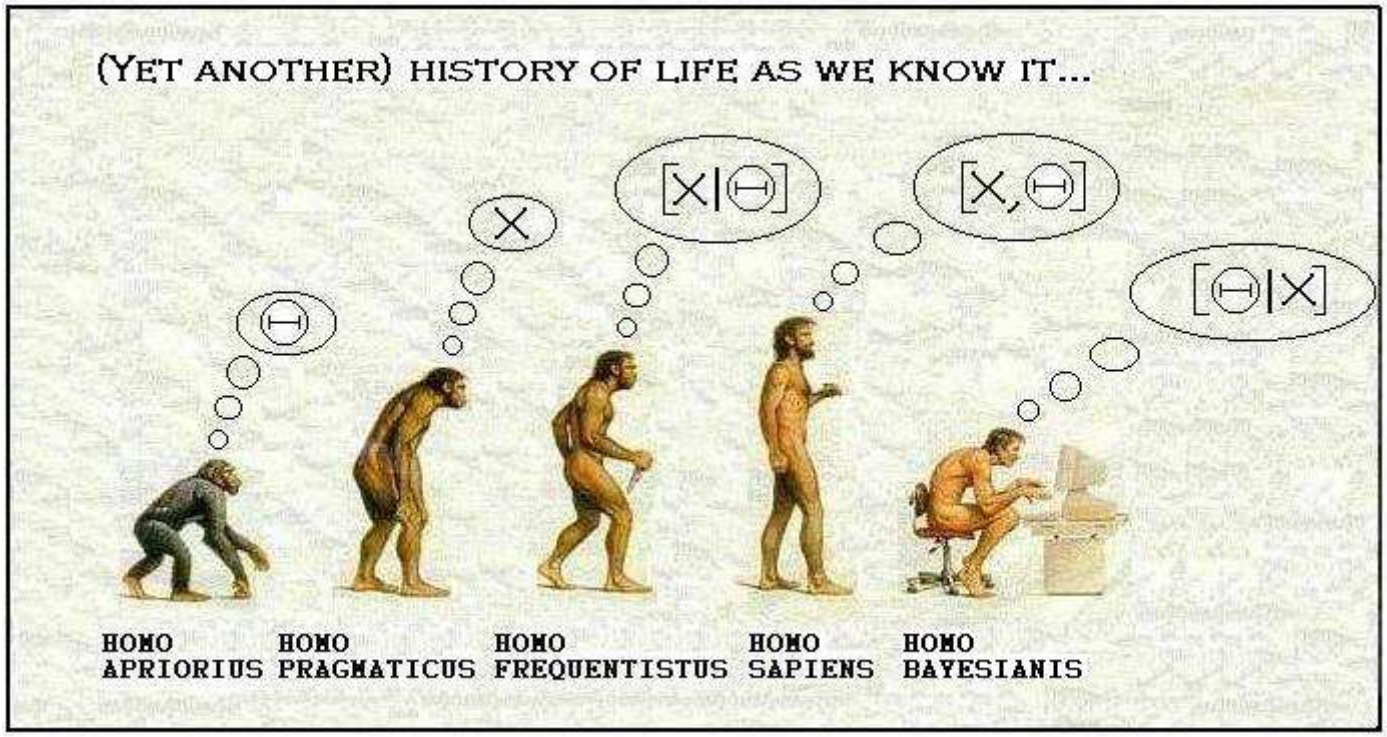
Software Safety in Context

Bayesian Belief Networks for Risk Assessments in ATM

Hans de Haan
EUROCONTROL

SW-SAF Workshop 7-8 May 2013 Luxembourg

Evolution


(YET ANOTHER) HISTORY OF LIFE AS WE KNOW IT...
HOMO APRIORIUS
HOMO PRAGMATICUS
HOMO FREQUENTISTUS
HOMO SAPIENS
HOMO BAYESIANIS

Software

What is software?

