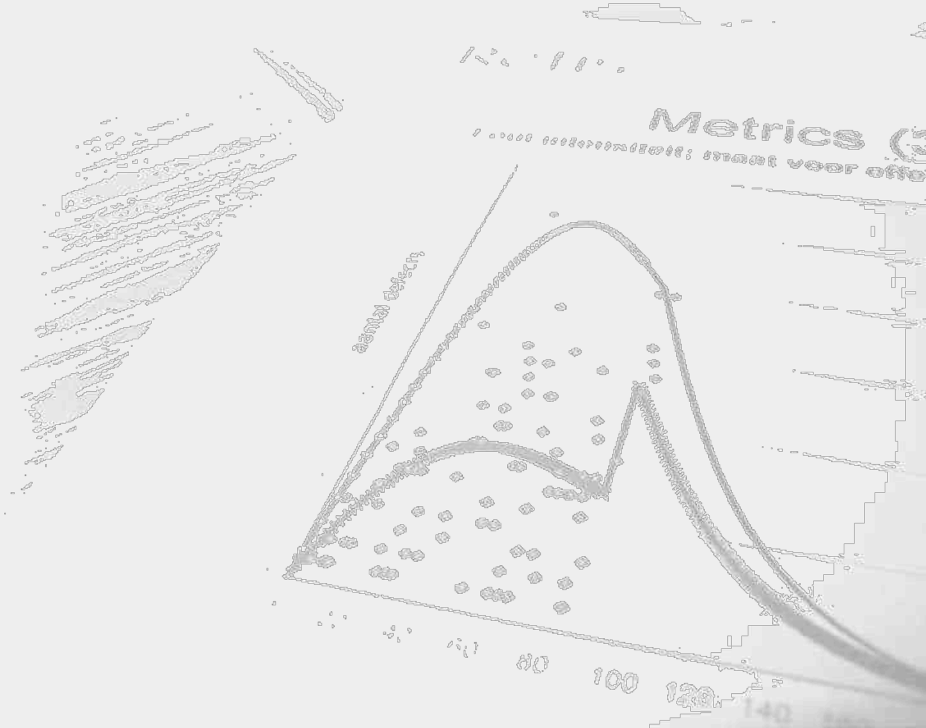
TOPAAS model

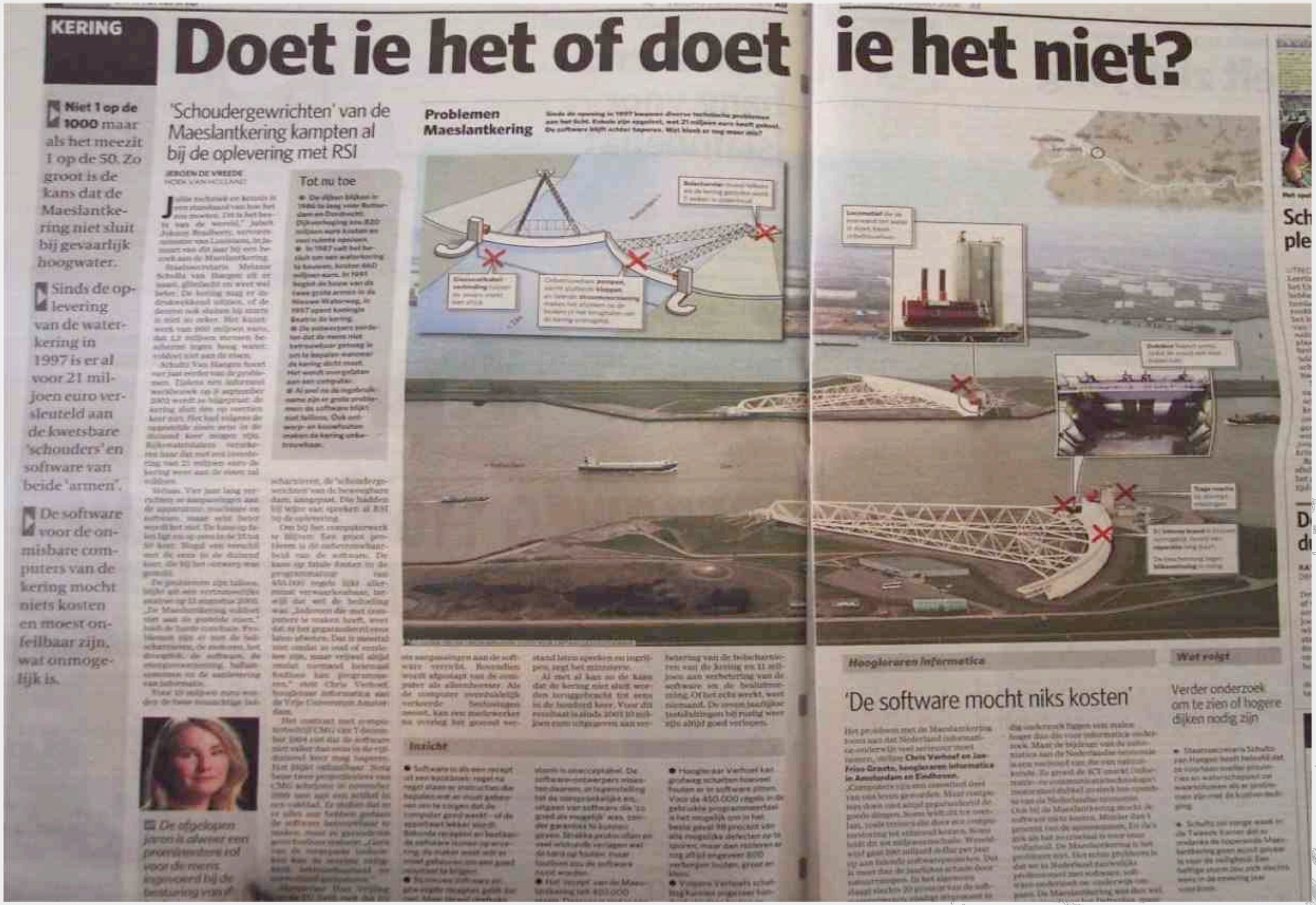
Ed Brandt

17th Dutch Testingday
November 29th 2011, TU Twente



Introduction

Refis
system reliability engineering



KERING

Doet ie het of doet ie het niet?

'Schoudergewrichten' van de Maeslantkering kampten al bij de oplevering met RSI

Niet 1 op de 1000 maar als het meezit 1 op de 50. Zo groot is de kans dat de Maeslantkering niet sluit bij gevaarlijk hoogwater.

Sinds de oplevering van de waterkering in 1997 is er al voor 21 miljoen euro versleuteld aan de kwetsbare 'schouders' en software van beide 'armen'.

De software voor de onmisbare computers van de kering mocht niets kosten en moest onfeilbaar zijn, wat onmogelijk is.

JEROEN DE VREEDE
HOEK VAN HOLLAND

[illegible]

De afgelopen jaren is alweer een prominentere rol voor de mens ingevoerd bij de besturing van de

Tot nu toe

[illegible]

Problemen Maeslantkering

[illegible]

Inzicht

[illegible]

Hoogleraren informatica

'De software mocht niks kosten'

[illegible] Chris Verhoef en Jan Friso Groote, hoogleraren informatica in Amsterdam en Eindhoven. [illegible]

