Collection of non-deterministic processes
- Asymmetric Communication through complementary pairwise actions ($a!$, $a?$), broadcast channels, or shared variables
- Checking invariant- and reachability properties by state-space exploration



Simulation of the ECU

Situation:

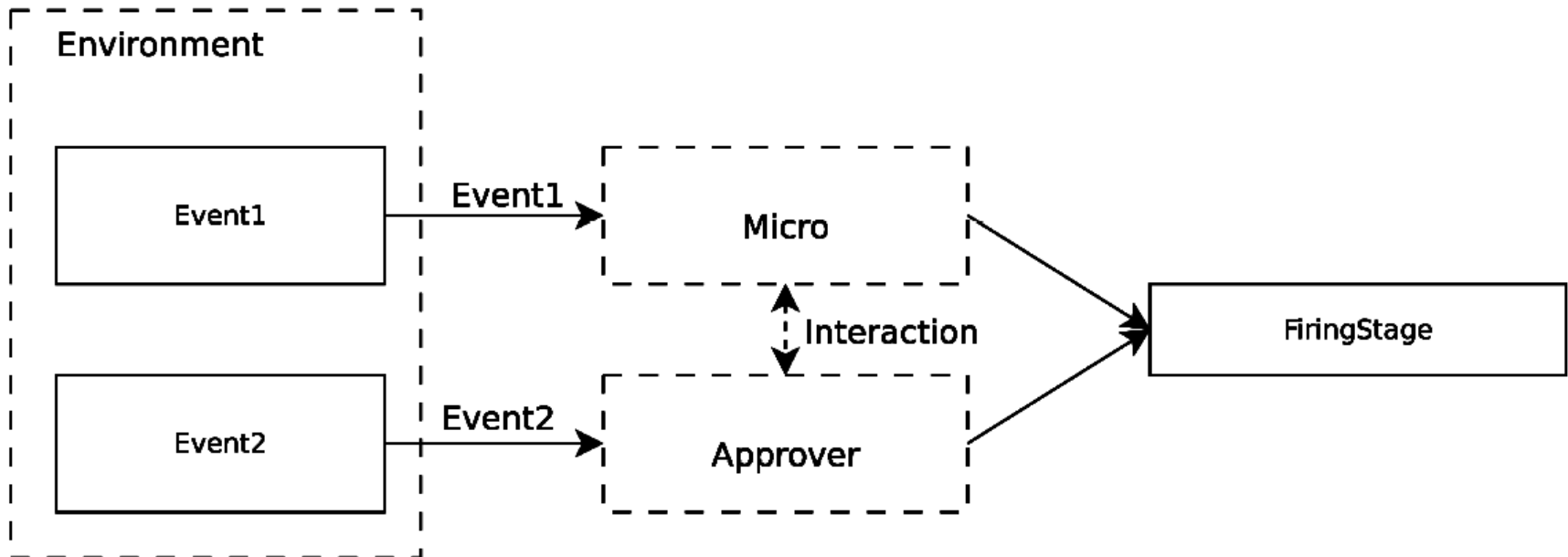
Critical behavior of the airbag control unit that could not be verified in Uppaal.

Goal

- Is it feasible to do model checking via simulation?
- How to adopt for broadcasting?



Scenario Overview





Properties of Interest:

- P0: A[] NOT deadlock
- P1: E<> FiringStage.Fire
- P2: E<> (Micro.Firing AND Approver.Enable AND NOT FiringStage.Firing)

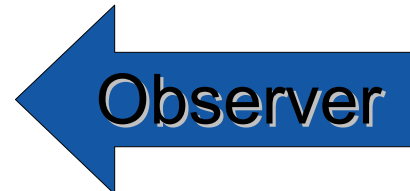
Properties of Interest:

- P0: A[] NOT deadlock



Simulation

- P1: E<> FiringStage.Fire



Observer

- P2: E<> (Micro.Firing AND
Approver.Enable AND
NOT FiringStage.Firing)



Observer



```
Process Observer_Prop1() {  
    when(LocationFiringStage==3)  
        Property1Satisfied {= Property1+=1 =}  
}
```

```
Process Observer_Prop2() {  
    when(LocationMicroFiring==1 &&  
        enable==1 &&  
        LocationFiringStage!=2)  
        Property2Violated {= Property2+=1 =}  
}
```

Simulation Results

- 1 000 batches
- Each for 1 million time units

	Mean Value	Confidence +/-
Property1	1	0
Property2	0	0

What about Property0?

Conclusion

● Pros

- ◆ Possible to simulate complex systems where state space exploration is failing
- ◆ Nice way to observe a model during execution
- ◆ Two valuable outputs usable (Trace Path, Reward Variables)

● Cons

- ◆ Simulation does never cover the whole state space
- ◆ Danger of purely basing results on simulation
- ◆ Statements about deadlock behavior are risky
- ◆ Awkward to adopt for broadcasting

On-Demand Failure Analysis

- Meet safety integrity requirements
- Does Airbag fails to work at times of an airbag relevant crash
- Determine the company's risk
- Critical point: Unintended or missing airbag deployment



Assumptions

- Overall operation time of one ECU 9.000 hours under normal usage (15 y, 600h/y)
- Total number N_0 of produced ECUs 30.000.000
- An airbag relevant Crash occurs exponentially distributed

