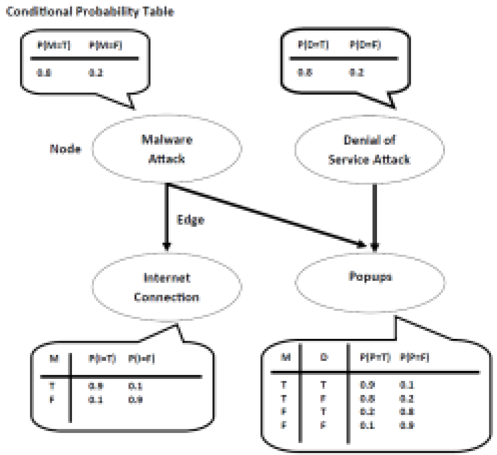
Combining Bayesian Networks and Fishbone Diagrams to Distinguish between Intentional Attacks and Accidental Technical Failures

Sabarathinam Chockalingam[1], Wolter Pieters[1], André Teixeira[2], Nima Khakzad[1] and Pieter van Gelder[1]

[1]Delft University of Technology (TUDelft), Netherlands.

[2]Uppsala University, Sweden.

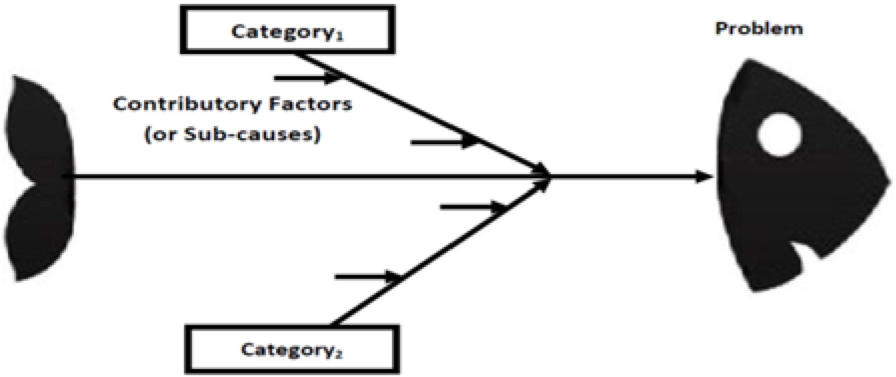


P(M=T)	P(M=F)
0.8	0.2

P(D=T)	P(D=F)
0.8	0.2

M	P(I=T)	P(I=F)
T	0.9	0.1
F	0.1	0.9

M	D	P(P=T)	P(P=F)
T	T	0.9	0.1
T	F	0.8	0.2
F	T	0.2	0.8
F	F	0.1	0.9



Presentation Outline

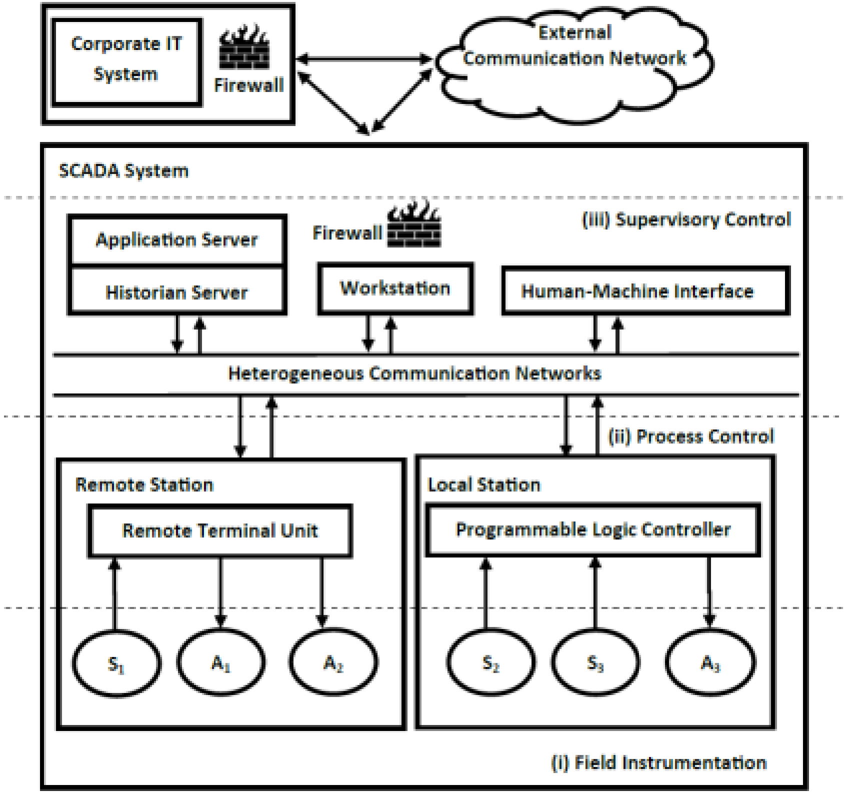
- Case Study in Water Management Domain
- Problem 1: Distinguishing Attacks and Technical Failures
- Introduction to Bayesian Networks
- Proposed BN Framework for Distinguishing Attacks and Technical Failures
- Problem 2: Knowledge Elicitation in BNs
- Introduction to Fishbone Diagrams
- Proposed Extended Fishbone Diagram for Knowledge Elicitation
- Key Takeaways

Secure Our Safety: Building Cyber Security for Flood Management (SOS4Flood) Project

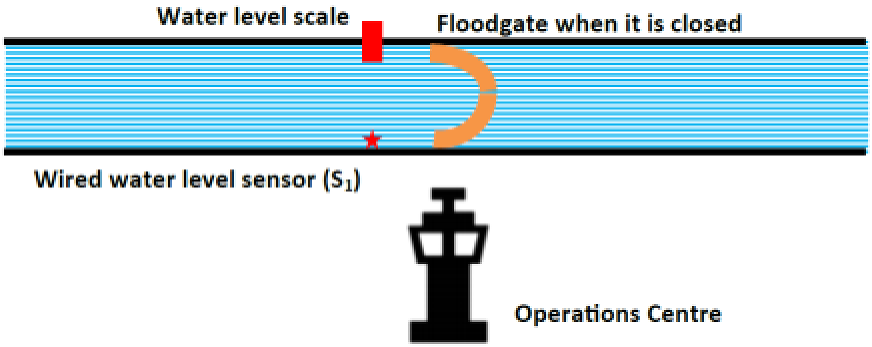
Netherlands Organisation for Scientific Research

