



**RISK &
RESILIENCE
ONLINE**

3, 4 & 5 NOVEMBER 2020



UNIVERSITY OF TWENTE.

CYBER RESILIENCE & CYBER RECOVERY

RICHARD BLIEK

16.00 – 16.10	Inleiding
16.10 – 16.30	Presentatie: R&R vanuit de bankensector.
16.30 – 16.40	Mogelijkheid tot vragen presentatie
16.40 – 16.45	Introductie panelleden
16.45 – 16.55	Korte pauze
16.55 – 17.45	Paneldiscussie met stellingen
17.45 – 17.55	Mogelijkheid tot vragen aan panelleden
17.55 – 18.00	Samenvatting en afsluiting

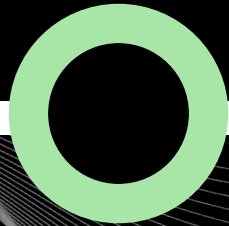
IN THIS PRESENTATION:



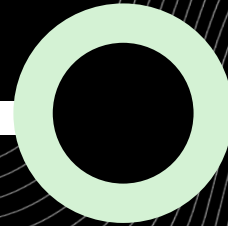
WHAT IS
RESILIENCE



WHY THE FUZZ



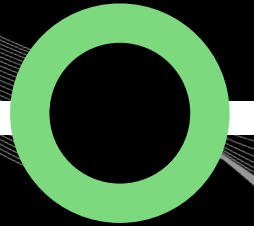
WHY NOW



THEORY



CYBER
RECOVERY

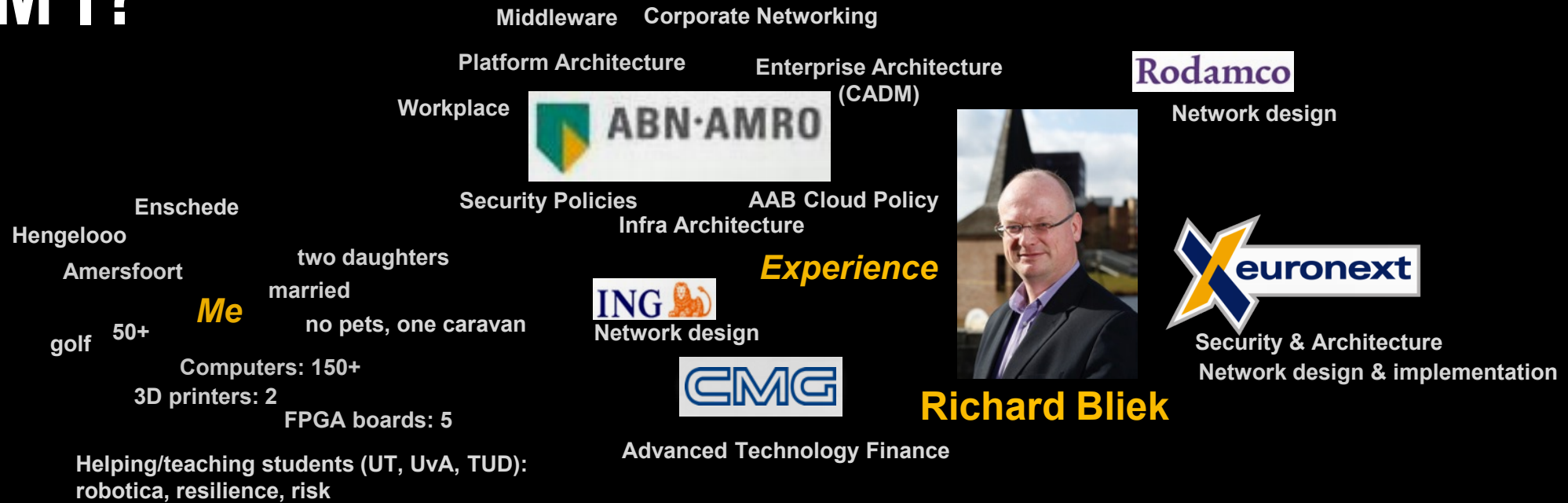


FOOD FOR
THOUGHT



UNIVERSITY
OF TWENTE.

