Fukushima

– A Failure of Institutional Defence in Depth

By

Mike Weightman

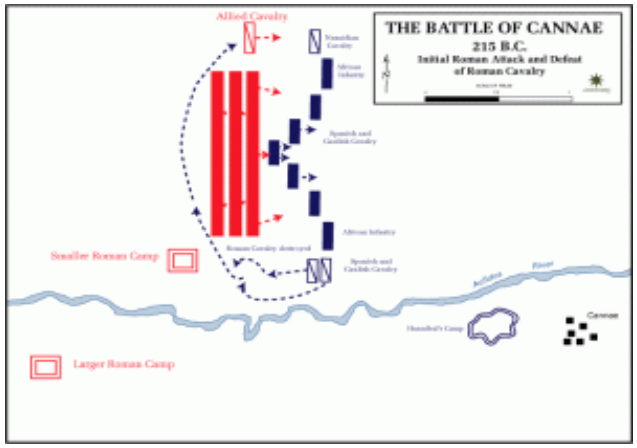
International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth
21-24 October 2013, Vienna

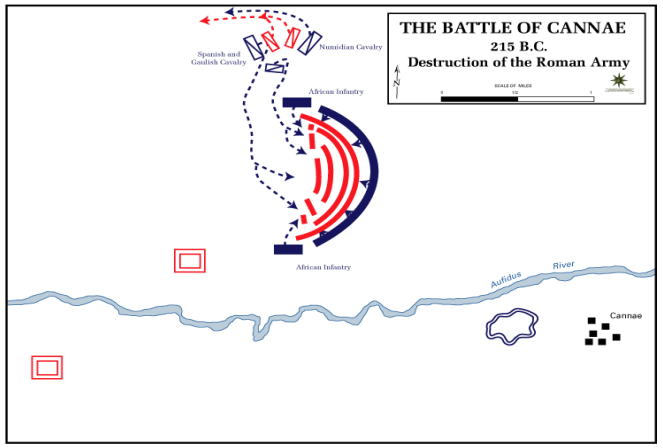
Contents

- Some generic principles for Defence in Depth
- Application to Fukushima
- Implications of Fukushima for DiD
- A Strong Nuclear Safety System – the three main DiD barriers
- Some Sub-barriers
- Assuring Strong Nuclear Safety Systems Worldwide

Defence in Depth – what do we mean?

Classically, it's about military strategies to defeat a much stronger enemy:



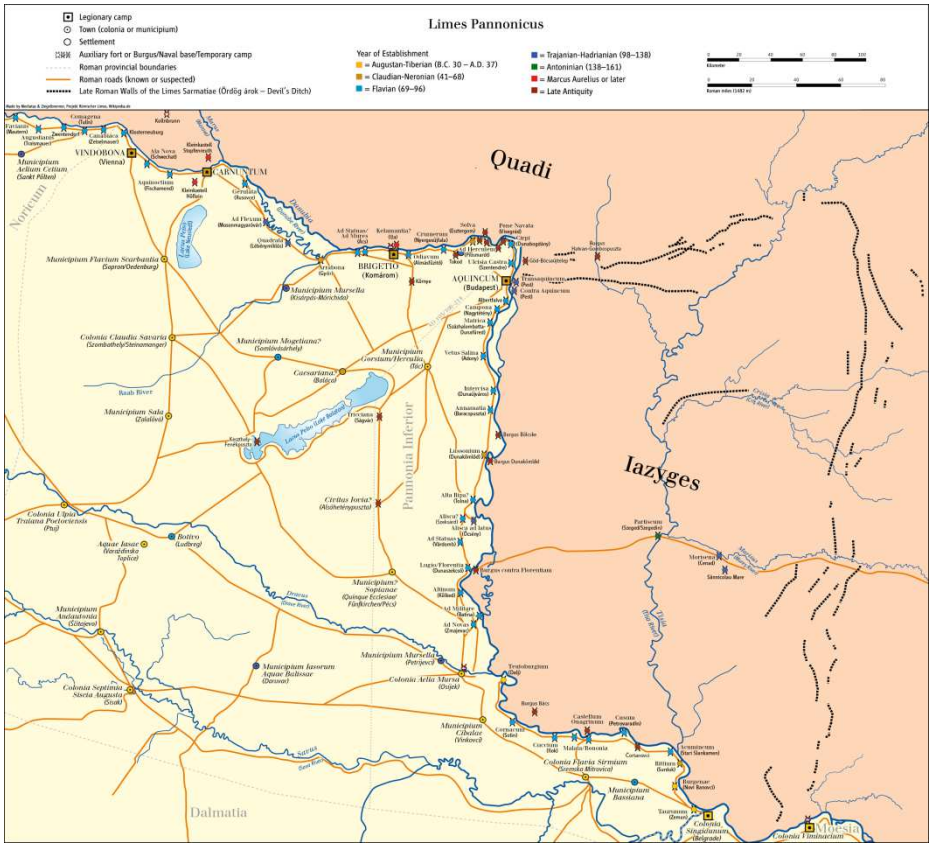


Having diversity means not putting all your forces in one block. But also about giving ground to weaken and engulf your enemy with your strongest forces.

Defence in Depth – what do we mean?

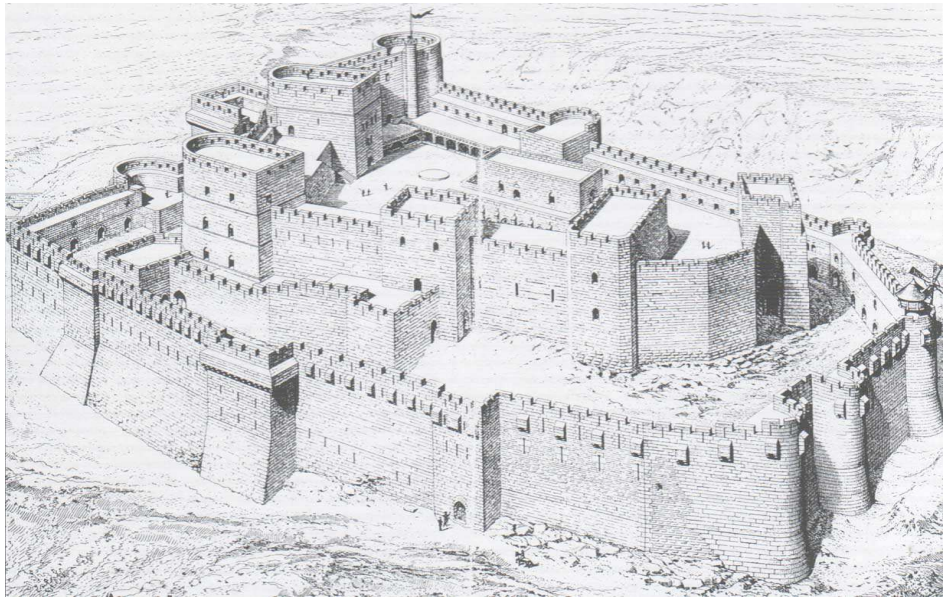
Change in Roman state defence strategy around 400AC:

Away from just very strong front line with intelligence about attacking forces in neighbouring states to multi-layered and diverse means of defeating attackers



Defence in Depth – what do we mean?

Used in castle design for centuries but also attention to siting:



Defence in Depth – what we mean: Some Principles

- Multiple layered defensive barriers
- Independence of Barriers
- Sub- barriers built on principles of:
  - diversity
  - redundancy
  - segregation
  - no single point failure
- But balance of barriers reflecting finite resources

Technical Defence In Depth - Generally Described in Five Levels

Level of defence in depth	Plant Status	Objective	Essential Means
Level 1	Normal Operation	Prevention of abnormal operation and failures by design	Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels
Level 2	Operational Occurrences	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Accidents	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Beyond Design Base Accidents e.g. core melt accident	Control of severe plant conditions in which the design basis may be exceeded, including the prevention of fault progression and mitigation of the consequences of severe accidents	Additional measures and procedures to prevent or mitigate fault progression and for on-site emergency management
Level 5	Significant off site release of radioactivity	Mitigation of radiological consequences of significant releases of radioactive materials	Emergency management and on-site and off-site emergency response