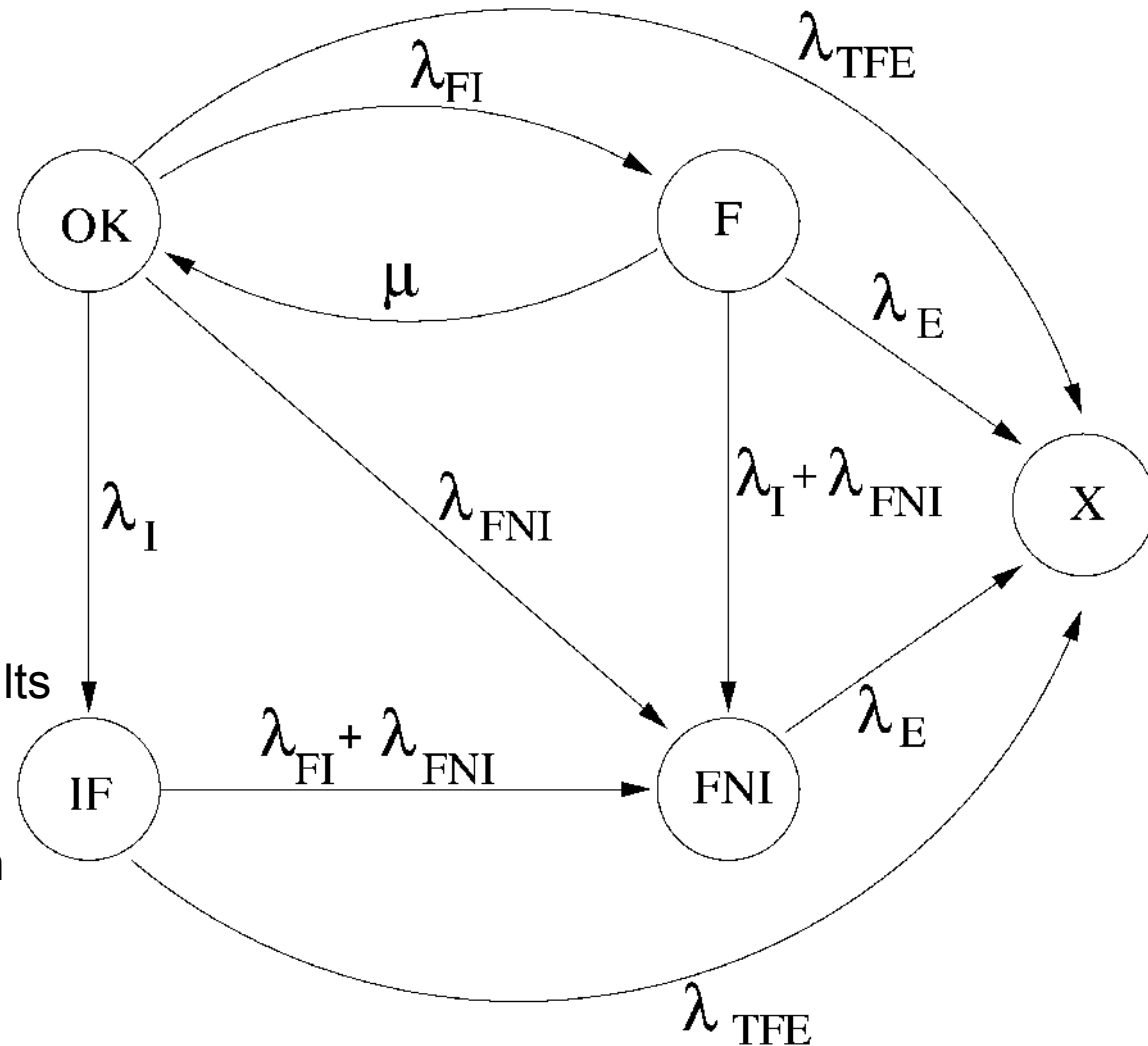
$$\lambda_E = 4.0 \cdot 10^{-5} h^{-1}$$

- Indicated Failures get repair after 20 hours on average

$$\mu_{repair} = 5.0 \cdot 10^{-2} h^{-1}$$



- λ_E
event crash rate
- λ_{FI}
rate of indicated failure
- λ_{FNI}
rate of not indicated failure
- λ_I
indication failure
- μ
repair rate
- P_{TFD}
probability of temporary faults upon processing demand
- λ_{TFE}
rate of temporary failure on demand



Sojourn Times

Time spend in each of the states

Variable	Mean Value	Confidence +/-	Prob
OK	9.9991E06	2.5300E03	9,18%
F	1.9930E-01	7.1528E-04	0,00%
IF	0.9890E8	2.5274E05	90,80%
FNI	2.4996E04	6.3255E00	0,02%

Sojourn Times

Time spend in each of the states

Variable	Mean Value	Confidence +/-	Prob
OK	9.9991E06	2.5300E03	9,18%
F	1.9930E-01	7.1528E-04	0,00%
IF	0.9890E8	2.5274E05	90,80%
FNI	2.4996E04	6.3255E00	0,02%

surprised?

Figures of Interest

- $MTTF$

Mean Time To Failure

- $P(X) |_{t=9.000 h}$

one airbag fails after 9000 hours of operation

- $EX_F = P(X) |_{t=9.000 h} \cdot N_0$

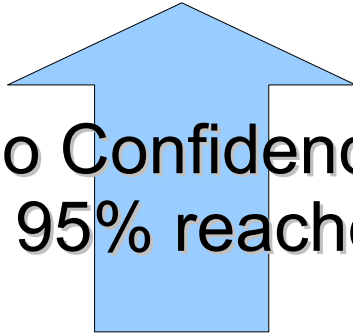
Expected number of failing ECU assuming N_0 are in operation

- $P_{\geq 1} = 1 - (1 - P(X) |_{t=9.000 h})^{N_0}$
at least one of N_0 ECU fails during T_0 of operation

Simulating the Model

- Simulation over 10^{15} time units
- 60 million batches

Variable	Mean Value	Confidence +/-
MTTF	1.0108E09	9.9995126E06
P(X) t=9.000h	1.6666E-08	3.2666666E-08
EX_F	0.5	
P>=1	0.3935	

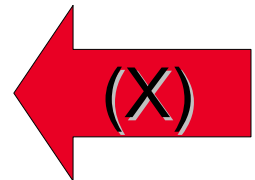


No Confidence
at 95% reached

Markov Chain Representation

$$Q = \begin{bmatrix} \mathbf{T} & T^0 \\ \mathbf{0} & 0 \end{bmatrix}$$

$$= \begin{pmatrix} -\sum & \lambda_{FI} & \lambda_I & \lambda_{FNI} & \lambda_{TFE} \\ \mu & -\sum & 0 & \lambda_I + \lambda_{FNI} & \lambda_E \\ 0 & 0 & -\sum & \lambda_{FI} + \lambda_{FNI} & \lambda_{TFE} \\ 0 & 0 & 0 & -\sum & \lambda_E \\ 0 & 0 & 0 & 0 & -\sum \end{pmatrix}$$



Interest in transient probabilities of being in state (X) at any time.

