MANCHESTER 1824

The University of Manchester

A framework for studying the influence of the information infrastructure on power system security

Prof. Daniel Kirschen

The University of Manchester

© D. Kirschen 2010

Power system infrastructure

- Electrical infrastructure
  - Lines, cables, generators, transformers, loads, …
  - Produce, transmit, distribute and consume electrical energy
- Information infrastructure
  - Control centres, communication links, measurement devices, protective relays, control systems, …
- Operators
  - Responsible for maintaining the security of the system (keeping the lights on)

© D. Kirschen 2010

Failures in the electrical infrastructure

- Examples:
  - Unplanned outage of generating plant
  - Fault on transmission line or cable
  - Failure of transformer
- Failures are unpredictable and unavoidable
- Always operate power system with a safety margin
- Allows uninterrupted operation after the loss of one component

© D. Kirschen 2010

Classical power system security framework

- *Normal state*
  - All electrical variables are within their normal range
  - Sufficient safety margin between the state of the system and its stability limits

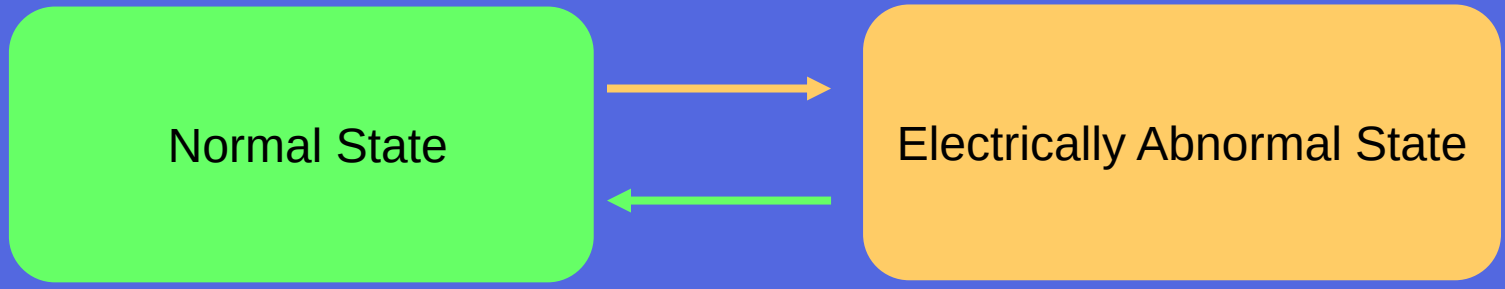
© D. Kirschen 2010

Classical power system security framework

- *Electrically abnormal state*
  - The margin between the operating state of the system and its stability limit does not meet the security criteria OR
  - An electrical component has been disconnected OR
  - Some load has been disconnected (either involuntarily or voluntarily to prevent a collapse of the system)
- Encompasses the alert, emergency, extremis and restorative states of the classification of Fink and Carlsen (1978).

© D. Kirschen 2010

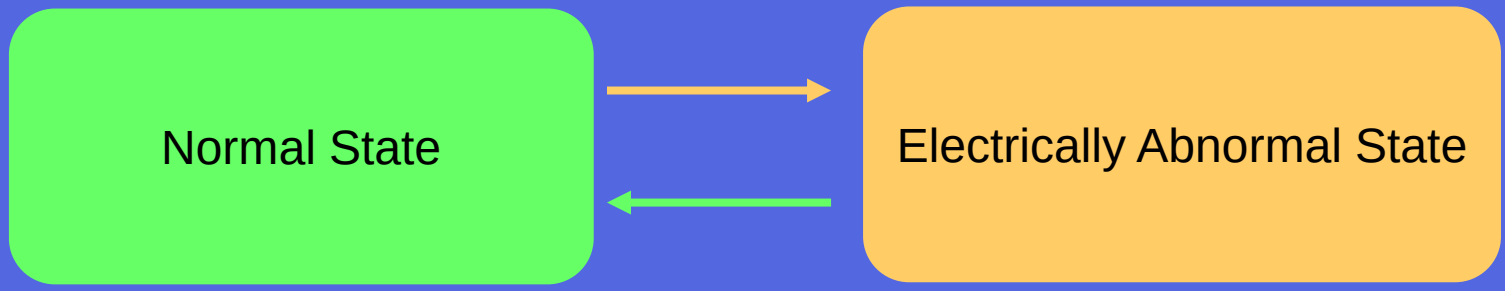
Classical power system security framework