Technical Defence In Depth - Generally Described in Five Levels

Level of defence in depth	Plant Status	Objective	Essential Means
Level 1	Normal Operation	Prevention o operation and failures by d	Conservative design, construction, maintenance and operation in accordance with appropriate safety margins, engineering practices and quality levels
Level 2	Operational Occurrences	Control of ab ration and detection of	Control, limiting and protection systems and other surveillance features
Level 3	Accidents	Control of ac in the design basis	Engineered safety features and accident procedures
Level 4	Beyond Design Base Accidents e.g. core melt accident	Control of se conditions in which the design b exceeded, including the of fault progress the consequen accidents	Additional measures and procedures to prevent or mitigate fault progression and for on-site emergency management
Level 5	Significant off site release of radioactivity	Mitigation of radi gical consequences of significant releases of radioactive materials	Emergency management and on-site and off-site emergency response

Post Fukushima

Reconsideration of the DiD concept:

- NEA Steering Committee Policy Debate
- Is there a better balance between prevention and mitigation?
- This Conference
- INSAG thinking about whether to revisit its existing guidance
- Has it failed?

Fukushima – A lack of defence in depth of the Nuclear Safety Institutional System

- Inadequate design basis for external events
- Inadequate internal challenge within TEPCO
- Inadequate peer group challenge from Japanese nuclear industry or from international peers
- Inadequate challenge from Japanese regulator
- Inadequate outcome from peer review of the regulator
- Inadequate challenge from stakeholders
- Underlying cultural and institutional failings

Fundamental lesson of Fukushima is that Technical DiD can be subject to common mode failure through Nuclear Safety Institutional System Failure:

Inadequate Defence in Depth of the Nuclear Safety Institutional System

Conclusion of Analysis

- Technical defence in depth approach and principles are basically sound
- Not applied properly
- Nuclear Institutional System did not address failing – not robust
- Need to use the same DiD concept and principles to build, assess and review and challenge the Nuclear Institutional System to improve
- Backed up by a new overarching peer review of a nation's nuclear institutional system undertaken by IAEA and WANO joint teams to review and challenge

Nuclear Safety Institutional System Defence in Depth: 3 main barriers

- Level A – Strong competent Industry
- Level B – Strong competent Regulator
- Level C – Strong competent Stakeholders

Principle:

independence between Levels and underpinned by a strong vibrant safety culture - welcoming challenge, passion to improve, openness and transparency, and accountability as a way of life

What do I mean by strong?

Inner strength not brute strength:

- Strong enough to listen and absorb others' ideas
- Strong enough to not be afraid of challenge
- Strong enough to welcome new ideas and learn from others
- Strong enough to tell it as it is
- Strong enough to recognise when you got it wrong and show that you are learning from it

David and Goliath
Skills, Strategy & Inner Strength for Success

What do we mean by a Strong Regulator?

- Powerful
  - but not looking to express power, in a sense failed if have to enforce although never afraid to do so if circumstances appropriate
  - power is not just legal power but power of arguments, skills, strategy, inner strength, capabilities and values,
- Not afraid to be proportionate
- Highest standards of technical and regulator excellence
- Independence in law, practice and culture – but greater independence means need for greater accountability
- Openness and transparency at core
- Welcomes challenge and seeking ways to learn and improve
- Outcome focused
- Strong values to earn respect

Nuclear System Defence in Depth – Strong Institutional Nuclear Industry Barrier

Components of the Nuclear Industry Barrier in a State or Region			
I.1	**I.2**	**I.3**	**I.4**
Licensee	**State/Region Industry Peer Pressure**	**International Industry Peer Pressure/Review**	**International Institutional Review**
SQEP Technical/Design/operational capability	Safety Directors Forum, INPO, etc.	WANO Missions and Requirements	IAEA OSART, Design Review , Siting, etc Missions
Independent Nuclear Safety Assessment	Nuclear Industry Association, Nuclear Energy Institute, ANS	Bilateral/Multilateral Organisations e.g. CANDU Owners Group	
Nuclear Safety Committee			
Nuclear Leadership/Culture/Values			