Phase Type distribution with representation $(\alpha, \mathbf{T})$ where

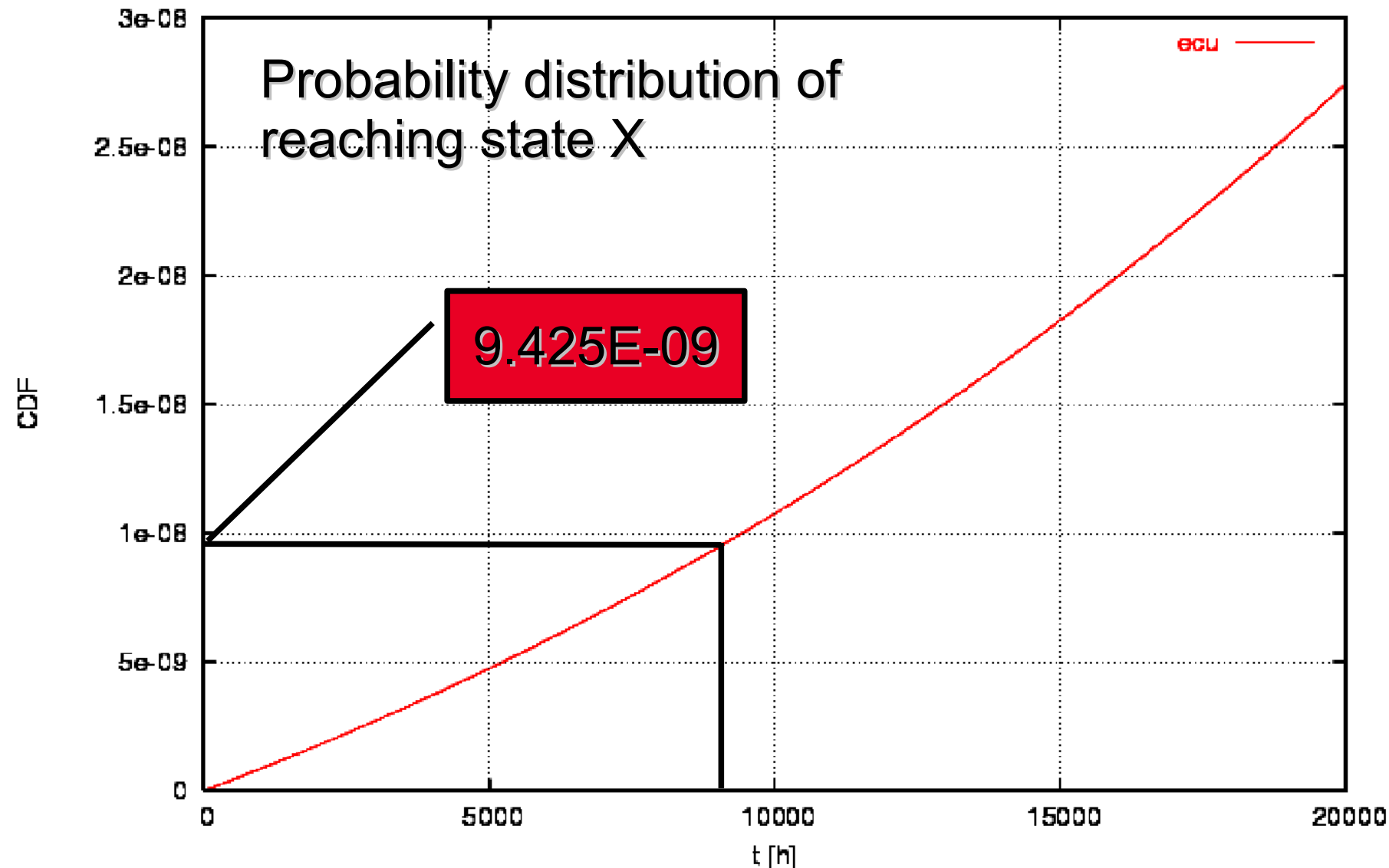
$$\alpha = (1 \ 0 \ 0 \ 0)$$

and

$$\mathbf{T} = \begin{pmatrix} -\sum & \lambda_{FI} & \lambda_I & \lambda_{FNI} \\ \mu & -\sum & 0 & \lambda_I + \lambda_{FNI} \\ 0 & 0 & -\sum & \lambda_{FI} + \lambda_{FNI} \\ 0 & 0 & 0 & -\sum \end{pmatrix}$$



Distribution





Comparison of Simulation and Analytical Results

Variable	Simulation	Analytical
$P(X) _{t=9.000h}$	1,667E-08	9,425E-06
EX_F	0,5000	0,2828
$P_{\geq 1}$	0,3935	0,2463

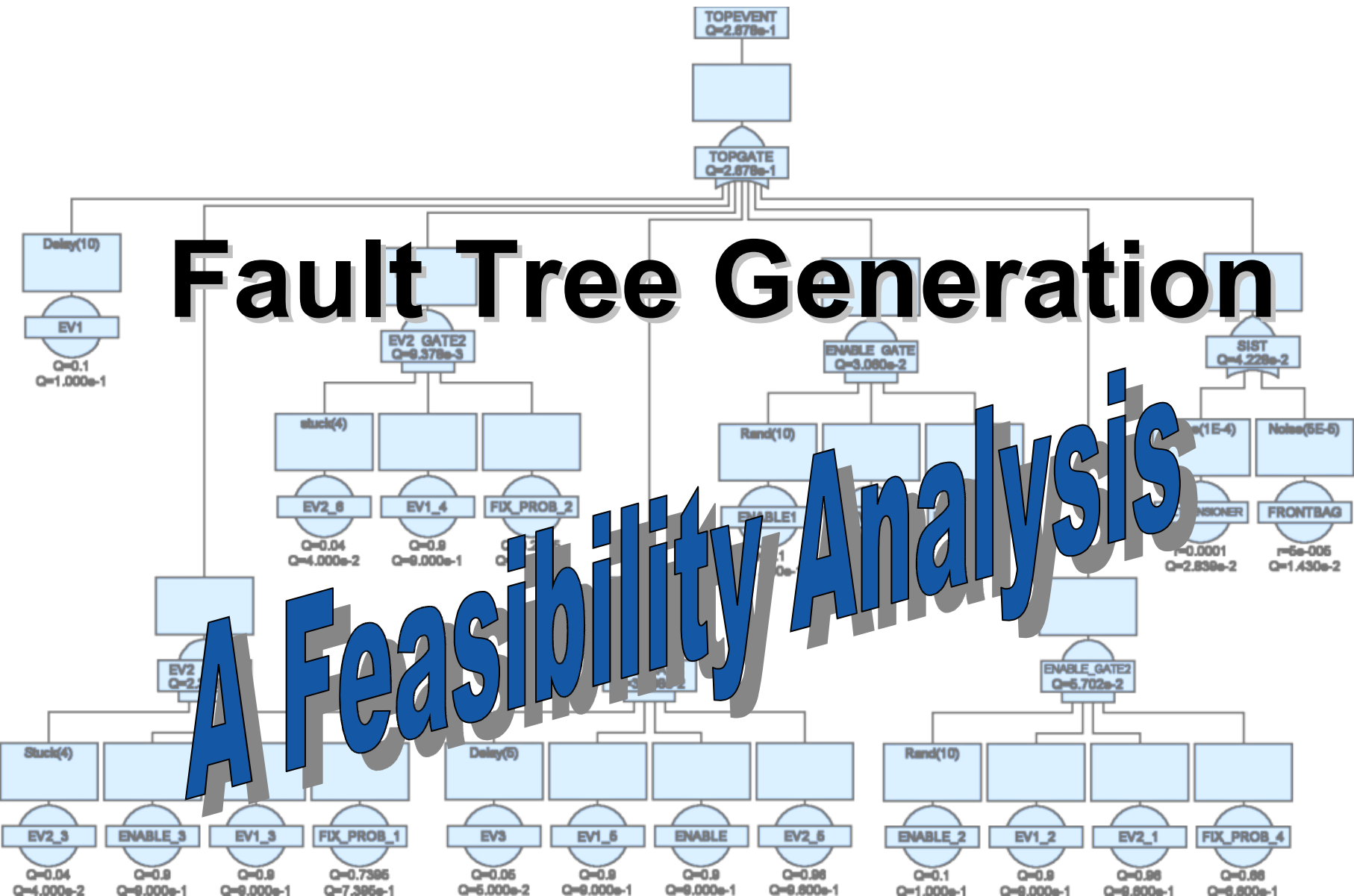
Conclusion

- **Way to simulate Markov Chains**
- **Drawback of simulation especially when dealing with small rates (many samples needed to reach confidence level)**
- **A long time spend in state IF (indication failure)**



