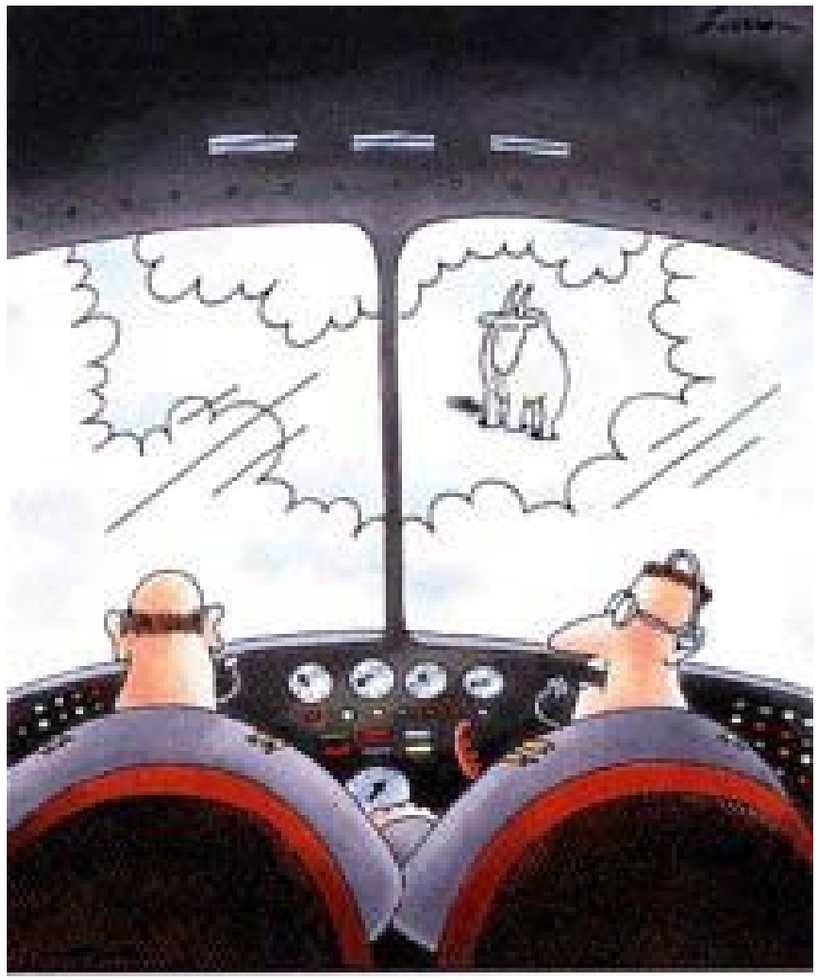


"Say, What's that mountain goat doing clear
up here in this cloud bank?"

Cybersecurity Metrics for Smart Grid Resilience

(if someone says "Cloud" I'll have bingo)

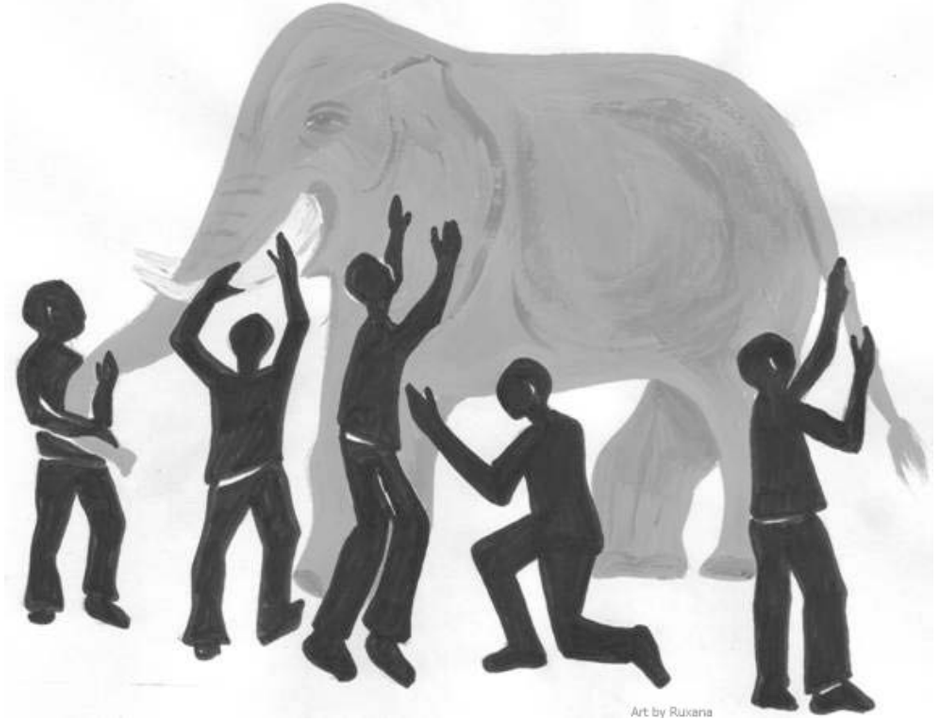
Resilience Issues

- What is "resilience"
- Three dimensions of resilience
- Composable resilience?
- Response and recovery across the grid
- Indications and warnings
- Create resilience standards
- Reusing what we are already doing

What Exactly is Resilience?