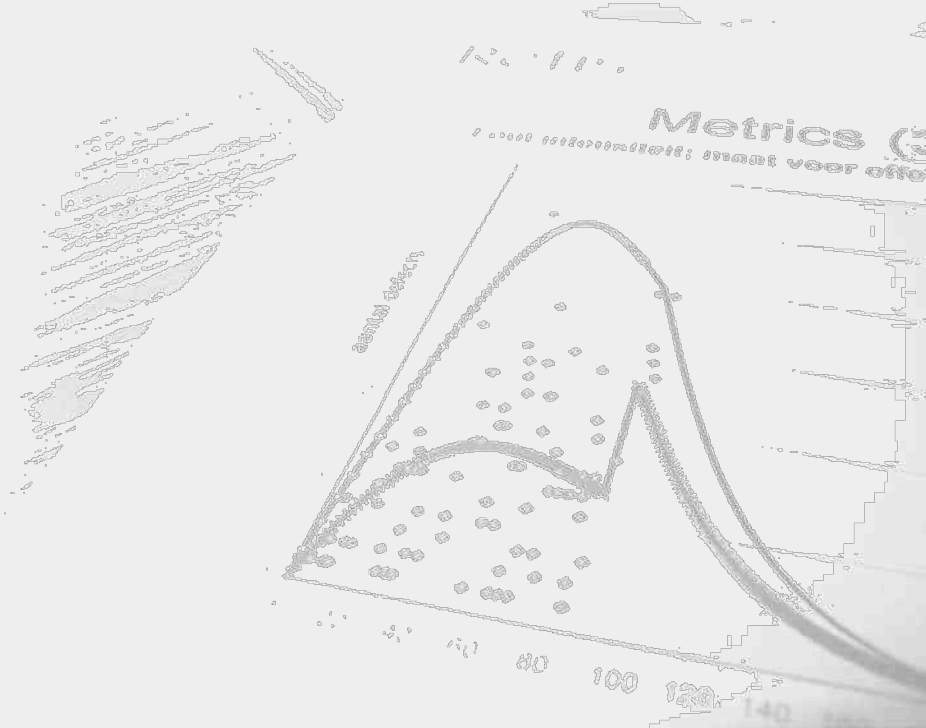
Wat volgt

Verder onderzoek om te zien of hogere dijken nodig zijn

[illegible]

Reliability analysis

- Reliability growth modelling
- Monte Carlo
- Formal methods
- IEC 61508 (Safety Integrity Levels)
- Factor driven model



Requirements

- Includes important parameters influencing software reliability
- Applicable for custom made and COTS product
- Aim at critical parts of software system
- Accepted by industry
- Supporting process management
- Free of license agreements