Fault Tree Generation

A Feasibility Analysis



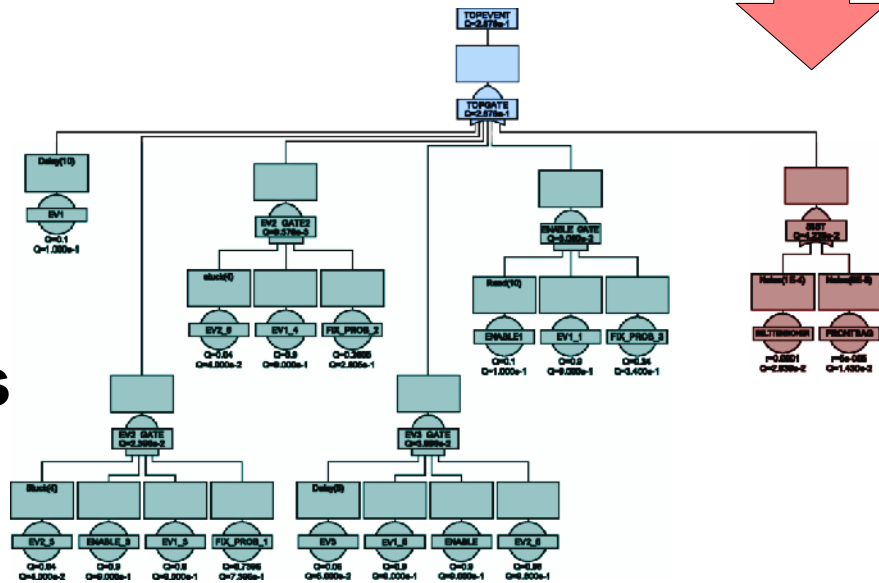
Fault Tree Generation

- Automate failure analysis of complex systems
- Generation of Fault Trees (FTs) by Simulation in MoDeST
- Using Separated Stochastic Independent Subtree (SIST) for stochastic components
- Implement preprocessor translations for errors using **gema**



- Modularize Event Groups
- Simulate Probabilistic Part for one time unit.
- Add exponential events to SIST

SIST



Probabilistic
Branch

Insertion of Errors into the Simulation Model

Probabilistic Errors for Actions

- `delay(a, p, t, clk)`
- `stuck(a, p)`

Probabilistic Errors for Variables

- `noise(x, p, m)`
- `rand(x, p, m)`

Preprocessor Translation:

```
delay(a,p,t,clk) ::=  
    float a_timer;  
    exception a_error;  
    {= a_timer=t+clk =};  
    palt{  
        :p:when(clk==a_timer)  
            urgent(true) throw a_error  
        :1-p: tau  
    }; a
```



Errors injected into the Model

Probabilistic
Events

	Error Type	Pr.	Values	Delay
Enable	RAND	10	[0,1]	
Event1	DELAY	10		5
Event2	STUCK	4		
Event3	DELAY	5		19

SIST

	Lambda	Delay Magnitude	
BT Delay	1E-04	60	30
FB Delay	5E-05	200	100

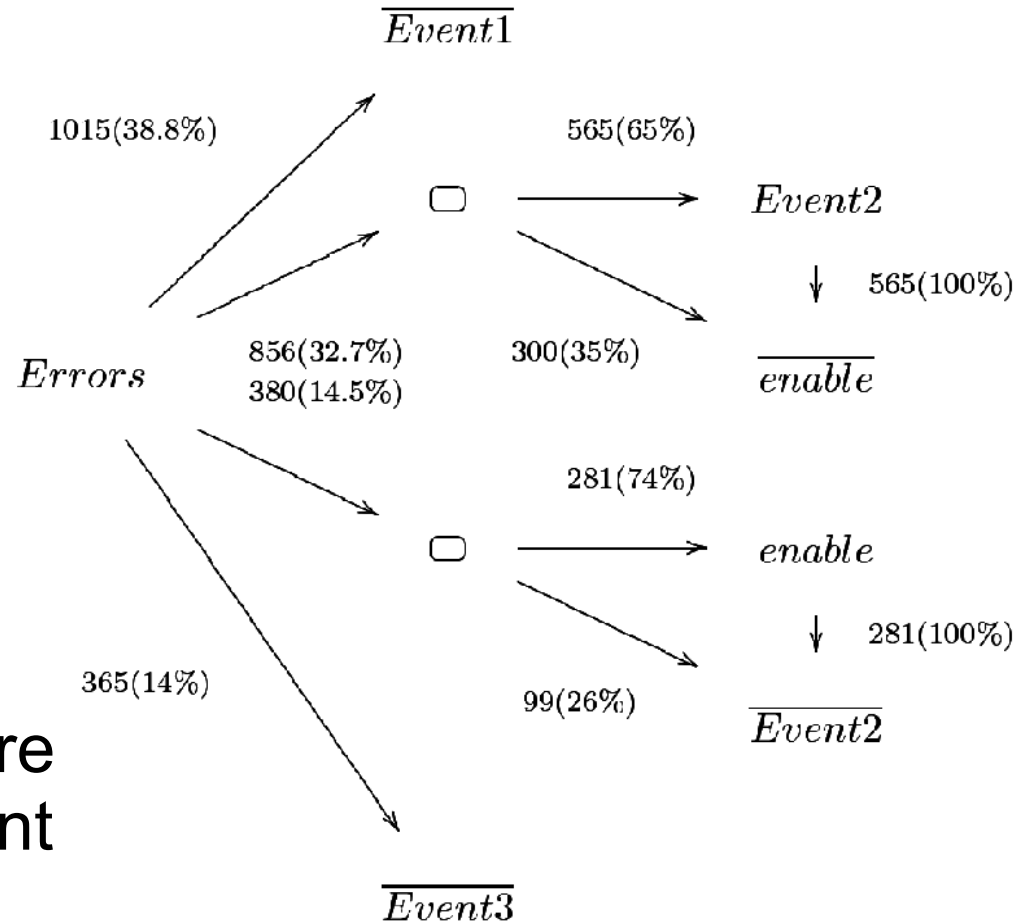
Simulation of the Behavior Model

- 10.000 batches
- Simulating each batch for 1 time unit (cf. SIST)



Use Trace to identity Error Events w.r.t.