TU Delft

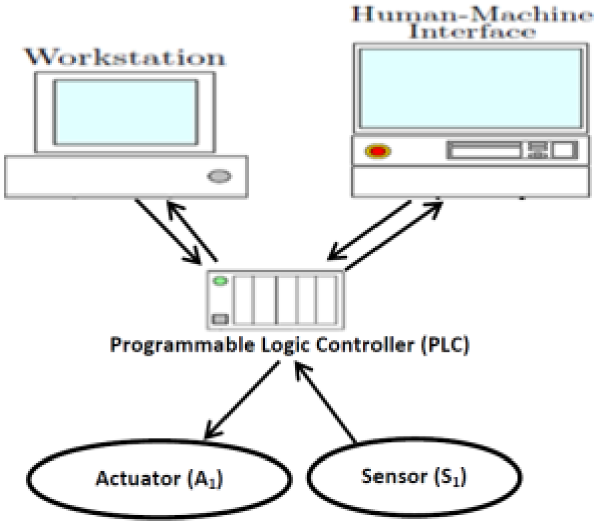
Industrial Control Systems: Typical Architecture (1/2)



Industrial Control Systems: Case Study (2/2)



Physical Layout of the Floodgate



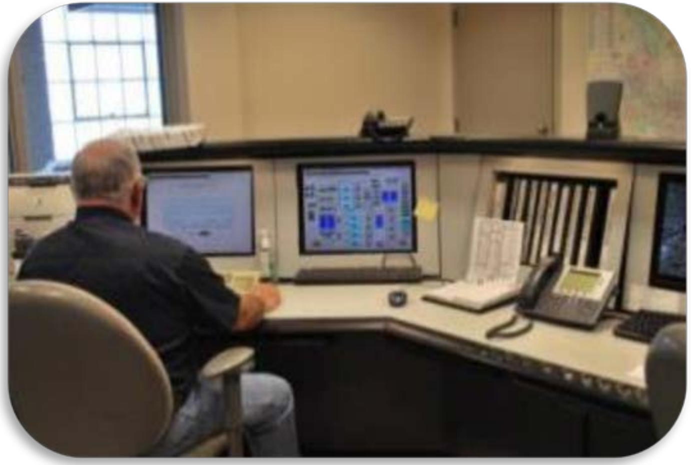
SCADA Architecture of the Floodgate

Safety vs. Security

Northeast Blackout (2003)

German Steel Mill Hack (2014)

Problem 1: Distinguishing Attacks and Technical Failures



Abnormal Behavior?

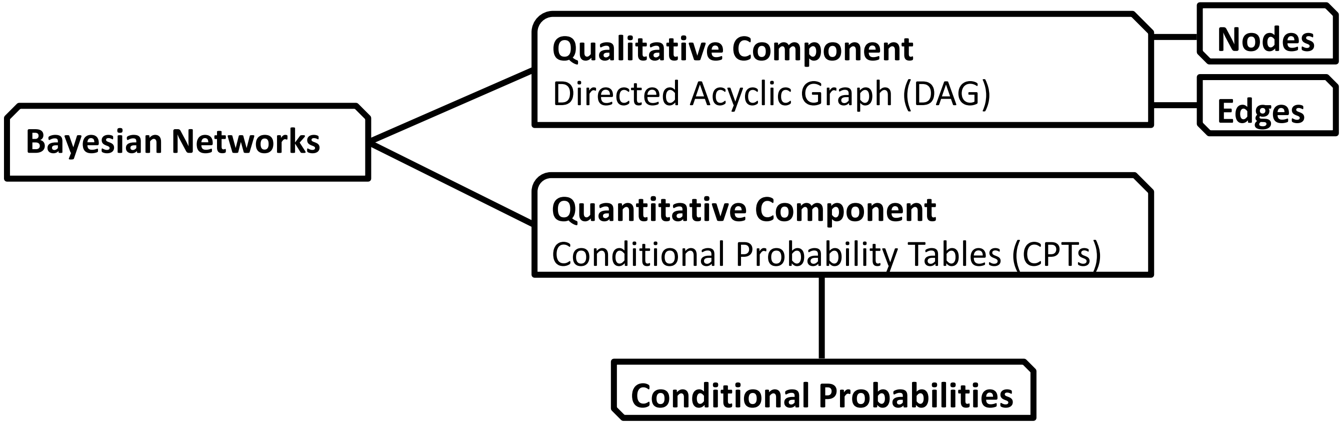
- ✓ Technical failure.
- ✓ Initiate corresponding response strategies.

Water Level Sensor

- ✗ **What about cyber-attack?**
- ✗ **Same response strategies** would be **effective** in case of a **cyber-attack**?

Lack of decision support to distinguish between intentional attacks and accidental technical failures.

Introduction to Bayesian Networks (1/2)



Bayesian Networks

Qualitative Component
Directed Acyclic Graph (DAG)

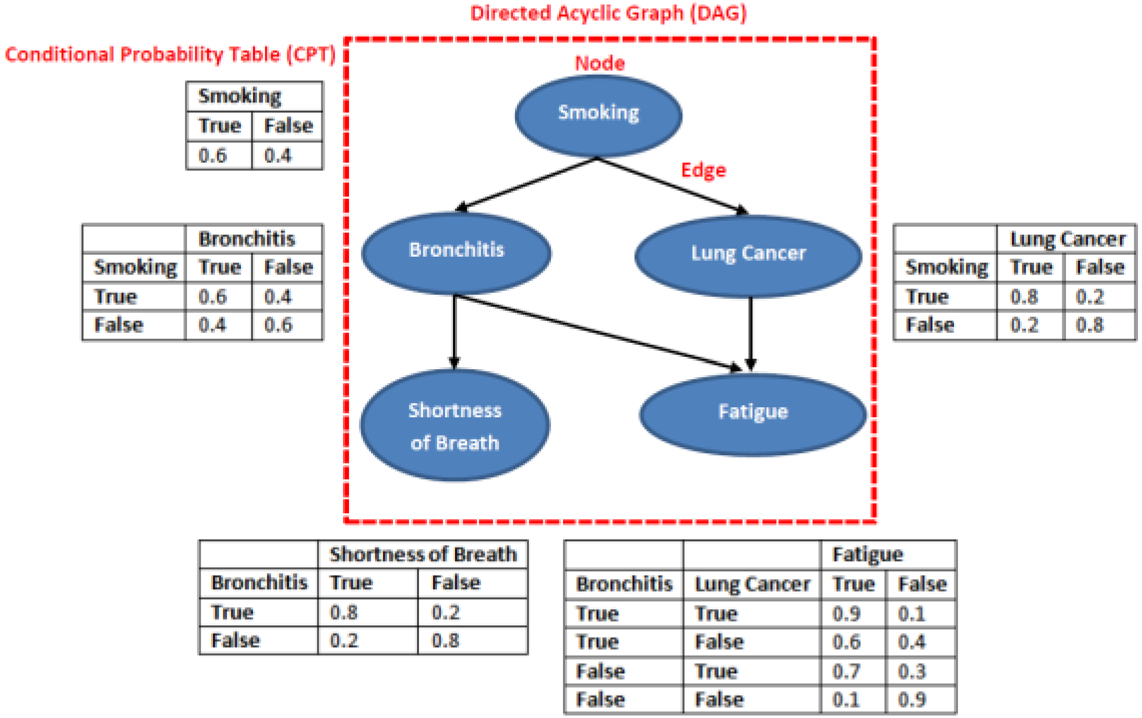
Nodes

Edges

Quantitative Component
Conditional Probability Tables (CPTs)

