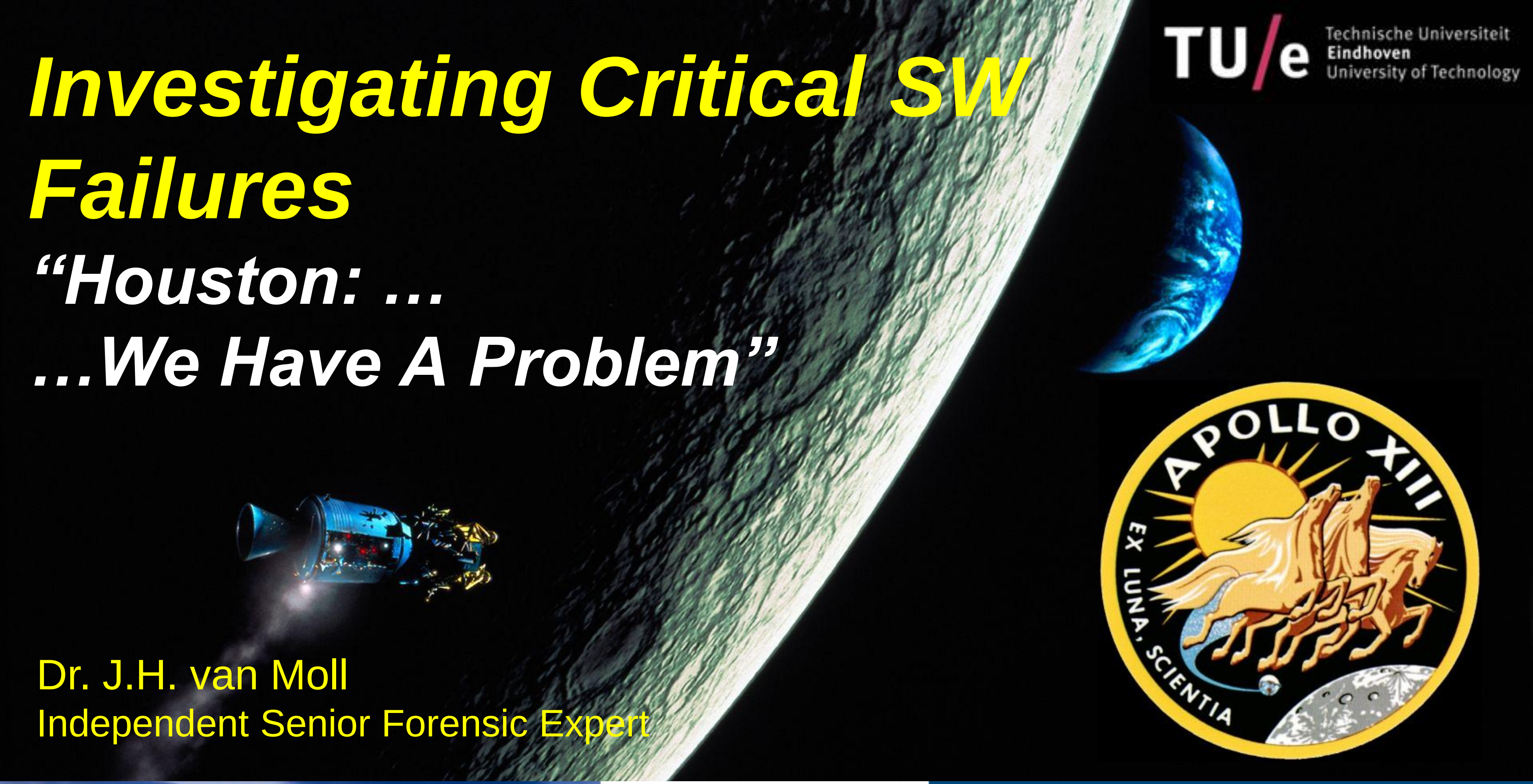


Technische Universiteit
Eindhoven
University of Technology

Investigating Critical SW Failures

"Houston: …
…We Have A Problem"