- their Frequency
- their Order

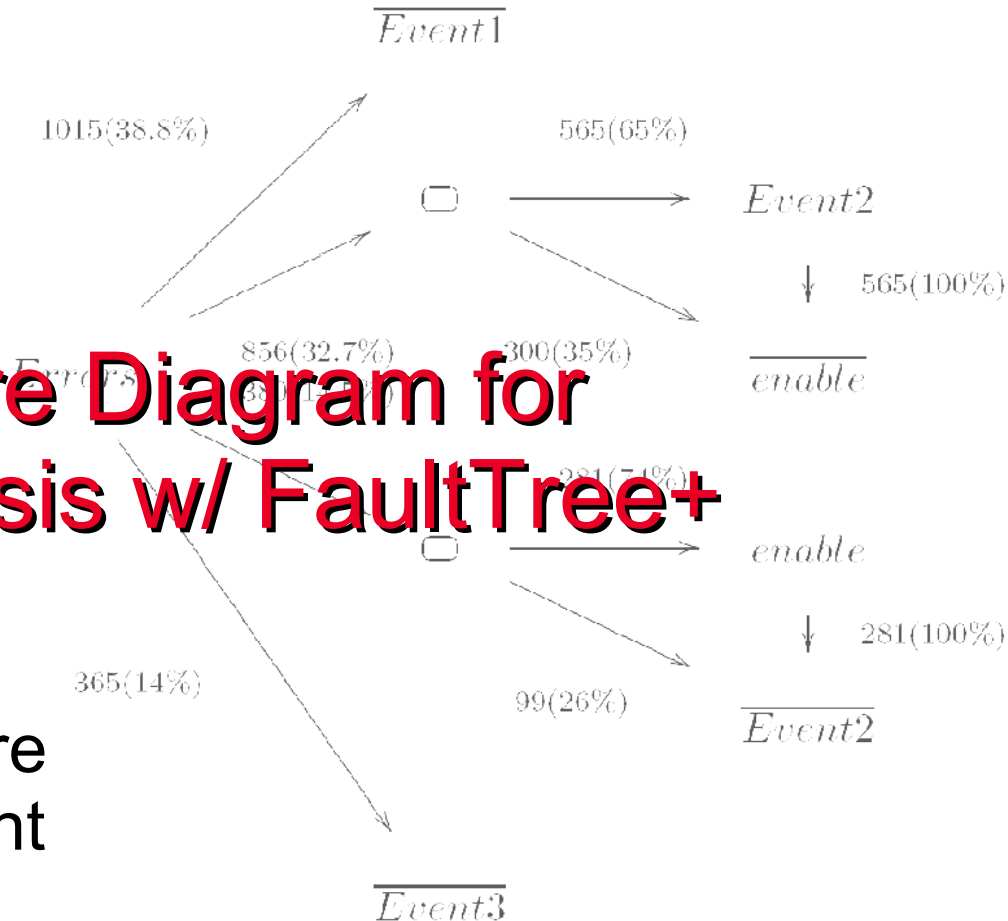


Event denotes failure of action/variable Event

Use Trace to identity Error Events w.r.t.

- their Frequency
- their Order

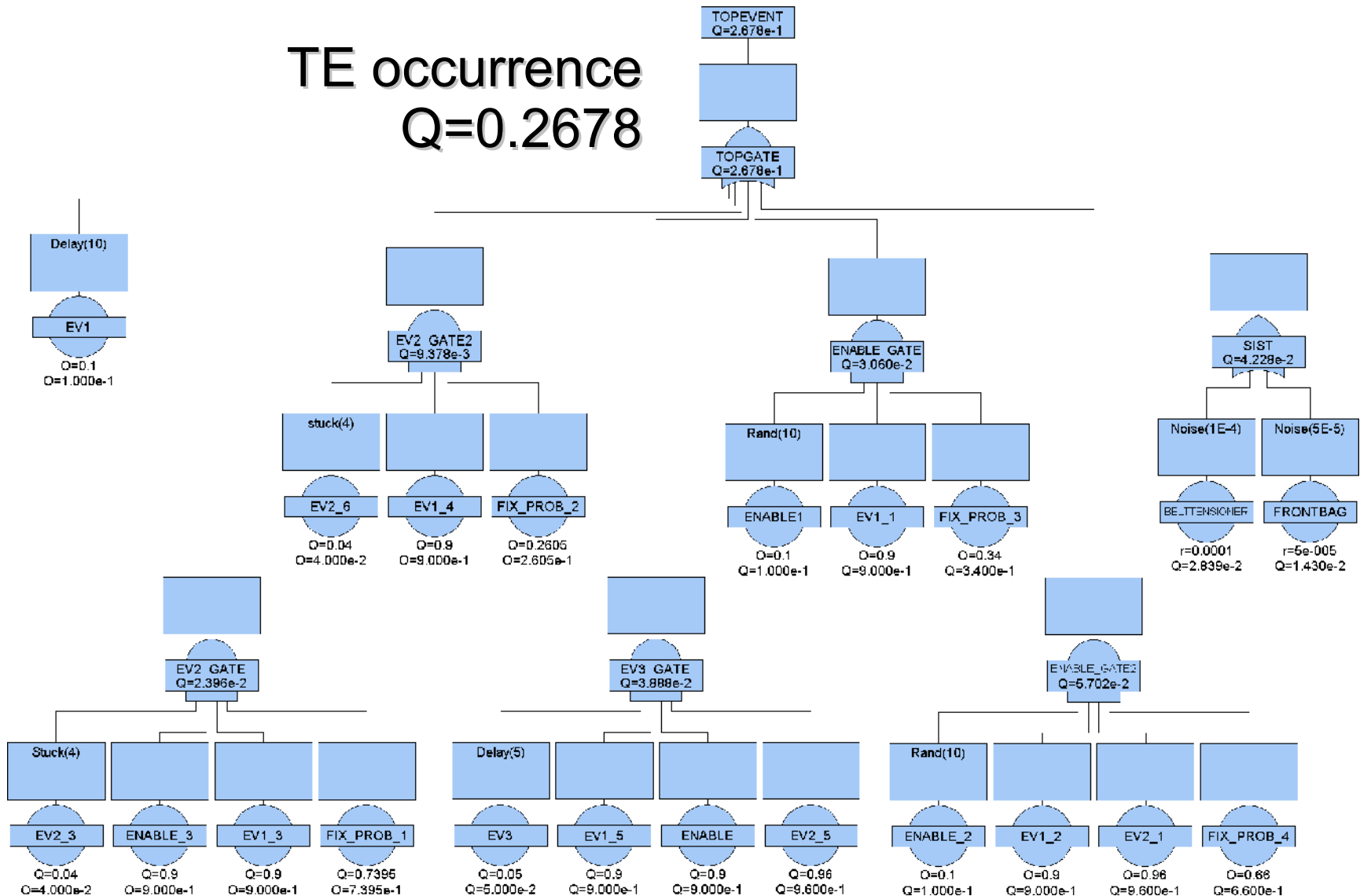
Use Failure Diagram for Failure Analysis w/ FaultTree+



