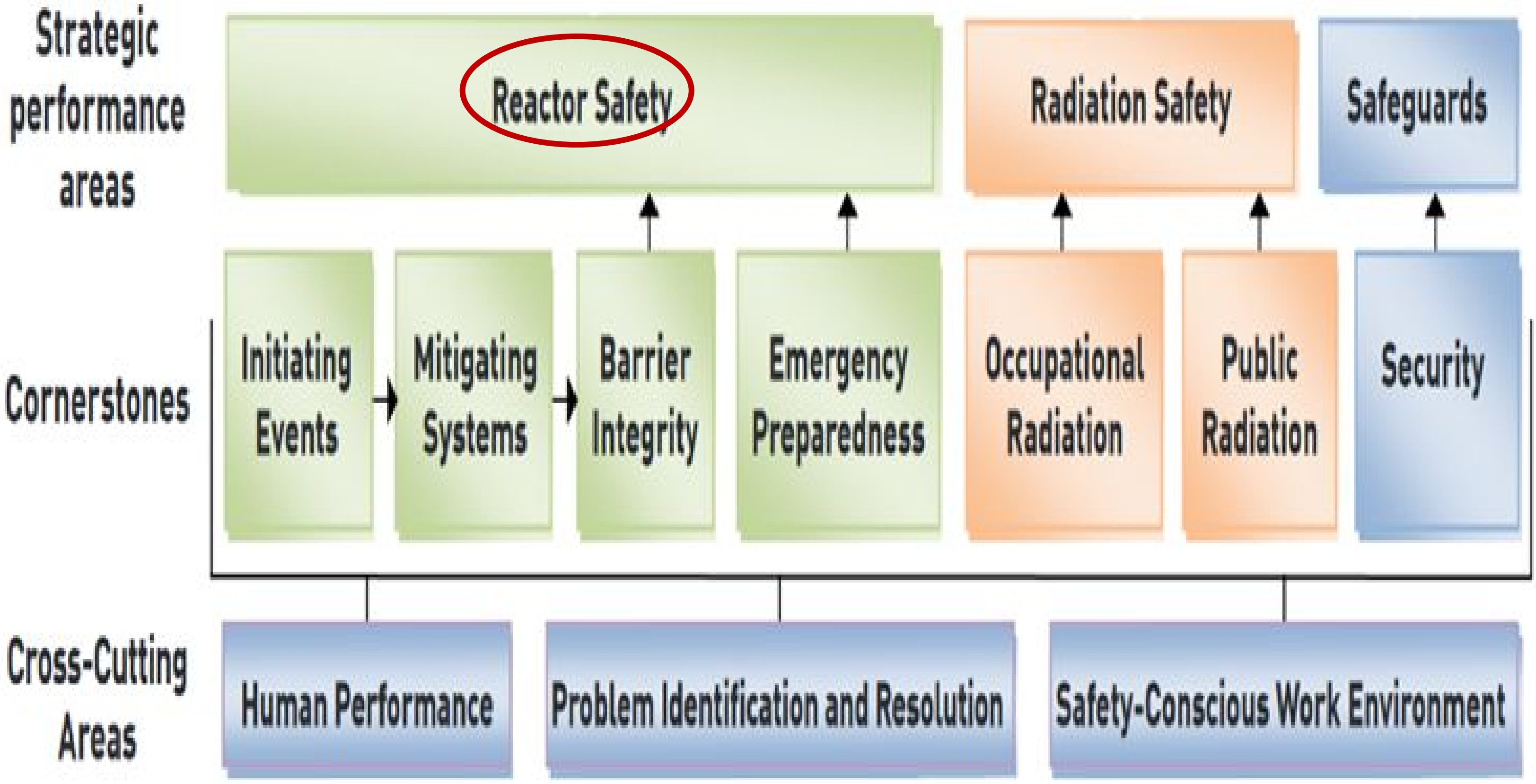
Modeling Nuclear Safety: Application of FRAM to Nuclear Safety