- Normal state is stable and secure
- In the abnormal state, system is vulnerable or unstable
- Operator must act to keep the system in the normal state or bring it back there

© D. Kirschen 2010

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

© D. Kirschen 2010

Role of the information infrastructure

- Monitoring
  - Keep the operator informed of the state of the system
    - 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

© D. Kirschen 2010

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…

© D. Kirschen 2010

New power system security framework

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

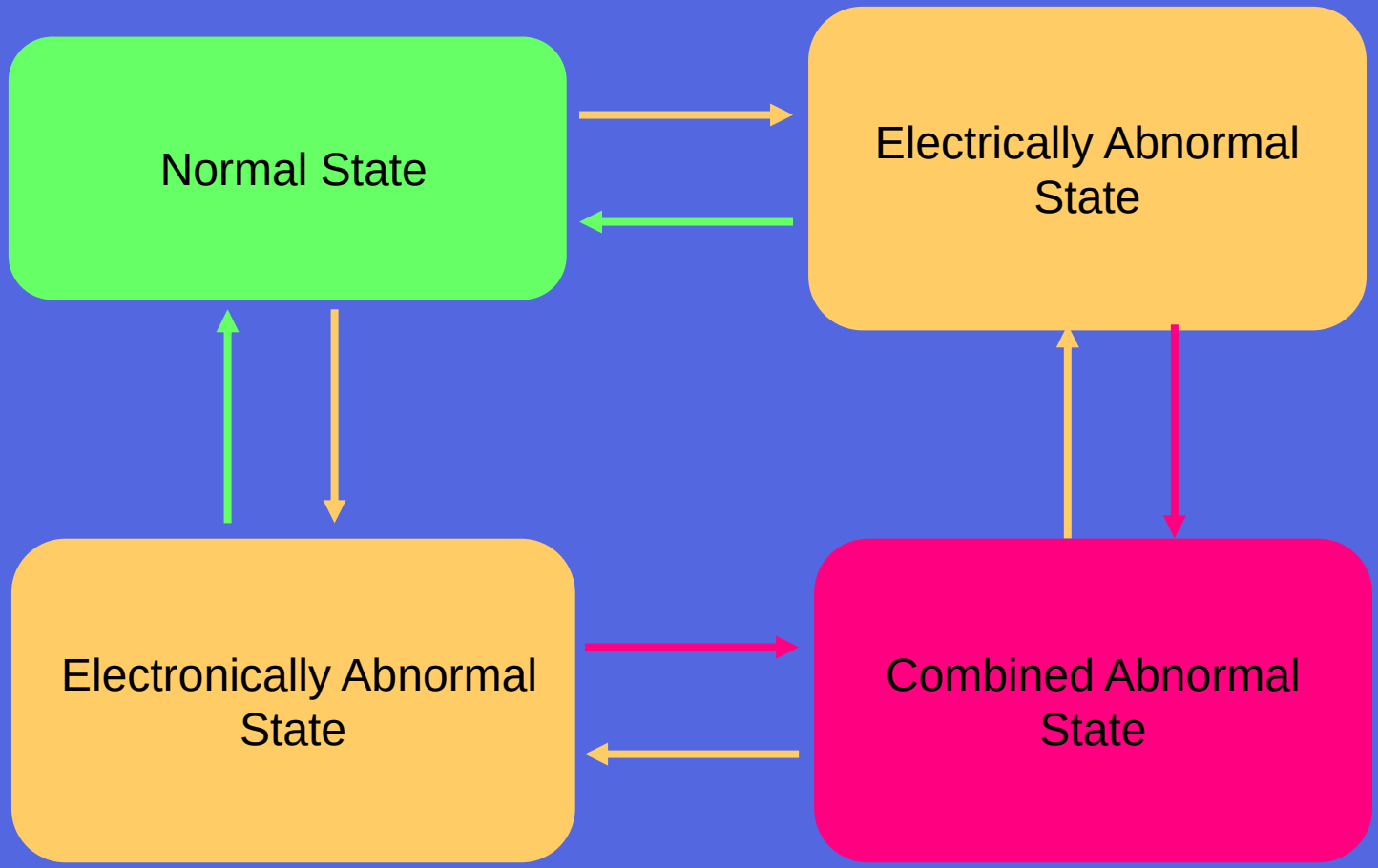
© D. Kirschen 2010

New power system security framework

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

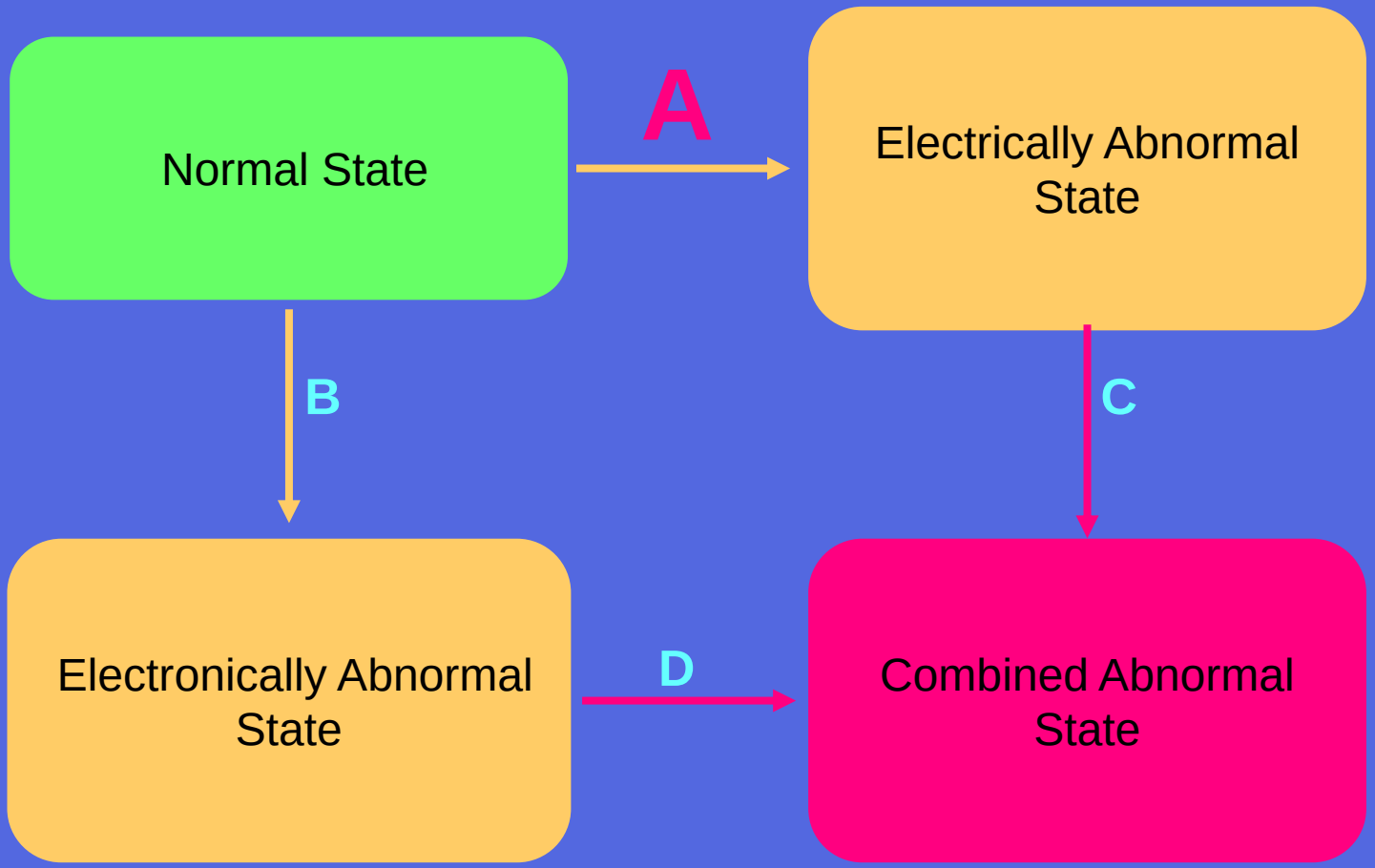