$\overline{Event}$ denotes failure of action/variable Event



TE occurrence
 $Q=0.2678$





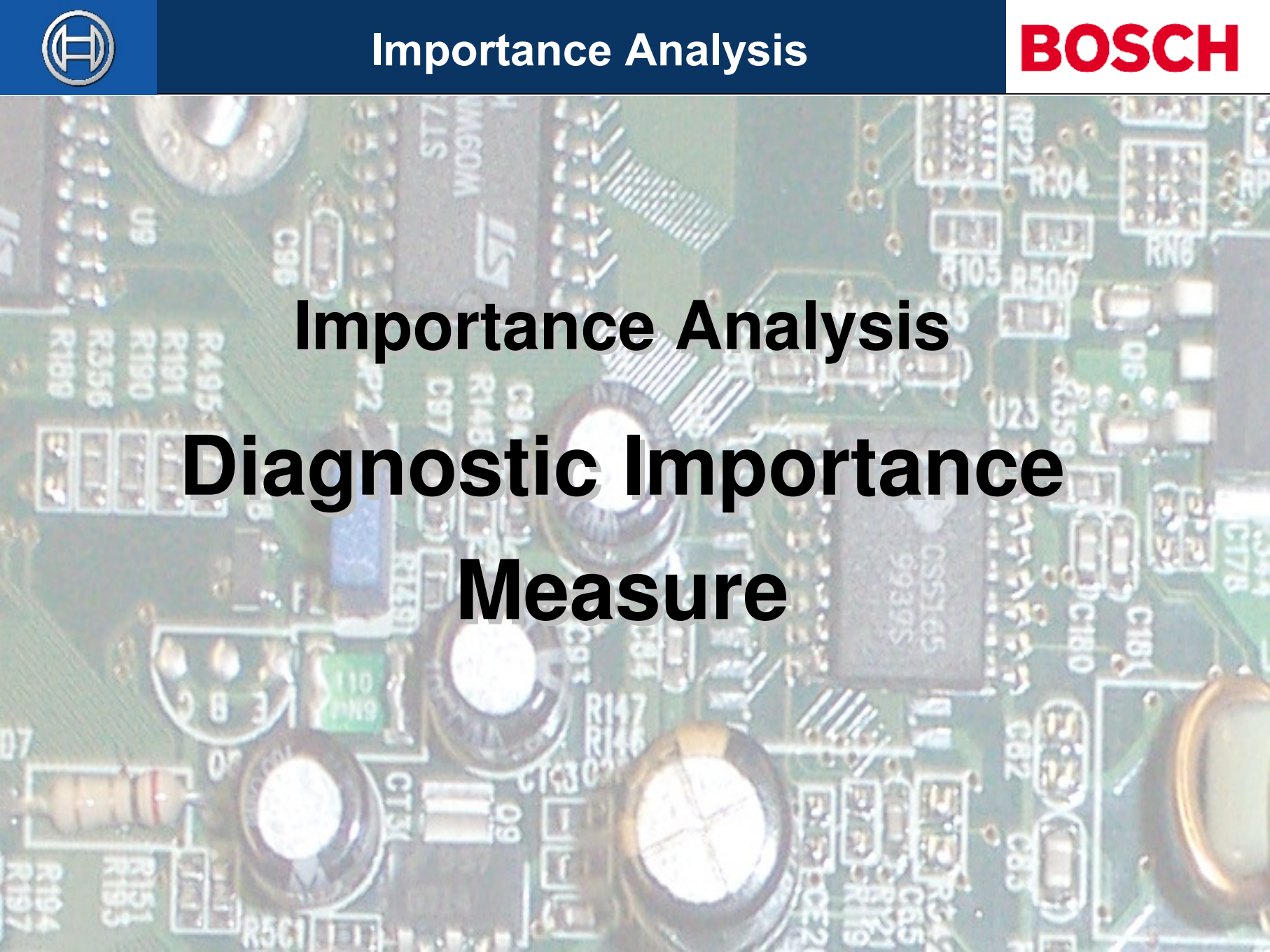
Advantages

- Feasibility of automating **Fault Tree Generation**
- Discrete Event simulation over 1 time unit is fast
- Traces not seen during simulation hardly contribute to the final TE probability
- Reflect realistic model behavior including recovery

Drawbacks

- Analysis of the simulation trace was done by hand
need for appropriate parsing mechanism