Abdullah Abalkhil
TU Delft, Netherlands

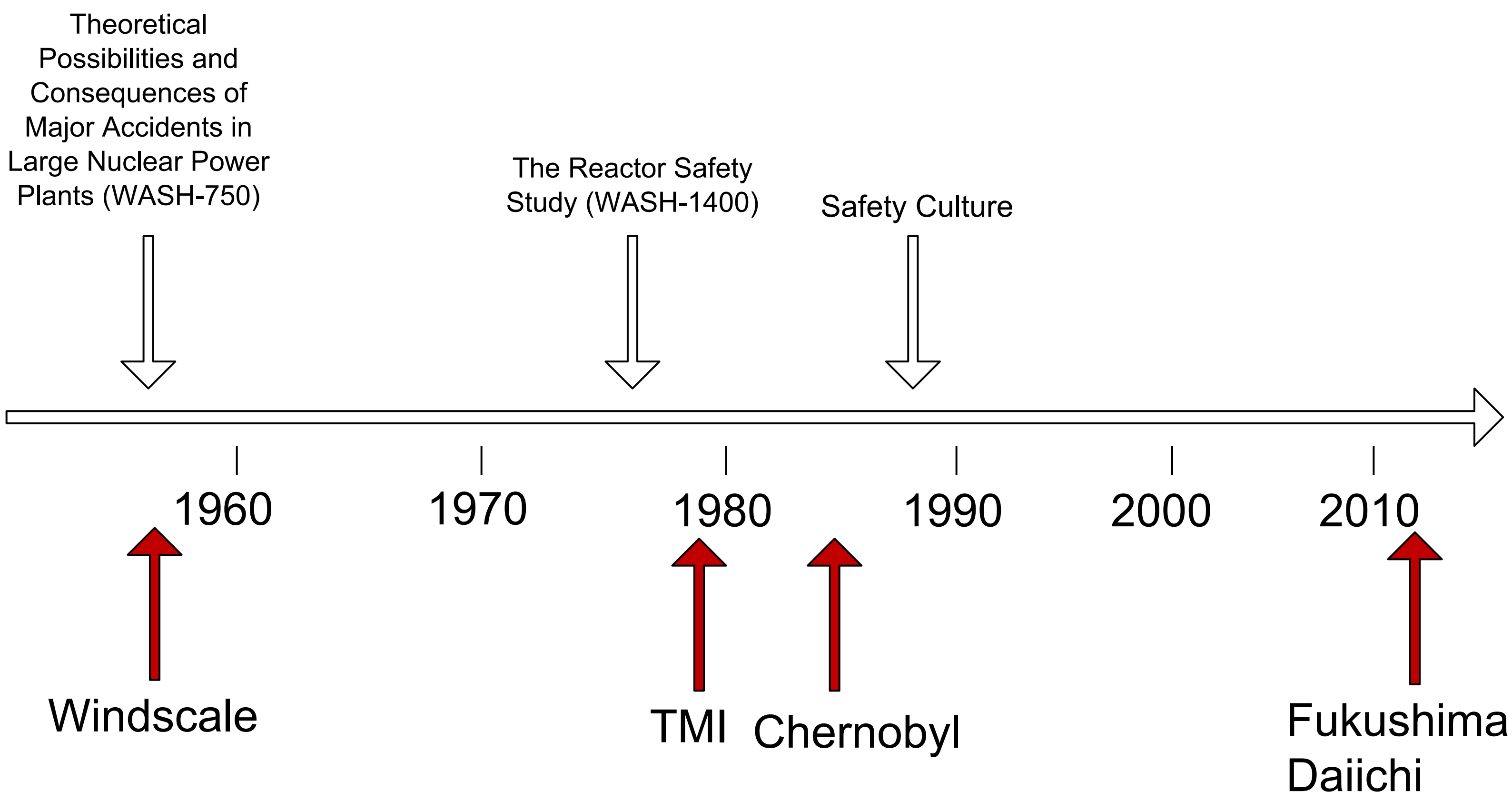
what?

