Keep the Lights on and the Information Flowing

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

© 2013 D. Kirschen and University of Washington

Acknowledgements

- Prof. François Bouffard (McGill University)
- Dr. Matheos Pantelli (University of Manchester)

© 2013 D. Kirschen & University of Washington

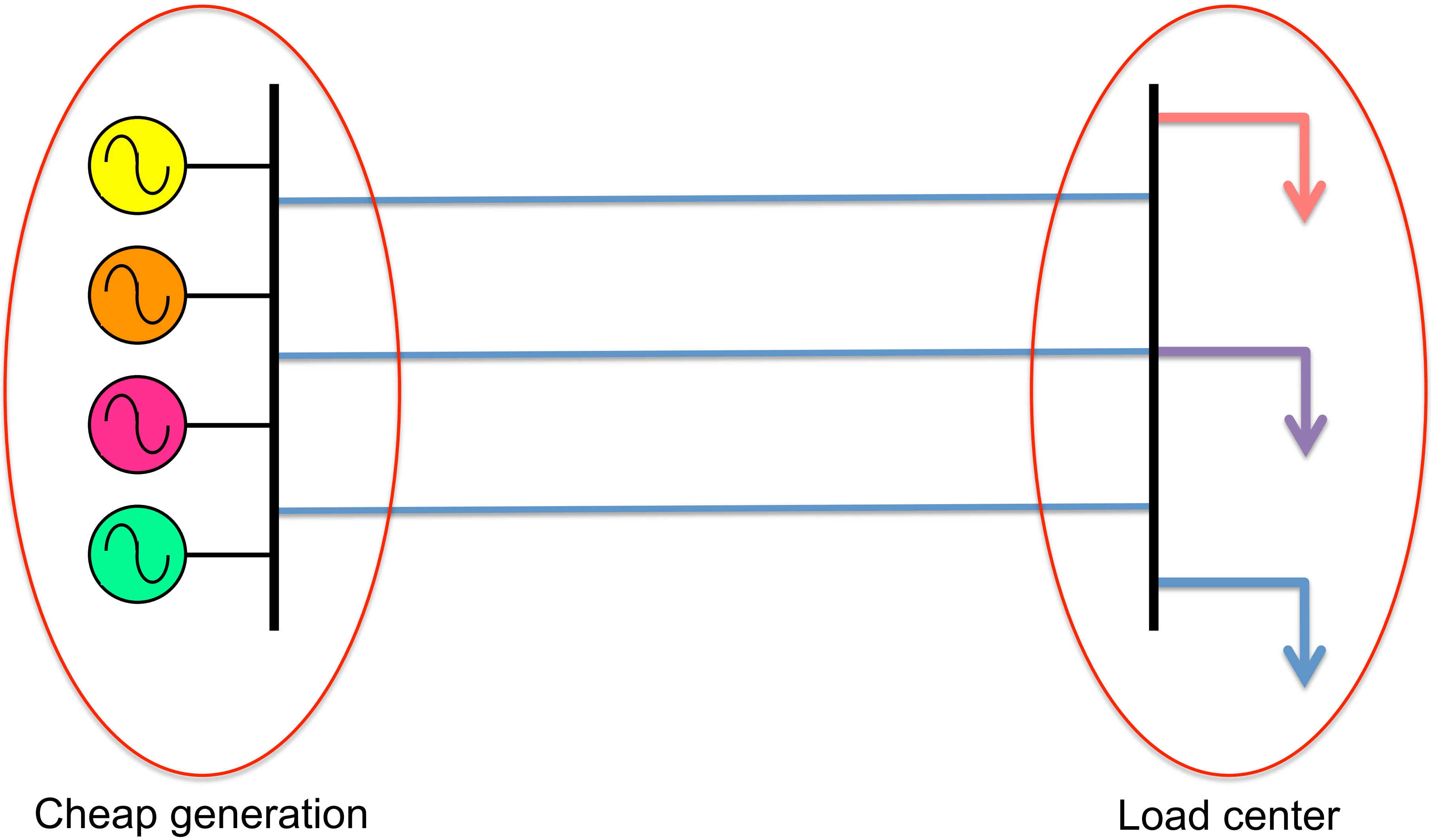
Why study blackouts?

- Cost of the blackouts
  - Direct cost (damaged equipment, ..)
  - Indirect cost (loss of economic activity)
  - Social cost