Result: TOPAAS-model

T ask

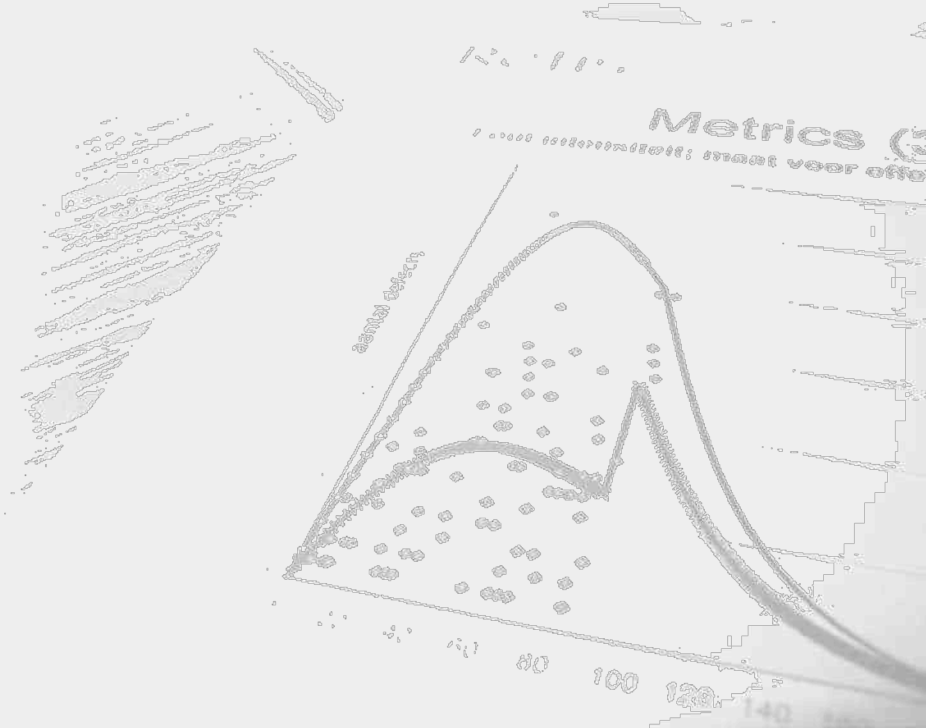
O riented

P robability
of

A bnormalities

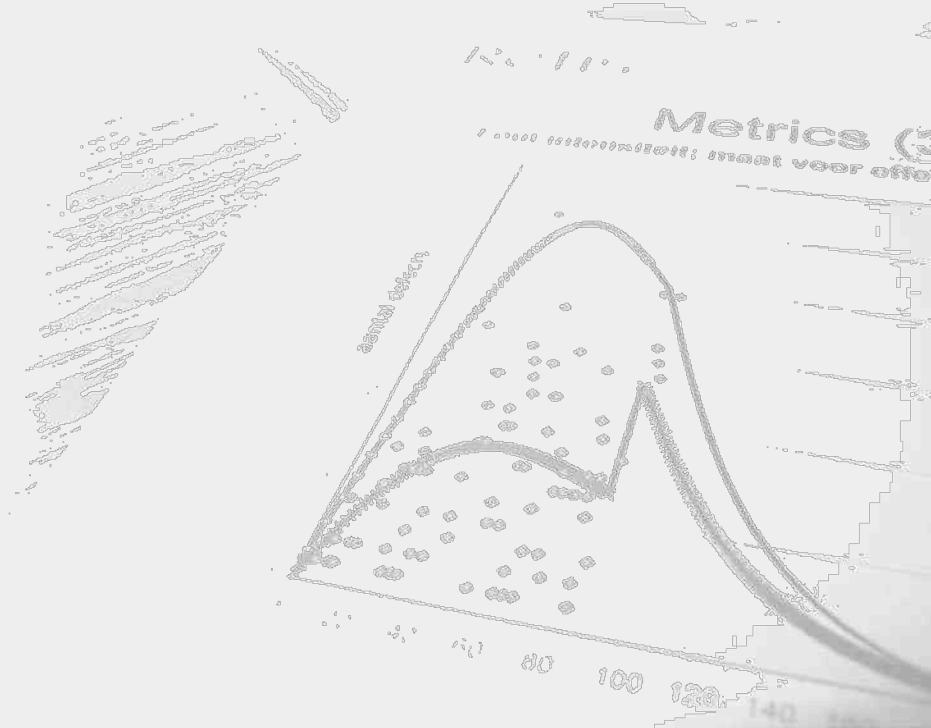
A nalysis
for

S oftware



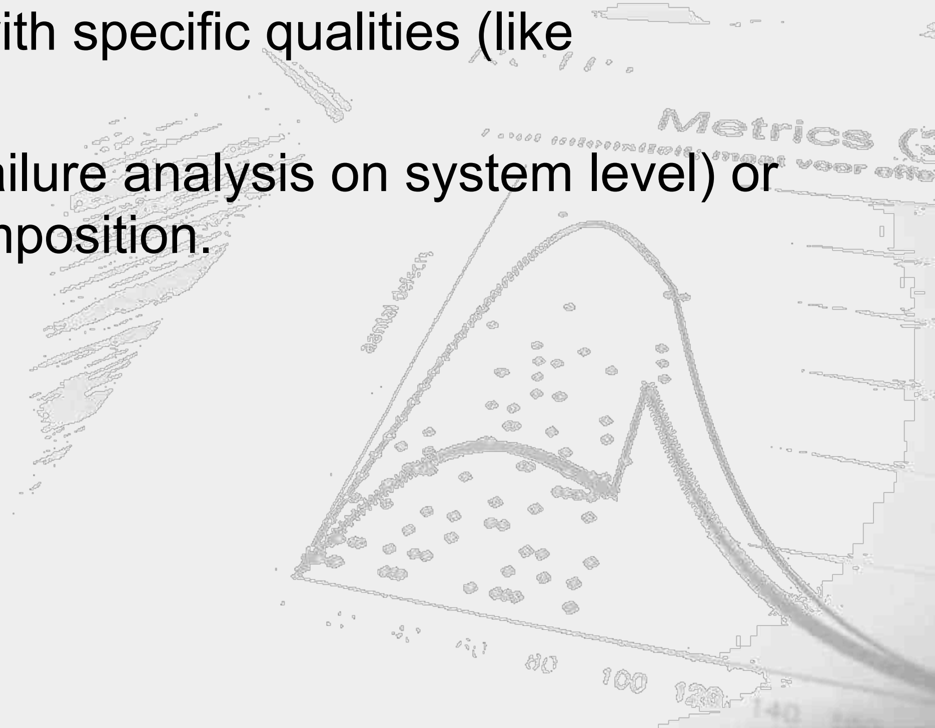
Software failure

- the absence (for too long) of desired task execution, or the incorrect task execution, by a software module with respect to the mission of the overall system,