Dr. J.H. van Moll
Independent Senior Forensic Expert

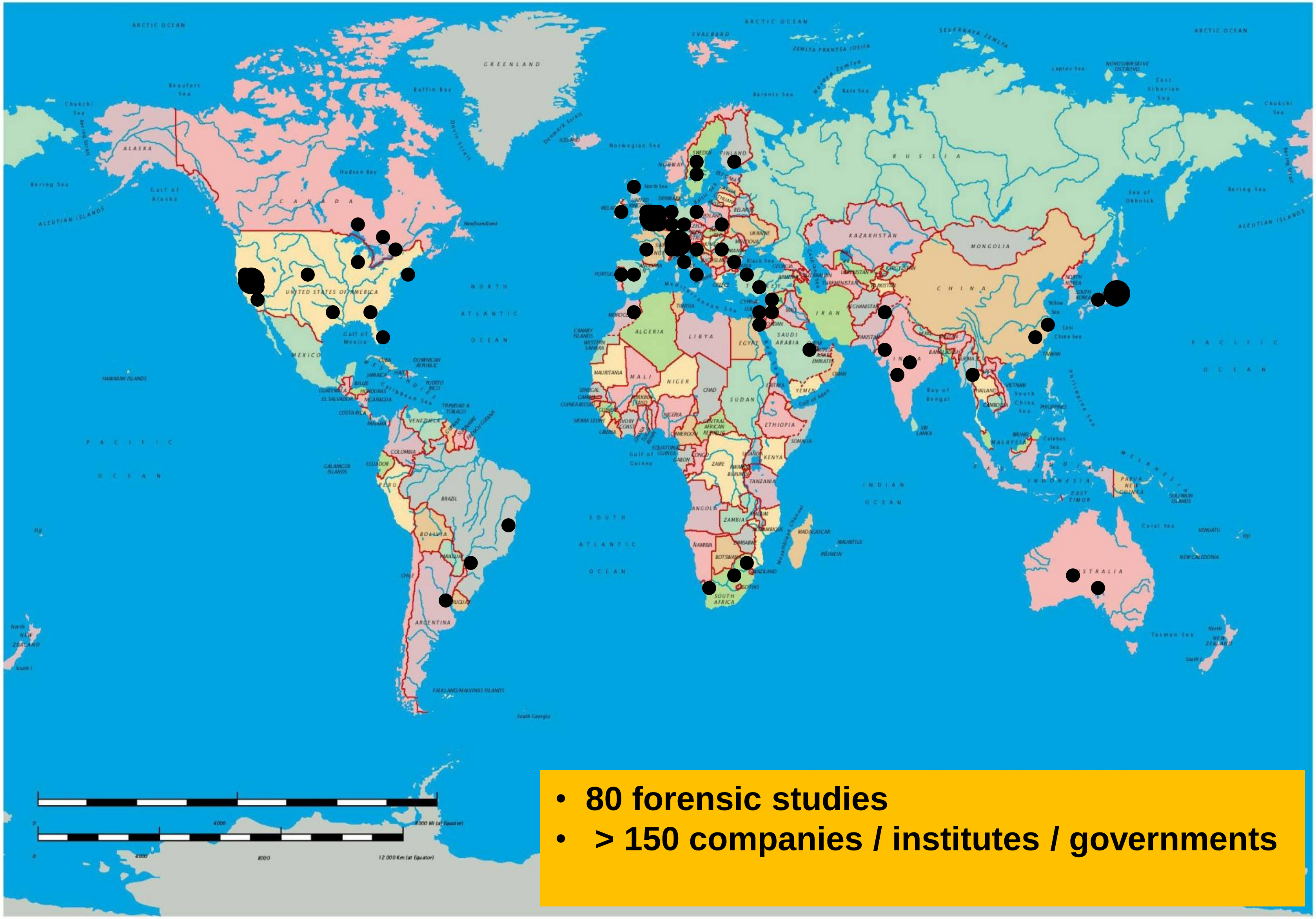
21E
NEDERLANDSE
TESTDAG
DUTCH
TESTING
DAY

6 oktober 2015
Conference Center
The Strip
High Tech Campus
Eindhoven
→ Where research,
education
and business meet

DISCLAIMER:

The photo material presented has been randomly picked to illustrate cases. The illustrations are in no way associated to the actual objects, companies or subjects involved in the actual critical incidents or examined cases