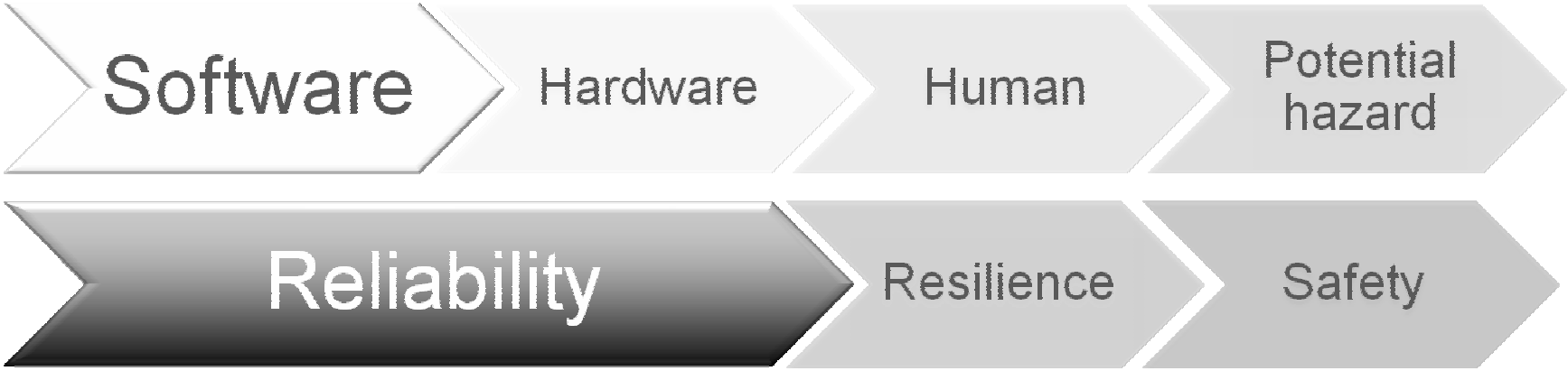
- Software is a description of computer actions
- Description is made on different abstraction levels each having their own syntax
- The semantic content, however, should be identical across all abstraction levels

Software safety

Does software safety exits?

- Software is no independent entity
  - It depends on:
    - Hardware
    - Humans
    - Context
- Therefore the concept of software safety in isolation has limited value

Software dependency in ATM



ATM Context

ATM Context Characteristics

- Socio-technical
  - Human Machine interaction plays an important role
- Complex
  - System shows self organisation and has limited predictability
- Open
  - Not all factors are under control of the system operator

Understanding the context

Causal Relationships

- Analyse causal relationships
- Assess risk
- The complexity of the system requires simplification through modeling

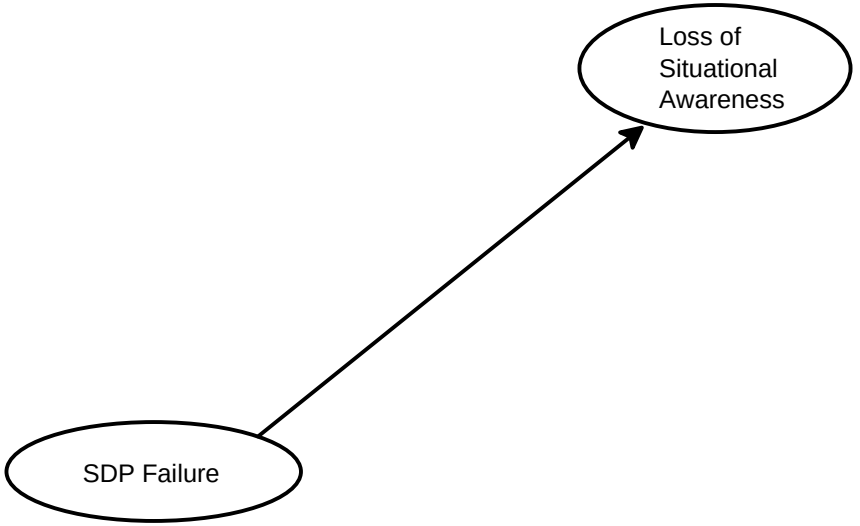
Models

Various Types of Models

- Process models
- Object models
- Data models
- Fault trees
- Causal networks

Causal Network

- Node represents an event as a random variable
- Arc represents (in this case) a causal relationship
- In words:
  - The loss of situational awareness is conditionally dependent on an SDP failure



