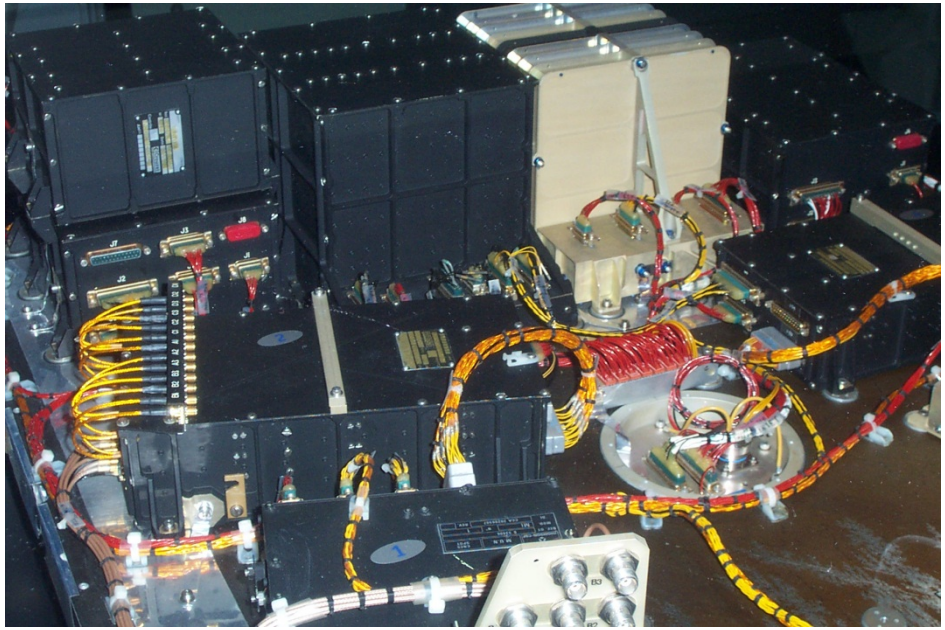
UniSA

Towards a Method to Describe Resilience to Assist System Specification

Scott Jackson, Stephen Cook & Tim Ferris



Contents

- The Challenge of Defining Resilience
- Mapping resilience behaviour onto a sequential automata
- A generic model of resilience
- A formal definition of resilience
- Using the model to define resilience
- Summary

Some Definitions

- **Resilience of an engineered system** can be thought of as the capability of the system to anticipate, survive and recover from being stressed by a threat situation.

- **A resilient system** is one which is designed to respond to threat conditions in a predictable manner, normally involving gracefulness of the amount and kind of degradation that occurs as a result of threat events.

- **Or is it? ….**

Some Definitions of Resilience

- The *Oxford English Dictionary (OED)* [6, p. 1807] defines "resilience" as "the act of rebounding or springing back."

- Hollnagel *et al* [6] regard resilience as starting with detection of an impending threat and proceeding through recovery. In contrast Richards [11] regards resilience as limited to the recovery phase whilst the original threat encounter is covered under the rubric "survivability", following definitions accepted by US DoD . But others place a heavy emphasis on the causes and prevention of accidents [8, 12, 13].

Some More Defintions

- Haimes *et al* [4] provide: “the degree of insensitivity of systems performance to errors in the assumptions of design parameters and variations in the operational. This second view is concerned with the capacity of the system to adapt to real environmental or operating conditions that differ from the design assumptions.