Speaker’s Forensic investigations 2005-2015

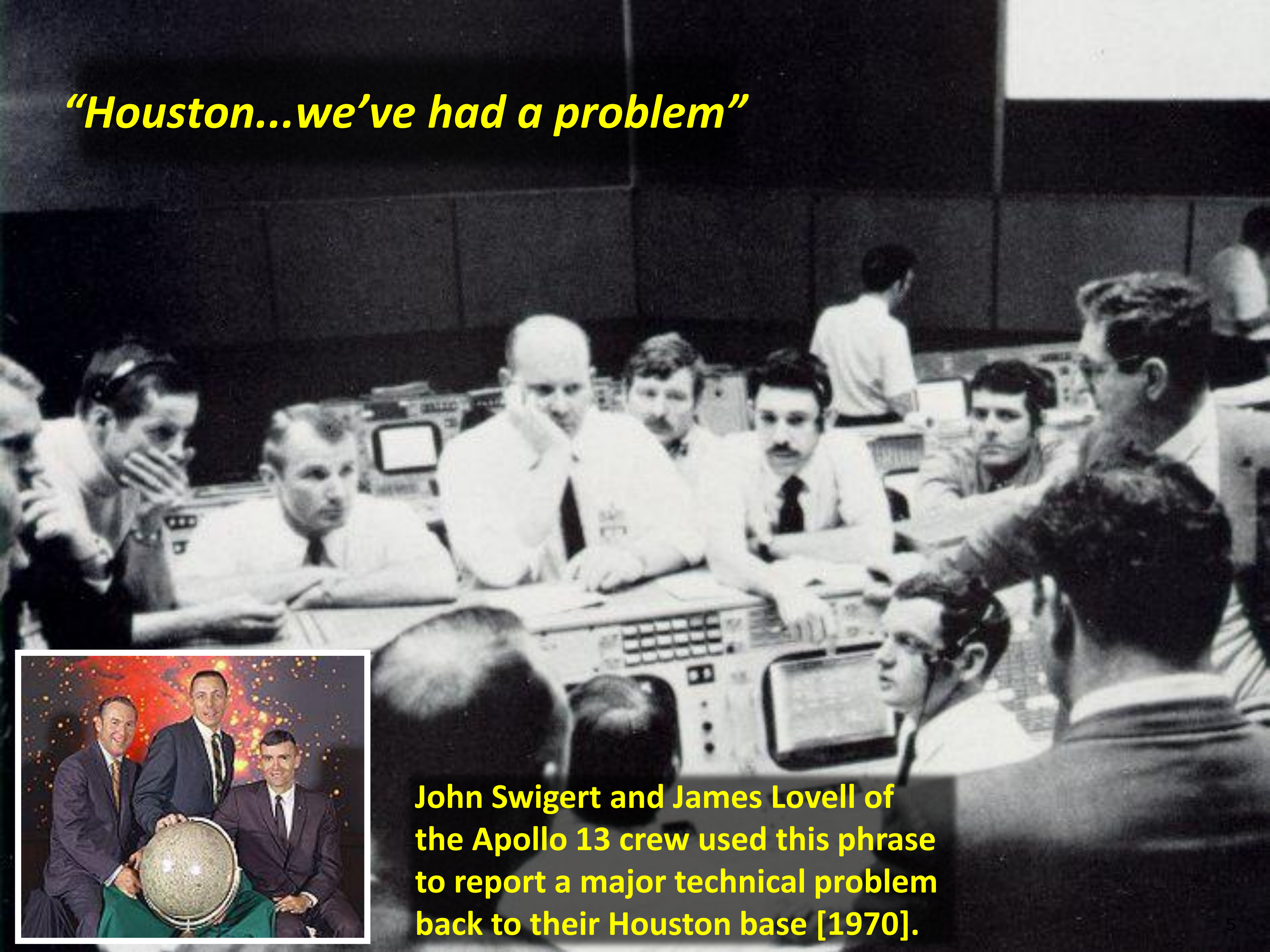


- **80 forensic studies**
- **> 150 companies / institutes / governments**

What we will see .....

- **Poor SW “Quality” is closer than you think !**
- **Why is Industry struggling with Root Cause Analysis?**
- **What is key to powerful RCA to solve & prevent problems?**

“Houston…we’ve had a problem”



John Swigert and James Lovell of the Apollo 13 crew used this phrase to report a major technical problem back to their Houston base [1970].

