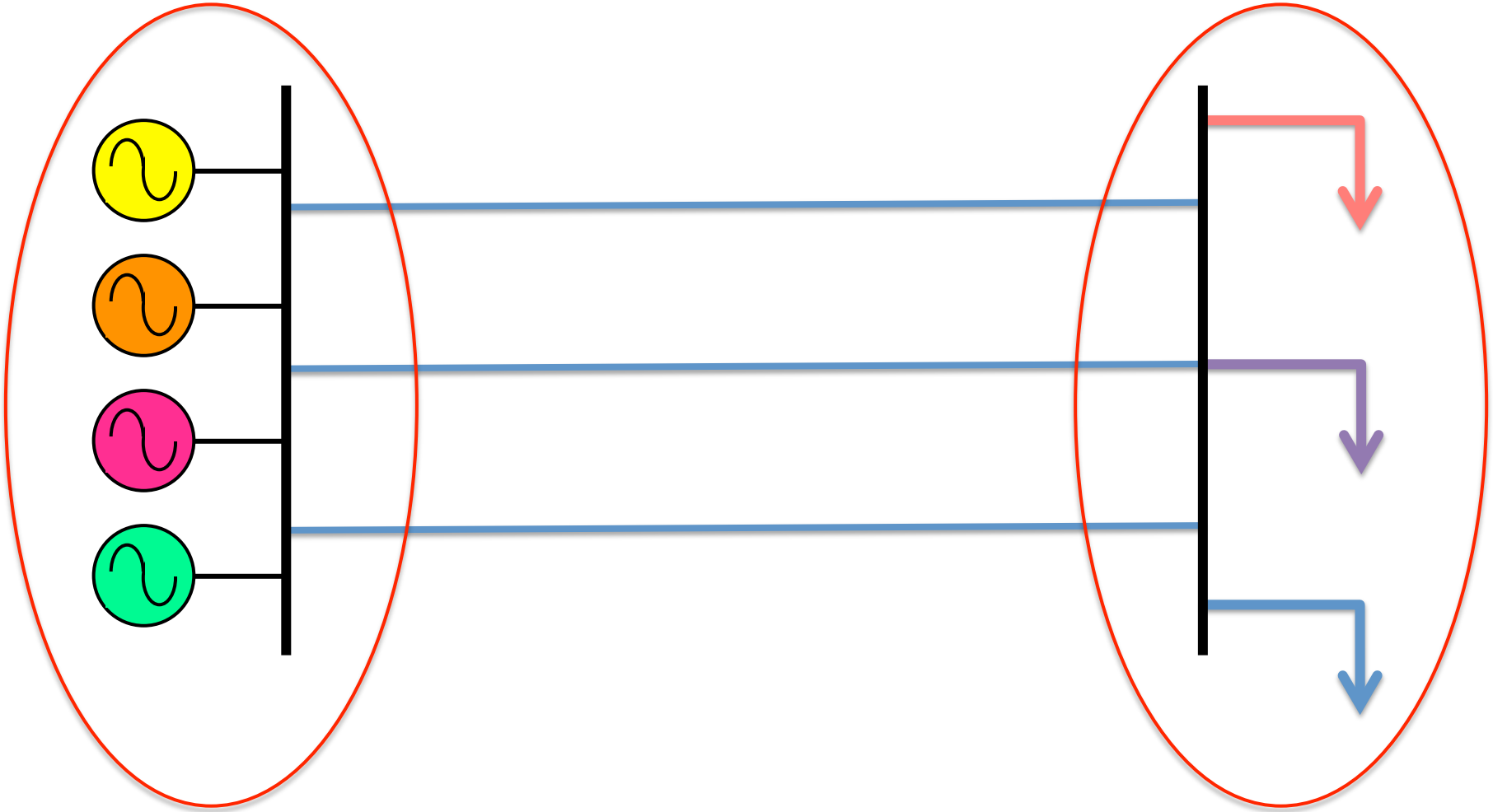
Keep the Lights on and the Information Flowing

Daniel Kirschen
Donald W. and Ruth Mary Close Professor of Electrical Engineering
University of Washington

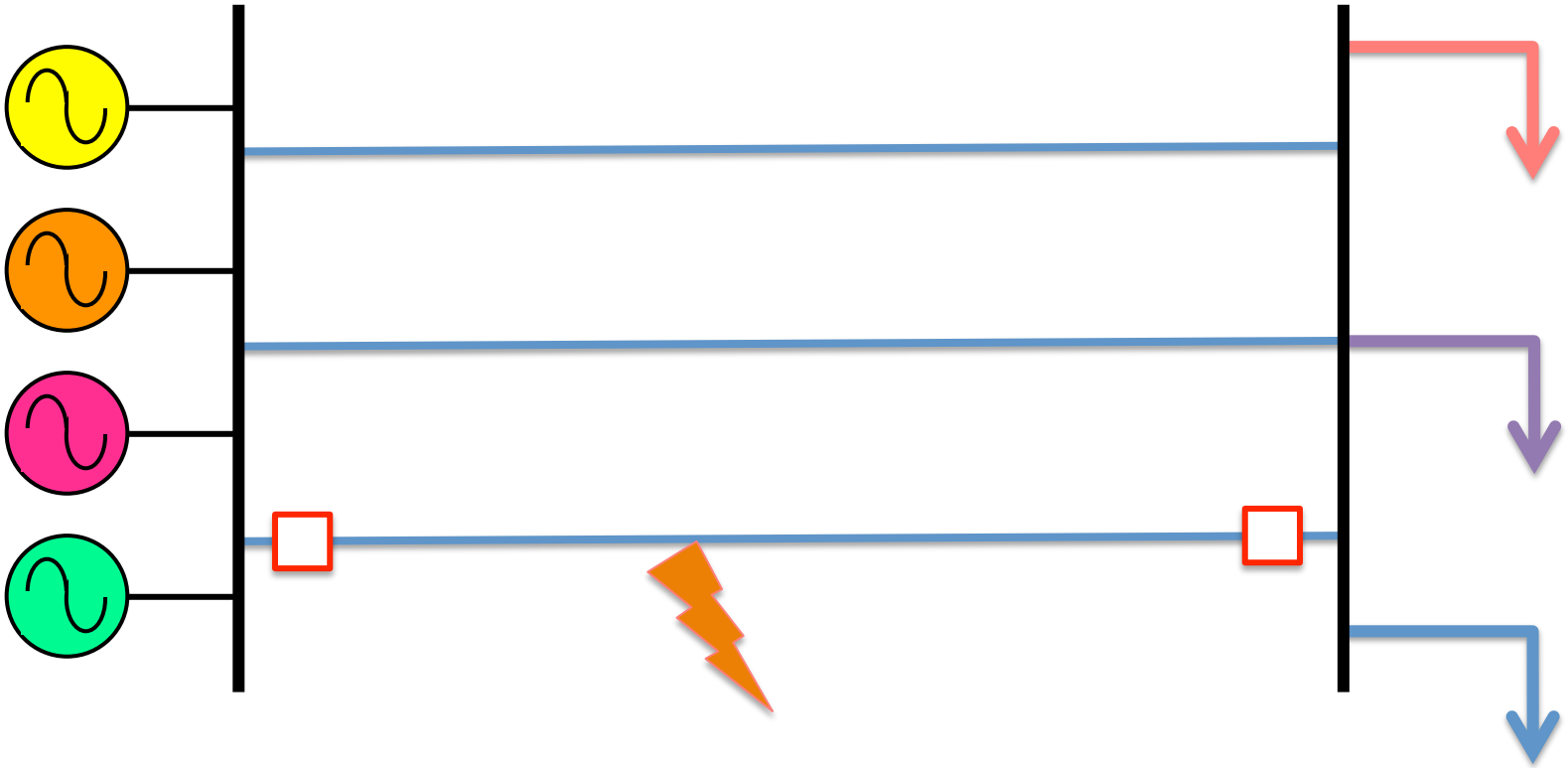
Why study blackouts?

- Cost of the blackouts
  - Direct cost (damaged equipment, ..)
  - Indirect cost (loss of economic activity)
  - Social cost
- Cost of preventing blackouts
  - Large, on-going
  - Are we spending our money wisely?