WHO AM I?



Doing resilience... since 2008:

- 2008 – Internet Banking Design Notes
- 2010 – M5K failover scenarios
- 2010 – Redhat Clustering Failover Concepts
- 2012 – BAN Availability Assessment
- 2013 – Improving the Service Risk Process
- 2014 – Design for failure
- 2014 – Hier Complex? Onmogelijk!
- 2016 – Change Impact Analysis in Cloud
- 2018 – Clustering Concepts Considered Harmful

2016
Risk Management (MSc, cum laude)
“Change Impact Analysis in Cloud”

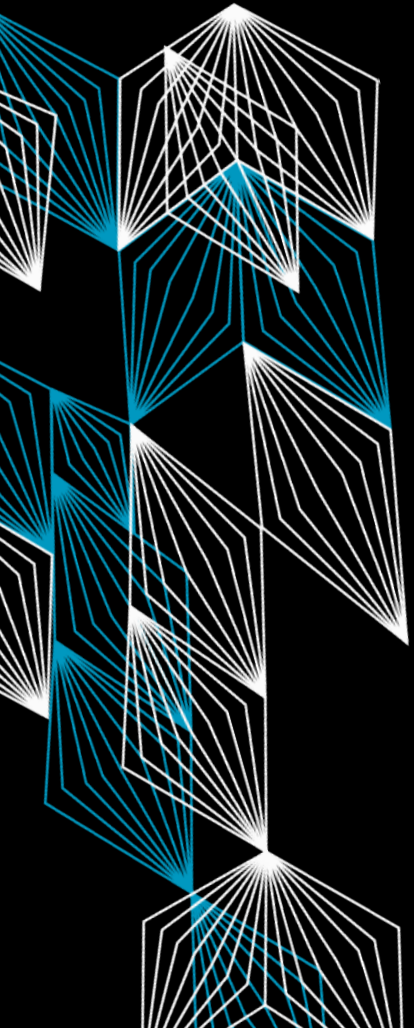
Education

1996
Computer Science (ir.)
“Experimental Evaluation
of
Connection Management Protocols”

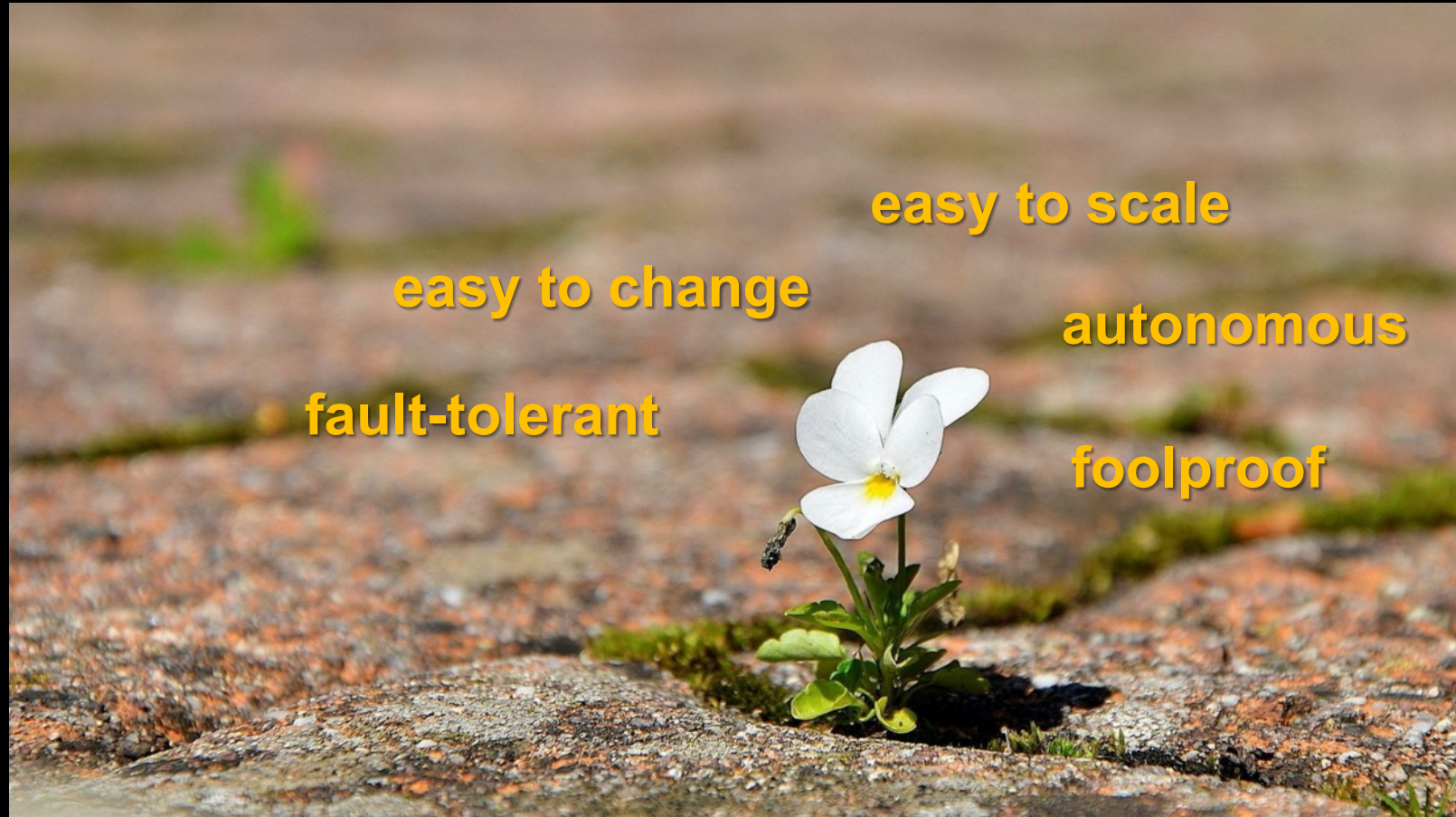
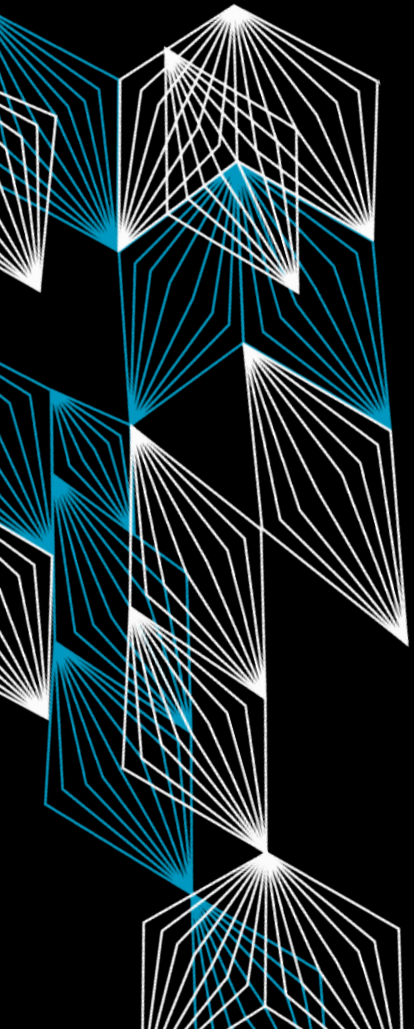


UNIVERSITY
OF TWENTE.