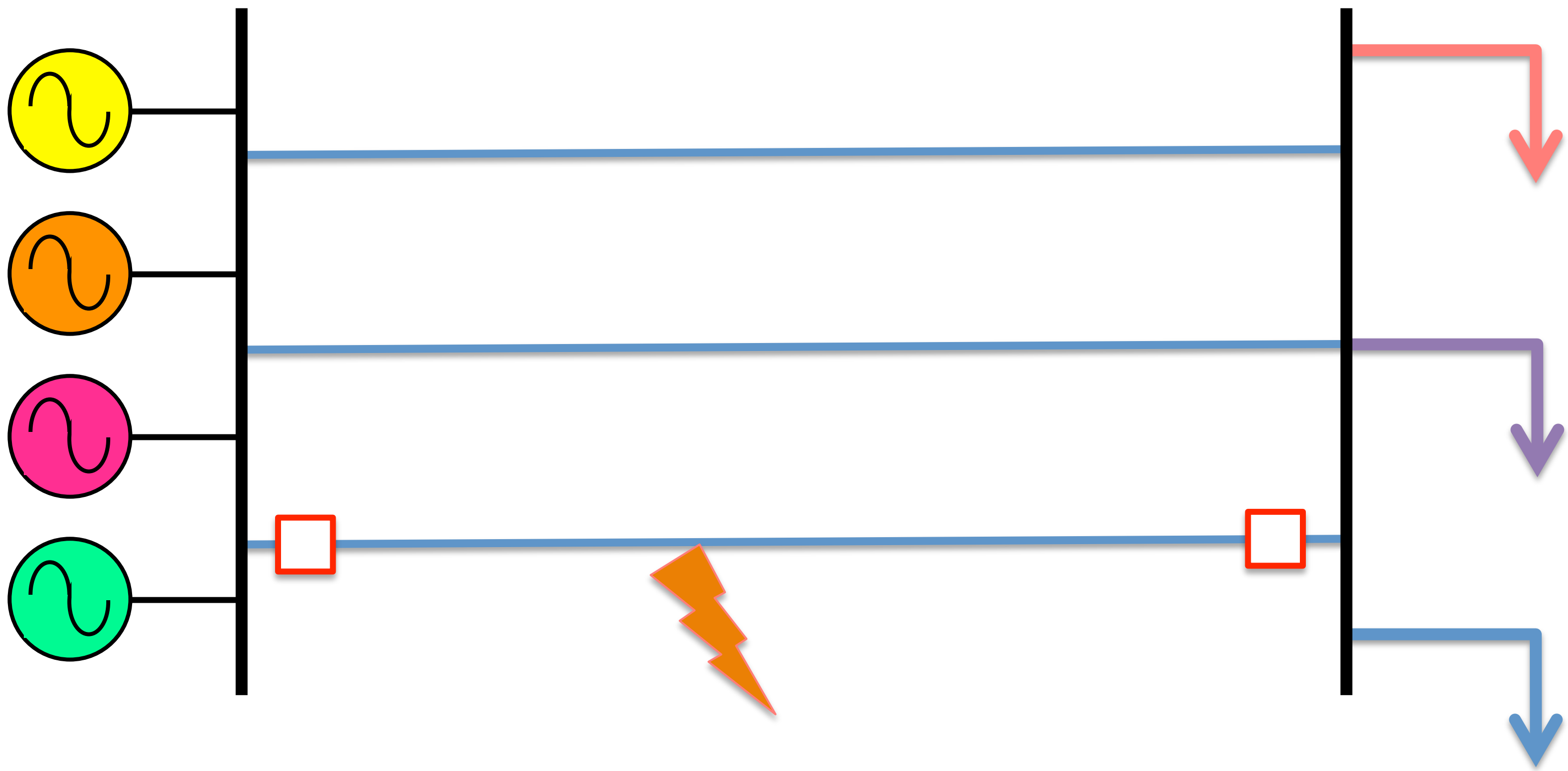
- Cost of preventing blackouts
  - Large, on-going
  - Are we spending our money wisely?