The Context: Software-intensive systems

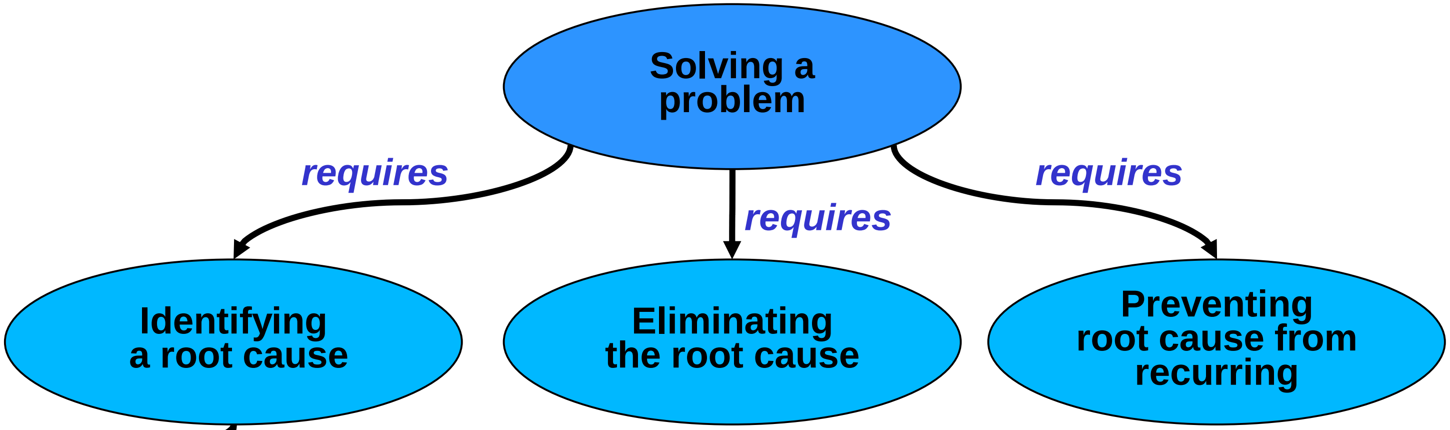
Quality issues are **NOT** about “culpable acts”

Headline news
“Can’t deny” incidents

“Near misses”
“Narrow escapes”

SW Quality Problems are like an iceberg:
We only get to see the tip of it

RCA and Problem solving



Solving a problem

requires

requires

requires

Identifying a root cause

Eliminating the root cause

Preventing root cause from recurring

Question 1:
How did the initial situation came into existence eventually leading to the undesired problem?

Sources

Origin

“Birth”

Question 2:
Given an initial situation favourable of producing an undesired consequence, why wasn’t the undesired consequence prevented from occurring?

Non-detection

Escalation

Propagation

Root Cause Factors for SW-intensive systems

Defect Introduction Factors

1	**Requirements**
2	**Developer Capability**
3	**Domain Knowledge**
4	**Communication**
5	**Product Complexity**
6	**Change Control**
7	**Project Management Maturity**
8	**Quality of Documentation**
9	**Team Composition**
10	**Development Environment**
11	**Collaboration**
12	**Process Maturity**
13	**Business Management Maturity**
14	**Innovation**
15	**External Disturbance**
16	**Team Distribution**