WHAT IS RESILIENCE



WHAT IS RESILIENCE

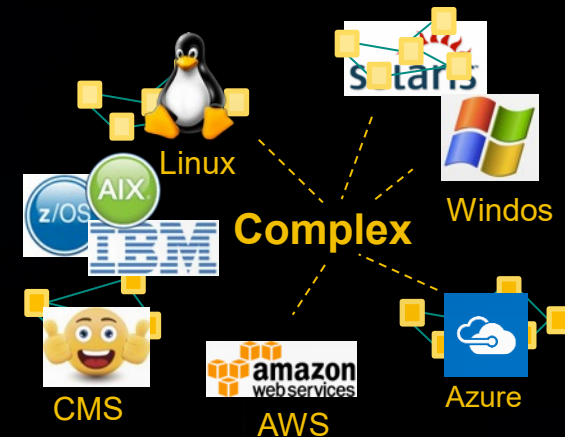
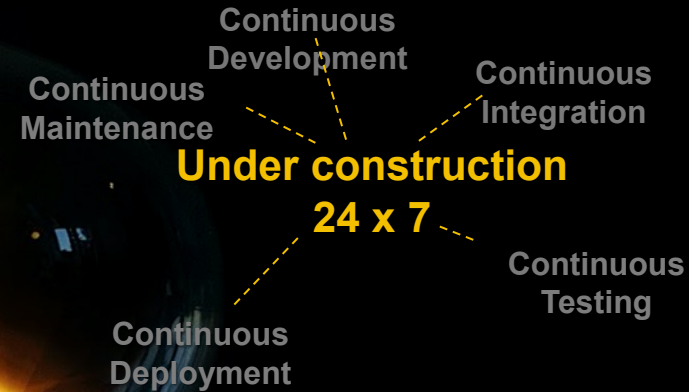


WHY THE FUZZ ... WHY NOW ...

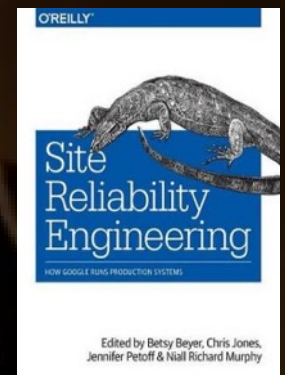
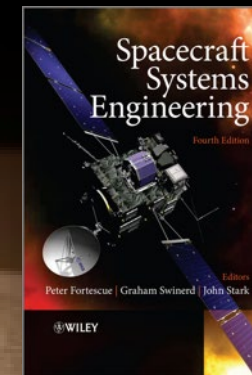
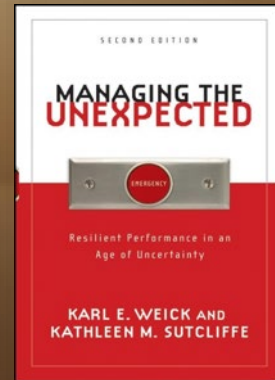
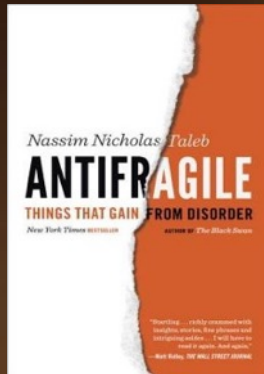
... more channels,
higher volume



Tikkie heeft ruim 4 miljoen
gebruikers
(source: nu.nl, 22-11-2018)



WHAT CAN WE LEARN FROM OTHERS ...



IT'S ABOUT TIME ...