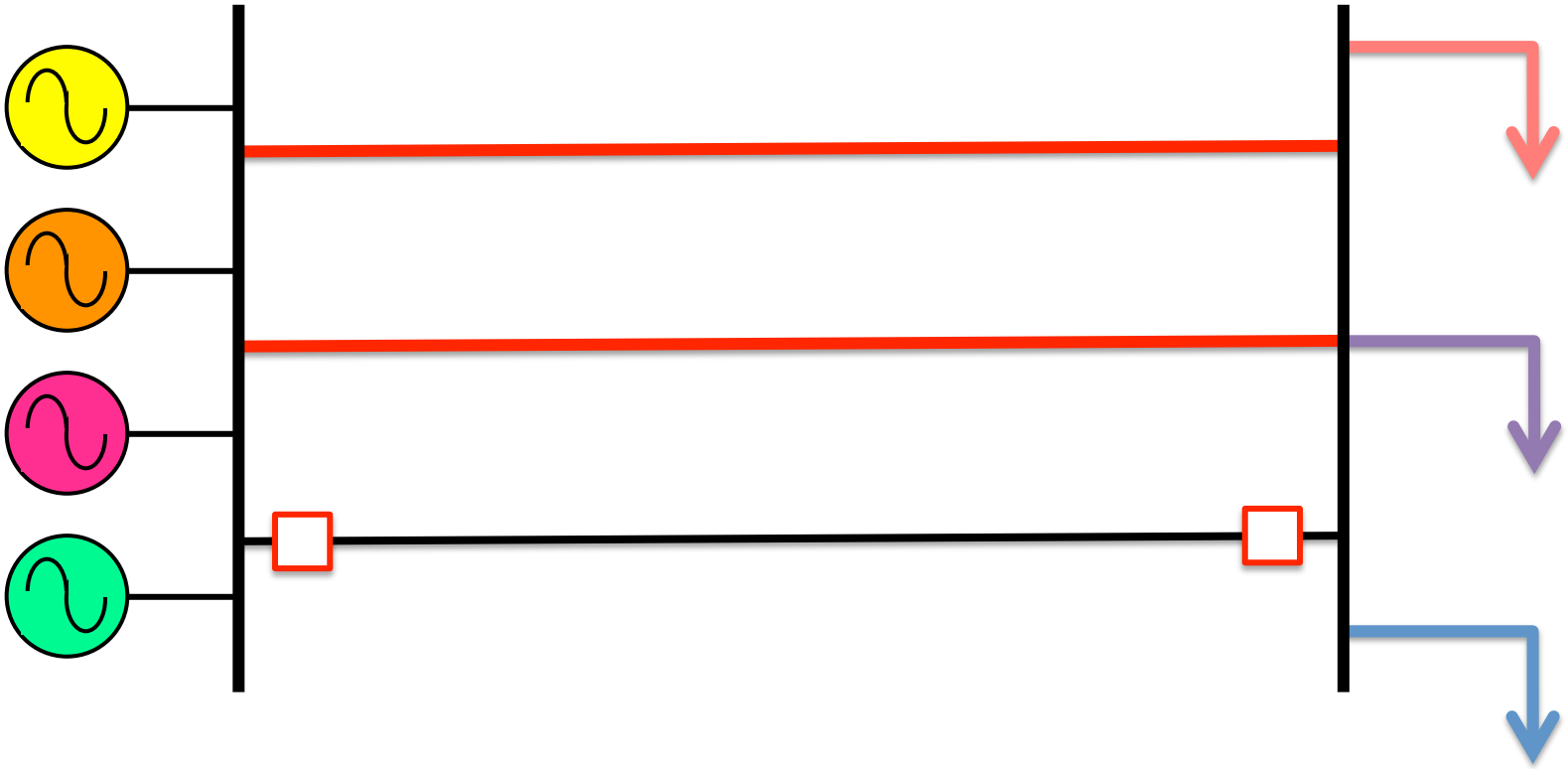
The conventional explanation



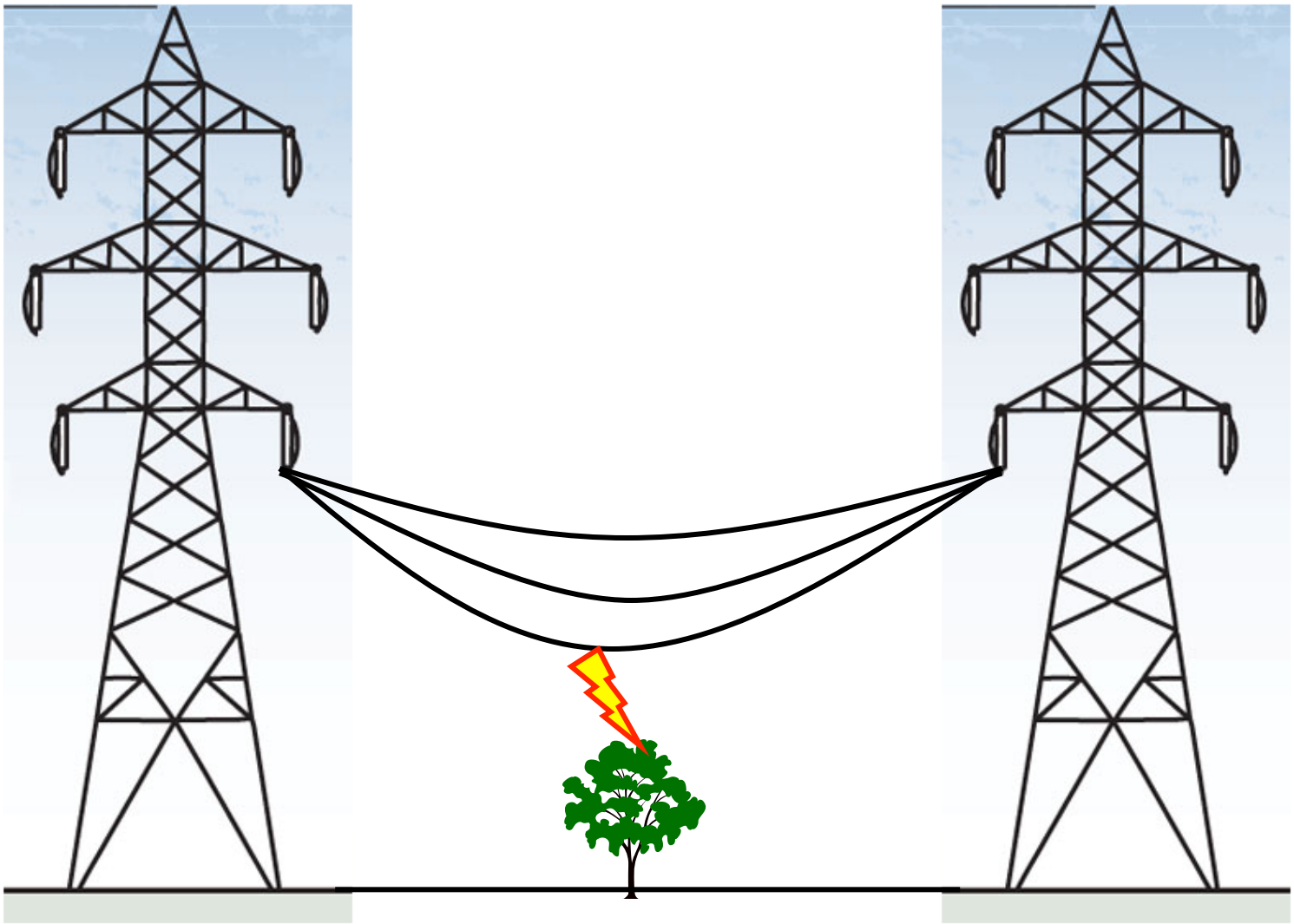
Triggering event



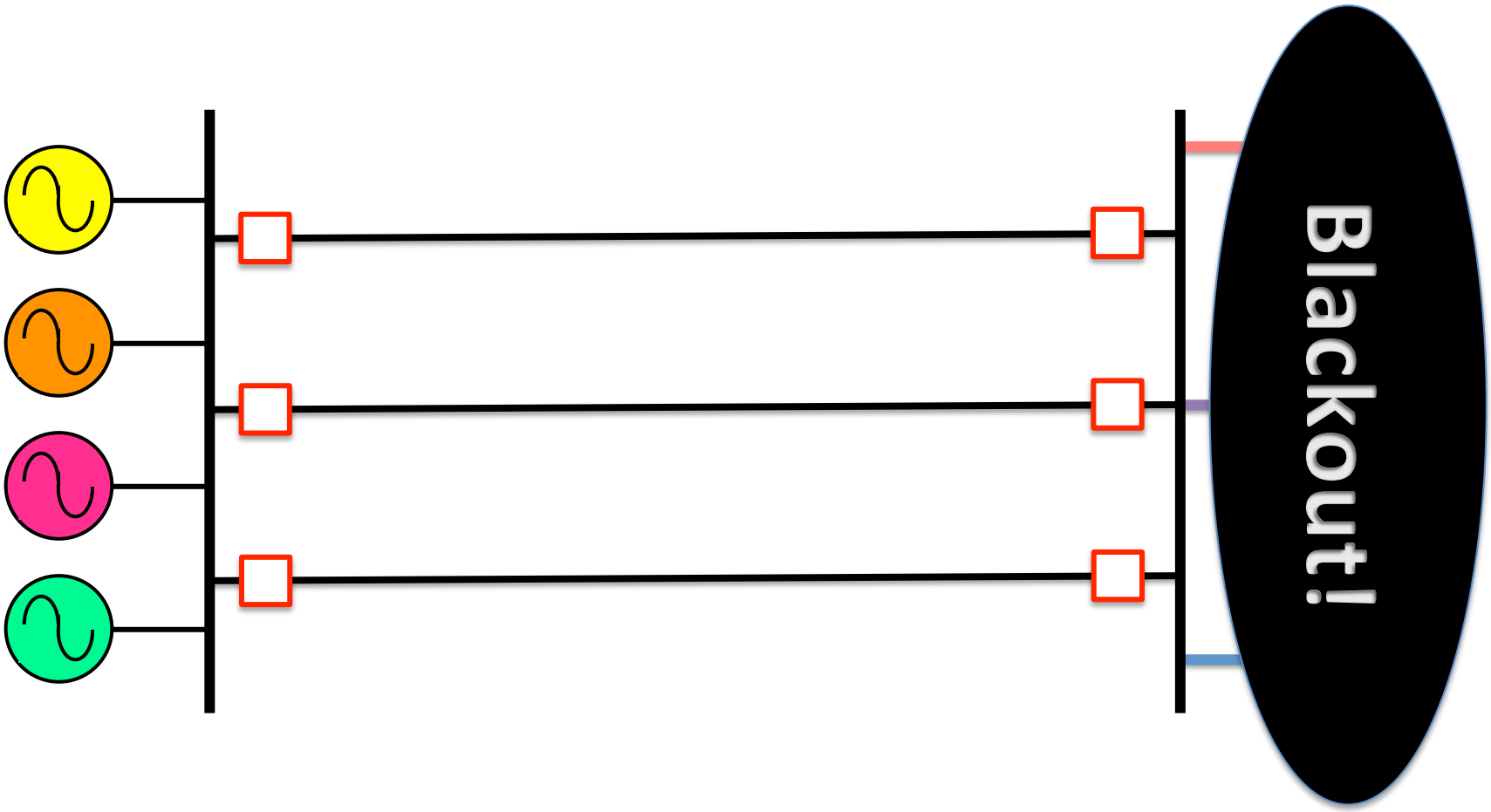
Triggering event



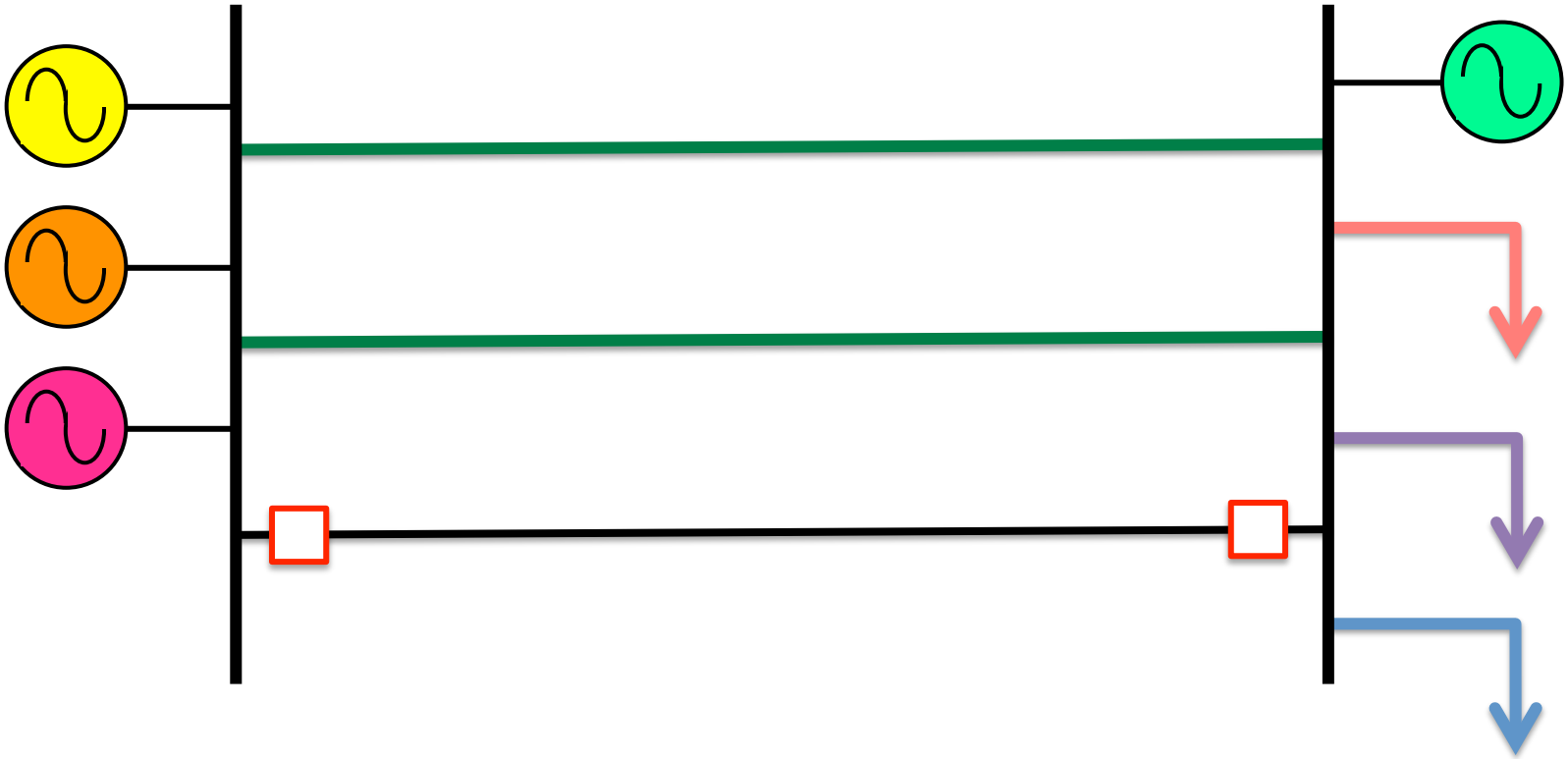
Sagging conductor



Cascading outages



N-1 security

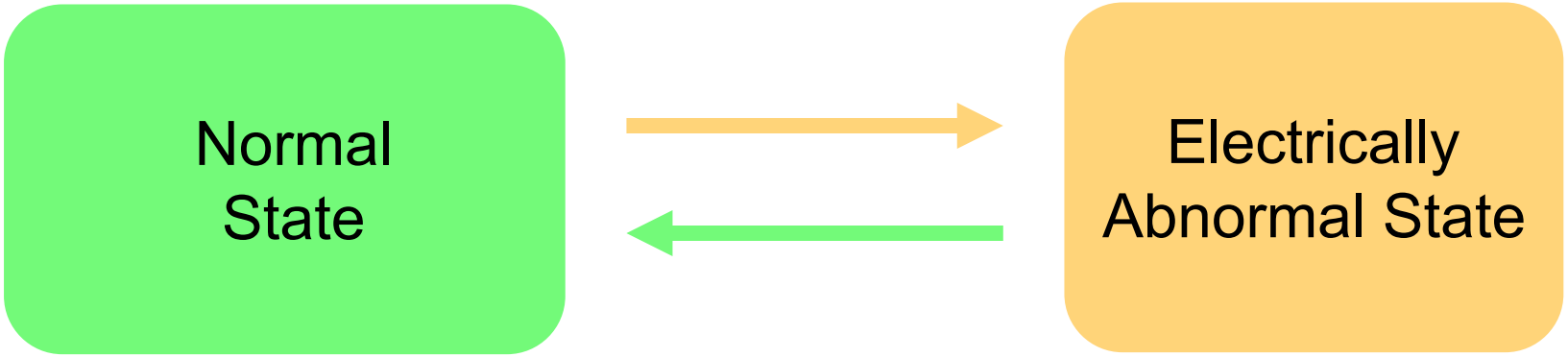


The system should remain stable following the loss of a single component

So, why do we get blackouts?

- Except under extreme weather conditions, the probability of losing two or more components nearly simultaneously is very small
- True if these outages are assumed to be statistically independent events
- Are they?

Classical power system security framework



- Operator must act to keep the system in the normal state or bring it back there if an incident takes it into the abnormal state

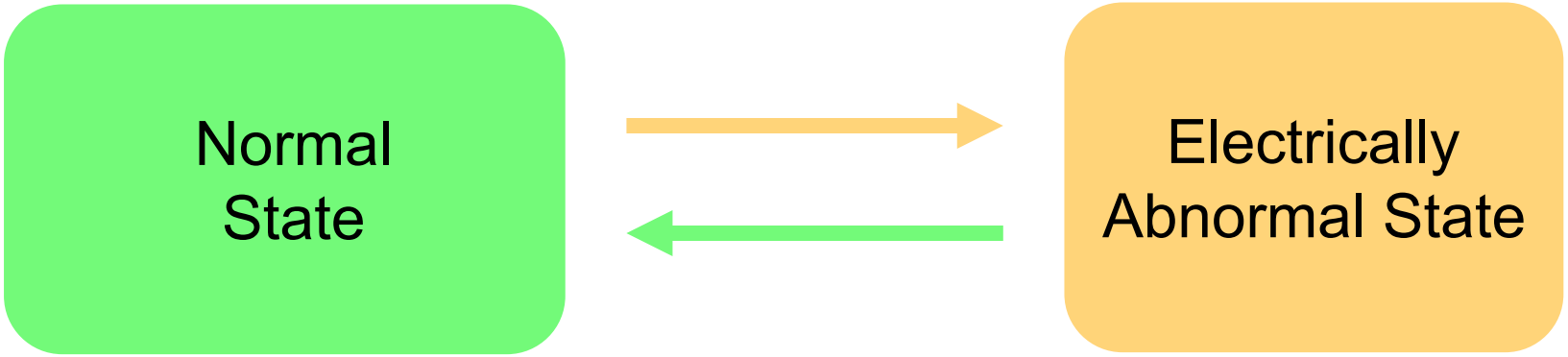
Normal state

- Stable
  - All electrical variables are within their normal range
- N-1 secure:
  - The safety margin between the state of the system and its stability limits is sufficient

Electrically abnormal state

- The margin between the operating state of the system and its stability limit does not meet the security criteria
  OR
- The system is unstable
  OR
- Some load has been disconnected (either involuntarily or voluntarily to prevent a collapse of the system)

Limitations of the classical framework



- Considers only the "electrical" part of the system
- Considers only "electrical" events
  - Faults on transmission lines
  - Failures of generating units
  - Changes in the load
- Assumes that the operator has a perfect knowledge and understanding of the state and behavior of the system

Power system infrastructure

- Electrical infrastructure
  - Lines, cables, generators, transformers, loads, …
- Information infrastructure
  - Control centers, communication links, measurement devices, protective relays, control systems, …
- Human infrastructure
  - Operators responsible for maintaining the security of the system (keeping the lights on)

Role of the information infrastructure

- Monitoring
  - Keep the operator informed
    - Status of component, voltage and flow measurements, state estimation, on-line security assessment
- Control
  - Automatic:
    - protection relays, automatic voltage regulators, automatic generation control
  - With operator intervention:
    - remote switching, optimal power flow, load shedding