© 2013 D. Kirschen and University of Washington

The conventional explanation

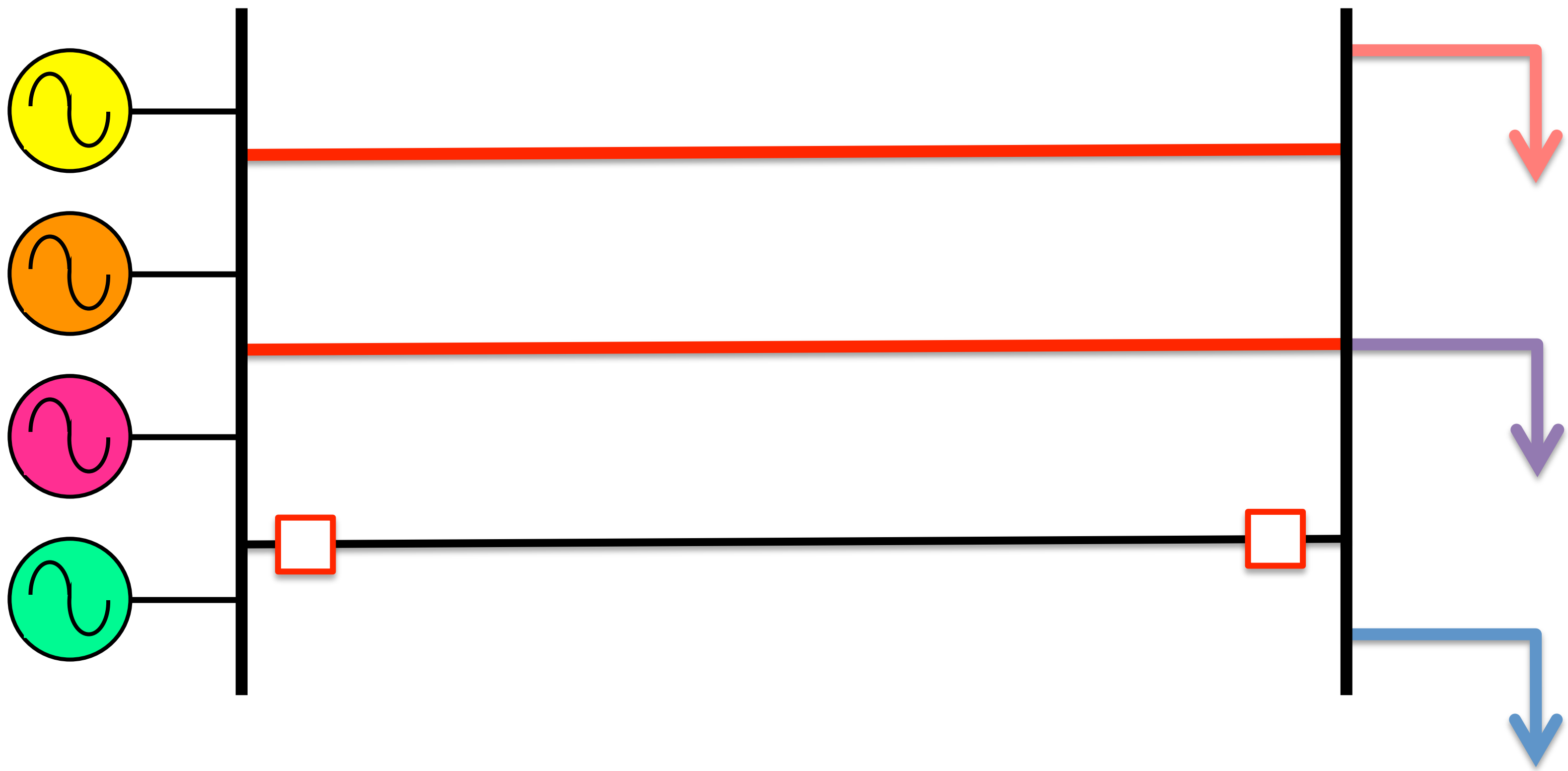


Triggering event



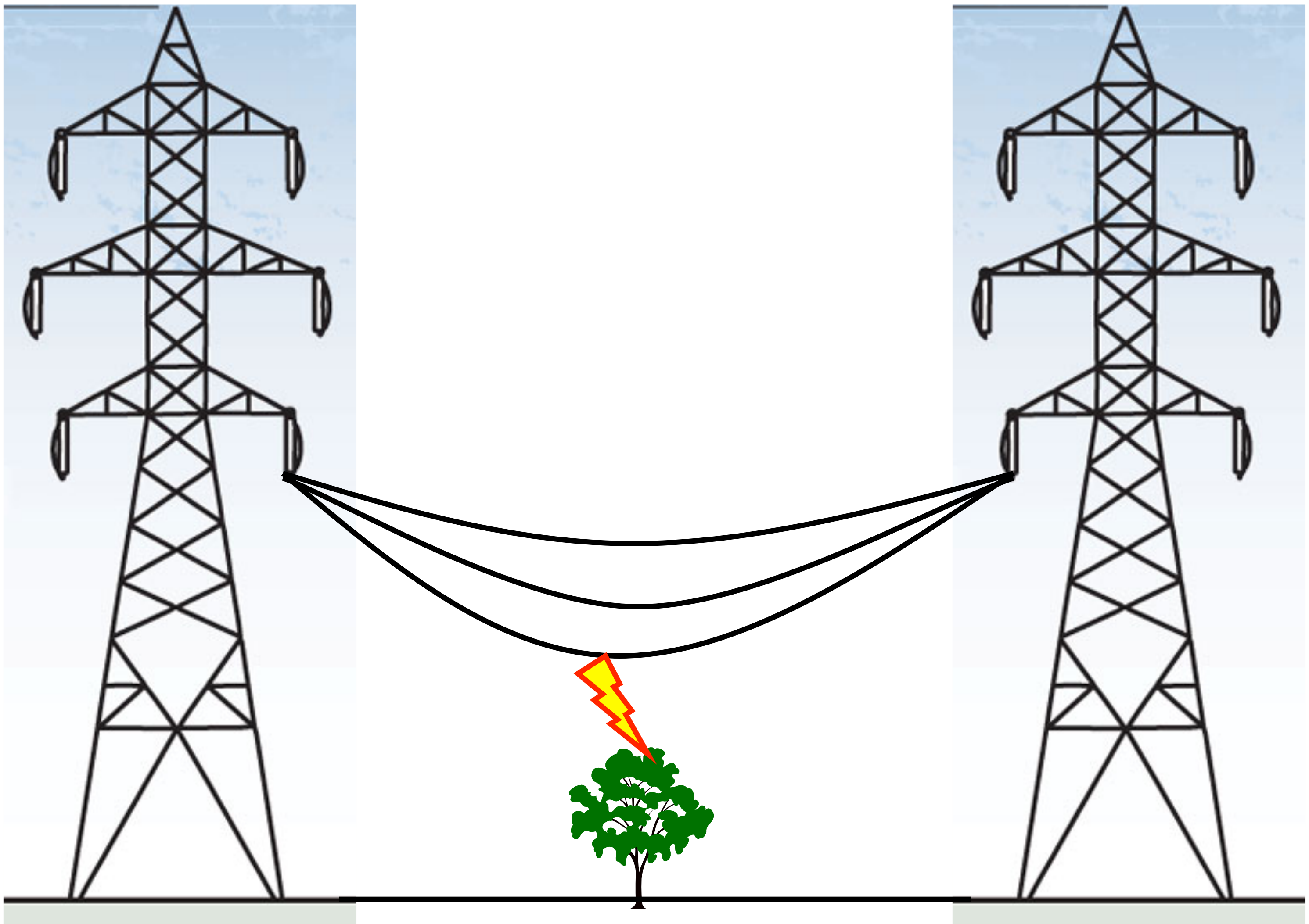
© 2013 D. Kirschen and University of Washington