The background of the slide is a detailed, close-up photograph of a green printed circuit board (PCB). It is densely packed with various electronic components, including integrated circuits, resistors, capacitors, and inductors. Numerous component labels are visible, such as 'U9', 'R190', 'R191', 'R194', 'R197', 'R199', 'R200', 'R201', 'R202', 'R203', 'R204', 'R205', 'R206', 'R207', 'R208', 'R209', 'R210', 'R211', 'R212', 'R213', 'R214', 'R215', 'R216', 'R217', 'R218', 'R219', 'R220', 'R221', 'R222', 'R223', 'R224', 'R225', 'R226', 'R227', 'R228', 'R229', 'R230', 'R231', 'R232', 'R233', 'R234', 'R235', 'R236', 'R237', 'R238', 'R239', 'R240', 'R241', 'R242', 'R243', 'R244', 'R245', 'R246', 'R247', 'R248', 'R249', 'R250', 'R251', 'R252', 'R253', 'R254', 'R255', 'R256', 'R257', 'R258', 'R259', 'R260', 'R261', 'R262', 'R263', 'R264', 'R265', 'R266', 'R267', 'R268', 'R269', 'R270', 'R271', 'R272', 'R273', 'R274', 'R275', 'R276', 'R277', 'R278', 'R279', 'R280', 'R281', 'R282', 'R283', 'R284', 'R285', 'R286', 'R287', 'R288', 'R289', 'R290', 'R291', 'R292', 'R293', 'R294', 'R295', 'R296', 'R297', 'R298', 'R299', 'R300', 'R301', 'R302', 'R303', 'R304', 'R305', 'R306', 'R307', 'R308', 'R309', 'R310', 'R311', 'R312', 'R313', 'R314', 'R315', 'R316', 'R317', 'R318', 'R319', 'R320', 'R321', 'R322', 'R323', 'R324', 'R325', 'R326', 'R327', 'R328', 'R329', 'R330', 'R331', 'R332', 'R333', 'R334', 'R335', 'R336', 'R337', 'R338', 'R339', 'R340', 'R341', 'R342', 'R343', 'R344', 'R345', 'R346', 'R347', 'R348', 'R349', 'R350', 'R351', 'R352', 'R353', 'R354', 'R355', 'R356', 'R357', 'R358', 'R359', 'R360', 'R361', 'R362', 'R363', 'R364', 'R365', 'R366', 'R367', 'R368', 'R369', 'R370', 'R371', 'R372', 'R373', 'R374', 'R375', 'R376', 'R377', 'R378', 'R379', 'R380', 'R381', 'R382', 'R383', 'R384', 'R385', 'R386', 'R387', 'R388', 'R389', 'R390', 'R391', 'R392', 'R393', 'R394', 'R395', 'R396', 'R397', 'R398', 'R399', 'R400', 'R401', 'R402', 'R403', 'R404', 'R405', 'R406', 'R407', 'R408', 'R409', 'R410', 'R411', 'R412', 'R413', 'R414', 'R415', 'R416', 'R417', 'R418', 'R419', 'R420', 'R421', 'R422', 'R423', 'R424', 'R425', 'R426', 'R427', 'R428', 'R429', 'R430', 'R431', 'R432', 'R433', 'R434', 'R435', 'R436', 'R437', 'R438', 'R439', 'R440', 'R441', 'R442', 'R443', 'R444', 'R445', 'R446', 'R447', 'R448', 'R449', 'R450', 'R451', 'R452', 'R453', 'R454', 'R455', 'R456', 'R457', 'R458', 'R459', 'R460', 'R461', 'R462', 'R463', 'R464', 'R465', 'R466', 'R467', 'R468', 'R469', 'R470', 'R471', 'R472', 'R473', 'R474', 'R475', 'R476', 'R477', 'R478', 'R479', 'R480', 'R481', 'R482', 'R483', 'R484', 'R485', 'R486', 'R487', 'R488', 'R489', 'R490', 'R491', 'R492', 'R493', 'R494', 'R495', 'R496', 'R497', 'R498', 'R499', 'R500', 'R501', 'R502', 'R503', 'R504', 'R505', 'R506', 'R507', 'R508', 'R509', 'R510', 'R511', 'R512', 'R513', 'R514', 'R515', 'R516', 'R517', 'R518', 'R519', 'R520', 'R521', 'R522', 'R523', 'R524', 'R525', 'R526', 'R527', 'R528', 'R529', 'R530', 'R531', 'R532', 'R533', 'R534', 'R535', 'R536', 'R537', 'R538', 'R539', 'R540', 'R541', 'R542', 'R543', 'R544', 'R545', 'R546', 'R547', 'R548', 'R549', 'R550', 'R551', 'R552', 'R553', 'R554', 'R555', 'R556', 'R557', 'R558', 'R559', 'R560', 'R561', 'R562', 'R563', 'R564', 'R565', 'R566', 'R567', 'R568', 'R569', 'R570', 'R571', 'R572', 'R573', 'R574', 'R575', 'R576', 'R577', 'R578', 'R579', 'R580', 'R581', 'R582', 'R583', 'R584', 'R585', 'R586', 'R587', 'R588', 'R589', 'R590', 'R591', 'R592', 'R593', 'R594', 'R595', 'R596', 'R597', 'R598', 'R599', 'R600', 'R601', 'R602', 'R603', 'R604', 'R605', 'R606', 'R607', 'R608', 'R609', 'R610', 'R611', 'R612', 'R613', 'R614', 'R615', 'R616', 'R617', 'R618', 'R619', 'R620', 'R621', 'R622', 'R623', 'R624', 'R625', 'R626', 'R627', 'R628', 'R629', 'R630', 'R631', 'R632', 'R633', 'R634', 'R635', 'R636', 'R637', 'R638', 'R639', 'R640', 'R641', 'R642', 'R643', 'R644', 'R645', 'R646', 'R647', 'R648', 'R649', 'R650', 'R651', 'R652', 'R653', 'R654', 'R655', 'R656', 'R657', 'R658', 'R659', 'R660', 'R661', 'R662', 'R663', 'R664', 'R665', 'R666', 'R667', 'R668', 'R669', 'R670', 'R671', 'R672', 'R673', 'R674', 'R675', 'R676', 'R677', 'R678', 'R679', 'R680', 'R681', 'R682', 'R683', 'R684', 'R685', 'R686', 'R687', 'R688', 'R689', 'R690', 'R691', 'R692', 'R693', 'R694', 'R695', 'R696', 'R697', 'R698', 'R699', 'R700', 'R701', 'R702', 'R703', 'R704', 'R705', 'R706', 'R707', 'R708', 'R709', 'R710', 'R711', 'R712', 'R713', 'R714', 'R715', 'R716', 'R717', 'R718', 'R719', 'R720', 'R721', 'R722', 'R723', 'R724', 'R725', 'R726', 'R727', 'R728', 'R729', 'R730', 'R731', 'R732', 'R733', 'R734', 'R735', 'R736', 'R737', 'R738', 'R739', 'R740', 'R741', 'R742', 'R743', 'R744', 'R745', 'R746', 'R747', 'R748', 'R749', 'R750', 'R751', 'R752', 'R753', 'R754', 'R755', 'R756', 'R757', 'R758', 'R759', 'R760', 'R761', 'R762', 'R763', 'R764', 'R765', 'R766', 'R767', 'R768', 'R769', 'R770', 'R771', 'R772', 'R773', 'R774', 'R775', 'R776', 'R777', 'R778', 'R779', 'R780', 'R781', 'R782', 'R783', 'R784', 'R785', 'R786', 'R787', 'R788', 'R789', 'R790', 'R791', 'R792', 'R793', 'R794', 'R795', 'R796', 'R797', 'R798', 'R799', 'R800', 'R801', 'R802', 'R803', 'R804', 'R805', 'R806', 'R807', 'R808', 'R809', 'R810', 'R811', 'R812', 'R813', 'R814', 'R815', 'R816', 'R817', 'R818', 'R819', 'R820', 'R821', 'R822', 'R823', 'R824', 'R825', 'R826', 'R827', 'R828', 'R829', 'R830', 'R831', 'R832', 'R833', 'R834', 'R835', 'R836', 'R837', 'R838', 'R839', 'R840', 'R841', 'R842', 'R843', 'R844', 'R845', 'R846', 'R847', 'R848', 'R849', 'R850', 'R851', 'R852', 'R853', 'R854', 'R855', 'R856', 'R857', 'R858', 'R859', 'R860', 'R861', 'R862', 'R863', 'R864', 'R865', 'R866', 'R867', 'R868', 'R869', 'R870', 'R871', 'R872', 'R873', 'R874', 'R875', 'R876', 'R877', 'R878', 'R879', 'R880', 'R881', 'R882', 'R883', 'R884', 'R885', 'R886', 'R887', 'R888', 'R889', 'R890', 'R891', 'R892', 'R893', 'R894', 'R895', 'R896', 'R897', 'R898', 'R899', 'R900', 'R901', 'R902', 'R903', 'R904', 'R905', 'R906', 'R907', 'R908', 'R909', 'R910', 'R911', 'R912', 'R913', 'R914', 'R915', 'R916', 'R917', 'R918', 'R919', 'R920', 'R921', 'R922', 'R923', 'R924', 'R925', 'R926', 'R927', 'R928', 'R929', 'R930', 'R931', 'R932', 'R933', 'R934', 'R935', 'R936', 'R937', 'R938', 'R939', 'R940', 'R941', 'R942', 'R943', 'R944', 'R945', 'R946', 'R947', 'R948', 'R949', 'R950', 'R951', 'R952', 'R953', 'R954', 'R955', 'R956', 'R957', 'R958', 'R959', 'R960', 'R961', 'R962', 'R963', 'R964', 'R965', 'R966', 'R967', 'R968', 'R969', 'R970', 'R971', 'R972', 'R973', 'R974', 'R975', 'R976', 'R977', 'R978', 'R979', 'R980', 'R981', 'R982', 'R983', 'R984', 'R985', 'R986', 'R987', 'R988', 'R989', 'R990', 'R991', 'R992', 'R993', 'R994', 'R995', 'R996', 'R997', 'R998', 'R999'.