Conditional Probabilities

Introduction to Bayesian Networks (2/2)


Directed Acyclic Graph (DAG)
Conditional Probability Table (CPT)
Node
Smoking
Edge
Bronchitis
Lung Cancer
Shortness of Breath
Fatigue

Smoking	
True	False
0.6	0.4

	Bronchitis	
Smoking	True	False
True	0.6	0.4
False	0.4	0.6

	Lung Cancer	
Smoking	True	False
True	0.8	0.2
False	0.2	0.8

	Shortness of Breath	
Bronchitis	True	False
True	0.8	0.2
False	0.2	0.8

		Fatigue	
Bronchitis	Lung Cancer	True	False
True	True	0.9	0.1
True	False	0.6	0.4
False	True	0.7	0.3
False	False	0.1	0.9

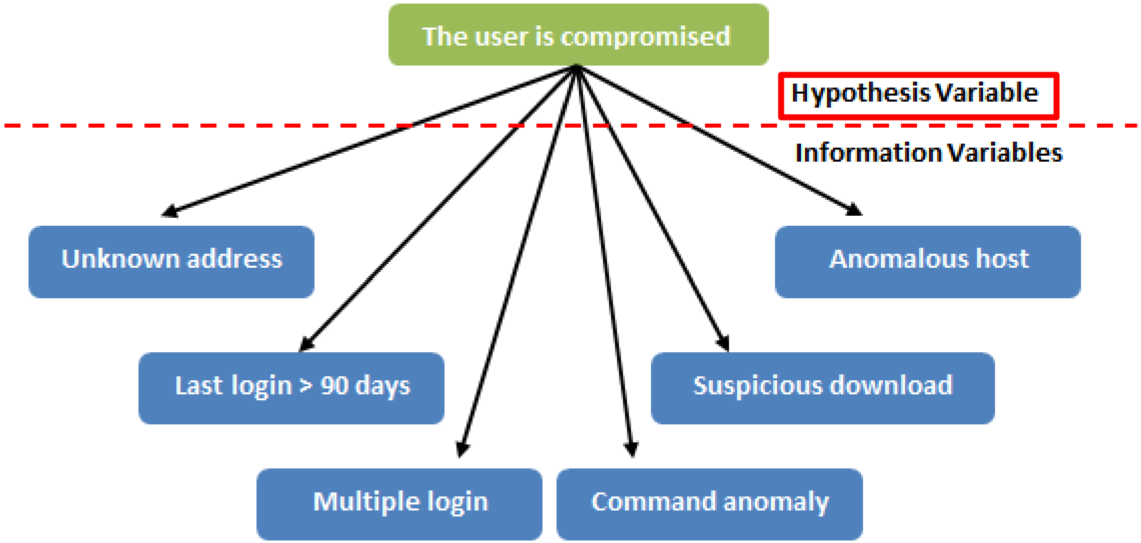
Medical Diagnosis: Example

Research Objective - 1

“To develop a framework for constructing Bayesian Network (BN) models for determining the major cause of an abnormal behavior in a component of Industrial Control Systems.”

- **Adopted and customised a set of variables from BN models used for diagnostic purposes in different domains.**

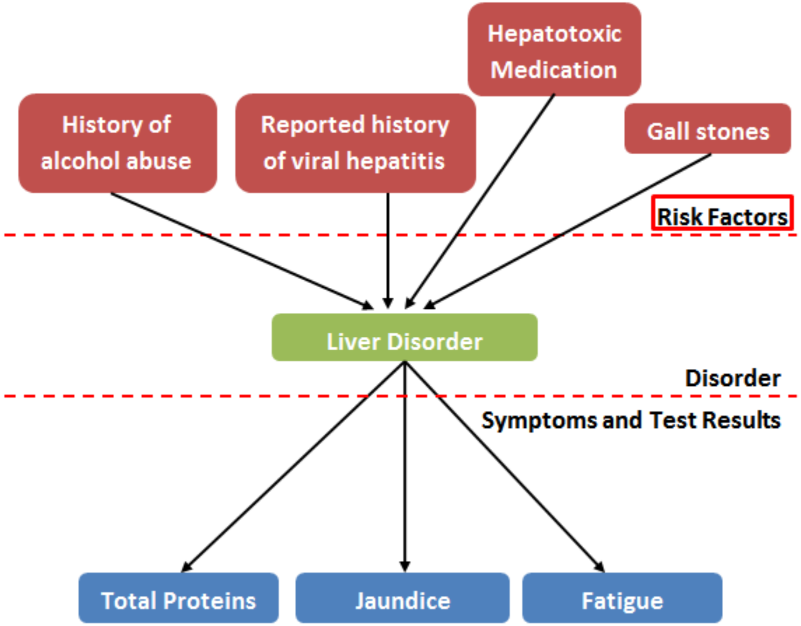
Related Work: Diagnostic BN Models (1/3)



Identifying Compromised Users in Shared Computing Infrastructure[1]

[1] Pecchia, A., Sharma, A., Kalbarczyk, Z., Cotroneo, D., Iyer, R.K.: Identifying Compromised Users in Shared Computing Infrastructures: A Data-driven Bayesian Network Approach. In: Reliable Distributed Systems (SRDS), 30th IEEE Symposium on, pp. 127-136. (2011)