Triggering event



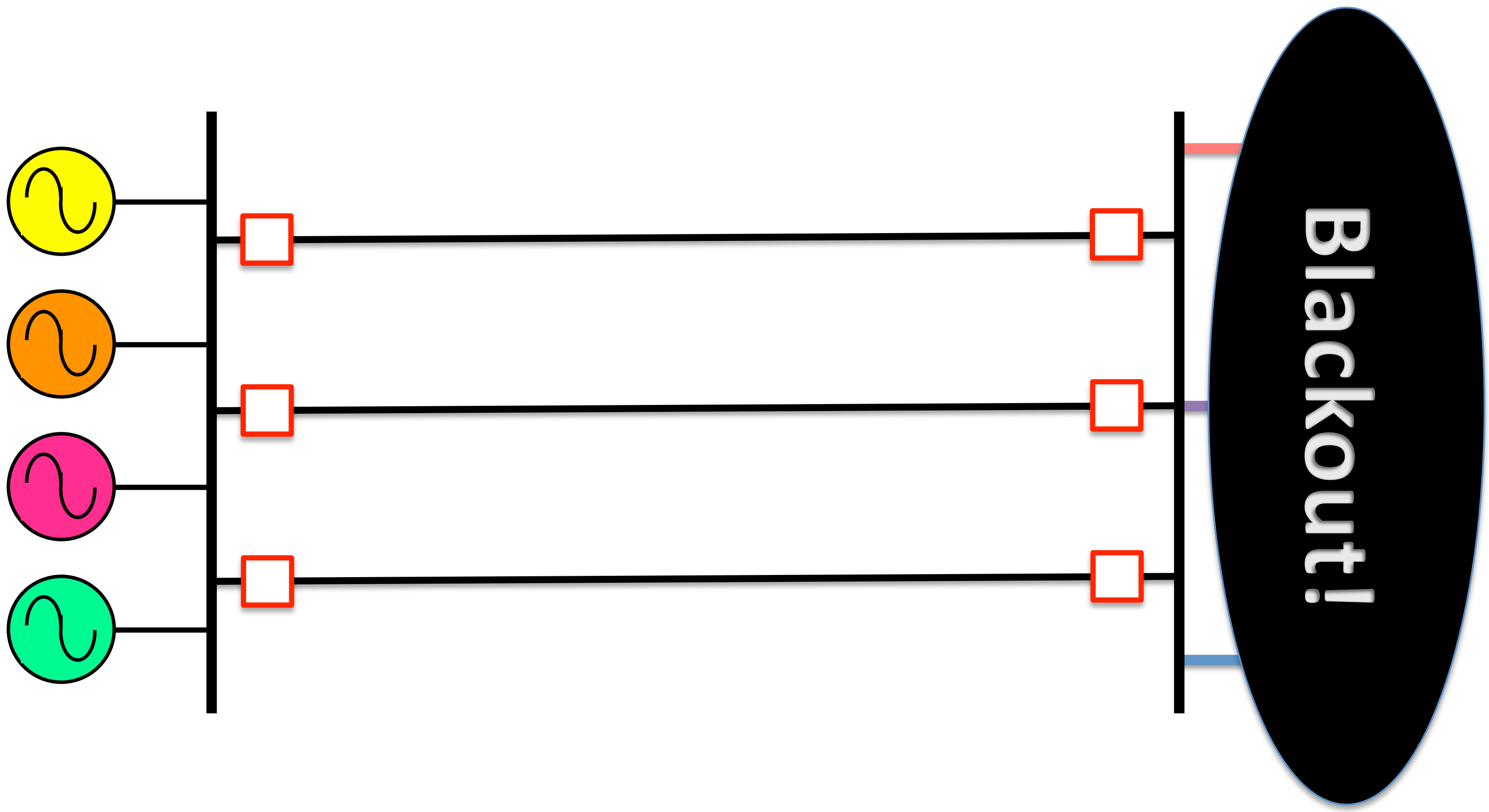
© 2013 D. Kirschen and University of Washington

Sagging conductor



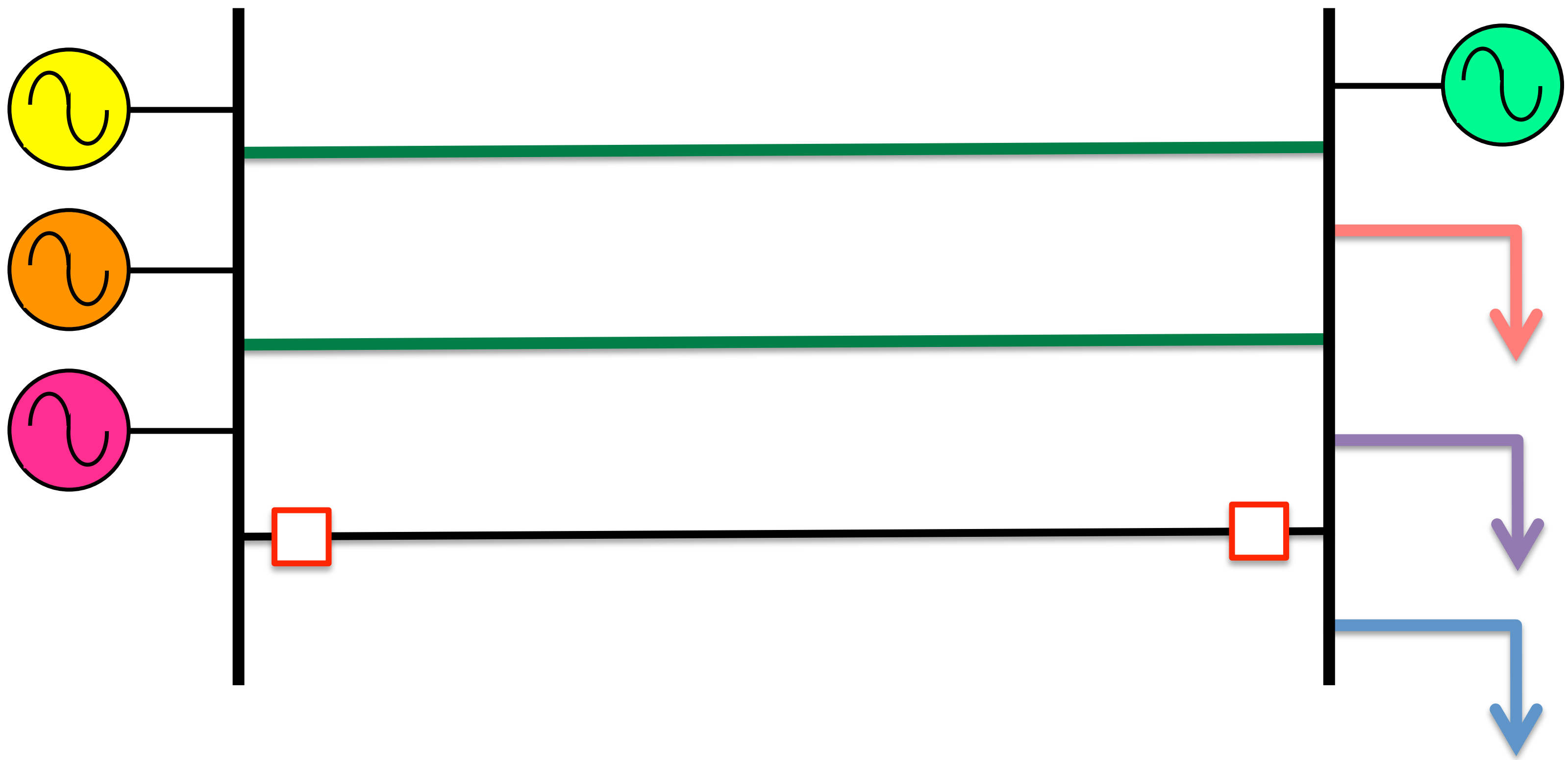
© 2013 D. Kirschen and University of Washington