Failures in the information infrastructure

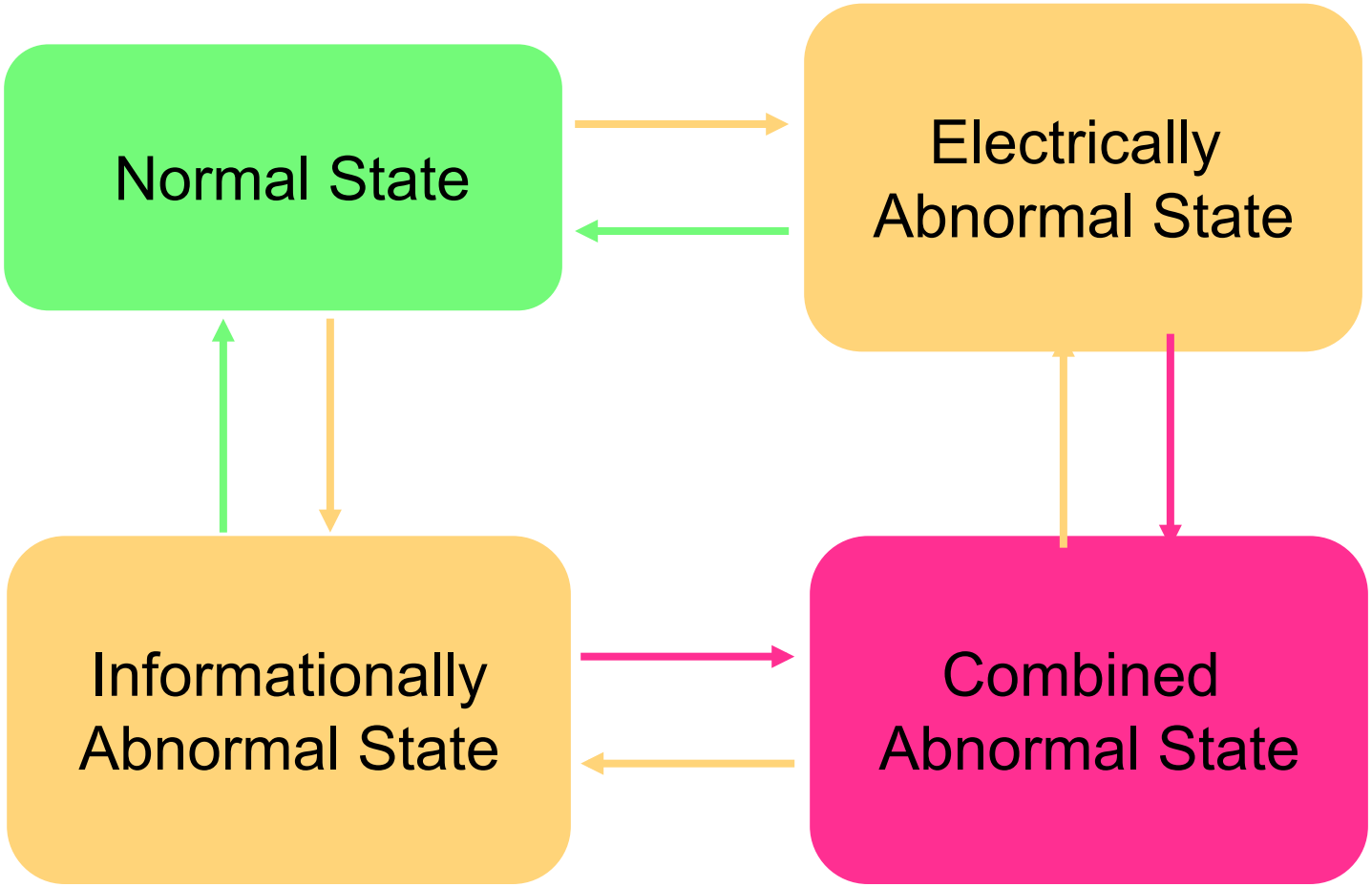
- Examples
  - Malfunctions of protection relay
  - Incorrect or unavailable measurement
  - Failure of a remote control command
  - Non-convergence of state estimator program
  - Loss of a communication link
  - Software crash
- Some redundancy:
  - Backup protection, backup computer system, etc…

New power system security framework

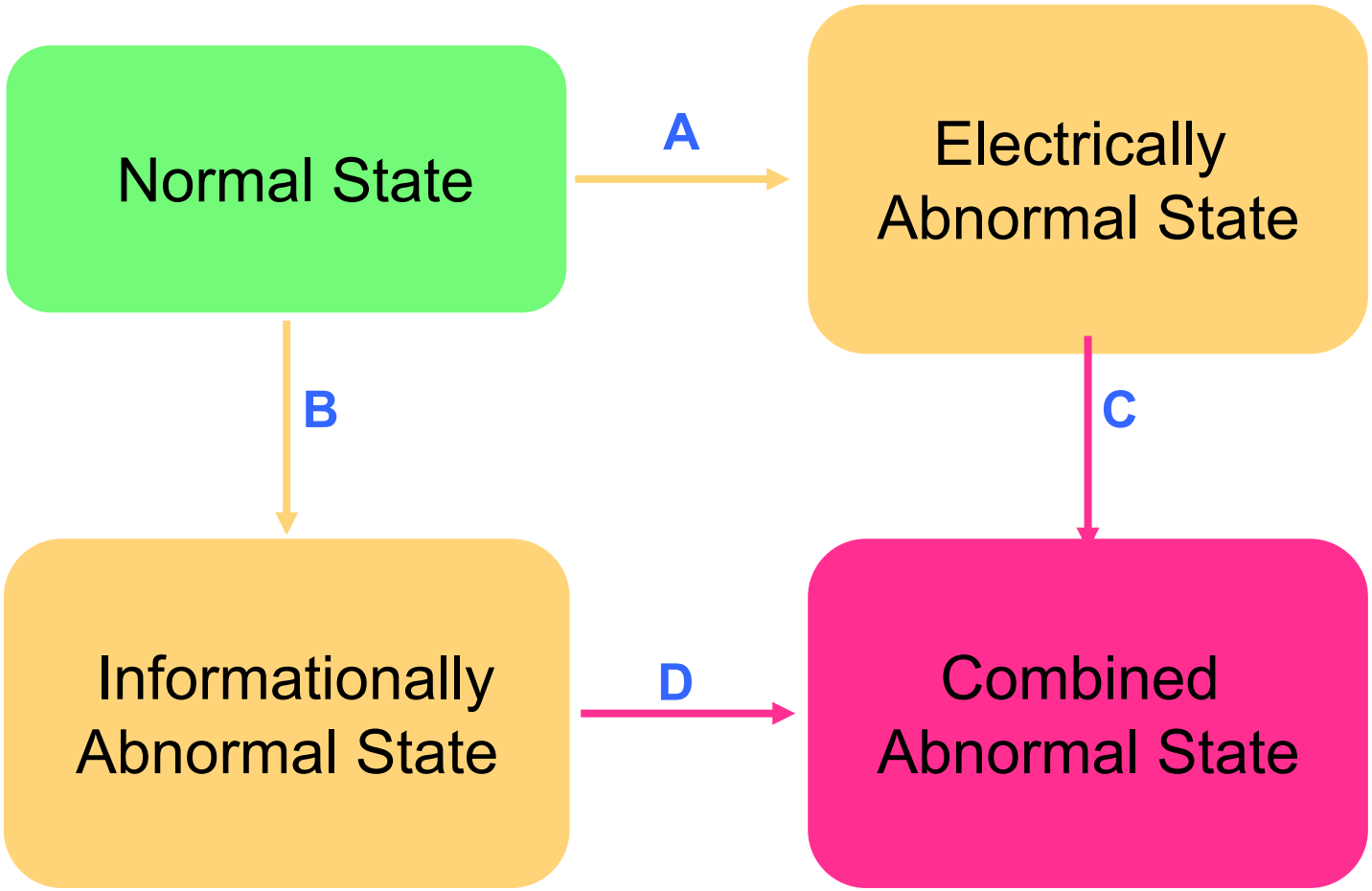
- *Informationally abnormal state*
  - Any component of the information infrastructure has stopped operating or has malfunctioned

- *Combined abnormal state*
  - Abnormal from both the electrical and informational perspectives