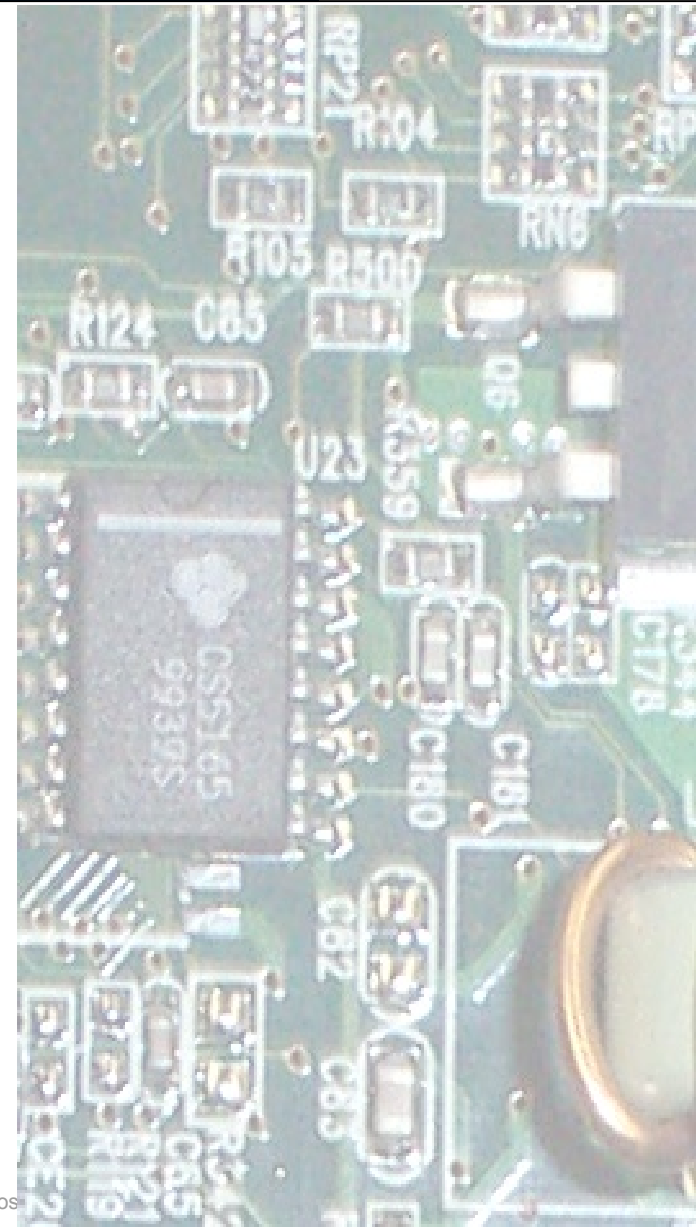
Importance Analysis

Diagnostic Importance

Measure

Safe and Failure Critical Systems

- Identity circuits in systems which have the greatest impact on the proper function of the system
- Identify gates within a circuit using Fussel-Vesely





Indicate an event's contribution to the system unavailability

$$I_D(i) = \frac{Q_{system} - Q_{system}(q_i = 1)}{Q_{system}}$$

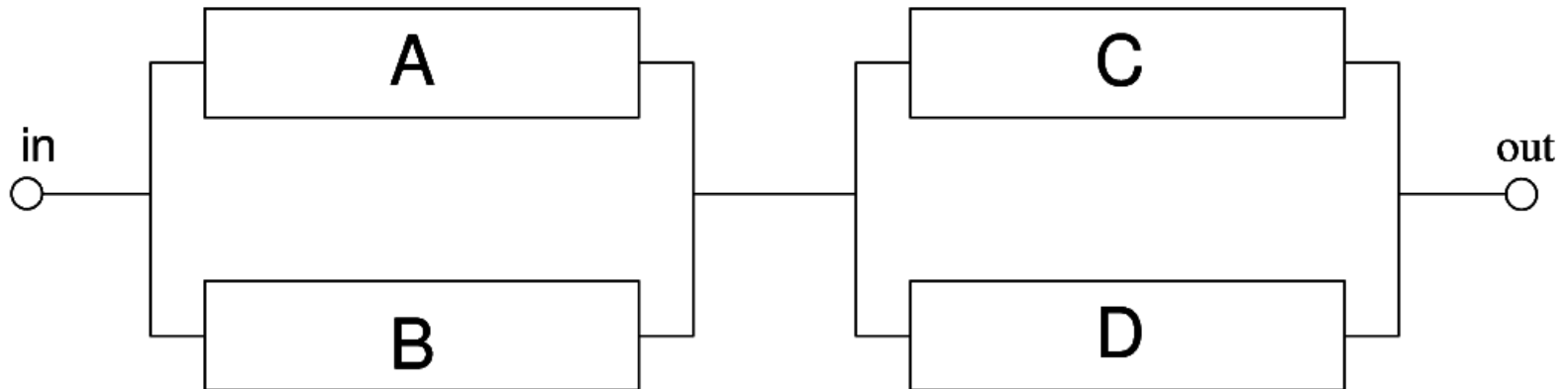
Q_{system}

Probability of the System failing

$Q_{system}(q_i = 1)$ Probability of gate i failing



Example





Obtaining the Diagnostic Importance via simulating 1 million batches

	Prob(i)	Sim DI(i)	FT+ DI(i)
A	1E-01	0,8306	0,8830
B	2E-02	0,1524	0,1670
C	3E-03	0,0031	0,0060
D	5E-01	0,9940	0,9940



Conclusion

- **A way to determine the Diagnostic Importance of gates within a circuit using simulation**
- **When using small rates many simulation runs are required**

Nuts and Bolts of Simulation

- **Versatile method for expressing complex systems like STA (Verification, Markov Chains, Failure Analysis, Importance Analysis)**
- **Even more powerful having a parser at hand**
- **Alternative approach to analyze system where state exploration fails**
- **When having small rates ($<1.0E-08$) many batches are needed for confidence**
- **No exhaustive state exploration**



- [Aue05] Marko Auerswald. SRS ECU Behavior Modeling, IST Project AMETIST. Technical report, Bosch Industrial Case Study, March 2005.
- [BHB+04] Matthias Bretschneider, Hans-Jürgen Holberg, Eckard Böde, Ingo Brückner, Thomas Peikenkamp, and Karriet Spenke. Model-based Safety Analysis of a Flap Control System. Technical report, ICOSE 2004
- [BHKK03] Henrik Bohnenkamp, Holger Hermanns, Jost-Pieter Katoen, and Ric Klaren. The MoDeST Modeling Tool and Its Implementation.
- [Bra01] Kraftfahrzeugtechnik, volume 2. Vieweg Handbuch, 2001.
- [Buc00] Kerstin Buchacker. Definition und Auswertung erweiterter Fehlerbäume für die Zuverlässigkeitsanalyse technischer Systeme. Dissertation, Universität Erlangen, Juli 2000. Band33, Nummer 3
- [DHKK01] P.R. D'Argenio, H. Hermanns, J.P. Katoen, and R. Klaren. MoDeST - a modelling and description language for stochastic timed systems.
- [Fau05] FaultTree+. Handbook and Demo-Licence, Version 11.0



- [Fau05] FaultTree+. Handbook and Demo-Licence at www.isograph-software.com, Version 11.0
- [Gra03] David. N. Gray. Gema - a general purpose macro processor.
- [Hub03] Thomas Huber. Zuverlässigkeit und Ausfallsicherheit elektronischer Systeme im Automobil. Technical report, Robert Bosch GmbH, IIR-Konferenz, 2003. Safety First - For Intelligent Restraint System Technologies.
- [LPY97] Kim G. Larsen, Paul Pettersson, and Wang Yi. Uppaal in a Nutshell. Int. Journal on Software Tools for Technology Transfer, October 1997.
- [MMT00] J. Mauss, V. May, and M. Tatar. Towards Model-based Engineering: Failure Analysis with MDS. Technical report, ECAI-2000 Workshop on Knowledge-Based Systems for Model-Based Engineering, August 2000.
- [Moc05] Ralf Mock. Risiko und Sicherheit von Netzwerken. Technical report, Laboratorium für Sicherheitsanalytik, Juni 2005. lecture notes.
- [Neu81] Marcel F. Neuts. Matrix-Geometric Solutions in Stochastic Models: An Algorithmic Approach. The John Hopkins University Press, 1981.



End

BOSCH

Thanks for paying attention