Cascading outages



© 2013 D. Kirschen and University of Washington

N-1 security



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

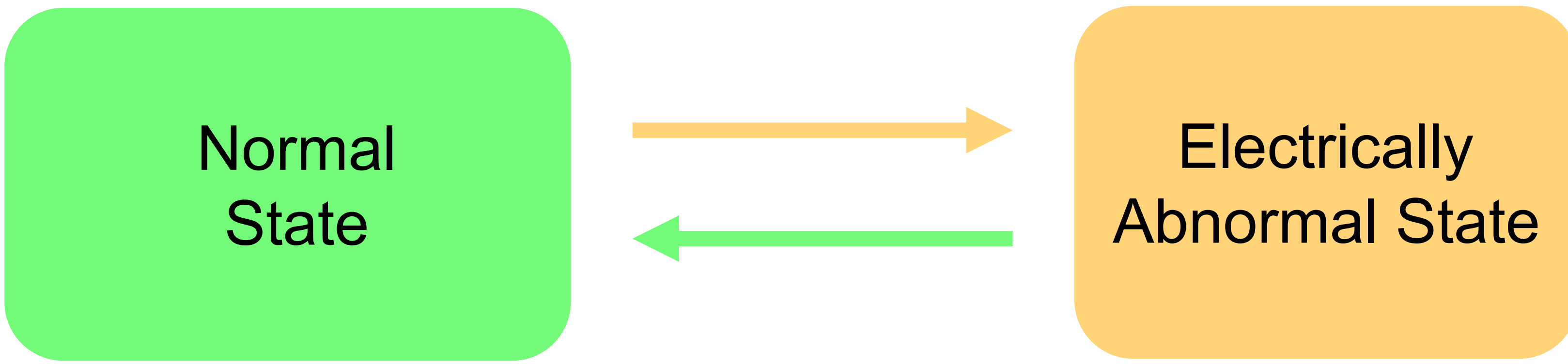
© 2013 D. Kirschen and University of Washington

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
- But aren't they?

© 2013 D. Kirschen and University of Washington

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

© 2013 D. Kirschen and University of Washington

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

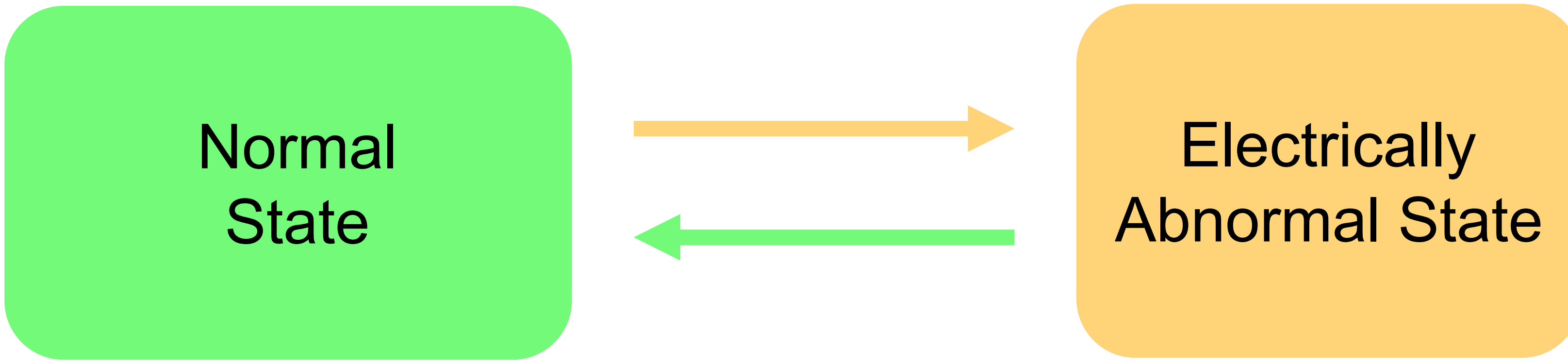
© 2013 D. Kirschen and University of Washington

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)

© 2013 D. Kirschen and University of Washington

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

© 2013 D. Kirschen and University of Washington

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)