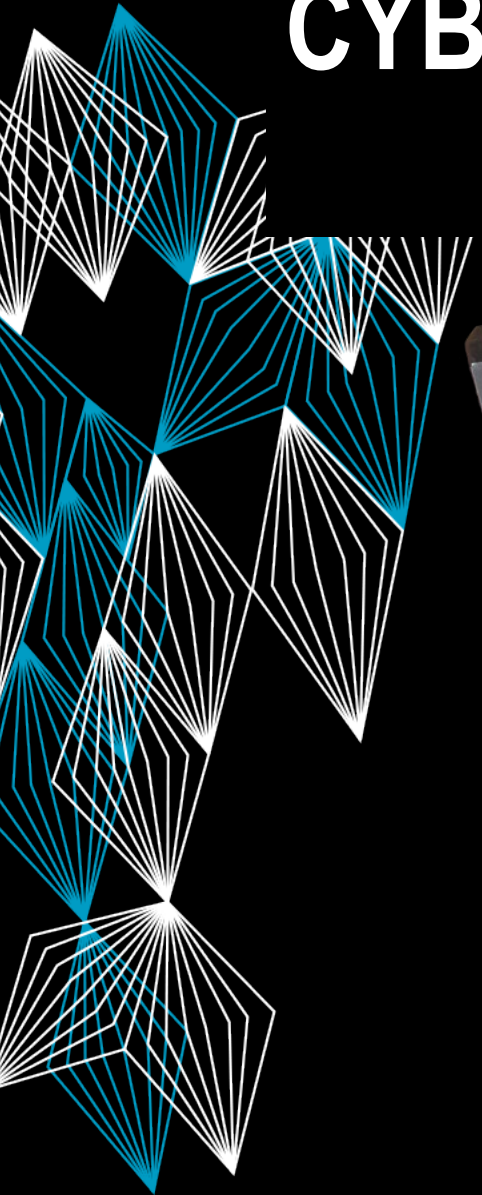
Resilience is the ability
to

{ detect
contain
correct }

... faster!



CYBER RECOVERY



Focus...

- Destructive Cyber Attack
- Recovery (i.e. in case Prevention and Protection were not successful)

Guidance and Requirements...

- Existential
- ECB (December 2018):
“Cyber Resilience Oversight Expectations for Financial Market Infrastructures”
- NIST (April 2018):
“Framework for Improving Critical Infrastructure Cybersecurity”

NIST CYBERSECURITY FRAMEWORK

*Restore
any capabilities or services
that were impaired due to a
cybersecurity incident.*