"Legacy" communities that enable resilience

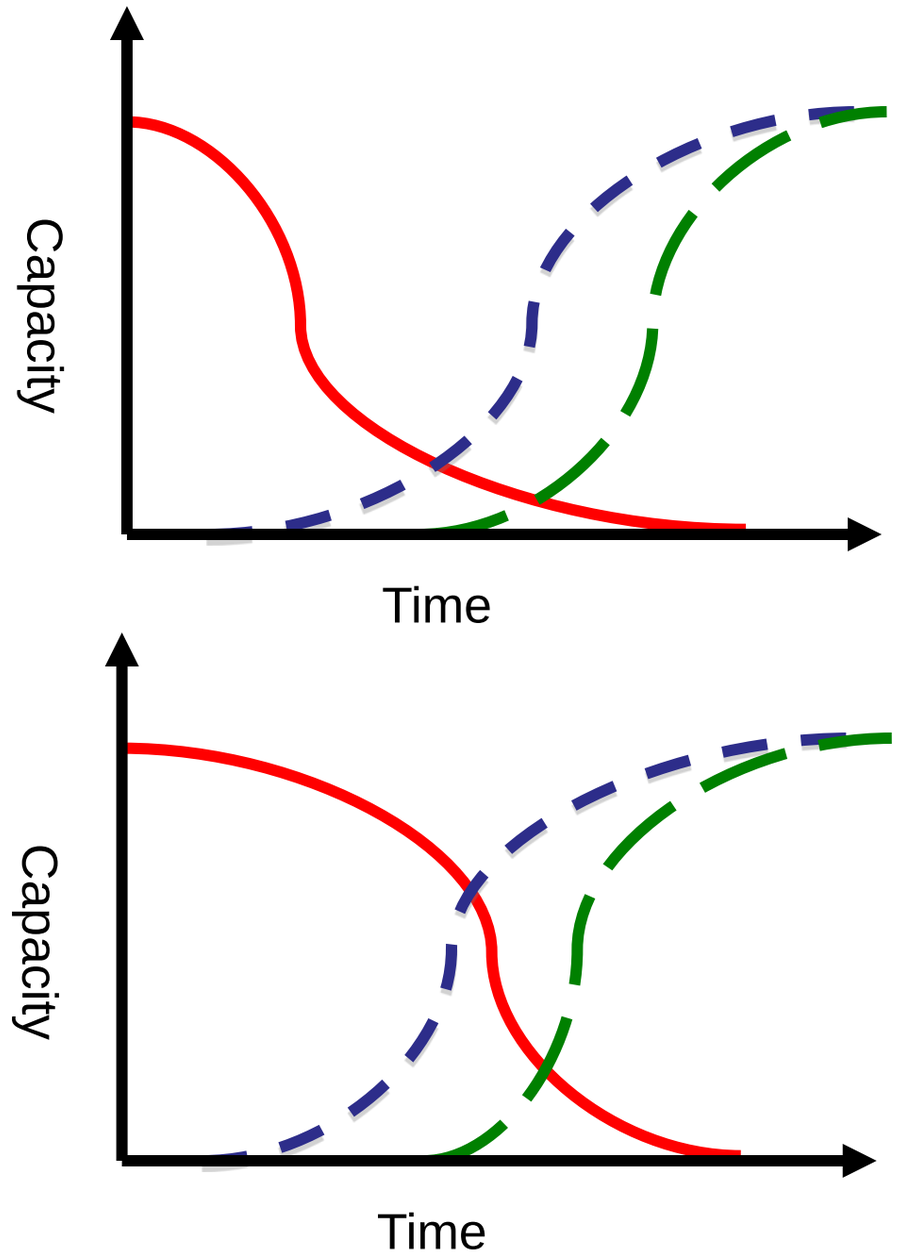
- High Assurance
- Fault Tolerance
- Reliability



Three Dimensions of Resilience

- Decay of total (or critical) capability over time
- Time to identify event/casualty/attack and take appropriate action
- Time to restore total (critical) capability

- Mission or situation specific
  - Critical functions may be different at different times (scenarios like battle, retreat, peaceful transit)
  - Ability to detect and respond may vary (Pearl Harbor?)



Composable Resilience

- Is my resilience compatible with yours?
- What is the impact of the mix of components that are State-of-the-Art and State-of-the-Past?

Indications and Warnings

- New types of monitoring
  - NASPInet information sharing
- Better synthesis of what we are monitoring now
- Better information sharing
  - Automatic
  - Actionable

Response and Recovery Across the Grid

- Who "owns" a grid wide recovery?
- Self interest versus national interests

Create Resilience Standards

- More standards?
- More regulations?

Reuse what we're already doing

For example . . .

- Leverage pertinent CIP artifacts
  - CIP 002 - risk assessment and critical assets
  - CIP 008 - response plans
  - CIP 009 - recovery plans