What	Why	How	FRAM

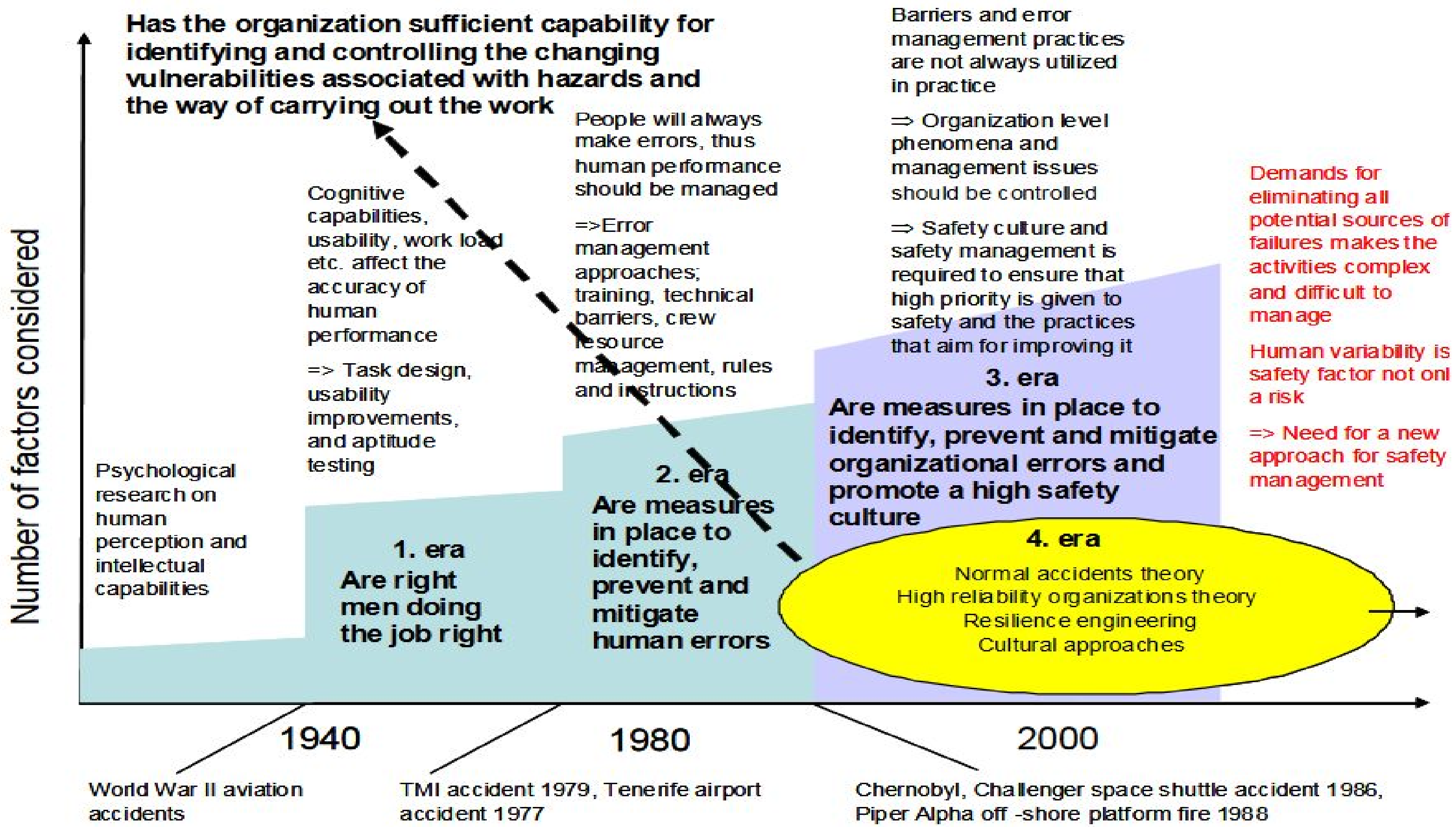


U.S. NRC (USNRC 2016)

Why ?

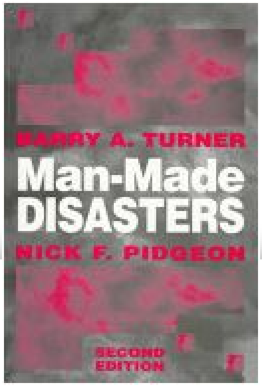


Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants (WASH-750)
The Reactor Safety Study (WASH-1400)
Safety Culture
1960
1970
1980
1990
2000
2010
Windscale
TMI
Chernobyl
Fukushima Daiichi



Evaluating safety-critical organizations– emphasis on the nuclear industry, VTT, Technical Research Centre of Finland 2009

Fukushima Daiichi Aftermath



A "manmade" disaster

The TEPCO Fukushima Nuclear Power Plant accident was the result of collusion between the government, the regulators and TEPCO, and the lack of governance by said parties. They effectively betrayed the nation's right to be safe from nuclear accidents. Therefore, we conclude that the accident was clearly "manmade." We believe that the root causes were the organizational and regulatory systems that supported faulty rationales for decisions and actions, rather than issues relating to the competency of any specific individual. (see Recommendation 1)

National Diet of Japan, 2012.The Official Report of The Fukushima Nuclear Accident Independent Investigation Commission: Executive Summary

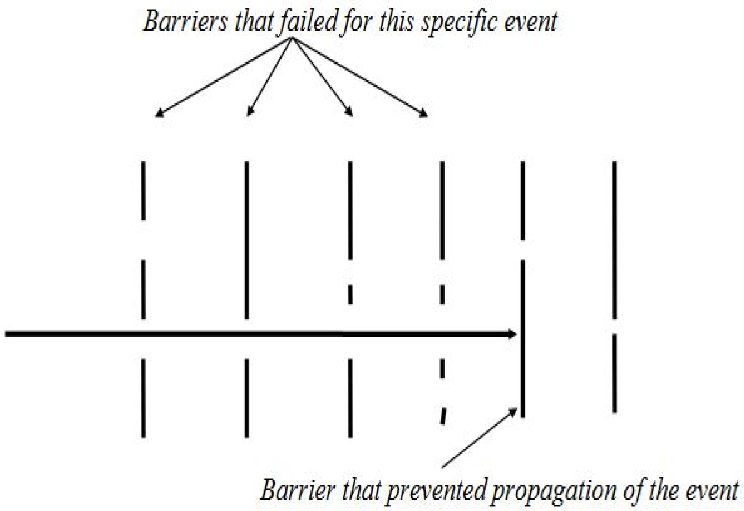
Fukushima Daiichi Aftermath

"Need to complement the traditional approach to safety with a systemic approach that considers not only the human, organizational and technological factors that contribute to safety but also the complexity of the interrelationships between them"