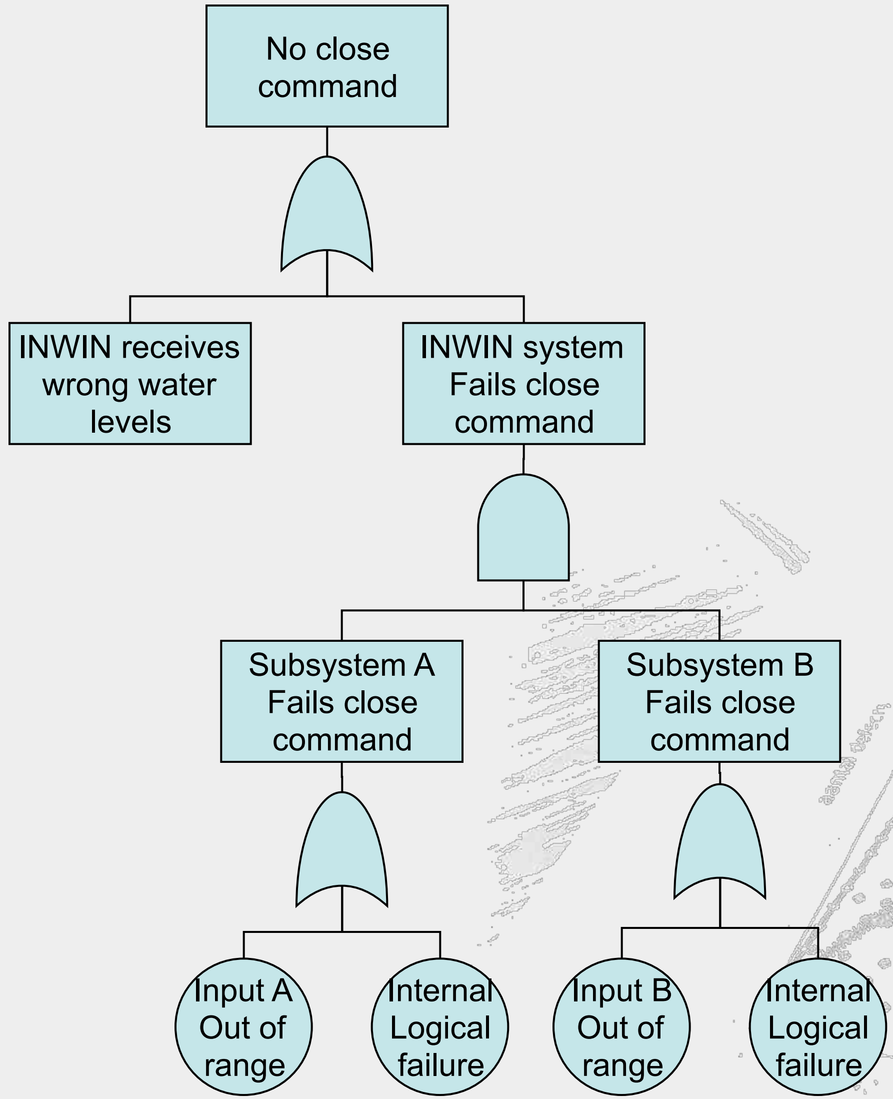


Software module

- A piece of software that is represented by a specific group of lines source code (or its graphical equivalent) with the following properties:
  - A clear distinction can be made with respect to other pieces of code and there is clear separated functionality provided by the module that is required by the system;
  - It exhibits observable behavior with specific qualities (like timeliness, reliability, etc.);
  - It isn’t useful (in the light of the failure analysis on system level) or possible to make a further decomposition.