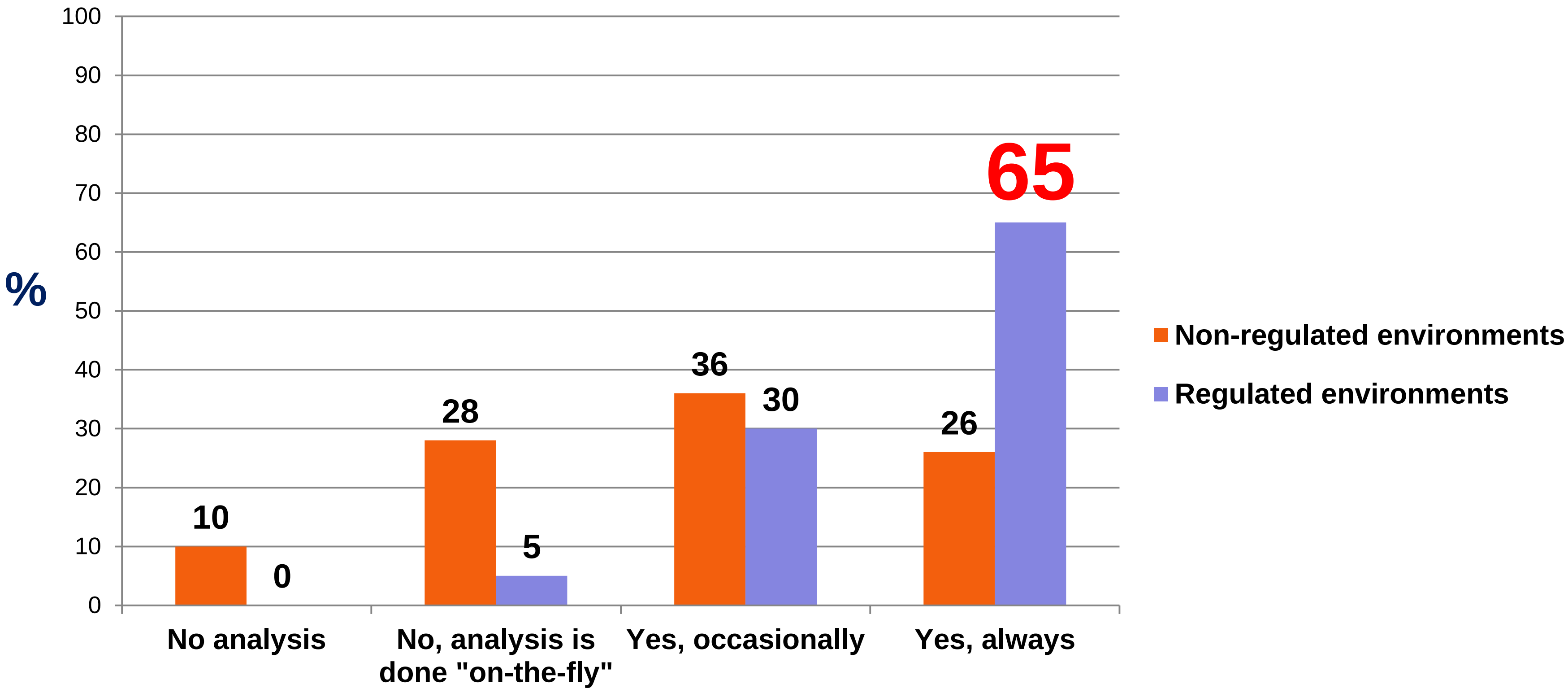
Defect Detection Factors

1	**Test Capability**
2	**Quality of Documentation**
3	**Management Attitude**
4	**Test Process Maturity**
5	**Testability**
6	**Communication**
7	**Test Environment**
8	**Product Complexity**
9	**Change Control**
10	**Development Process Maturity**
11	**Test Planning**
12	**Product Integration**
13	**Test Team Organization**
14	**Adherence to Plan**
15	**Support for Testing**
16	**Test Team Cohesion**
17	**Team Distribution**

***** The Adverse Effects of Virtual Product Development on Product Quality and Their Influencing Factors, Eindhoven University of Technology, 2007, J.C. Jacobs & J.H.van Moll (URL: http://alexandria.tue.nl/extra2/200711967.pdf)***

Some data on RCA from SW-intensive industries

Q: In case of significant product quality problems, is a structured approach to root cause analysis being used?



Pictures used for illustration only.
These are NOT the actual subjects!

'Hidden' Incidents – Selfscan System

Zelfscan
[redacted]
Wij controleren vanaf heden iedere klant.
Onze excuses voor het ongemak.
Vragen of hulp nodig met scannen?
Wij helpen u graag.
Heerlijk voorjaar

- **Unjustified client checking at cashier desk**
- **Triple-fault conditions induced by customer behavior erroneously triggered security flags**

Time between 'awareness' and RC : 5 months

Pictures used for illustration only.
These are NOT the actual subjects!