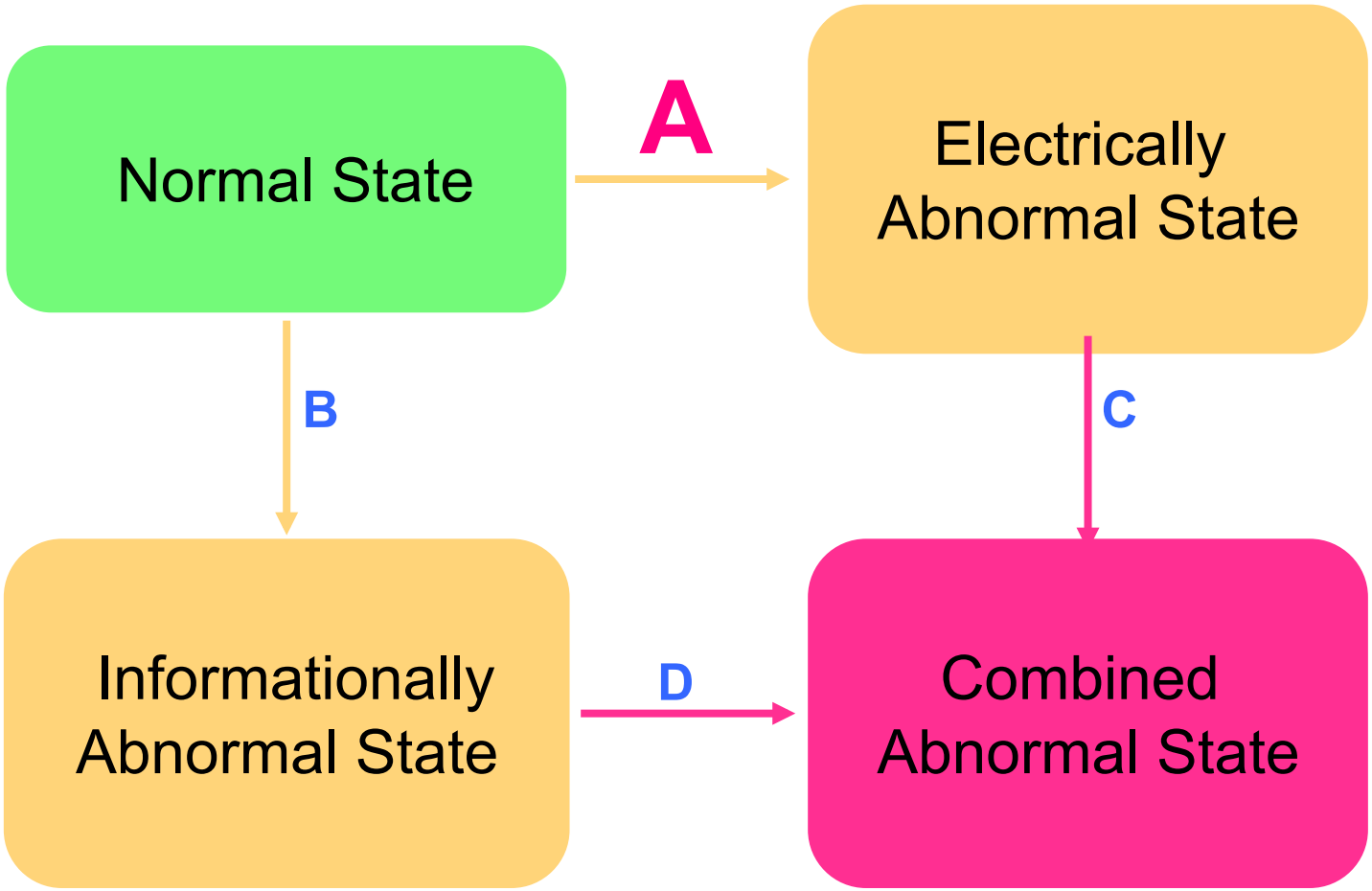
New power system security framework



Transitions



Transitions



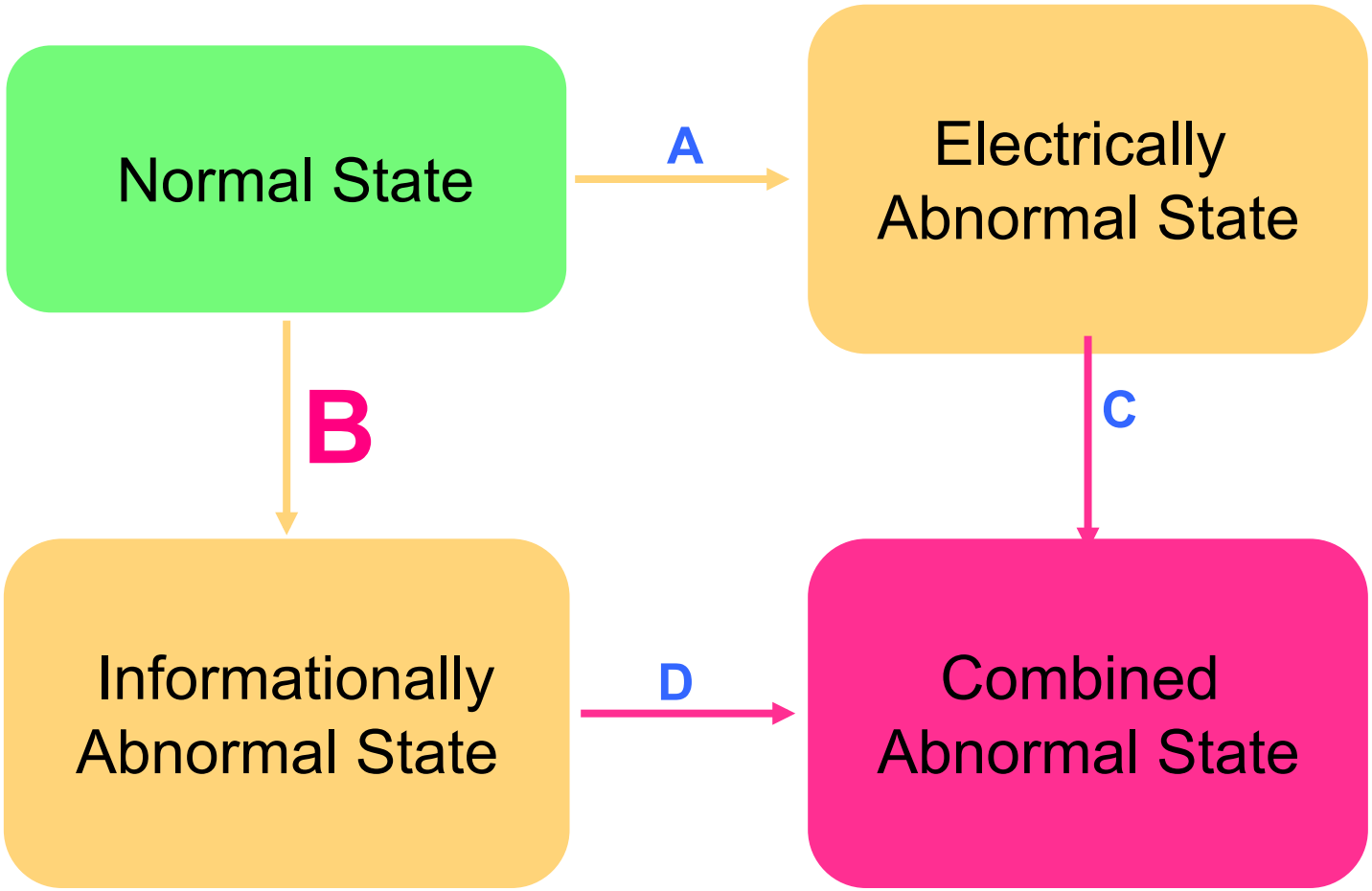
A: Normal to electrically abnormal

- Examples:
  - Failure of one or more electrical components
  - Unexpectedly large or fast change in the load
  - Failure by the operator to react in a timely manner to a change in system conditions

A: Normal to electrically abnormal

- Not all electrical failures lead to the electrically abnormal state (e.g. when the system is not stressed)
- Further degradation within electrically abnormal state can happen (e.g. cascade outages)
- Return to normal state involves re-adjustment of electrical control variables (e.g. generation dispatch)

Transitions



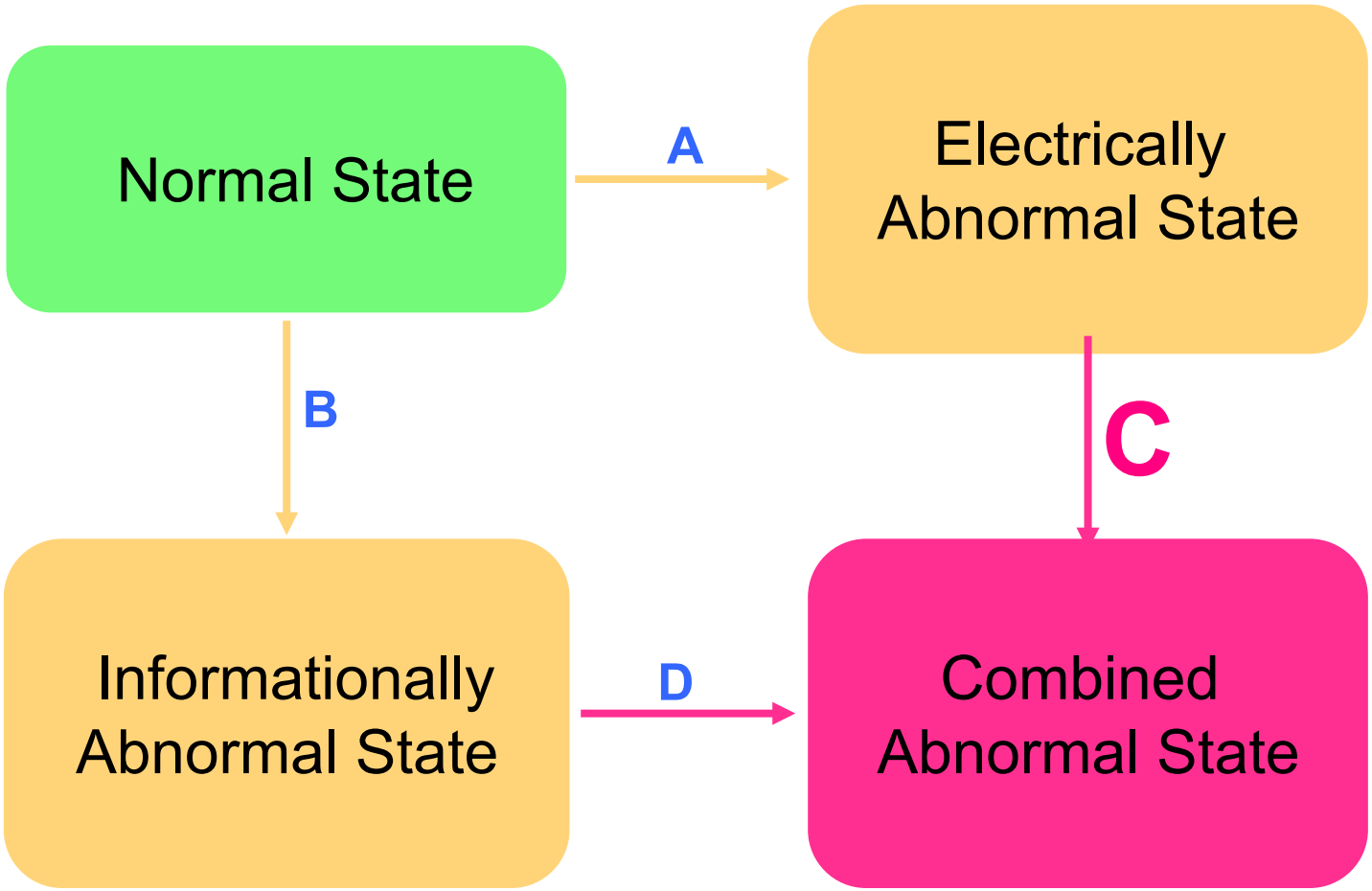
B: Normal to informationally abnormal

- Examples
  - Failure of any element in a measurement chain
  - Failure of any element in a remote control chain
  - Failure of a local control system (e.g. AVR, governor)
  - Failure of a communication link between a substation and the control center
  - Failure of a protective device to react properly to an electrical fault
  - Inappropriate action by a protective device
  - Failure of one of the computer programs that support the monitoring of the system by the operator