IAEA Report on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, International Experts Meeting, Vienna, Austria

How?

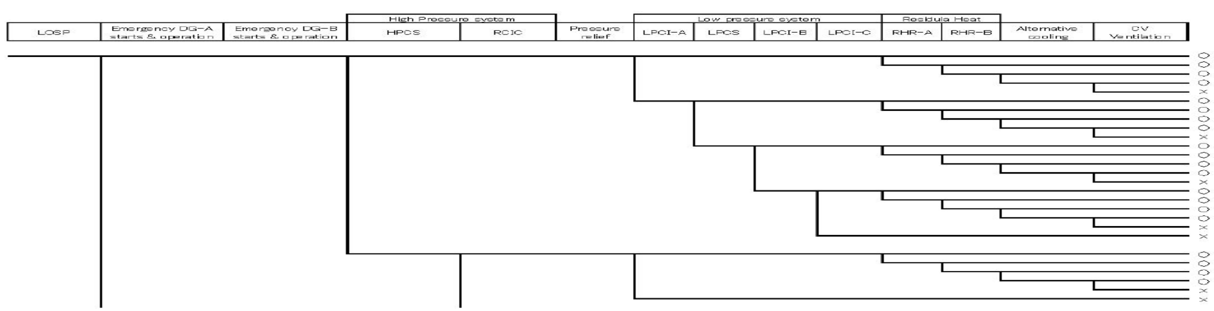
Identify and evaluate accident scenarios in order to design the system around them.



Account for the emergent factors to prepare the system to adjust itself to cope with real-world complexity .

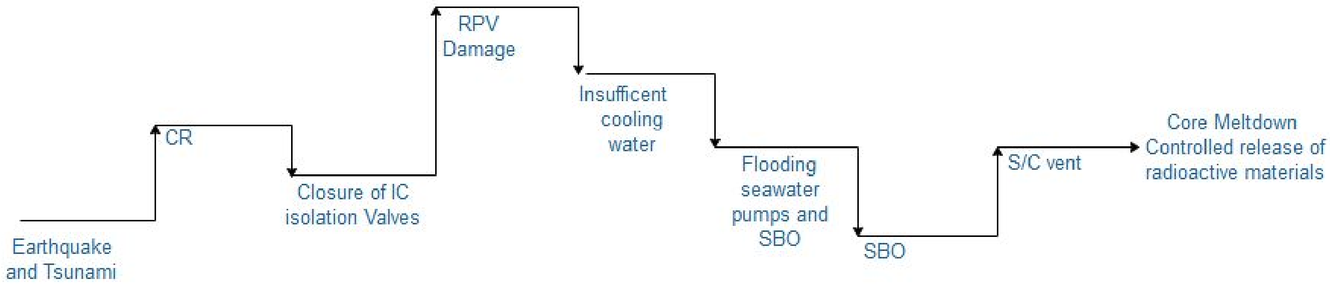
Step 1: Identification of functions

- Core functions = Safety functions and component classification
- Boundary Functions = Direct contact with safety functions



Identification of functions

IE	Reactor Shutdown	Core Cooling at High Pressure	Reactor Depressurization	Core Cooling At Low Pressure	Residual Heat Removal	PCV cooling	PCV Venting	Final State



Identification of functions

Function	Variability of the output
Reactor Shutdown	Precise
Core cooling at high pressure	Too late, closure of IC isolation valves
Reactor depressurization	Too early, PRV damage
Core cooling at low pressure	Too late, insufficient amount of water
Residual heat removal	Too late, flooding of seawater pumps
PCV cooling	Too late, site Blackout
PCV venting	Imprecise, suppression chamber ventilation

Identification of functions

Name of the function	(Reactor Shutdown) due to seismic activity
Description	Emergency Insertion of control rode
Input	SCRAM signal
Output	Reactor SCRAM
Precondition	All Instrumentation and Control (I&C) are accounted for.
Resources	--
Control	Increasing seismic acceleration procedure
Time	Immediately

Discussion

- Identification of functions
- System boundaries
- Model validation

Ciao