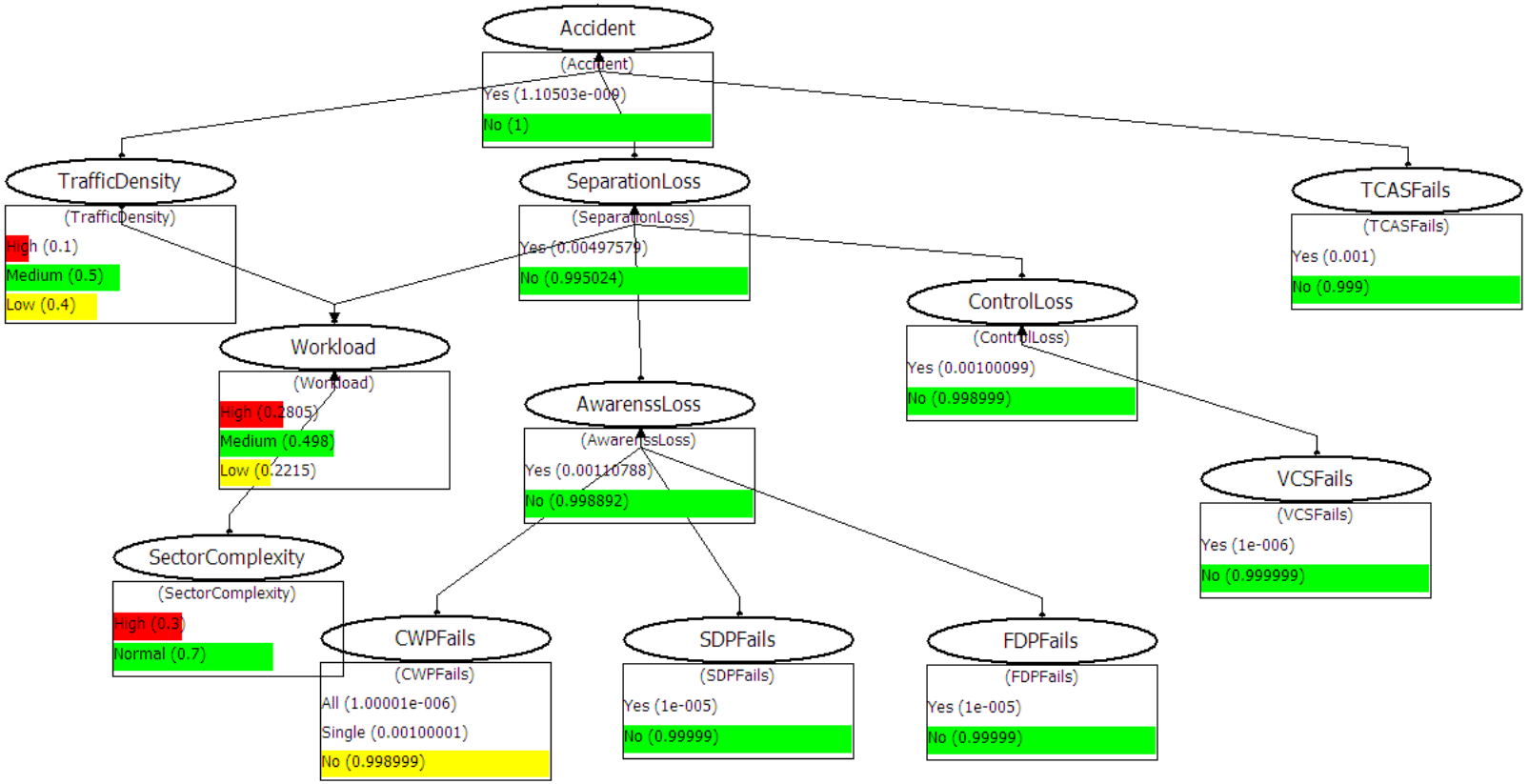
The Bayes' Theorem

- Mathematically the relationship from the previous slide is handled by the Bayes Theorem:
  - $P(A|B) = \frac{P(B|A)*P(A)}{P(B)}$
- Since we apply the theorem to events it is easy that it comes from the definition of conditional probability:
  - $P(A|B) = \frac{P(A \cap B)}{P(B)}$, if $P(B) \neq 0$
  - $P(B|A) = \frac{P(A \cap B)}{P(A)}$, if $P(A) \neq 0$
- Some definitions:
  - $P(A)$: prior probability is the probability of A before B is observed
  - $P(A|B)$: posterior probability is the probability of A after B is observed
  - $P(B|A)$: likelihood
  - $P(B)$: marginal likelihood