© 2013 D. Kirschen and University of Washington

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

© 2013 D. Kirschen and University of Washington

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…

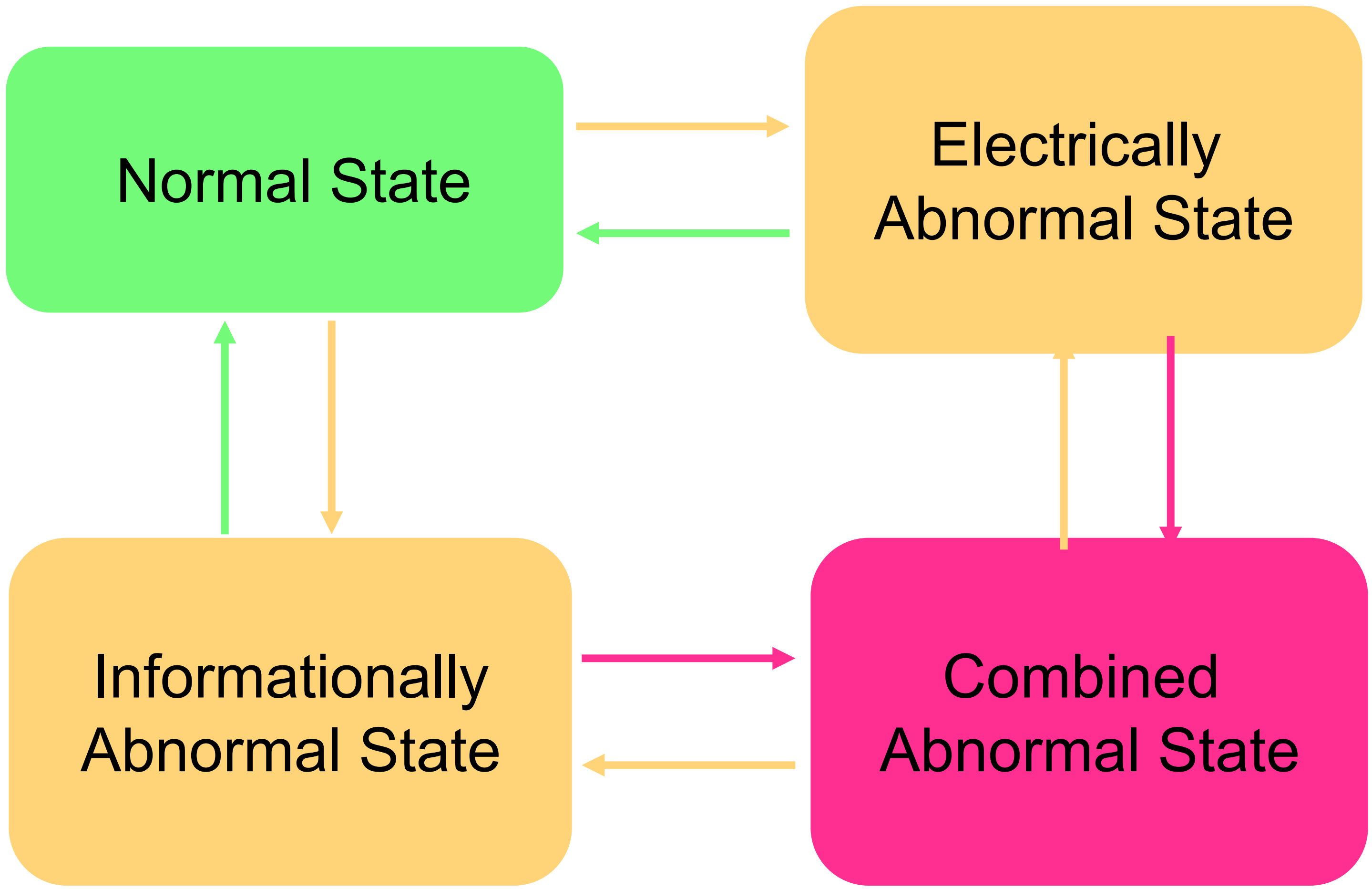
© 2013 D. Kirschen and University of Washington

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

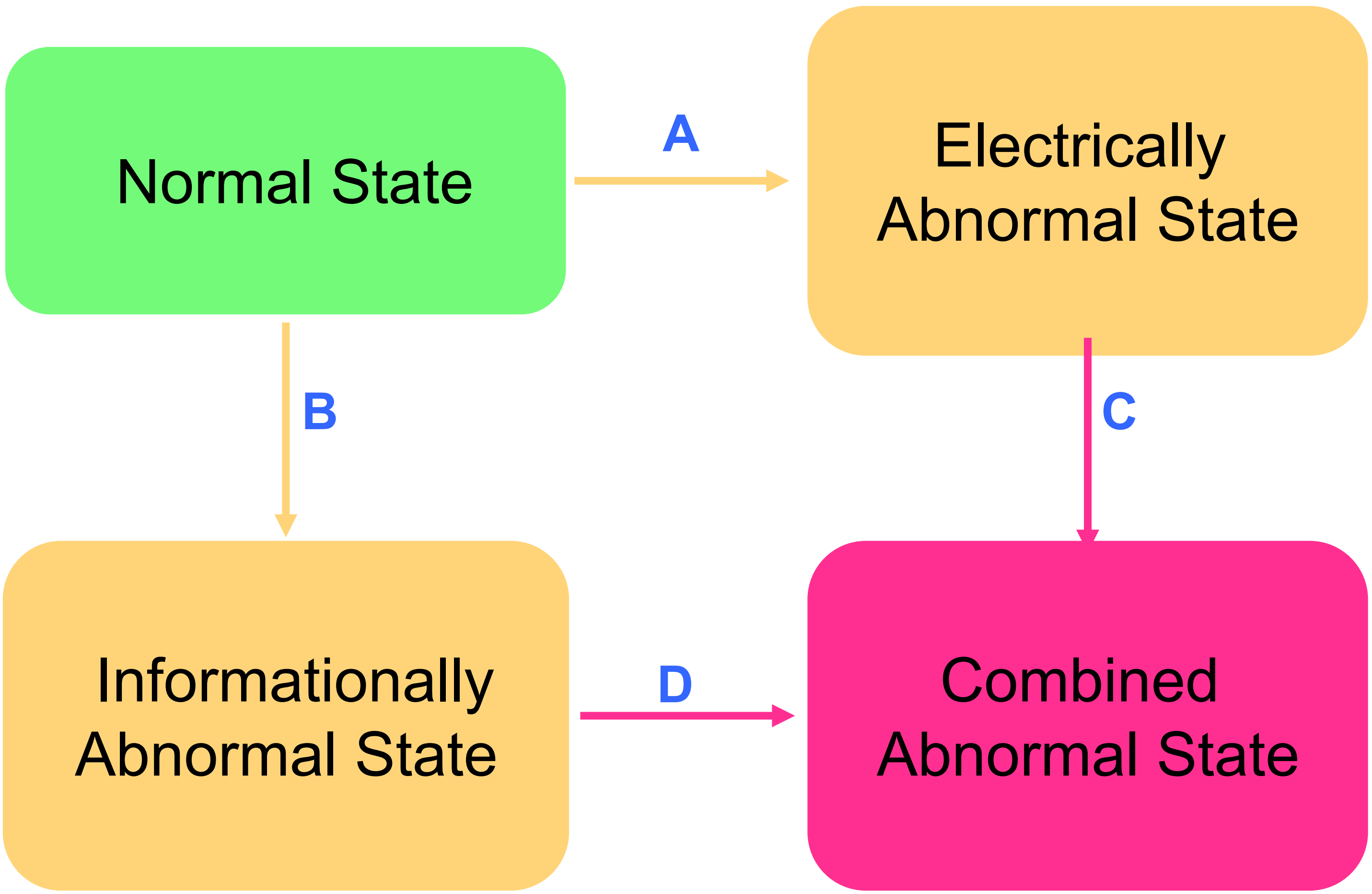
© 2013 D. Kirschen and University of Washington