Nuclear System Defence in Depth – Strong Institutional Nuclear Regulator Barrier

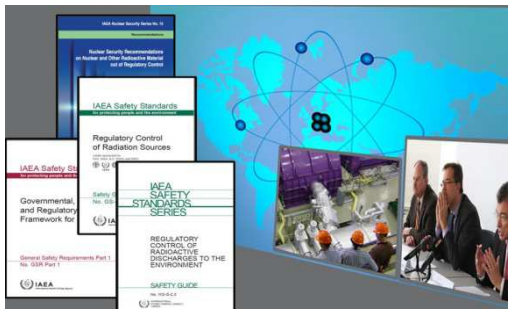
Components of a Strong Institution Regulatory Barrier			
R.1	R.2	R.3	R.4
Regulatory Authority	Special Outside Technical Advice	International Peer Pressure	International Peer Reviews
World Class Technical/Regulatory Capability	E.g. Standing Panel of experts nominated by stakeholders – CNI Advisory Panel/ Groupe Permanent d' Experts	NEA CNRA & CSNI committees and working groups	IAEA IRRS missions
Organisational Structure with internal standards, assurance, OEF, policy, strategy, etc.	Special Expert Topic Groups - Fukushima - Aircraft Crash	WENRA – reference levels, reviews, groups INRA – top regulators	ENSREG Reviews
Accountability to Governing Body – Board, Commission, etc.		IAEA Safety Standard meetings, etc.	
Nuclear Leadership/Culture/Values			

Nuclear System Defence in Depth – Strong Institutional Stakeholder Barrier

Components of the Strong Stakeholder Institutional Barrier						
S.1	S.2	S.3	S.4	S.5	S.6	S.7
Workers	Public	Parliament	National & Local Gov.	Neighbours	Media	NGOs
Industry and Regulatory Routine Supply of Information						
Routine Reports on Activities and Decisions						
Special Reports on Matters of Interest						
Responsiveness to Requests for Information						
Routine and Special Meetings						
Openness & Transparency, Accountability, Assurance – Industry/Regulator Culture and Capability						

Assuring a Strong Nuclear Safety Institutional System

- The Model of Strong Nuclear System for a MS cuts across several organisational systems – industry, regulators, governments, etc.
- And topic areas – organisational design, government agency structures, leadership, cultures and values
- Not covered in total by Any Existing Review Service
- Several Review Services touch on Particular Aspects: e.g. OSART, ISCA, IRRS, INIRM, etc
- But none give a Complete Overview of the System – nearest Integrated Nuclear Infrastructure Review Mission used for new entrants mainly
- Also, need WANO input especially on Industrial corporate/site structures, leadership and cultures



W A N O

World Association of Nuclear Operators

Proposal – New Cross Cutting Review Service for Nuclear Safety System

- Based on the Defence in Depth model of the nuclear safety assurance system
- At high level
- Using components from existing services and others as needed
- Run jointly by the IAEA and WANO, also using expertise of NEA
- Targeting the organisational, cultural, competence, values, etc. aspects of the system, independence of the barriers and sub-barriers and use of the principles of DiD

A Way Forward?

- Agree in principle – WANO & IAEA
- Review and Refine the Model
- Produce Guidance
- Pilot the Review Service
- Review and Refine Model, Guidance, Review Service
- Look to use as part of the Convention Review Process

Summary

- Defence in Depth as a concept for establishing effective technical barriers is still valid
- However, it may need re-balancing &reinforcing
- Fukushima teaches us that this it is not sufficient – you need an effective Nuclear Safety Institutional System build on the same DiD concept and principles
- Major independent barriers in the system:
  - Strong Nuclear Industry Barrier
  - Strong Nuclear Regulator Barrier
  - Strong Nuclear Stakeholder Barrier
- Need a new IAEA/WANO led review service to ensure such systems are in place worldwide feeding into Convention Review Meetings

To Better Serve the People & Society