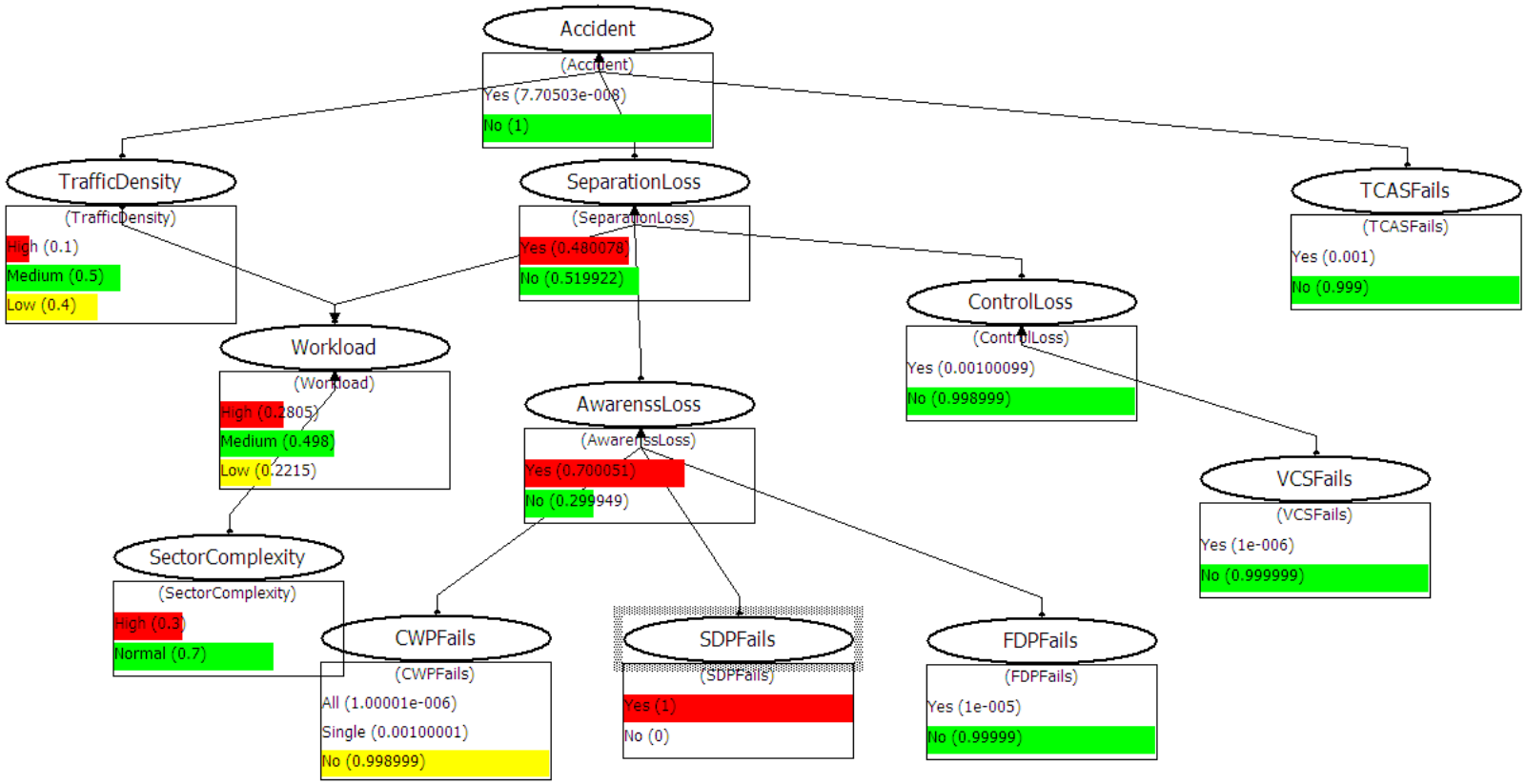
Some words of caution

- The following example is not intended to provide an accurate model of ATM operations.
- It contains both events and states. From the mathematical as well as modeling perspective, this is allowed. However, great care should be taken to avoid comparing “apples with pears”.
- Since every input adds another dimension to the conditional probability table of a node, the model should be created in a way that nodes do not contain more than 4 input arcs.