New power system security framework



© 2013 D. Kirschen and University of Washington

Transitions

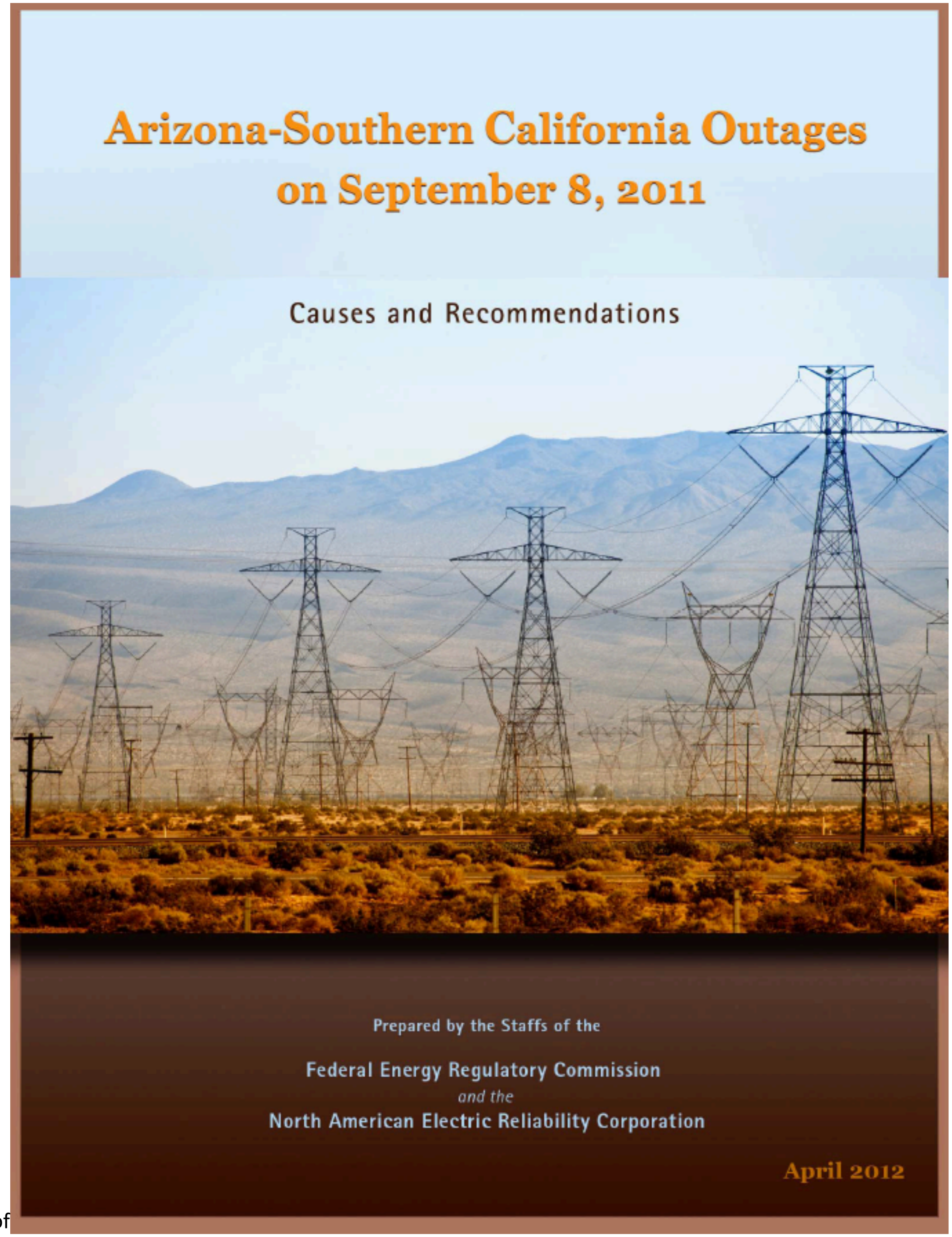


© 2013 D. Kirschen and University of Washington

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)	-

© 2013 D. Kirschen and University of Washington


Arizona-Southern California Outages
on September 8, 2011
Causes and Recommendations
Prepared by the Staffs of the
Federal Energy Regulatory Commission
and the
North American Electric Reliability Corporation
April 2012

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

© 2013 D. Kirschen and University of Washington

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
  - ?