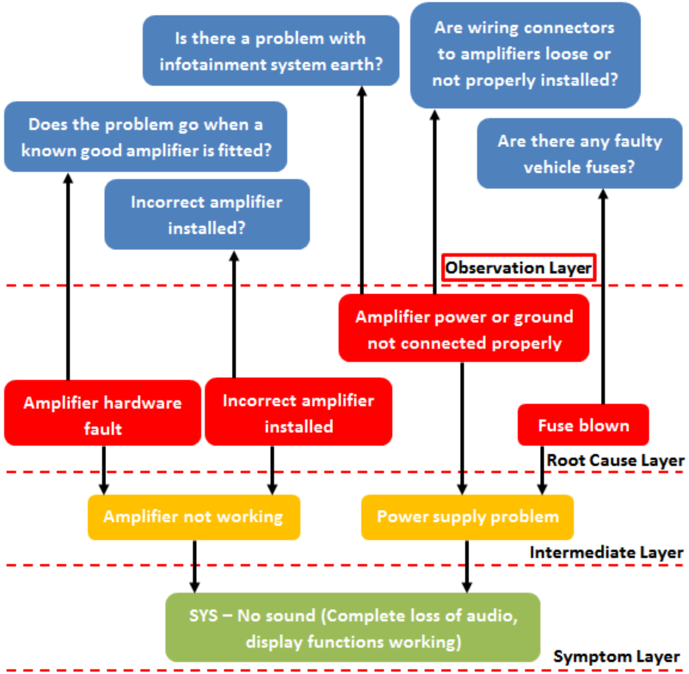
Related Work: Diagnostic BN Models (2/3)



Single-disorder Diagnosis[2]

[2] Onisko, A., Druzdzel, M.J., Wasyluk, H.: Extension of the Hepar II Model to Multiple-Disorder Diagnosis. Intelligent Information Systems, pp. 303-313. Springer (2000)

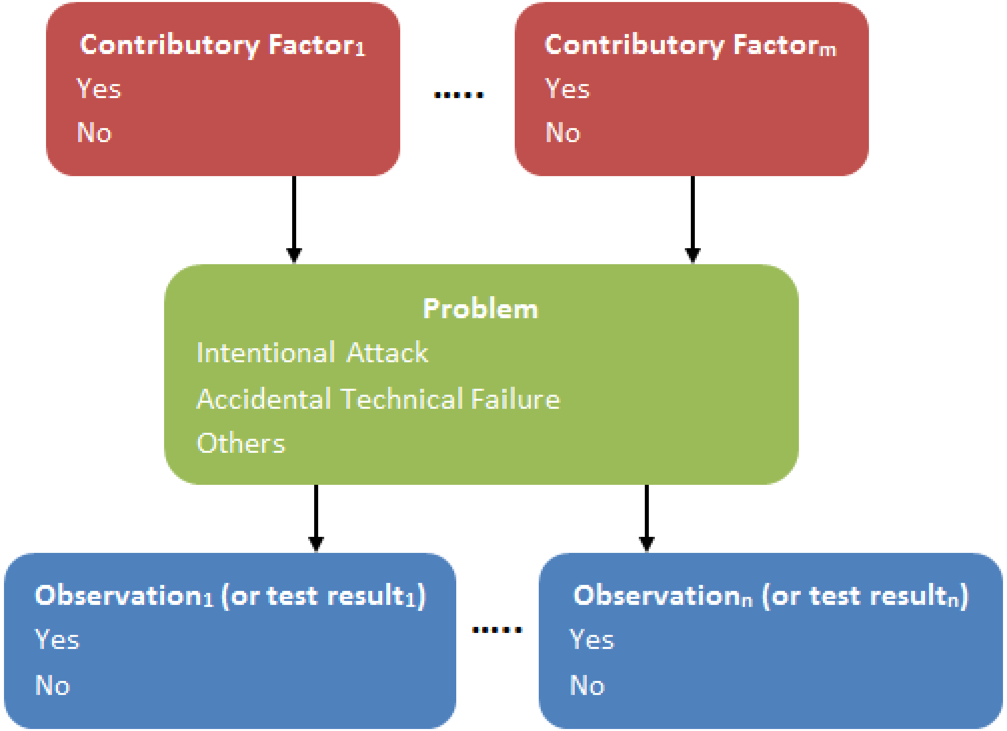
Related Work: Diagnostic BN Models (3/3)


Is there a problem with infotainment system earth?
Are wiring connectors to amplifiers loose or not properly installed?
Does the problem go when a known good amplifier is fitted?
Are there any faulty vehicle fuses?
Incorrect amplifier installed?
Observation Layer
Amplifier power or ground not connected properly
Amplifier hardware fault
Incorrect amplifier installed
Fuse blown
Root Cause Layer
Amplifier not working
Power supply problem
Intermediate Layer
SYS – No sound (Complete loss of audio, display functions working)
Symptom Layer

Vehicle Infotainment System Fault Diagnosis[3]

[3] Huang, Y., McMurran, R., Dhadyalla, G., Jones, R.P.: Probability based Vehicle Fault Diagnosis: Bayesian Network Method. Journal of Intelligent Manufacturing. no. 19, pp. 301-311. (2008)

Proposed BN Framework (1/2)



Contributory Factor$_1$
Yes
No

.....

Contributory Factor$_m$
Yes
No

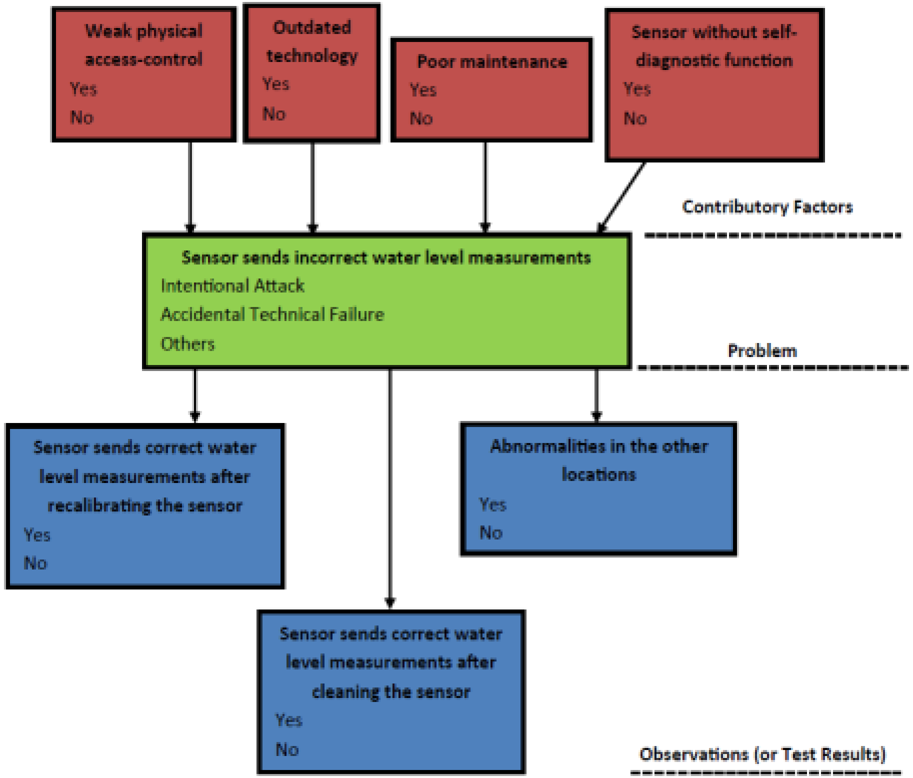
Problem
Intentional Attack
Accidental Technical Failure
Others

Observation$_1$ (or test result$_1$)
Yes
No

.....