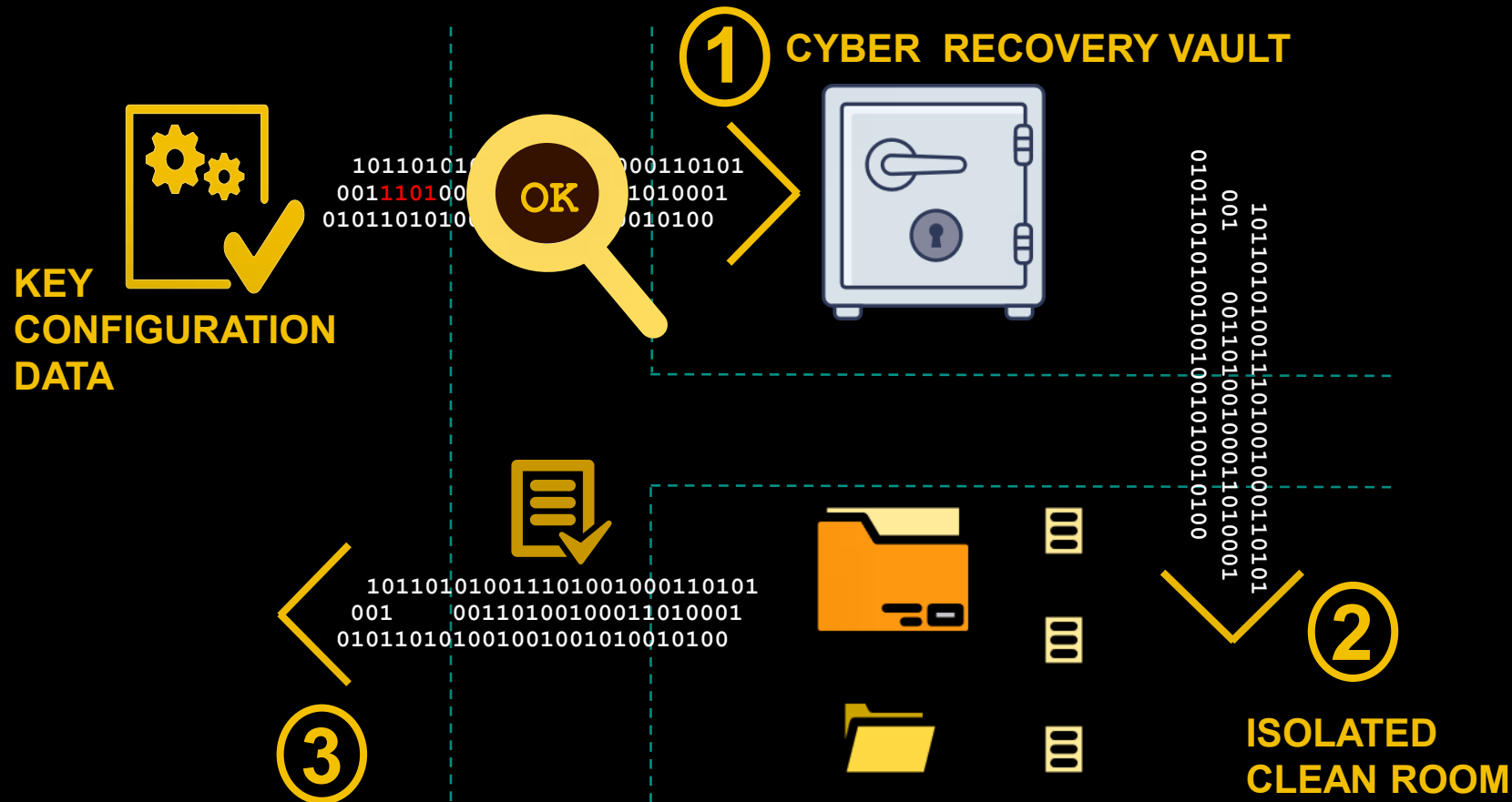
*Organizational Understanding
to manage cybersecurity risk to
systems, people, assets, data, and
capabilities.*

*Activities
to take action regarding a detected
cybersecurity incident.*

*Safeguards
to ensure delivery of critical
services.*

*Activities
to identify the occurrence of a cybersecurity event.*

BASIC CYBER RECOVERY CAPABILITY



FOOD FOR THOUGHT... IT RESILIENCE FRAMEWORK



VISION
"IT Resilience must lead to an automatic IT-landscape that bounces back after disruptions, is easy to change, easy to scale and that will call for help if and only if manual intervention is required"

STRATEGY
"IT Resilience must ensure that all errors and failures are detected, contained and corrected without customers noticing that something went wrong"