© 2013 D. Kirschen and University of Washington

What is the state of the system?

Actual State

↓

Reported State

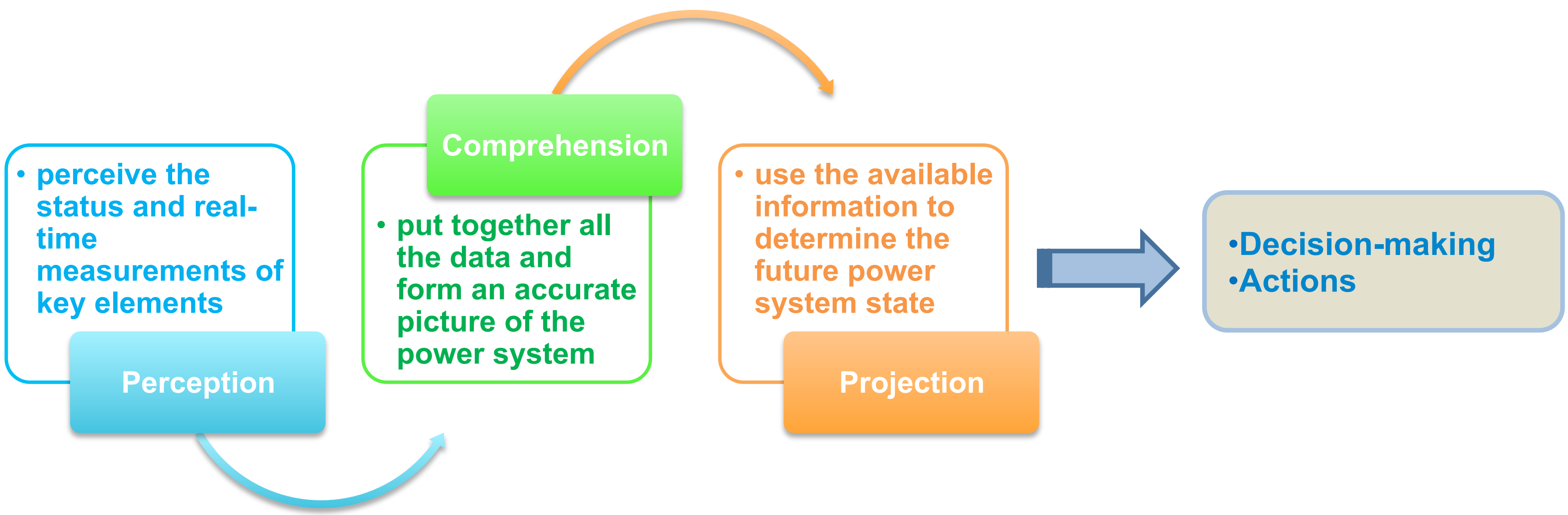
↓

Perceived State

© 2013 D. Kirschen and University of Washington

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".



© 2013 D. Kirschen and University of Washington

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

© 2013 D. Kirschen and University of Washington

A very simple model of SA

Sufficient

Operators are able to receive and interpret correctly the required information

Effective reaction to electrical disturbance

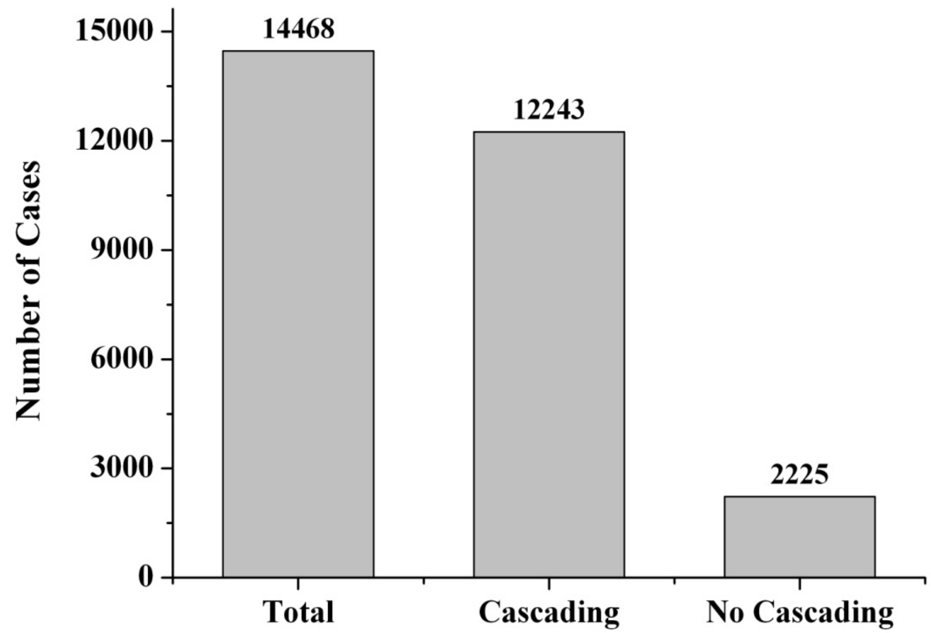
Insufficient

Operators fail to form an accurate and complete picture of their control area

1. No action
2. Correct but delayed action
3. Incorrect action

© 2013 D. Kirschen and University of Washington

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

© 2013 D. Kirschen and University of Washington

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

© 2013 D. Kirschen and University of Washington