Task Oriented



No close command

INWIN receives wrong water levels

INWIN system Fails close command

Subsystem A Fails close command

Subsystem B Fails close command

Input A Out of range

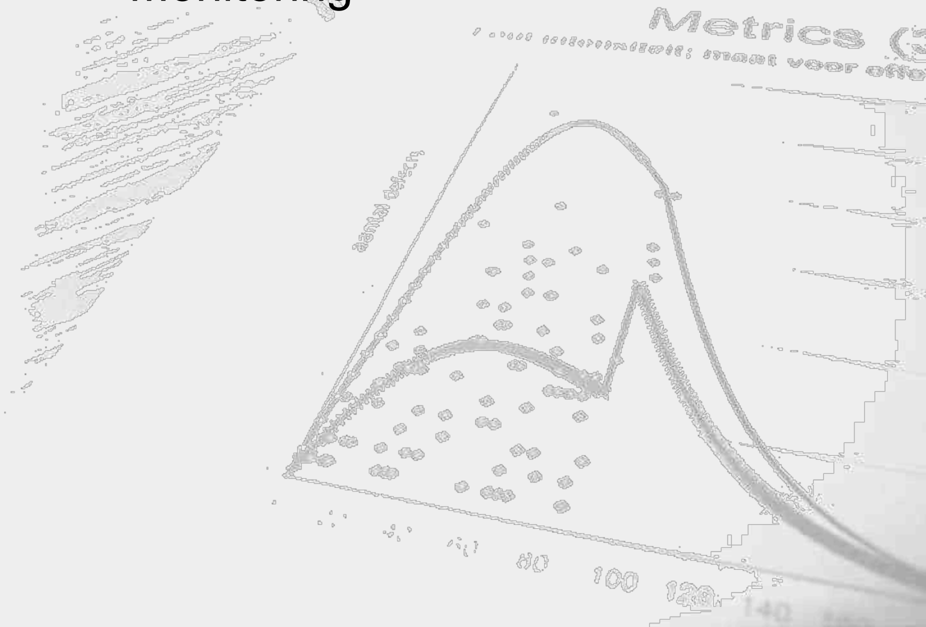
Internal Logical failure

Input B Out of range

Internal Logical failure

TOPAAS dimensions & factors

- Development process
  - Safety Integrity Level
  - Inspections
  - Design modifications
  - Maturity organisation
  - Knowledge and experience
  - Cooperation
- Product properties
  - Complexity
  - Size
  - Transparancy architecture
  - Certified compiler
- Requirements
  - traceability
- Testing
  - techniques and coverage
- Operational use
  - Multi processor
  - Field data available
  - Monitoring



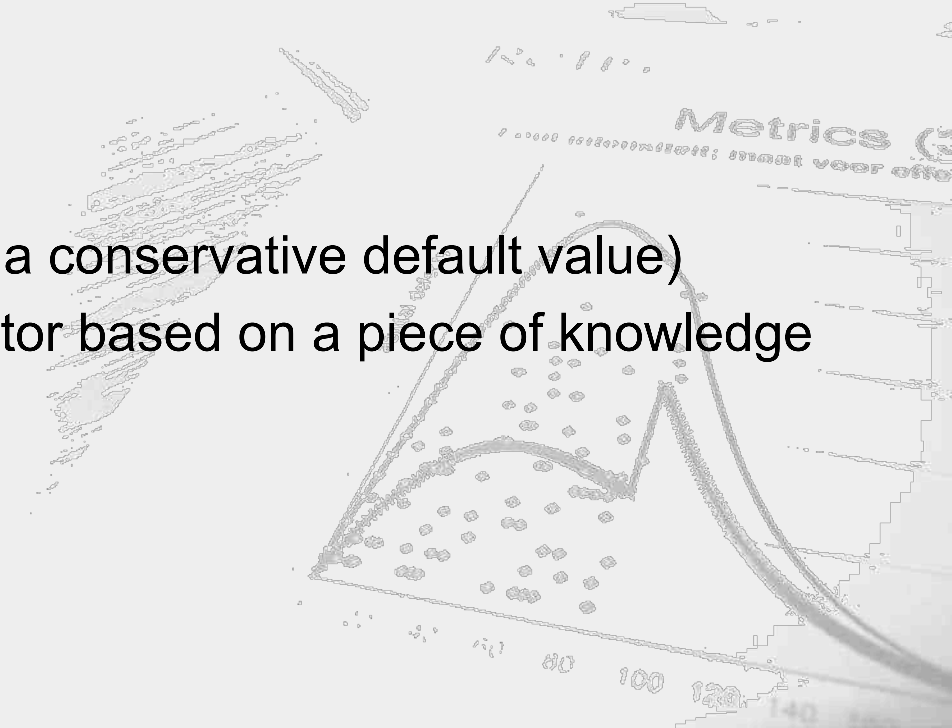
Factor driven model

- From mathematical point of view:

  factor driven model provides *n* factors *Fi* to determine failure probility *P*

  $$P = PB * F1 * F2 * ... * Fn$$

- Where
  - PB is the base failure rate (1 as a conservative default value)
  - Fx is the impact of a specific factor based on a piece of knowledge