© D. Kirschen 2010

New power system security framework



© D. Kirschen 2010

Transitions



© D. Kirschen 2010

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

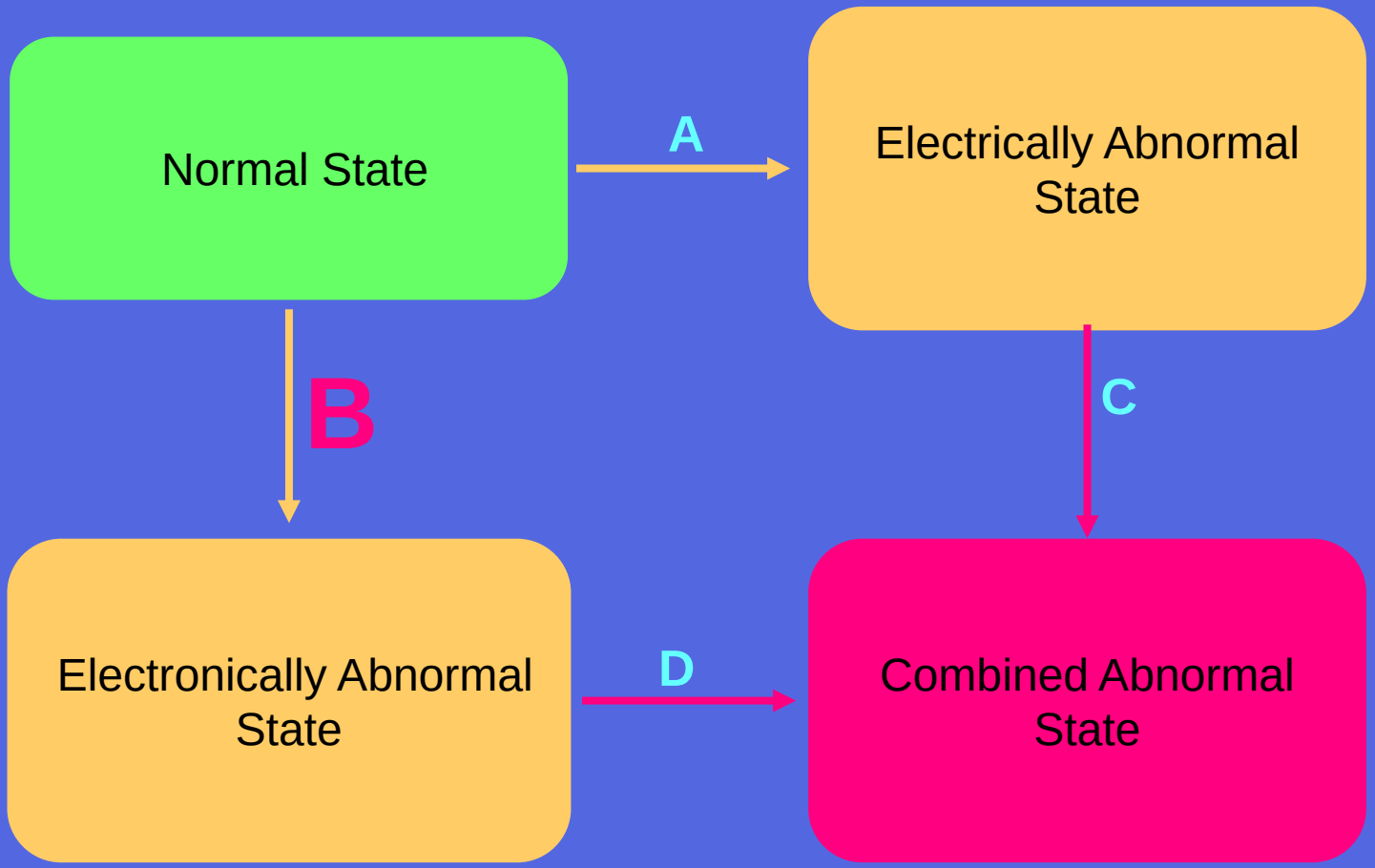
© D. Kirschen 2010

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)

© D. Kirschen 2010

Transitions



© D. Kirschen 2010

B: Normal to electronically 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