Aspects of Resilience

Source	Distinct aspects of resilience
Billings [12]	Prevention of accidents is dependent on the interaction among the elements of the system
Dekker [7]	Resilience effected in the hard and soft aspects of an organisation
Haimes *et al* 2008 [4]	Protective, preventive actions/preparation for response Asset level/fleet or service provision level Resilience is insensitivity to deviations from system design assumptions
Haimes 2009 [5]	Resilience includes pre-threat-encounter epoch
Hollnagel *et al* [6]	Resilience timeline starts at threat detection and ends at recovery Resilience effected in the hard and soft aspects of an organisation
Kahan [16]	Domains of interest: infrastructure/communities/organisations/ecosystems Goal: maintain continuity of function; graceful degradation; recovery function to desired level in designated time; and inhibit basic state change (with other options). Event cycle: before event; during event; post event. Approach: outcome based; process based.
Madni and Jackson [9]	Both organisational and other issues matter
Manyena [2]	Resilience as reactive/proactive Vulnerability is distinct from but not the opposite of resilience
Neches and Madni [15]	Resilience is the capacity of a system type to respond to changes of need
O'Rourke [14]	Robustness is the capacity of the system to withstand external demand without loss of functionality
Paté-Cornell [10]	Both organisational and other issues matter
Petroski [13]	Prevention of accidents can be achieved by studying past failures
Reason [8]	Both organisational and other issues matter Prevention of accidents is critical
Richards [11]	Resilience only includes the "recovery phase"
TISP [3]	Preparation/response Types of threat Threats expected/unexpected Avoidance/mitigation/recovery Assets/operations/services Minimisation of damage/disruption Public health and safety, economy, environment, National security

Dimensions of Resilience

Name	Description	Contributing Authors
Event timeline	A timeline representing the sequence of events in an encounter with a threat; this includes before, during and after encounter with the threat; with phases: Prepare/protect/design, Detection of threat, Encounter with threat, Immediate aftermath, Working towards recovery, Recovery achieved.	Kahan [16], Haimes *et al* [4], Haimes [5], Hollnagel *et al* [6], TISP [3], Richards [11], Petroski [13], Billings [12]
Hard or soft system	A continuous scale with extreme points of the hard assets and the organisation.	Dekker *et al* [7], Hollnagel *et al* [6], [9], Paté-Cornell [10], Reason [8]
Assets or services	The focus may be on the resilience of individual assets or the capacity to deliver services through a combination of assets and methods.	TISP [3], Haimes [4], Kahan [16]
Goal	A continuous scale with extreme points of robust (able to withstand threats without loss of function) through to orderly shutdown and retirement from service after threat encounter	TISP [3], O'Rourke [14], Kahan [16]
System participation	The dimension categorises the kind of response the system makes to threats with principle points: passive, reactive, proactive.	Manyena [2]
Sectoral Domain	Nominal scale; includes domains of application including (but not limited to): Infrastructure; National security; Community; Organizations; Ecosystem; Public Health; Economy.	Kahan [16], TISP [3]
Type of threat	A category scale itemising types of threat to systems, including: wind, rain, flood, earthquake, electromagnetic interference, impact, etc. Secondary threats due to interdependency.	TISP [3]
Intensity of threat	For each type of threat (type of threat dimension) a range of intensities can be defined which would distinguish the system response considered acceptable in the circumstances.	
Items that do not fit	Approach: outcome based or process based Vulnerability is distinct from but not opposite resilience Resilience is insensitivity to deviations from design assumptions	Kahan [16], Manyena [2], Haimes [4], Neches and Madni [15]

The Challenge of Defining Resilience

- Very many definitions exist and they differ in
  - The ability to anticipate and minimise threats
  - Whether the threats are limited to external threats
  - What level of stress the threats represent compared to design values
  - What constitutes recovery
  - Tolerable levels of system degradation
  - Time required to recover
- One could write papers on how best to define resilience!

Some Thoughts

- Let's assert that the system starts in the nominal operating state
- When the system encounters a threat event beyond its design limits it may transition to partially functional states and sometimes to completely non-functional states
- The transitions between these states are dependent on the type and magnitude of the threat event, the resilience of the system as determined by its design, and the decisions and actions undertaken by its operators, and the conditions including thresholds that trigger transitions.
- If the system can be repaired it can also transition back to the nominal state.