Observation$_n$ (or test result$_n$)
Yes
No

Proposed BN Framework (2/2)



Weak physical access-control
Yes
No

Outdated technology
Yes
No

Poor maintenance
Yes
No

Sensor without self-diagnostic function
Yes
No

Contributory Factors

Sensor sends incorrect water level measurements
Intentional Attack
Accidental Technical Failure
Others

Problem

Sensor sends correct water level measurements after recalibrating the sensor
Yes
No

Abnormalities in the other locations
Yes
No

Sensor sends correct water level measurements after cleaning the sensor
Yes
No

Observations (or Test Results)

Problem 2: Knowledge Elicitation in BNs

Expert Knowledge

Empirical Data (Literature)

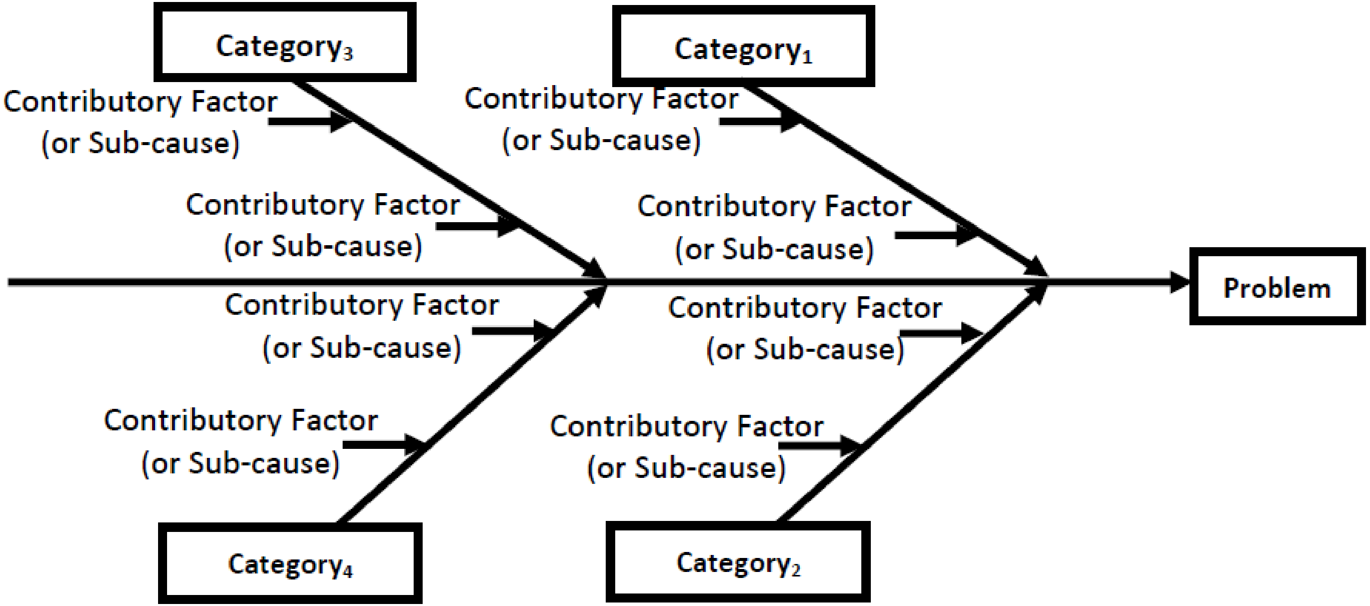
Data Sources used to Construct DAGs and Populate CPTs[4]

BNs are not easy to use for brainstorming

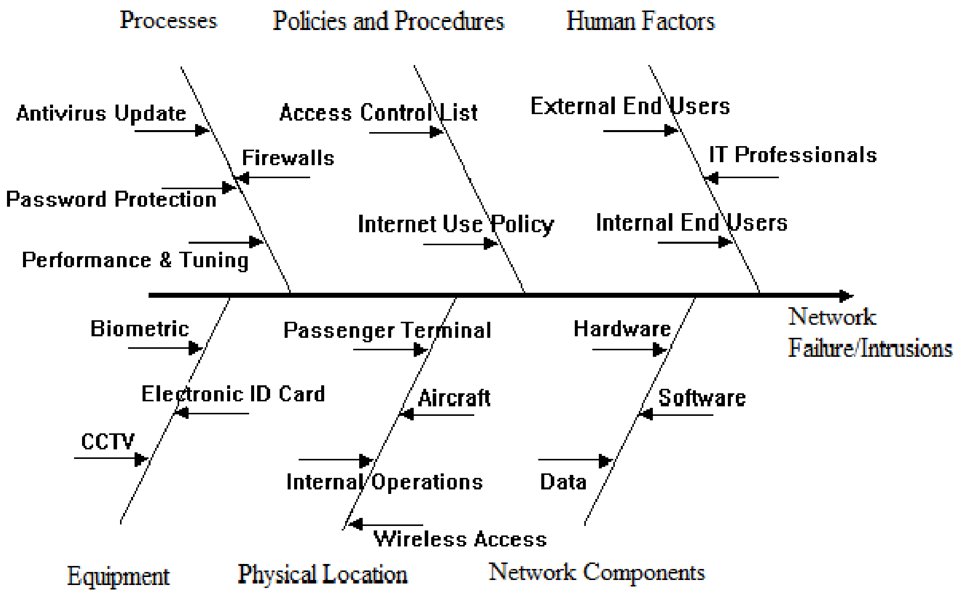
- ✗ Time-consuming to explain the notion of BN.
- ✗ Slow BN structure changes based on discussions.