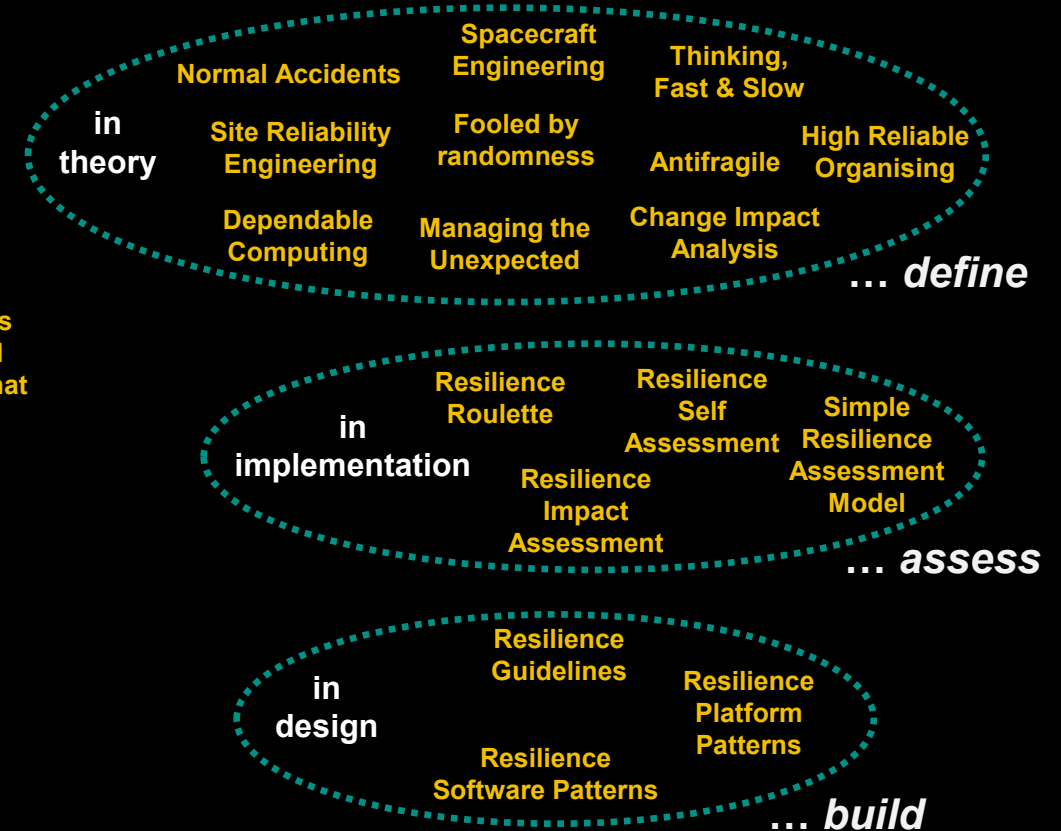
CRISIS MGT
avoid the morgue

Disaster
Recovery

HIGH AVAILABILITY
avoid intensive care
(IT) components monitoring
component redundancy
fault avoidance
scenario analysis / prediction
rely on testing & documentation
react on failures

RESILIENCE
avoid the hospital
(IT) services monitoring
service dependability
fault tolerance
expect the unexpected
rely on experience
react on "near misses"

... we need both!
(resilience $\approx$ availability++)



FOOD FOR THOUGHT... CYBER RECOVERY

CYBER RECOVERY IS ABOUT...

Knowing what to do...

AFTER

**PROTECT, DETECT,
RESPOND**

Have FAILED



REFERENCES...

- Anderson, R. S., Benjamin, J., Wright, V. L., Quinones, L., & Paz, J. (2017). Cyber-Informed Engineering (No. INL/EXT-16-40099). Idaho National Lab.(INL), Idaho Falls, ID (United States).
- Gritzalis, D., Theocharidou, M., & Stergiopoulos, G. (2019). Critical Infrastructure Security and Resilience. Cham: Springer
- DiBiasi, J. R. (2007). CyberTerrorism: Cyber Prevention vs Cyber Recovery. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.
- Kieseberg, P., & Weippl, E. (2018, January). Security challenges in cyber-physical production systems. In International conference on software quality (pp. 3-16). Springer, Cham.
- Stine, K., Quill, K., & Witte, G. (2014). Framework for improving critical infrastructure cybersecurity (No. ITL Bulletin February 2014). National Institute of Standards and Technology.
- NIST18, Framework for Improving Critical Infrastructure Cybersecurity <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>
- ... and some books:
 - Perrow – “Normal Accidents”
 - Weick/Suttcliffe – “Managing the Unexpected”
 - Bever, Jones, Petoff & Murphy – “Site Reliability Engineering”,
 - Taleb – “Antifragile”