Items Needed to Define Resilience

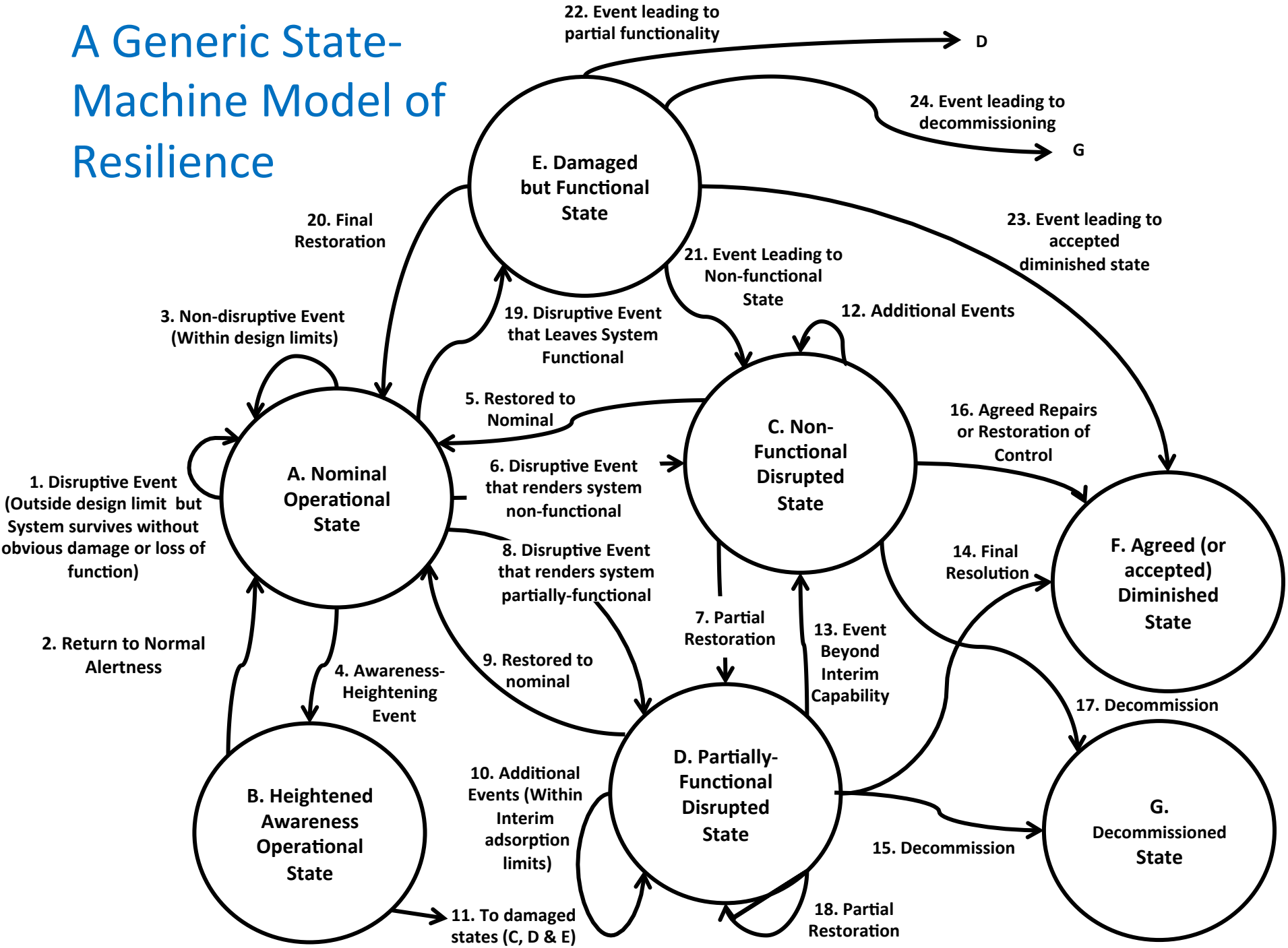
- Current operating state of the system
- The other possible states of the system
- The threats that are to be considered
- The events that trigger state transitions
- The state to which the system is expected to transition for a given event
- States to which the system should not transition
- Maximum length of duration in new state(s)
- Stochastic definitions of most of the above

Experiential Approach to Model Design

- Model: a Mealy sequential automata that comprises:
  - A set of states with defined system capability values
  - A set of transitions between states
  - A set of pre-defined state-transition triggers
  - and produces outputs based on any inputs which exceed transition thresholds.
- Model is asynchronous and stays in current state until a state-transition trigger is received.
- Model populated from a set of resilience case studies