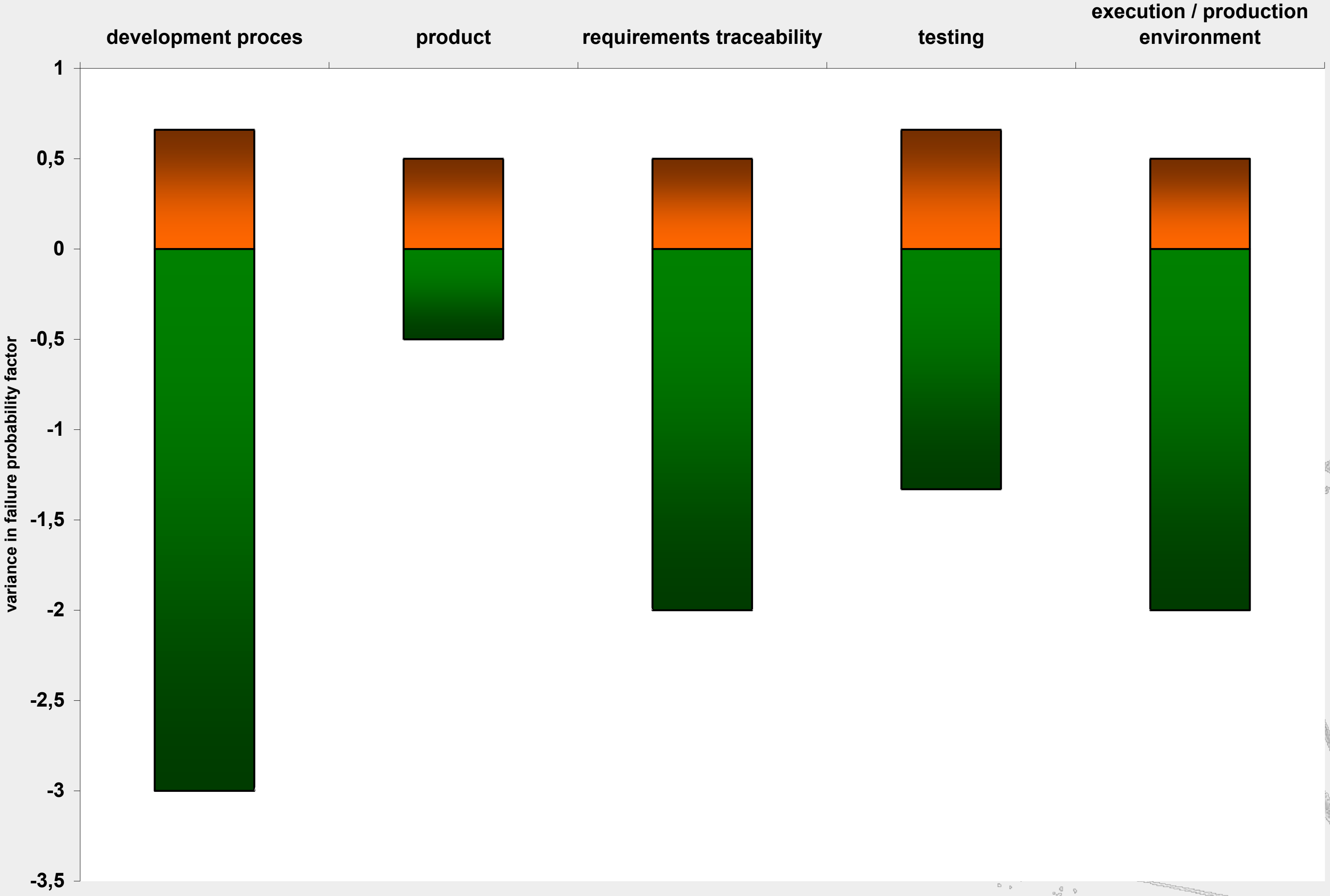
Development process

2 Inspections			
		Normal	**SIL3/SIL4**
1	unknown	0	NVT
2	No inspections performed	⅓	NVT
3	Inspections performed on design and code	0	⅓
4	Documented Fagan inspections performed	-½	0

Testing

12 Test techniques and coverage			
		Normal	**SIL3/SIL4**
1	Unknown	0	NVT
2	No documented test execution	0	NVT
3	Documented test execution, no techniques, unknown coverage	-⅓	NVT
4	Formal test techniques, low coverage	-½	⅔
5	Formal test techniques, medium coverage	-⅔	½
6	Formal test techniques, high coverage	-1	0
7	Formal test techniques, high documented coverage	-1⅓	-⅓