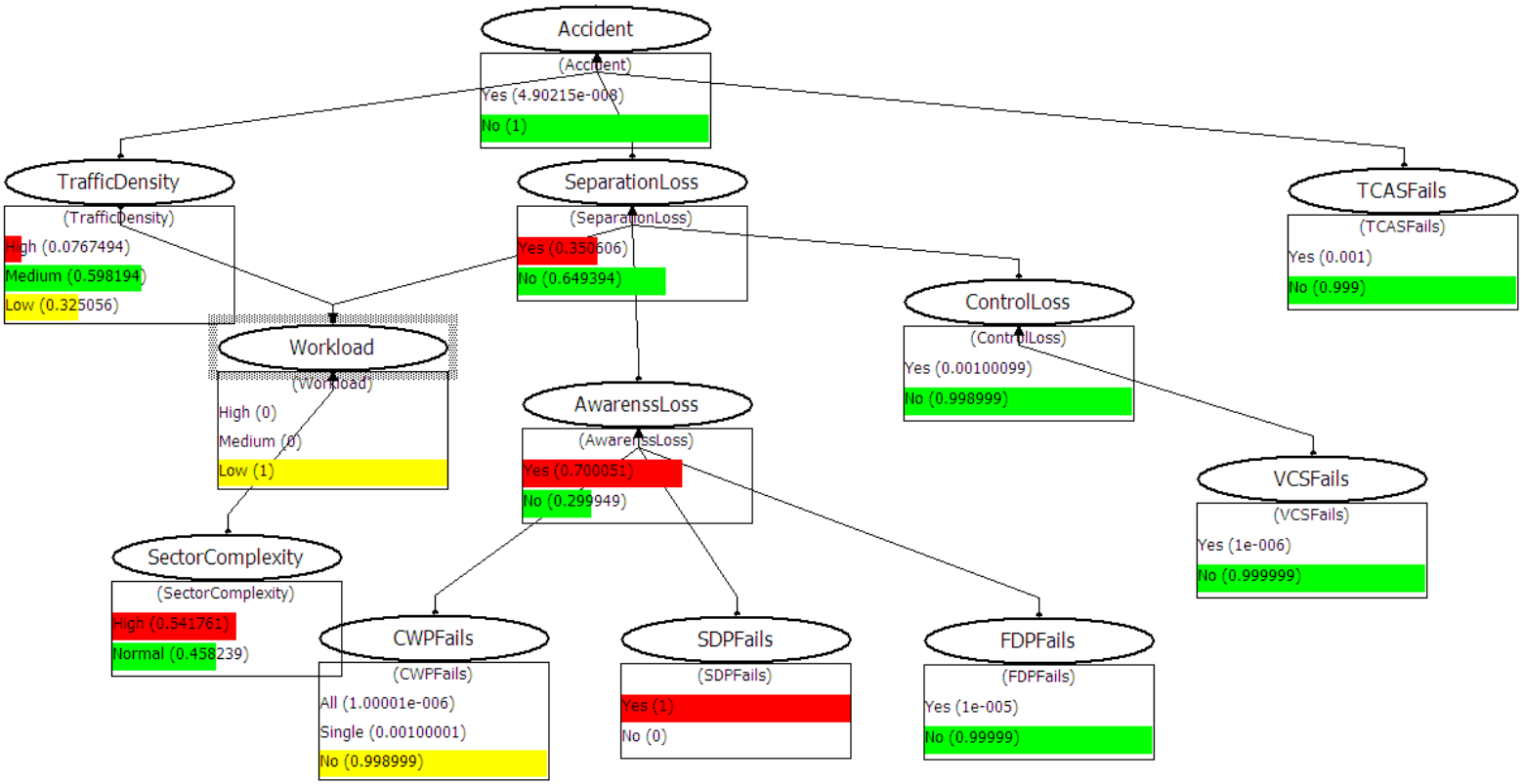
Normal situation



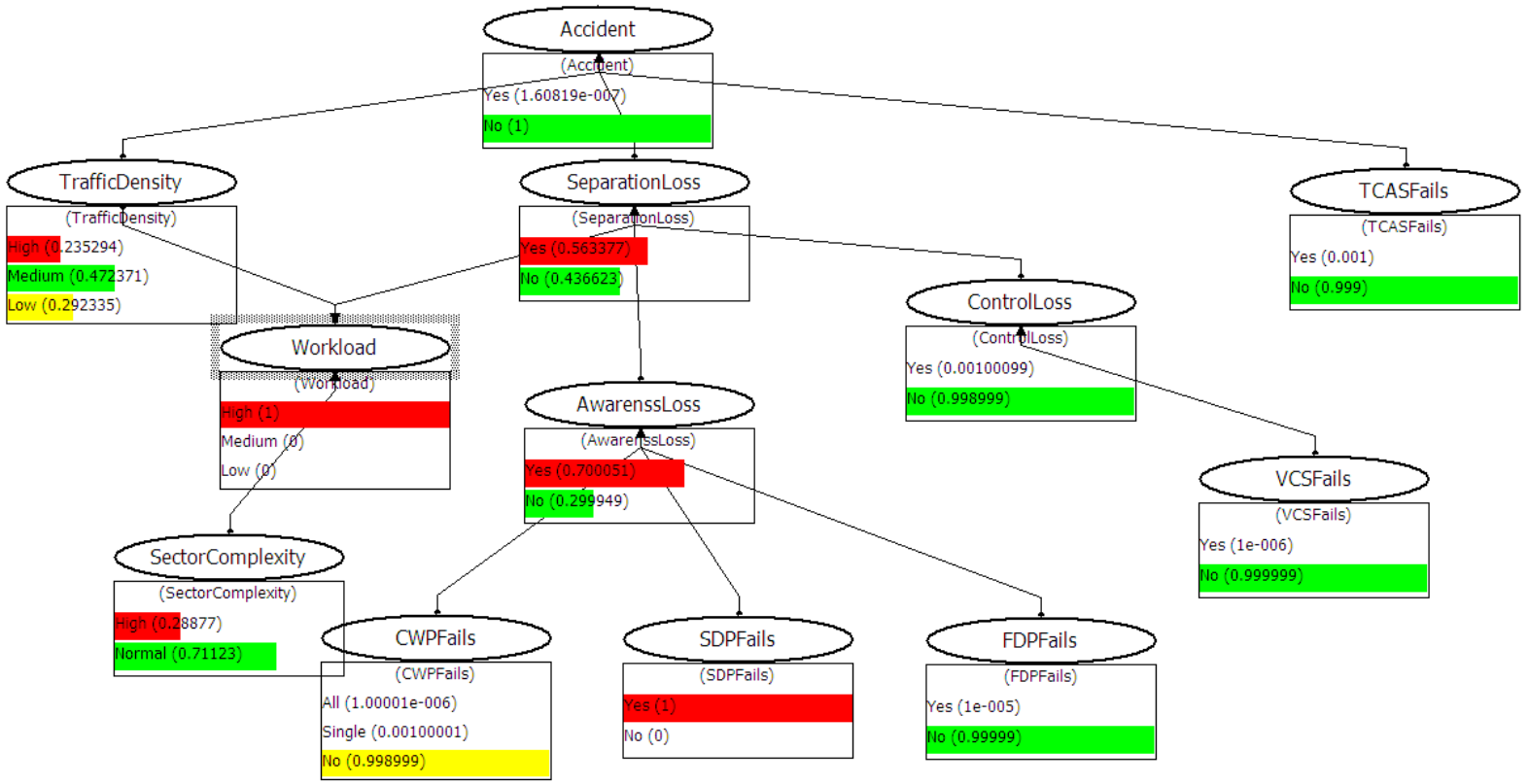
SDP fails


Accident
(Accident)
Yes (7.70503e-008)
No (1)
TrafficDensity
(TrafficDensity)
High (0.1)
Medium (0.5)
Low (0.4)
SeparationLoss
(SeparationLoss)
Yes (0.480078)
No (0.519922)
TCASFails
(TCASFails)
Yes (0.001)
No (0.999)
ControlLoss
(ControlLoss)
Yes (0.00100099)
No (0.998999)
Workload
(Workload)
High (0.2805)
Medium (0.498)
Low (0.2215)
AwarenssLoss
(AwarenssLoss)
Yes (0.700051)
No (0.299949)
VCSFails
(VCSFails)
Yes (1e-006)
No (0.999999)
SectorComplexity
(SectorComplexity)
High (0.3)
Normal (0.7)
CWPFails
(CWPFails)
All (1.00001e-006)
Single (0.00100001)
No (0.998999)
SDPFails
(SDPFails)
Yes (1)
No (0)
FDPFails
(FDPFails)
Yes (1e-005)
No (0.99999)