- See paper for description of states and transitions

A Generic State-Machine Model of Resilience



Refined to become A Formal Definition of Resilience

- A formal Mealy state machine is defined as a 5-tuple $\langle Q,E,F,N,W \rangle$, where:
  - $Q=\{q\downarrow 1, q\downarrow 2, \cdots, q\downarrow |Q|\}$ is the set of discrete internal states selected to define the possible states of the system.
  - $E=\{e\downarrow 1, e\downarrow 2, \cdots, e\downarrow |E|\}$ is the set of events that can cause state transitions in the system;
  - $F=\{f\downarrow 1, f\downarrow 2, \cdots, f\downarrow |F|\}$ is the set of functional capability levels that might be exhibited by the system;
  - N is the function that relates every pair of elements $(e\downarrow t, q\downarrow t)$ from E and Q to the next state q_{t+1}, i.e. the state transitions;
  - W is the function that relates every pair of elements $(e\downarrow t, q\downarrow t)$ to an element in F, *i.e.* f_{t+1}; and
  - $|Q|, |E|, |F|$ are the number of elements in Q, E, and F respectively.

Constructing a Model for a Specific System

- Enumerate the events that need to be considered, *E*
- Decide the number of system functionality levels *F* and hence the number of states *Q*
- Complete the tables that holds *N* and *W*
- *(These would be expected to be a subset of the generic model)*

- Add any additional elements and transitions necessary to capture key information.

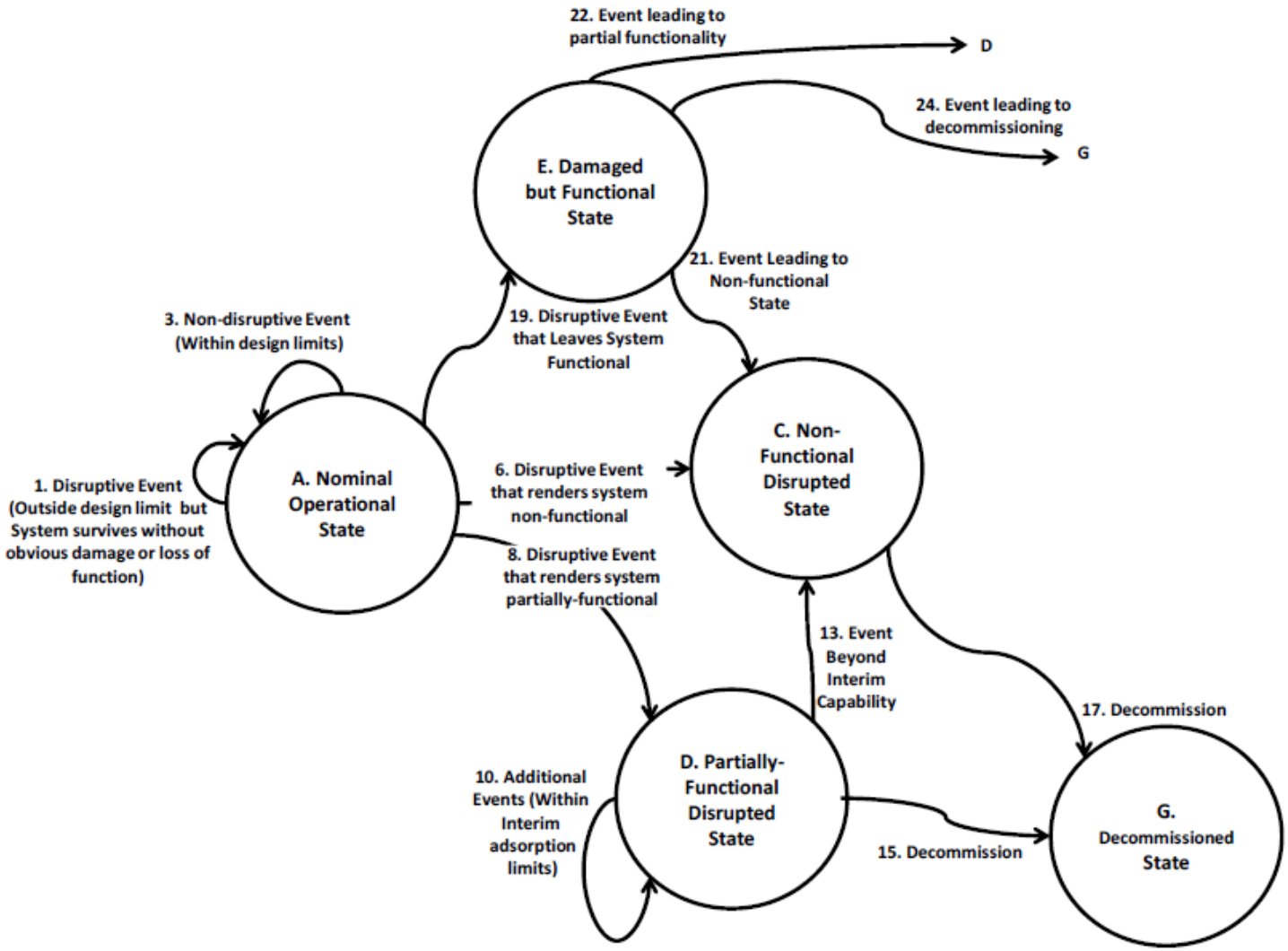
Example: Resilience States for a Electricity Generation and Distribution System