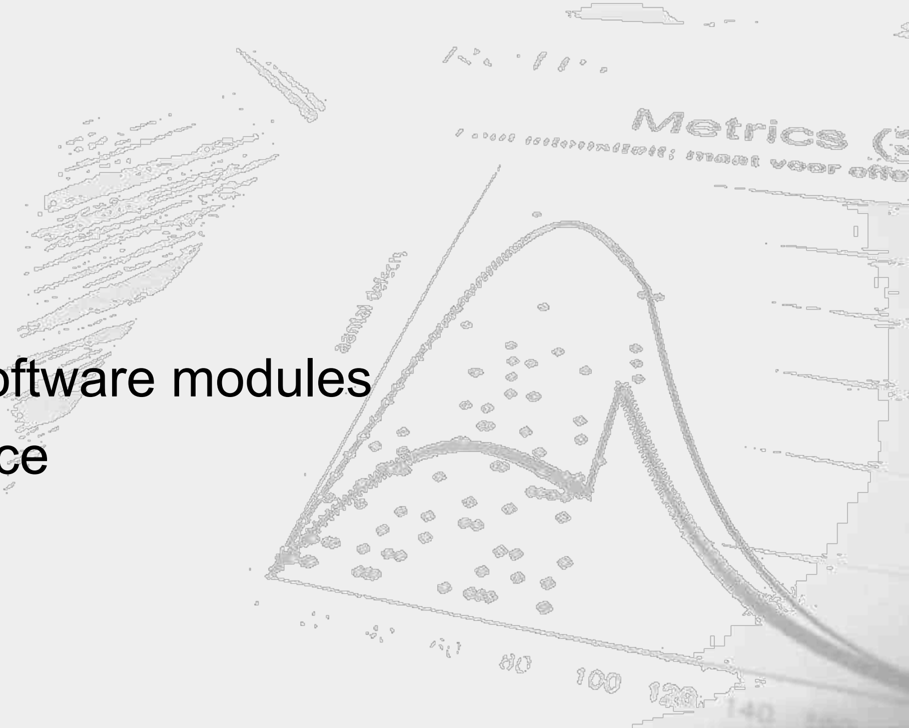
TOPAAS dimensions



Done & To be done

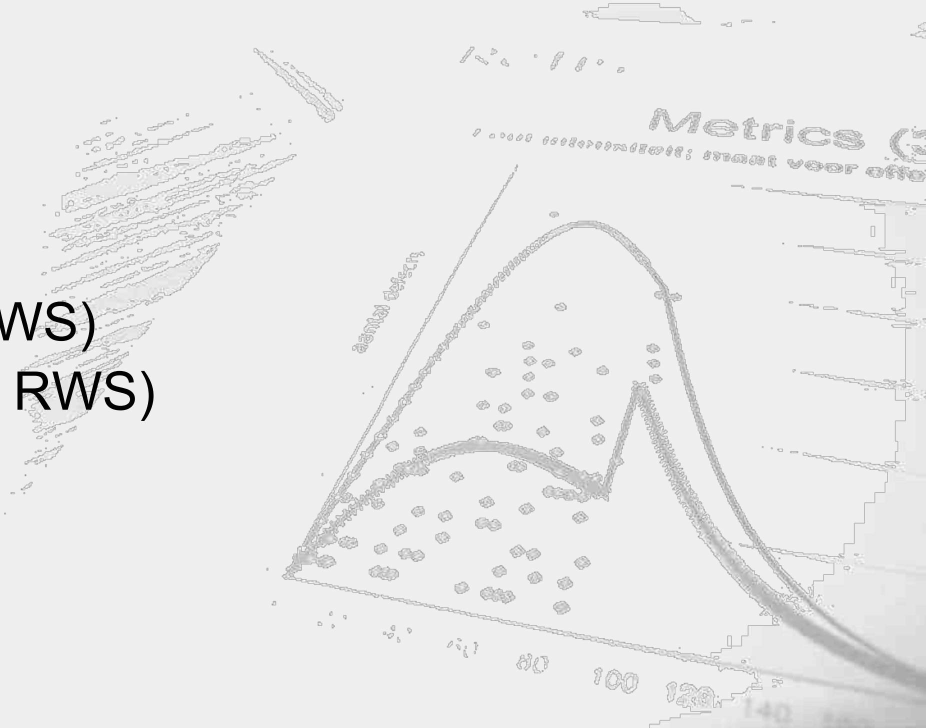
- **Done**
  - Evaluation using reference models
  - Launch version 2
  - Applied by several suppliers

- **To be done**
  - Manual & tooling
  - Broad access & usage
  - Further review & referencing
  - Calibration against statistical data
  - Investigate correlation between software modules
  - User forum and model maintenance



Credits

- **Authors**
  - Alessandro Di Bucchianico (TU/e)
  - Jaap van Ekris (DNV)
  - Jan-Friso Groote (TU/e)
  - Wouter Geurts (Logica)
  - Gerben Heslinga (Intermedion)
  - Gea Kolk (Movares)
  - Ed Brandt (Refis)
- **Reviewers**
  - Sipke van Manen (Bouwdienst RWS)
  - Harry van der Graaf (Bouwdienst RWS)
  - Peter van Gestel (Delta Pi)
  - Piet de Groot (NRG)



TOPAAS paper

- Download: http://www.refis.nl/media/artikelen.php

- Comments: edbrandt@refis.nl