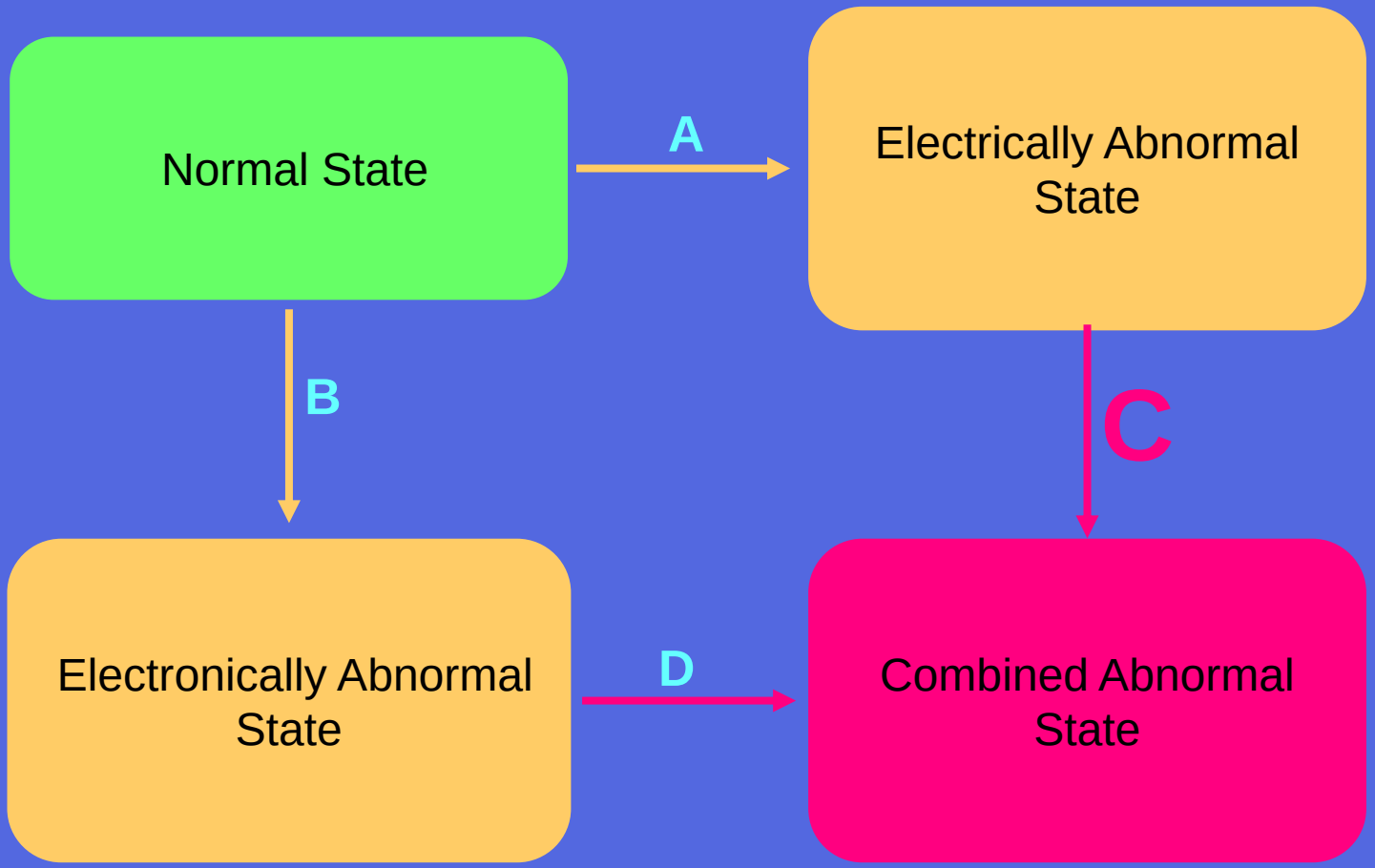
© D. Kirschen 2010

B: Normal to electronically 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