[4] Chockalingam, S., Pieters, W., Teixeira, A., van Gelder, P.: Bayesian Network Models in Cyber Security: A Systematic Review. In: Nordic Conference on Secure IT Systems, pp. 105-122. Springer (2017)

Introduction to Fishbone Diagrams (1/3)


Category$_3$
Category$_1$
Contributory Factor (or Sub-cause)
Contributory Factor (or Sub-cause)
Contributory Factor (or Sub-cause)
Contributory Factor (or Sub-cause)
Problem
Contributory Factor (or Sub-cause)
Contributory Factor (or Sub-cause)
Contributory Factor (or Sub-cause)
Contributory Factor (or Sub-cause)
Category$_4$
Category$_2$

Introduction to Fishbone Diagrams (2/3)



Fishbone Diagram for *"Network Failure/Intrusion"* Problem in an Airport: Example[5]

[5] Asllani, A., Ali, A.: Securing Information Systems in Airports: A Practical Approach. In: Internet Technology and Secured Transactions (ICITST), International Conference for, pp. 314-318. (2011)

Introduction to Fishbone Diagrams (3/3)

Easy to use for brainstorming

- ✓ Easily changeable based on discussions[6].
- ✓ Encourages and guides data collection[6,7].
- ✓ Stimulates group participation[6,7].
- ✓ Helps to stay focused on the content of the problem[6].

[6] Doggett, A.M.: Root Cause Analysis: A Framework for Tool Selection. The Quality Management Journal 12, 34 (2005)

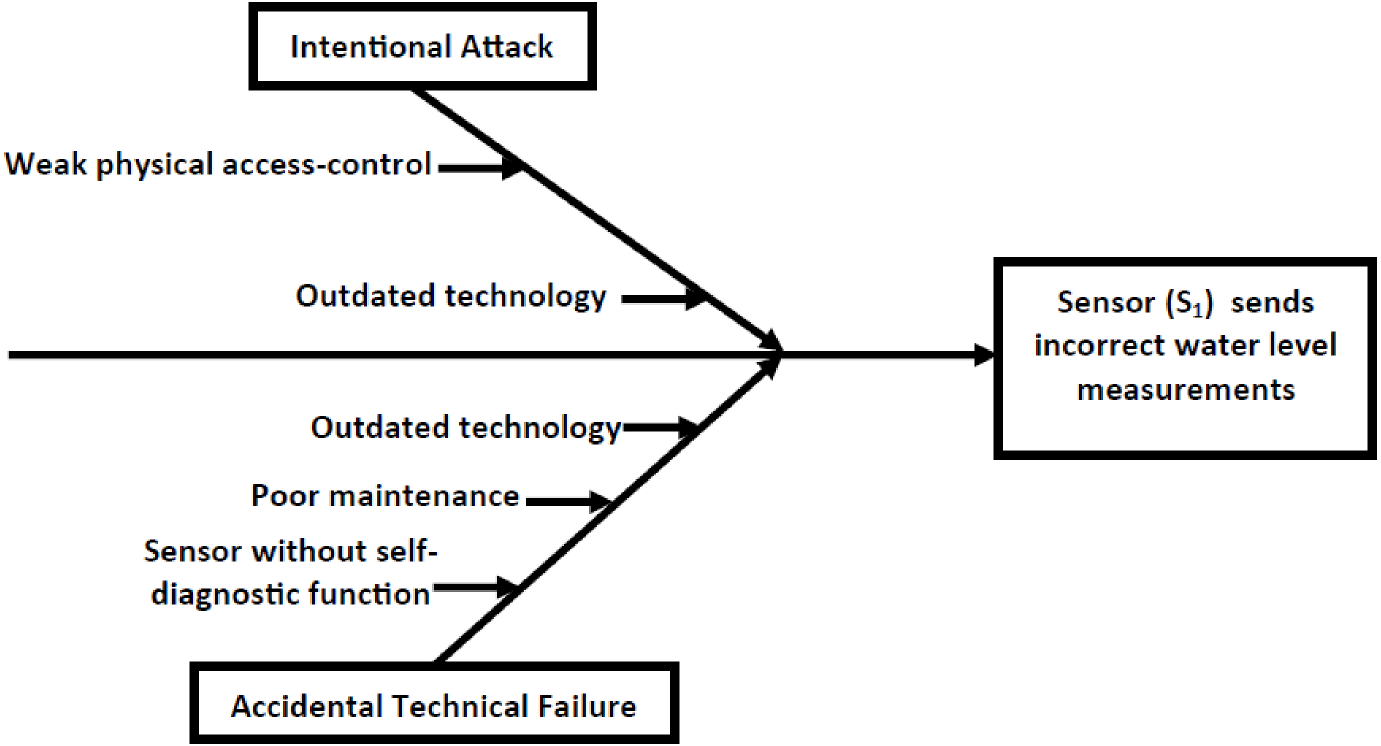
[7] Ilie, G., Ciocoiu, C.N.: Application of Fishbone Diagram to Determine the Risk of an Event with Multiple Causes. Management Research and Practice 2, 1-20 (2010)

Research Objective - 2

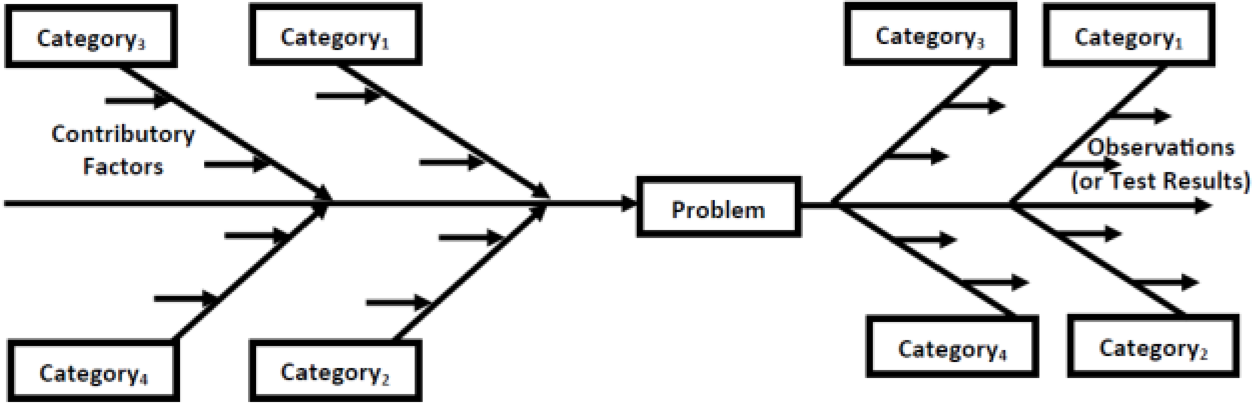
“To leverage fishbone diagrams for knowledge elicitation within our BN framework, and demonstrate the application of the developed methodology via a case study.”