‘Hidden’ Incidents – Warning Light

Time between ‘awareness’ and RC : 7 months

Spontaneous illumination

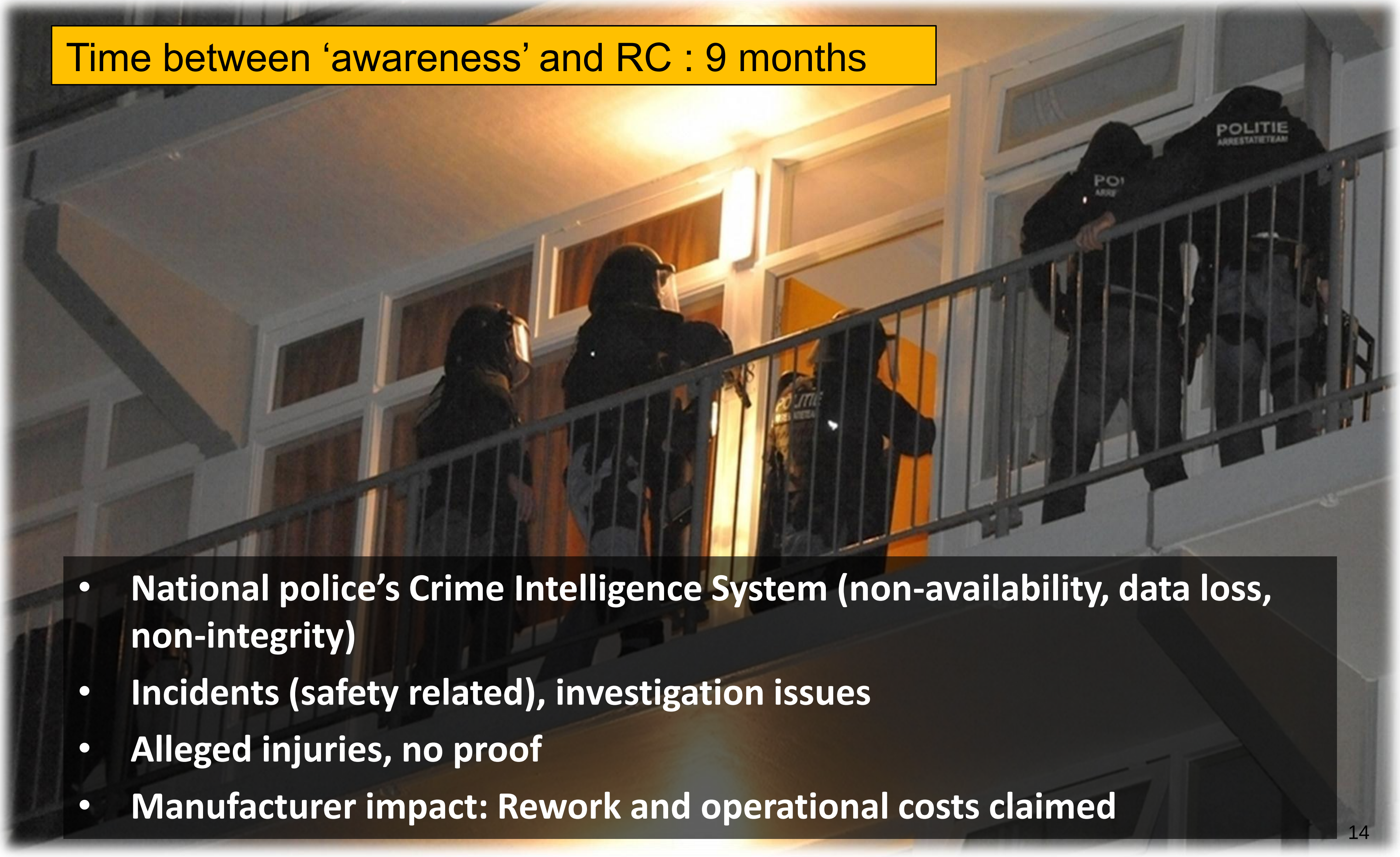
Detected by: dealer ‘statistics’

Injuries: No, but 4 severe (known) traffic incidents

Manufacturer impact: Massive recall

Pictures used for illustration only.
These are NOT the actual subjects!