© D. Kirschen 2010

Transitions



© D. Kirschen 2010

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

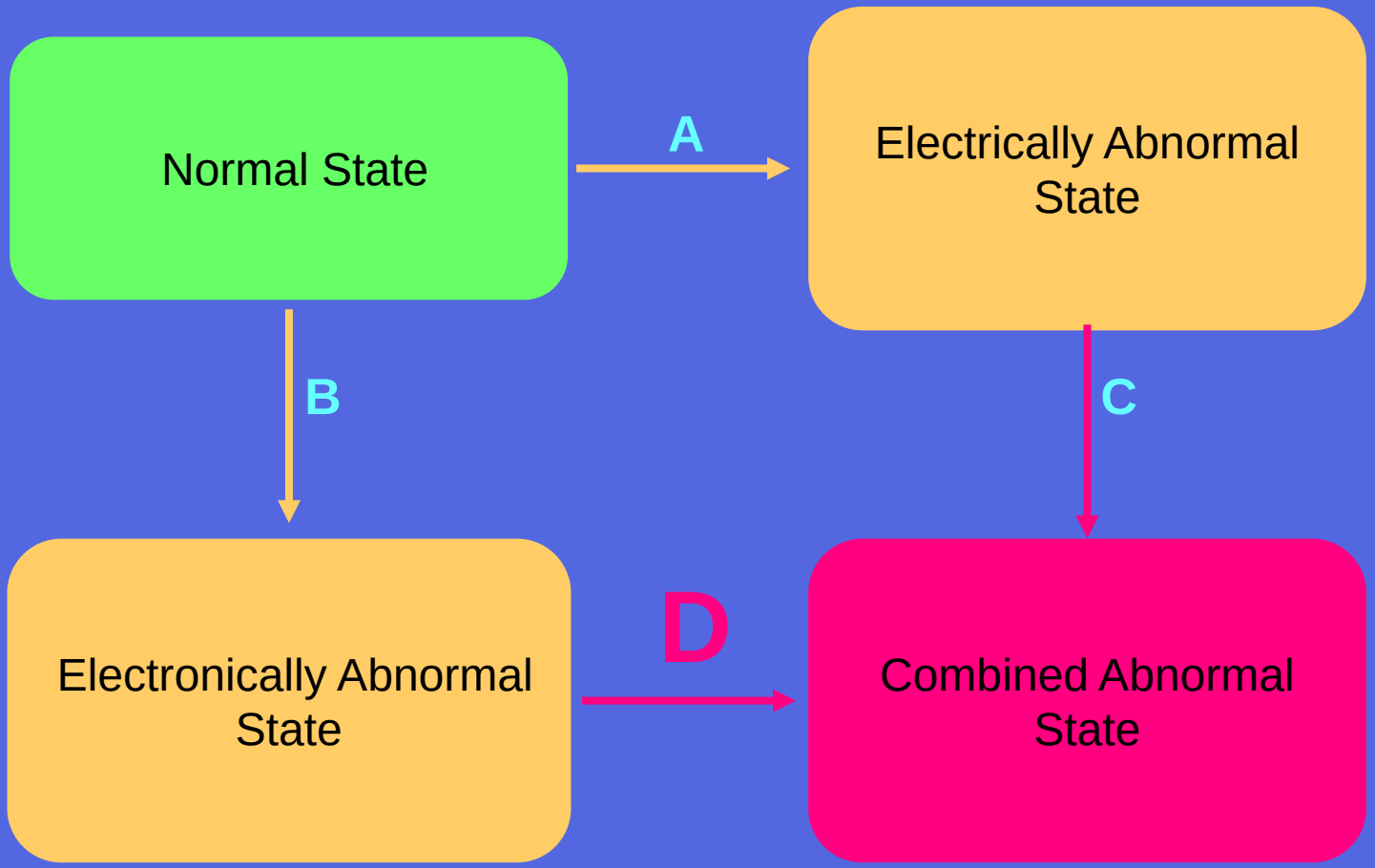
© D. Kirschen 2010

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)

© D. Kirschen 2010

Transitions



© D. Kirschen 2010

D: Electronically 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. Kirschen 2010

D: Electronically 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?

© D. Kirschen 2010

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
Quˇbec (1988)	D2
Quˇbec (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

© D. Kirschen 2010

Enhancing the information infrastructure

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

➔Significant reduction in risk of customer outages

© D. Kirschen 2010

Directions for further work

- Electrical infrastructure
  - Excellent structural and functional models
  - Reasonably good reliability data
- ICT infrastructure
  - Good structural models
  - Very poor functional models
  - Complete lack of reliability data
- Operator response
  - ?