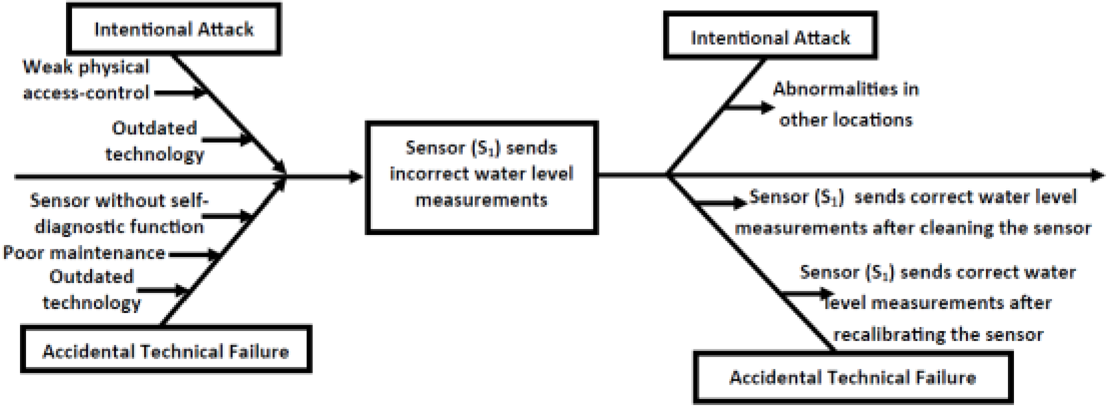
- **Extended fishbone diagrams and utilised extended fishbone diagrams for knowledge elicitation within our BN framework.**
- **Demonstrated the application of the developed methodology based on a case study in the water management domain.**

Extended Fishbone Diagrams (1/2)


Intentional Attack
Weak physical access-control
Outdated technology
Sensor (S_1) sends incorrect water level measurements
Outdated technology
Poor maintenance
Sensor without self-diagnostic function
Accidental Technical Failure

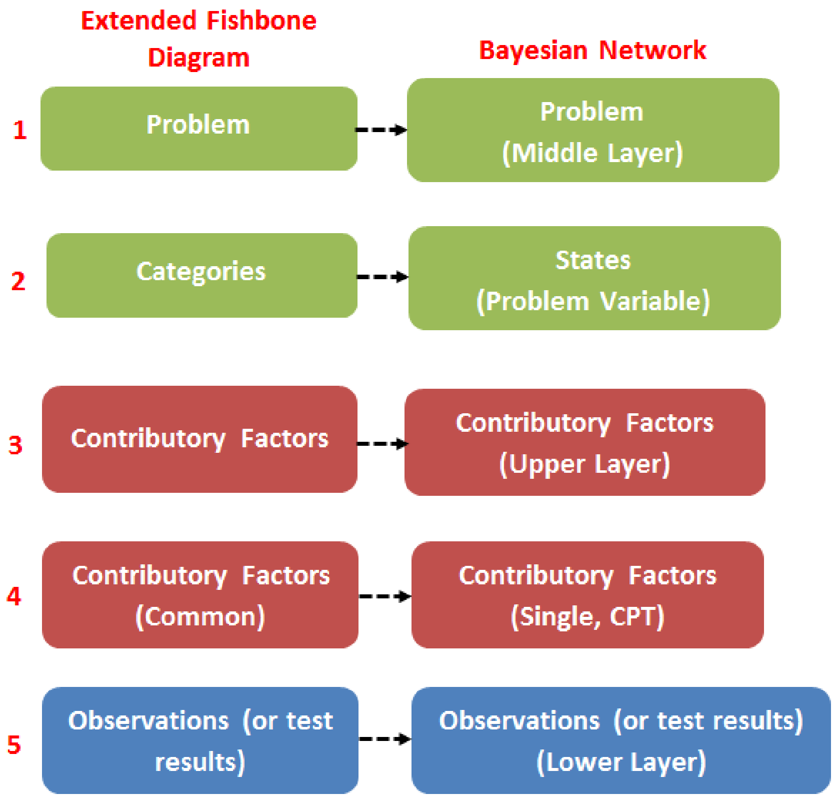
Extended Fishbone Diagrams (2/2)





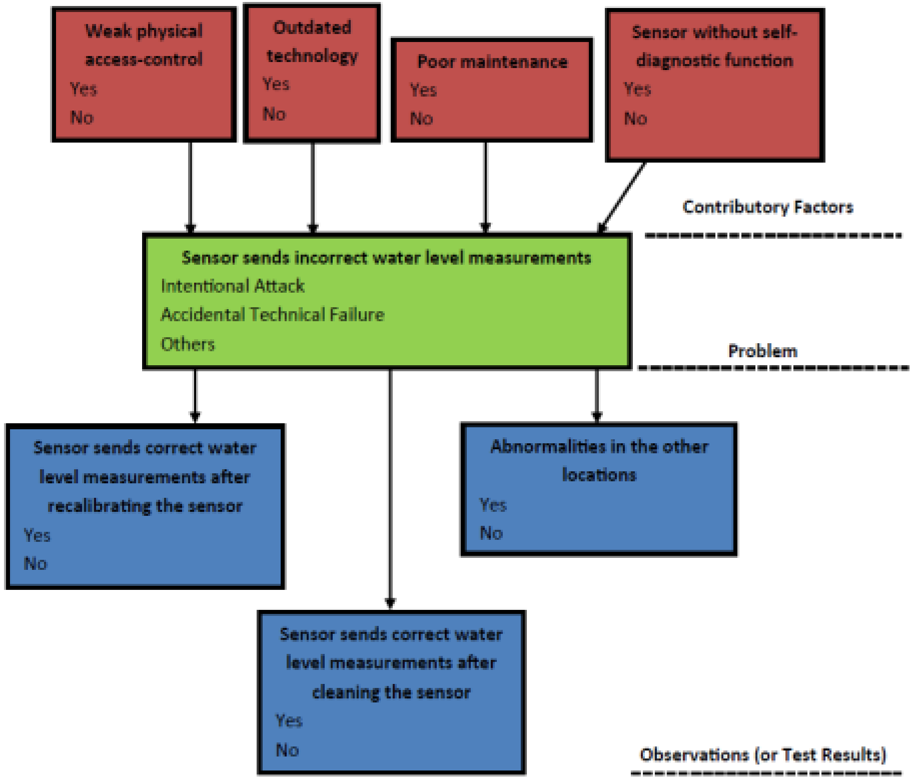
Intentional Attack
Weak physical access-control
Outdated technology
Sensor without self-diagnostic function
Poor maintenance
Outdated technology
Accidental Technical Failure
Sensor (S$_1$) sends incorrect water level measurements
Intentional Attack
Abnormalities in other locations
Sensor (S$_1$) sends correct water level measurements after cleaning the sensor
Sensor (S$_1$) sends correct water level measurements after recalibrating the sensor
Accidental Technical Failure

Translated BN from Extended Fishbone Diagram (1/2)