B: Normal to informationally abnormal

- Causes of Type B transitions
  - Hardware failures
  - Software faults
  - Malicious attacks
- Some type B transitions are easily detected:
  - e.g. failure of a communication link
- Other type B transitions are almost impossible to detect:
  - e.g. hidden failures in protection relays
- Return to normal state requires hardware repair or software reset

Transitions



C: Electrically abnormal to combined abnormal

C1 Electronic failure due to loss of power supply

C2 Hidden failure in protection system revealed by electrical fault

C3 Alarm processing function at the control center is overwhelmed by number of alarms triggered by electrical problem

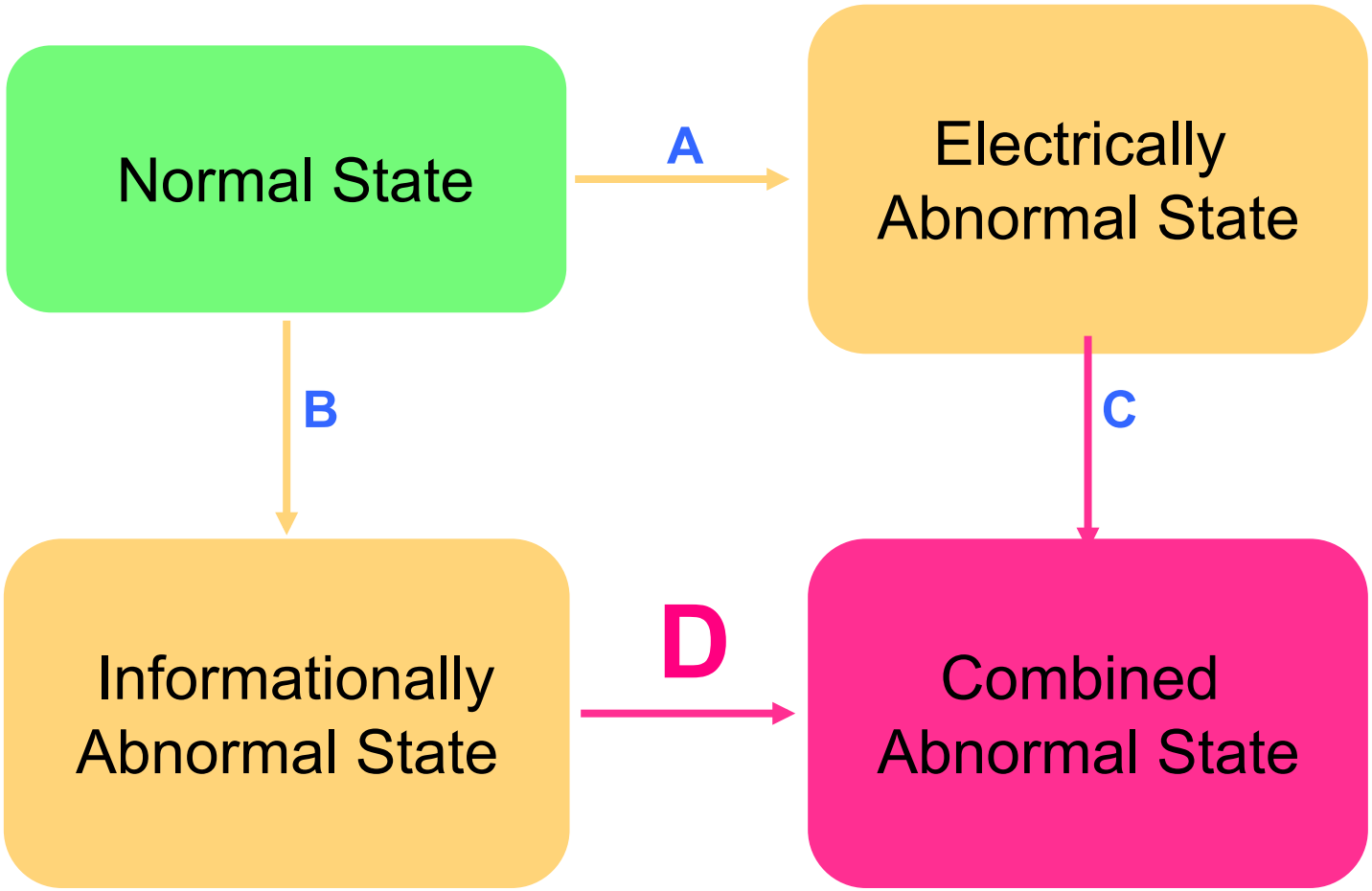
C4 State estimator fails to converge because the electrical system has moved too close to the stability boundary

C5 An unrelated electronic failure happens after the electrical state has become abnormal

C: Electrically abnormal to combined abnormal

- These transitions are dangerous because:
  - They reduce the operator's ability to respond to the electrical problem (C1, C3, C4, C5)
  - They make the electrical problem worse (C2)

Transitions



D: Informationally abnormal to combined abnormal

D1 Abnormal electronic state prevents the operator from becoming aware that corrective action is required.

D2 Abnormal electronic state prevents the operator from taking appropriate corrective action.

D3 Based on incorrect information or advice, the operator takes inappropriate action(s)

D4 The failure of an electronic component triggers an electrical transition.

D5 A cyber attacker triggers actions that deteriorate the electrical state of the system

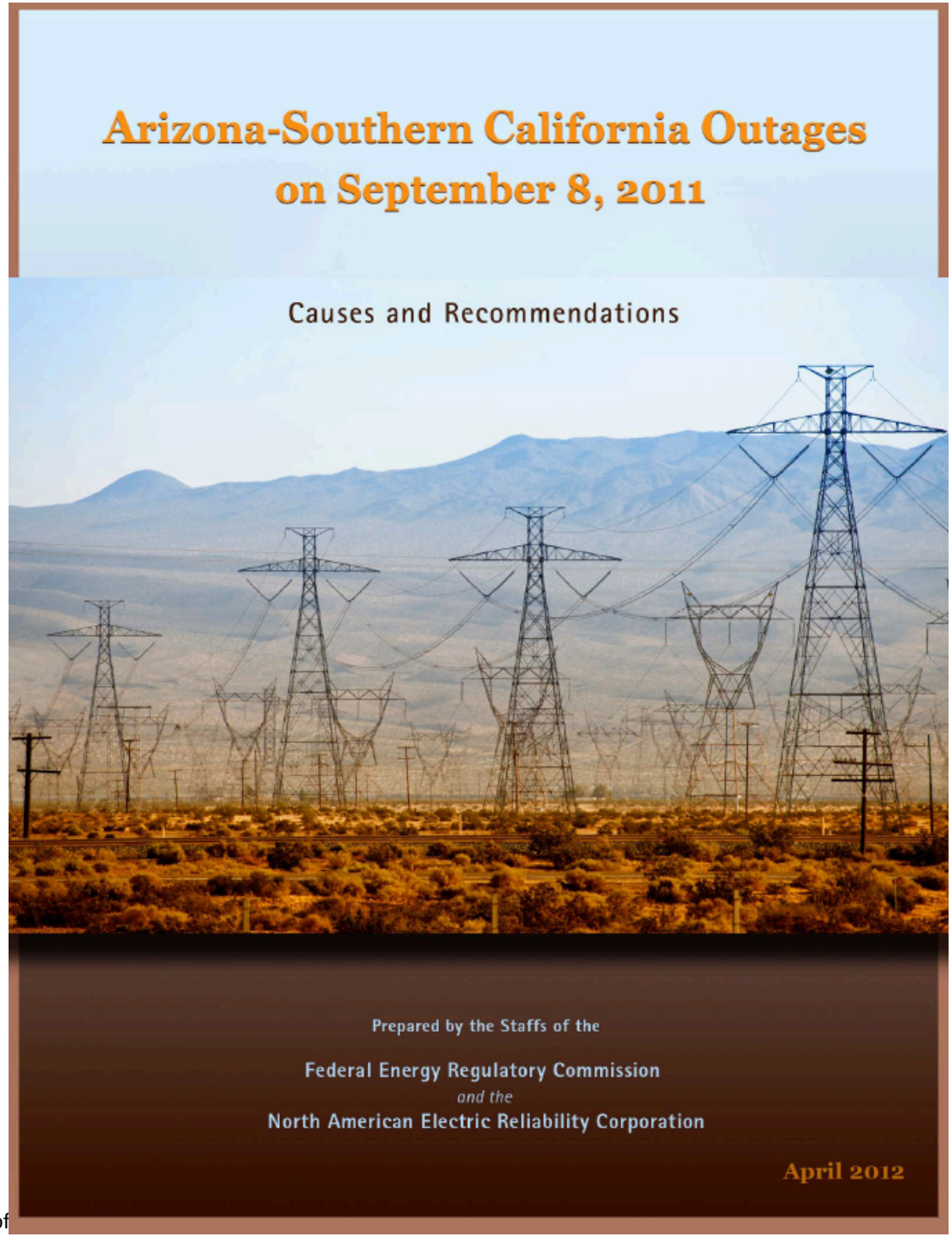
D6 An unrelated electrical deterioration takes place after the electronic state has become abnormal.