State	Discussion	Relevance to Smartphone Design
***A*: Nominal Operational State**	Primary state which the phone *should* be in for all of its useful life	Very important.
***B*: Heightened Awareness Operational State**	The phone has no awareness of threats. The user may become aware of a threat such as wet weather, potential to fall onto a hard surface and secure the phone. This is really a normal operational event and practice.	Not relevant.
***C*: Non-functional Disrupted State**	A threat event has occurred leading to damage of the phone sufficient to stop it working.	If still under warranty or covered by insurance – a claim may arise If not covered – very rare for repairs to be done with the exception of shattered screens which are likely to be replaced.
***D*: Partially-functional Disrupted State**	A threat event has resulted in some loss of function, but other functions continue to work.	If still under warranty or covered by insurance – a claim may arise If no warranty or not covered by insurance – very rare for repairs to be done with the exception of shattered screens which are likely to be replaced.
***E*: Damaged but Functional State**	User will continue to use until the user chooses to replace (probably brings forward the replacement decision).	Shattered screens are likely to be replaced, particularly if the phone is otherwise fully functional.
***F*: Accepted Diminished State**	User will continue to use until the user chooses to replace (probably brings forward the replacement decision).	Not relevant.
***G*: Decommissioned State**	User ceases use, and most likely obtains a replacement phone.	Not relevant beyond compliance with relevant laws.

Example: State Transition Table for an Electricity Generation and Distribution System

	e_1 Single Generator Failure	e_2 Start Back-up Generator 1	e_3 Start Back-up Generator 2	e_4 Repair Generator(s)	e_5 Reduce Demand
q_1 **Nominal**	q_2, 75% capacity	q_1, 100% capacity	q_1, 100% capacity	q_1, 100% capacity	q_1, 100% capacity
q_2 **Partially-Functional Disrupted**	q_2, additional 25% capacity reduction per generator lost	q_2, 12.5% additional capacity	q_1 100% capacity for single generator failure	q_1, 100% capacity	q_3, unchanged capacity level f_t
q_3 **Damaged but Functional**	q_2, additional 25% capacity reduction per generator lost	q_3, 12.5% additional capacity	q_1 100% capacity for single generator failure	q_1, 100% capacity	q_3, unchanged capacity level f_t
q_4 **Non-functional Disrupted State**	q_4, 0% capacity	q_2, 12.5% additional capacity	q_2, 12.5% additional capacity	q_1, 100% capacity	q_2, unchanged capacity level f_t
q_5 **Agreed Diminished State**	q_2, additional 25% capacity reduction per generator lost	q_5, 12.5% additional capacity	q_5, 12.5% additional capacity	q_5, 100% of original capacity	q_5, unchanged capacity level f_t

Example: State Machine Diagram for the Resilience of a Smart Phone



Conclusion

- A generic resilience model has been described.
- Model can inform specifiers, designers, operators and regulators of a particular system by providing clear identification of the resilience-related issues.
- Enables better specification of resilience characteristics, eg
  - Events that need to be considered along with magnitude and extent
  - Conditions around repair, such as repair times
  - Internal threats such as potential obsolescence of components
- Such a specification of the desired outcomes of resilience usefully informs system design and T&E

Questions?