	Extended Fishbone Diagram	Bayesian Network
1	Problem	Problem (Middle Layer)
2	Categories	States (Problem Variable)
3	Contributory Factors	Contributory Factors (Upper Layer)
4	Contributory Factors (Common)	Contributory Factors (Single, CPT)
5	Observations (or test results)	Observations (or test results) (Lower Layer)

Translated BN from Extended Fishbone Diagram (2/2)



Weak physical access-control
Yes
No

Outdated technology
Yes
No

Poor maintenance
Yes
No

Sensor without self-diagnostic function
Yes
No

Contributory Factors

Sensor sends incorrect water level measurements
Intentional Attack
Accidental Technical Failure
Others

Problem

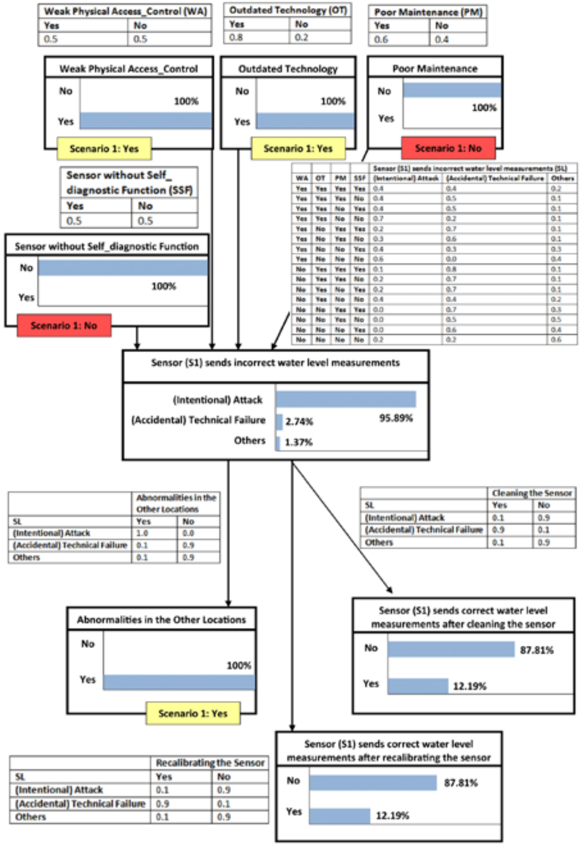
Sensor sends correct water level measurements after recalibrating the sensor
Yes
No

Abnormalities in the other locations
Yes
No

Sensor sends correct water level measurements after cleaning the sensor
Yes
No

Observations (or Test Results)

BN Example: Distinguishing Attacks and Technical Failures



Weak Physical Access_Control (WA)	
Yes	No
0.5	0.5

Outdated Technology (OT)	
Yes	No
0.8	0.2

Poor Maintenance (PM)	
Yes	No
0.6	0.4

Weak Physical Access_Control

No

Yes 100%

Scenario 1: Yes

Outdated Technology

No

Yes 100%

Scenario 1: Yes

Poor Maintenance

No 100%

Yes

Scenario 1: No

Sensor without Self_ diagnostic Function (SSF)	
Yes	No
0.5	0.5

Sensor without Self_diagnostic Function

No 100%

Yes

Scenario 1: No

				Sensor (S1) sends incorrect water level measurements (SL)		
WA	OT	PM	SSF	(Intentional) Attack	(Accidental) Technical Failure	Others
Yes	Yes	Yes	Yes	0.4	0.4	0.2
Yes	Yes	Yes	No	0.4	0.5	0.1
Yes	Yes	No	Yes	0.4	0.5	0.1
Yes	Yes	No	No	0.7	0.2	0.1
Yes	No	Yes	Yes	0.2	0.7	0.1
Yes	No	Yes	No	0.3	0.6	0.1
Yes	No	No	Yes	0.4	0.3	0.3
Yes	No	No	No	0.6	0.0	0.4
No	Yes	Yes	Yes	0.1	0.8	0.1
No	Yes	Yes	No	0.2	0.7	0.1
No	Yes	No	Yes	0.2	0.7	0.1
No	Yes	No	No	0.4	0.4	0.2
No	No	Yes	Yes	0.0	0.7	0.3
No	No	Yes	No	0.0	0.5	0.5
No	No	No	Yes	0.0	0.6	0.4
No	No	No	No	0.2	0.2	0.6

Sensor (S1) sends incorrect water level measurements

(Intentional) Attack 95.89%

(Accidental) Technical Failure 2.74%

Others 1.37%

	Abnormalities in the Other Locations	
SL	Yes	No
(Intentional) Attack	1.0	0.0
(Accidental) Technical Failure	0.1	0.9
Others	0.1	0.9

	Cleaning the Sensor	
SL	Yes	No
(Intentional) Attack	0.1	0.9
(Accidental) Technical Failure	0.9	0.1
Others	0.1	0.9

Abnormalities in the Other Locations

No

Yes 100%

Scenario 1: Yes

Sensor (S1) sends correct water level measurements after cleaning the sensor

No 87.81%

Yes 12.19%

	Recalibrating the Sensor	
SL	Yes	No
(Intentional) Attack	0.1	0.9
(Accidental) Technical Failure	0.9	0.1
Others	0.1	0.9

Sensor (S1) sends correct water level measurements after recalibrating the sensor

No 87.81%

Yes 12.19%

Key Takeaways (1/2)

- **Adequate decision support** for distinguishing intentional attacks and accidental technical failures is **missing**.

- BNs can be potentially used to tackle this challenge as they enable **diagnostic reasoning (disease diagnosis, fault diagnosis).**

- We **customised** and utilised three different types of **variables** from **existing diagnostic BN models** in our BN framework **(contributory factors, problem, and observations (or test results))**.

- **Expert knowledge, and empirical data (literature)** were the predominant data sources utilised to construct DAGs and populate CPTs.

Key Takeaways (2/2)

- **BNs** are **not easy to use** for **brainstorming**. However, **fishbone diagrams** can be potentially used to **tackle** this **challenge**.
- We **extended fishbone diagrams** and **utilised** extended fishbone diagrams for **knowledge elicitation** within our BN framework.
- We **demonstrated** the **developed methodology** based on a case study in the **water management domain**.
- **Future research directions:** I. How fishbone diagrams could be used to elicit knowledge for cases where several problems arise at the same time?, II. Can fishbone diagrams be used to elicit CPTs?, III. Evaluation of our methodology based on applications in water management domain.

ANY QUESTIONS?

Saba Chockalingam

S.Chockalingam@tudelft.nl

Secure Our Safety: Building Cyber Security for Flood Management (SOS4Flood) Project