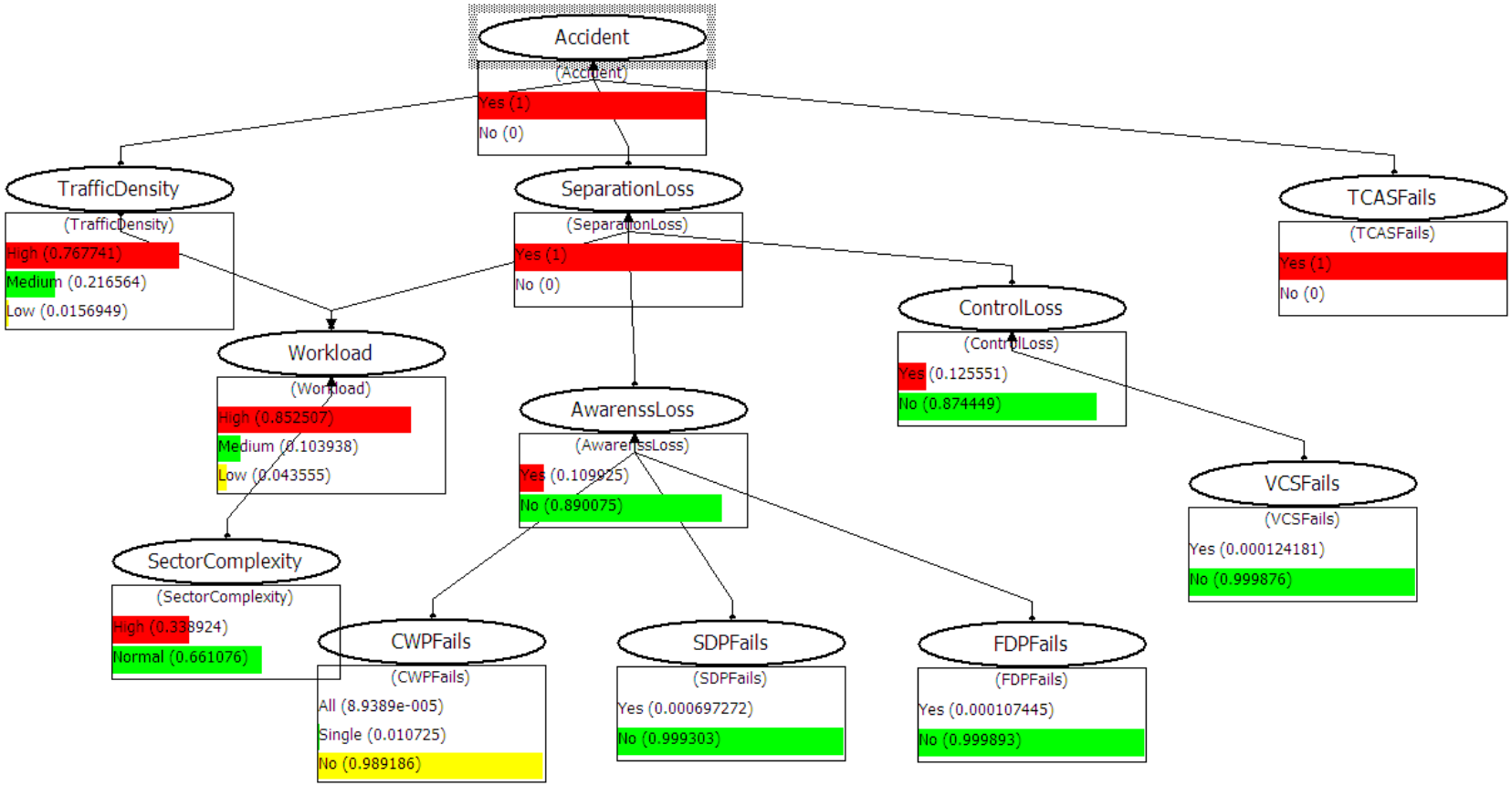
SDP fails with low traffic density



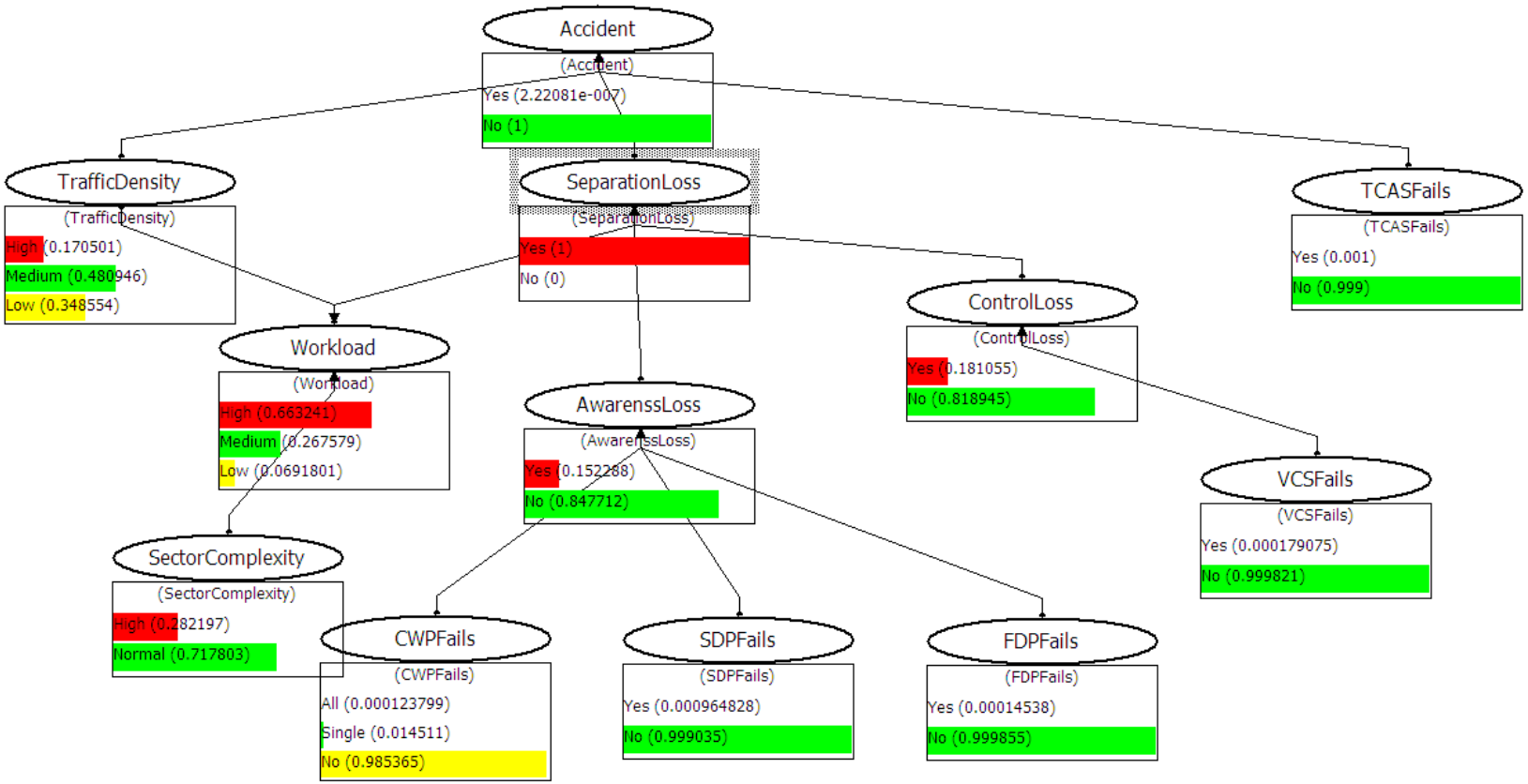
SDP fails with high traffic density



Finding the most probable cause



Finding the most probable cause



General Conclusions

- Looking at software reliability is not enough (to date none of the mid-air collisions were caused by a software reliability problem)
- It is important to understand that the “safety” of software is determined by the context in which it is used
- The resilience of the ATM system depends for a significant part on the predictability (which of course includes reliability) of the software.
- Factors that may even play a bigger role in safety than software reliability are:
  - Human Factors
  - Security Issues
- They should be taken into account when analysing the context

BBN Conclusions

- Bayesian Belief Networks are a powerful tool in helping to understand the causal relationships within the ATM system
- Understanding these relationships, will help to identify weak spots and assessing the efficiency of mitigation measures
- When the states and events are carefully defined, the BBN can be used in real-time mode as a decision aid, based on traffic and system state data.
- Bayesian Belief Networks are NOT the solution of all safety problems

Questions?

Bayesian Belief Networks for Risk Assessments in ATM

Hans de Haan
EUROCONTROL
SW-SAF Workshop 7 May 2013 Luxembourg