D: Informationally abnormal to combined abnormal

- Probably the most dangerous transitions
- Failures of type D4 are not very likely because of built-in fail-safe mechanisms
- Need to study the details of types D1, D2, & D3
  - How likely are these transitions?
  - How quickly would an electronic failure cause electrical problems?
  - How could such problems be mitigated?
  - How could such transitions be caused maliciously?

Examples

Incident	Transition
North America (2003)	D1
London, UK (2003)	C2
West Midlands, UK (2003)	C2
Italy (2003)	D1
UCTE (2006)	D1
WSCC (1996)	C2
Ireland (2005)	D4
Québec (1988)	D2
Québec (c. 1985)	C3
Sweden/Denmark (2003)	-



Enhancing the information infrastructure

- Enhanced functionality
  - Better information about the state of the system
  - Faster, more accurate control actions

  ➔Need for safety margin is reduced

  ➔Economics pushes towards operation at the limit

  ➔Risk of customer outages is not necessarily reduced

Enhancing the information infrastructure

- Enhanced reliability
  - Reduce risks
    - Missing or incorrect information
    - Incorrect or failed control action

➔Significant reduction in risk of customer outages

Enhanced modeling

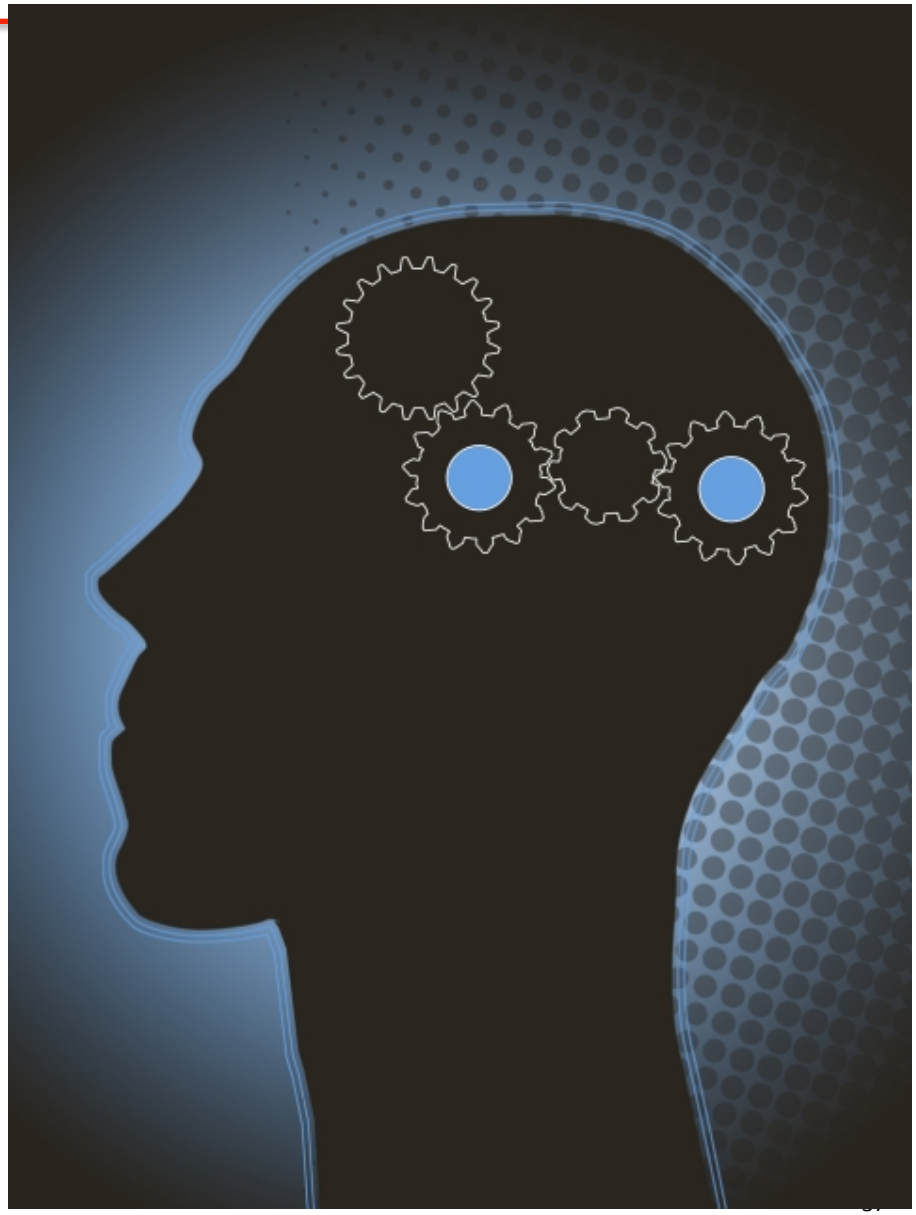
- Electrical infrastructure
  - Excellent structural and functional models
  - Reasonably good reliability data
- Information infrastructure
  - Good structural models
  - Very poor functional models
  - Complete lack of reliability data
- Human infrastructure
  - ?

What is the state of the system?

Actual State

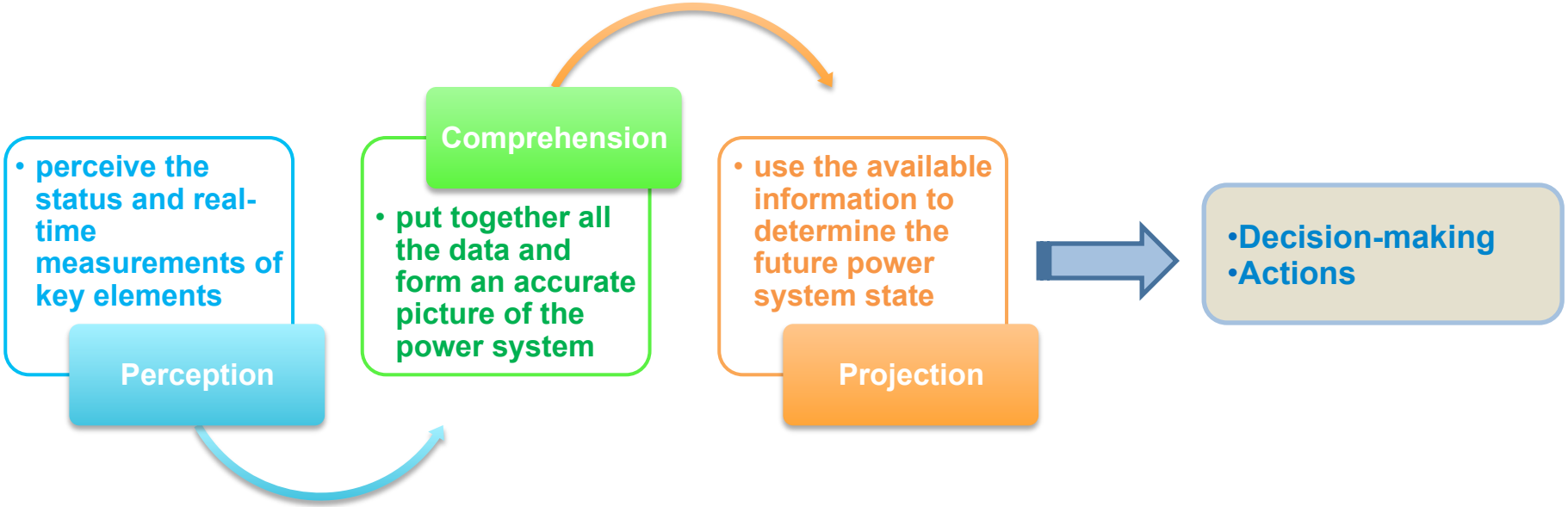
Reported State

Perceived State



Situation Awareness (SA)

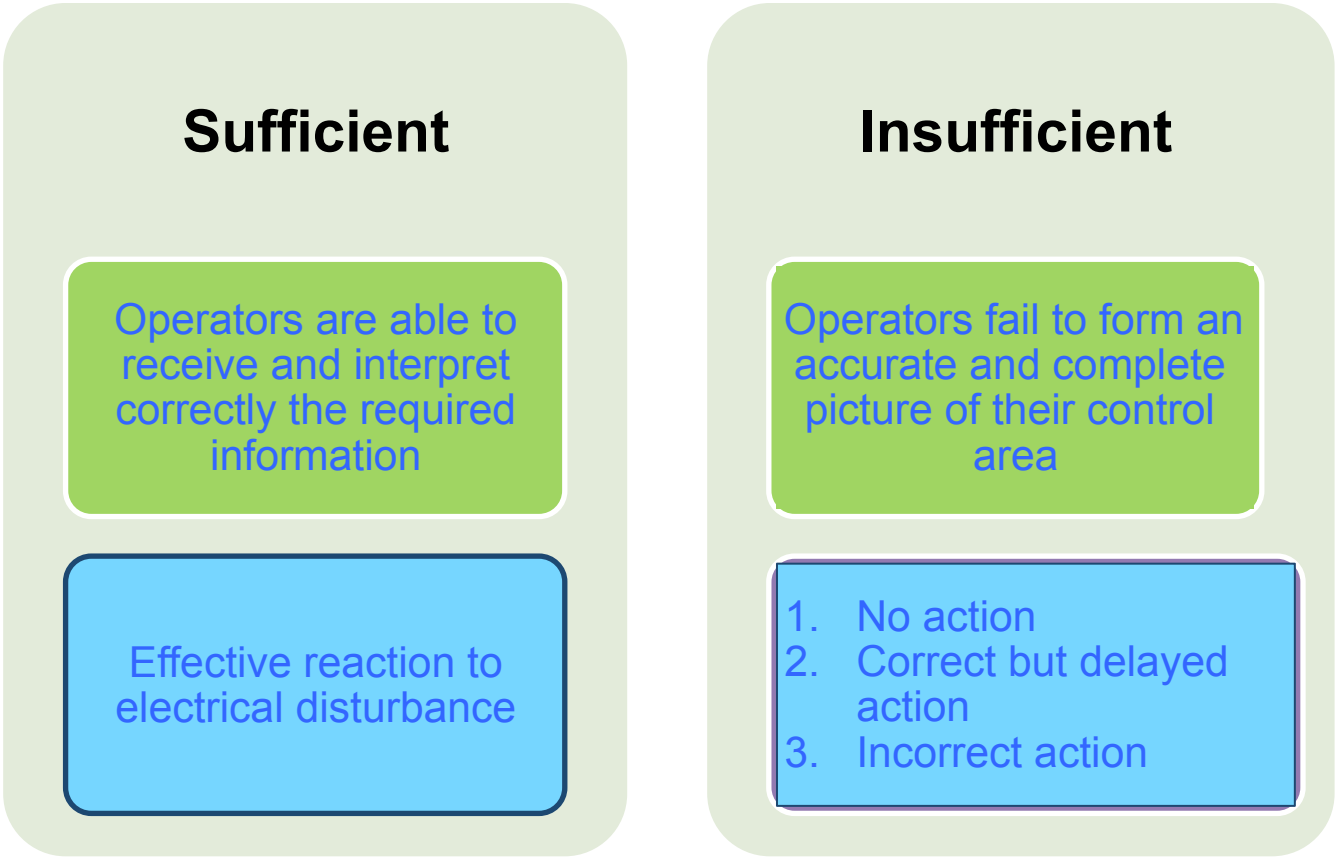
"The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future".