‘Hidden’ Incidents – Crime Intelligence System

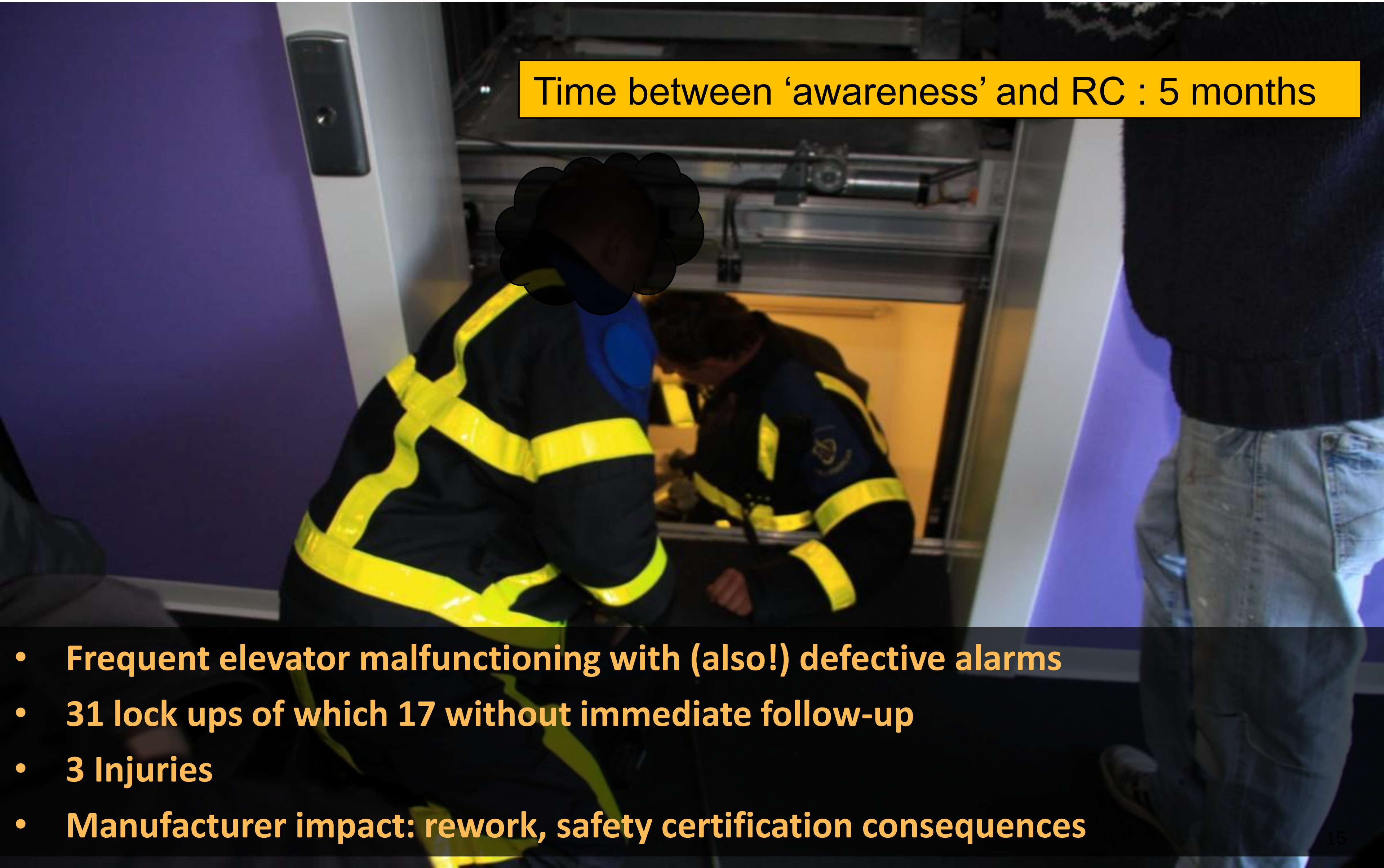


Time between ‘awareness’ and RC : 9 months

- **National police’s Crime Intelligence System (non-availability, data loss, non-integrity)**
- **Incidents (safety related), investigation issues**
- **Alleged injuries, no proof**
- **Manufacturer impact: Rework and operational costs claimed**

Pictures used for illustration only.
These are NOT the actual subjects!

‘Hidden’ Incidents – Elevator Control Malfunction



Time between ‘awareness’ and RC : 5 months

- **Frequent elevator malfunctioning with (also!) defective alarms**
- **31 lock ups of which 17 without immediate follow-up**
- **3 Injuries**
- **Manufacturer impact: rework, safety certification consequences**

RCA merely a solution-oriented activity

No consensus about the problem

No clear start, end and scope of RCA

RCA merely a window-dressing activity

WHY ?

Information-hiding: fear of consequences, embarrassment

'Isolated' RCA, no involvement of stakeholders

Pressure: hurrying the RCA with 'forced' conclusions

Investigator bias: using only 'familiar' analysis tools

Problems in assessing Human and Environmental Factors

Rich data from testing activities not used

Early termination of the RCA ('external cause')

Conflict of interest: analyzer is involved in the problem

So how to start adequate RCA ??