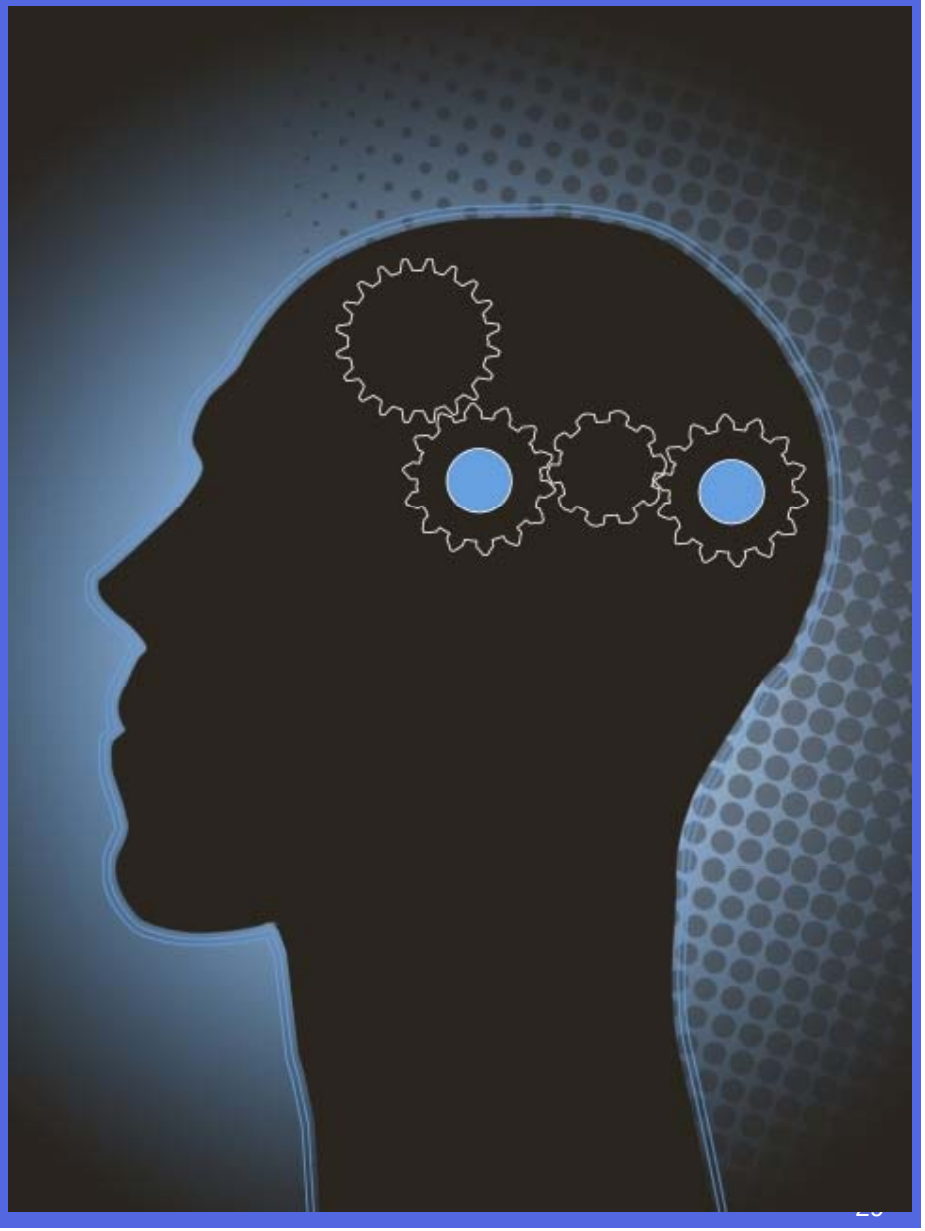
© D. Kirschen 2010

What is the state of the system?

Actual State

Reported State

Perceived State



© D. Kirschen 2010

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 analysing in more details the mechanisms that could lead to major problems
- Analysis of actual incidents shows that this framework matches real-life

© D. Kirschen 2010

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
Quˇbec (1988)	D2	Not Available
Quˇbec (c. 1985)	C3	Not Available
Sweden/Denmark (2003)	-	http://www.svk.se/web/Page.aspx?id=5687