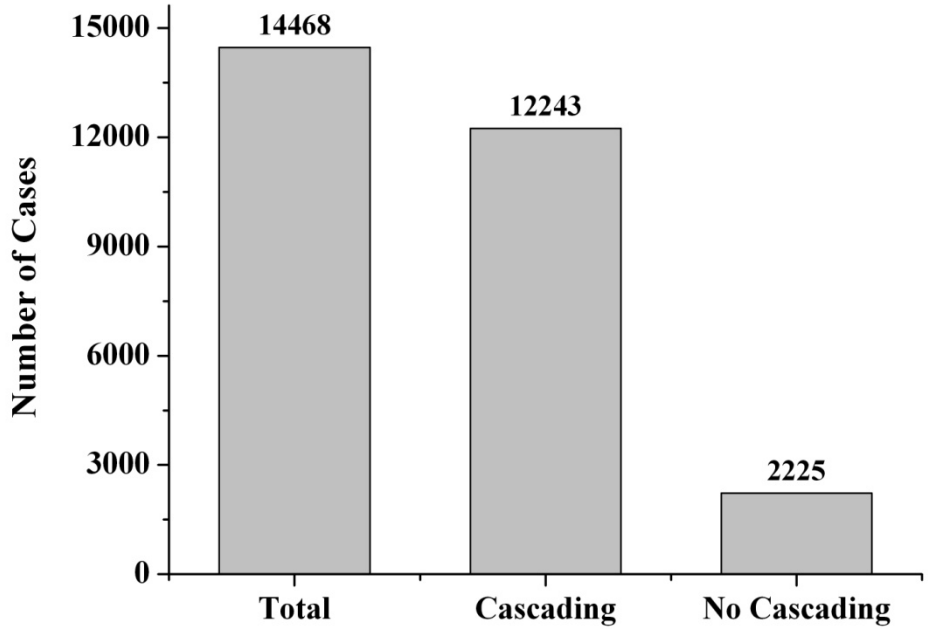
Main sources of lack of SA

Software applications	• Examples: Alarm processing, State estimator, contingency analysis tools, mimic diagram • USA/Canada blackout in 2003
Real-time measurements	• Missing, conflicting or ambiguous data can create confusion
Automation	• Out-of-the-loop syndrome • Lack of operators' timely and effective reaction when required
Environmental factors	• Data/alarm overload, high complexity of Graphical User Interface, time pressure, ambient noise levels
Individual factors	• Lack of experience and training, fatigue, limited working memory capacity, inadequate knowledge • UCTE incident in 2006
Communication with others	• Communication within the same control center or with different control centers • Italian blackout in 2003

A very simple model of SA



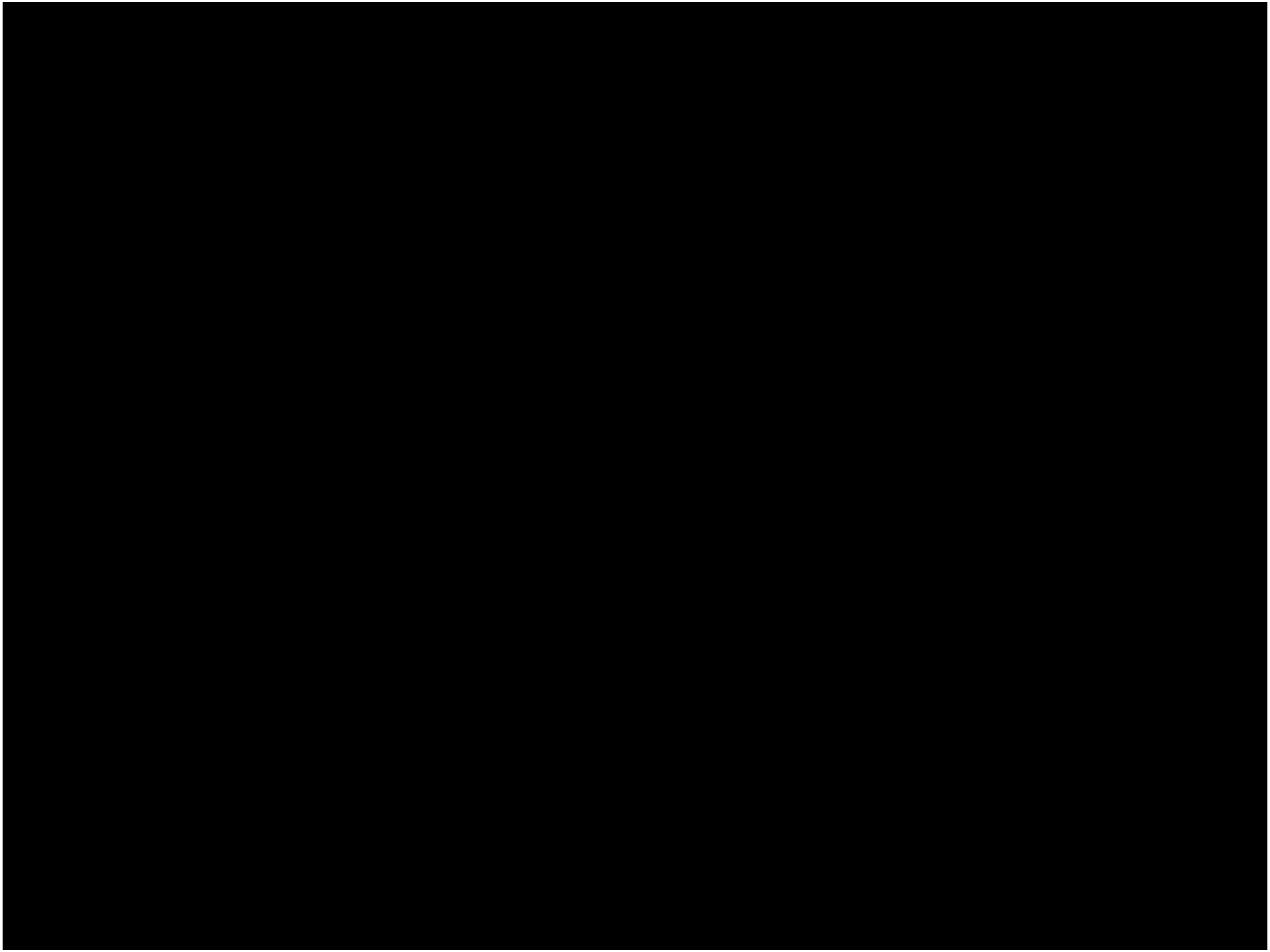
Results based on this simple model



- Insufficient SA: 85 % of the critical overloads lead to cascading phase due to lack of operators' response.
- Sufficient SA: no cascading failures or load shedding

Conclusions

- Proposed framework clarifies how failures in the information infrastructure affect the ability of the power system to deliver energy to consumers
- Provides a basis for analyzing in more details the mechanisms that could lead to major problems
- Analysis of actual incidents shows that this framework matches real-life
- Need to get a better understanding of SA
- Need quantification of SA



Examples with references

Incident	Transition	Reference
North America (2003)	D1	https://reports.energy.gov/
London, UK (2003)	C2	http://www.ofgem.gov.uk/About%20us/enforcement/Investigations/ClosedInvest/Pages/Closed.aspx
West Midlands, UK (2003)	C2	http://www.ofgem.gov.uk/About%20us/enforcement/Investigations/ClosedInvest/Pages/Closed.aspx
Italy (2003)	D1	http://www.ucte.org/publications/otherreports/
UCTE (2006)	D1	http://www.ucte.org/publications/otherreports/
WSCC (1996)	C2	http://www.nerc.com/~filez/reports.html
Ireland (2005)	D4	http://www.eirgrid.com/EirgridPortal/uploads/Transmission%20System%20Performance%20Report%202005/EirGrid%20TSPR%202005.pdf
Québec (1988)	D2	Not Available
Québec (c. 1985)	C3	Not Available
Sweden/Denmark (2003)	-	http://www.svk.se/web/Page.aspx?id=5687