What proper RCA needs....

- **Problem consensus**
- **Sound research principles (factual evidence, verifiability)**
- **‘Investigation-minded’ persons**
- **Objectivity**
- **Multiple RCA techniques**

- **Corrective Actions to prevent similar problems**
- **Effective communication**

**** In cooperation with Robert (Bob) J. Latino, Reliability Center, Inc., U.S.A.***

Your first steps

Adopt the usage of proper and proven RCA techniques and tools, like:

- Cause Effect graphing
- ECFA (Events and Causal Factors Analysis)
- Current Reality Tree
- Change Analysis, Why-Because Analysis
- Re-enactment
- Fault Tree Analysis
- MORT
- Logic Trees
- Barrier Analysis
- MES (Multi-Linear Event Sequencing)
- STEP (Sequential Timed Event Plotting)
- CIT (Critical Incident Technique)
- Is-Is Not Matrix
- 5-times Why
- HFA (Human Factors Assessment)
- Storytelling
- Realitycharting, ...

Keep in mind:

a 'one-size-fits-all' technique for RCA does not exist !!

Take this home !!!

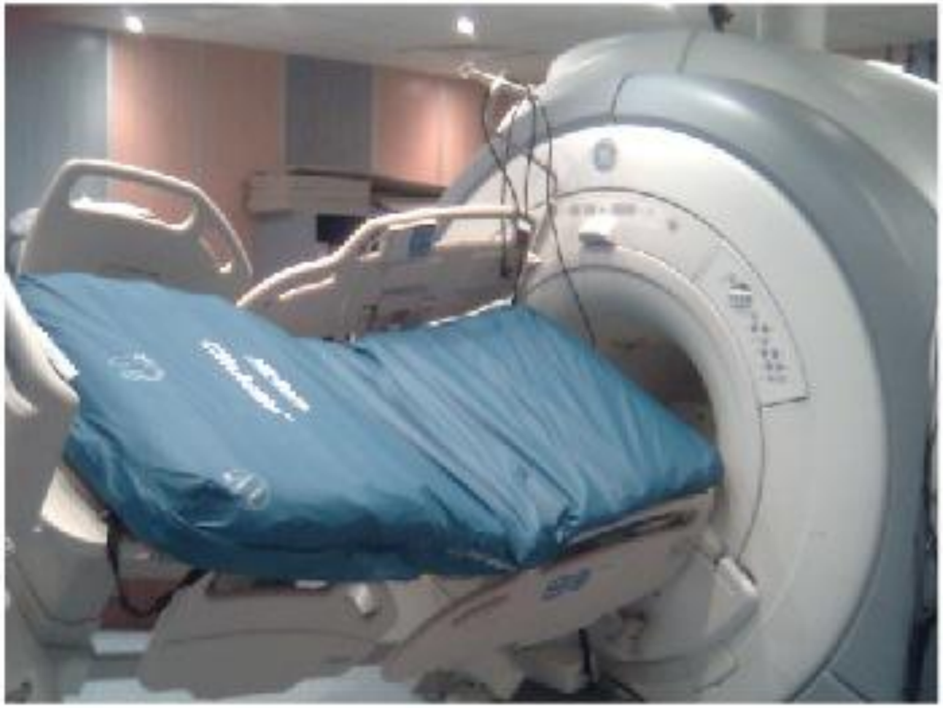
Start learning from failures by doing RCA on your post-release defects / issues !!

- **Testers are the perfect RCA participants !**
- **Start mastering adequate methodologies and tools for RCA (please do forget about ‘5-times Why’ ☺)**
- **Feedback RCA learnings into your test strategy**
- **Admit your testing omissions: Testers are still human !**

Mister Tester !! ..and I told you we shall catch ALL defects before release !!

For your RCA future

A final thought….



“S MR-027 : The product must be safe”

RCA is an ‘after-the-fact’ activity at all times !

You should avoid problems by design but do realize you can only do your utmost best to avoid; there is never a guarantee.

You will never be able to anticipate all failure mechanisms of today’s complex products and systems.

Thank you !
Questions, or interested in learning more?

Feel free to contact me:

Linked in ®