Planning and operation of electric power and energy systems

Module 3

Reliability management of bulk electric power systems

Lecture 1

Louis Wehenkel and Efthymios Karangelos

March-April 2021

LIÈGE université

Overview of Module 3

- Topics to be covered
  - The notions of bulk power systems security, reliability, and resilience
  - Current practice of security assessment and control
  - Towards probabilistic risk management approaches
  - Emerging topic of cyber-physical risk management

- Learning outcomes
  - Understand the needs and practical implications for power systems reliability management strategies and decision support software tools
  - Have a good idea of current research topics in this subject area

LIÈGE université

Lecture 1 (Today)

- Motivation for bulk power systems reliability management
- The notions of contingency and of power system response to contingencies
- The Dy Liacco state diagram for power system operation
- The N-1 reliability standard for power system operation
- The SCOPF formulation of the preventive vs corrective security control trade-off
- Implications for operation planning, asset management and system development activities

Lecture 2 (Next week)

- Motivation: what's missing in the N-1 approach?
- Risk-based real-time operation: how to account for the (low) likelihood and potential impact of contingencies?
- Planning under uncertainty: how to tackle the daily randomness of renewable power generation?
- The need for resilience: what can go wrong will go wrong?

Lecture 3 (in two weeks)

- Cyber-physical risk management in power systems

- Instructions for preparation: everybody should read the paper

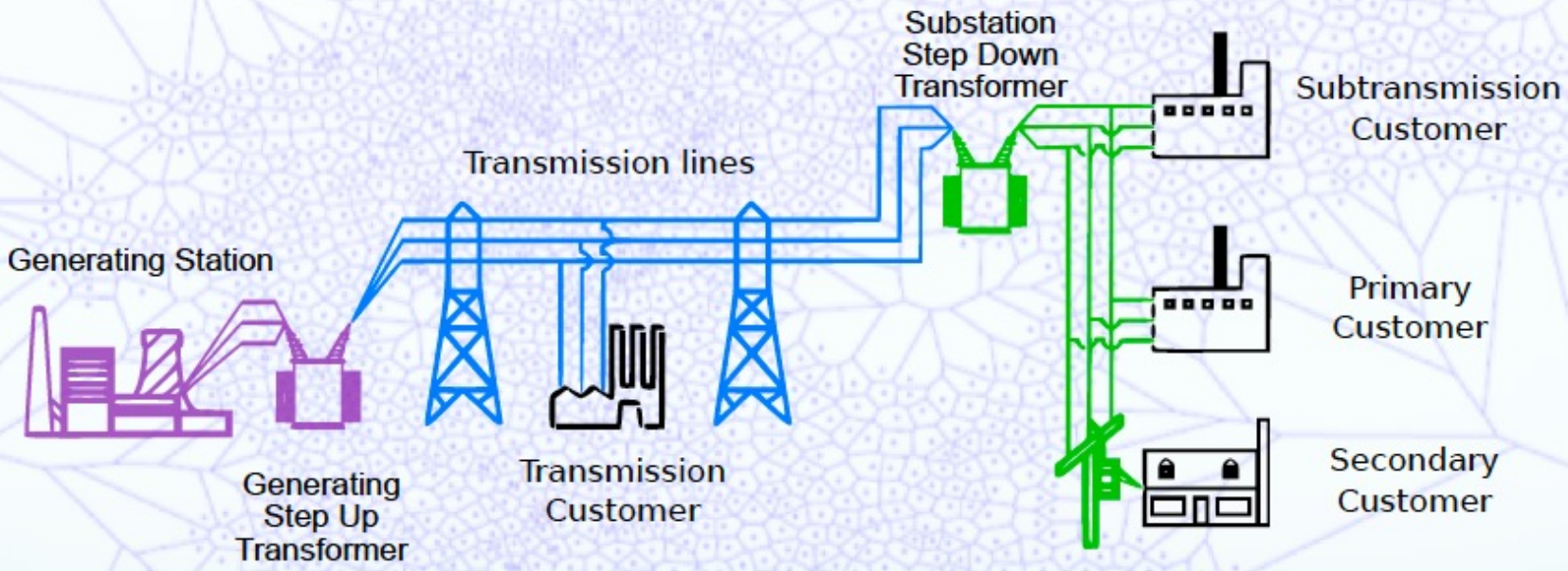
  "Cyber security of a power grid: State-of-the-art", CC Sun, A Hahn, CC Liu, *EPES, Vol* 99, 2018, pp 45–56

- 3 groups of two students will present the following papers:
  - "Physical system consequences of unobservable state-and-topology cyber-physical attacks", J Zhang, L Sankar, *IEEE Transactions on Smart Grid*, Vol 7-4, 2016, pp 2016-2025
  - "Power system security with cyber-physical power system operation", PA Oyewole, D Jayaweera, *IEEE Access*, 2020
  - "Distributed blockchain-based data protection framework for modern power systems against cyber attacks", G Liang , SR Weller, F Luo, J Zhao, Z Yang Dong, *IEEE Transactions on Smart Grid*, Vol 10-3, 2019, pp 3162-3173

Motivations for bulk power systems reliability/security management

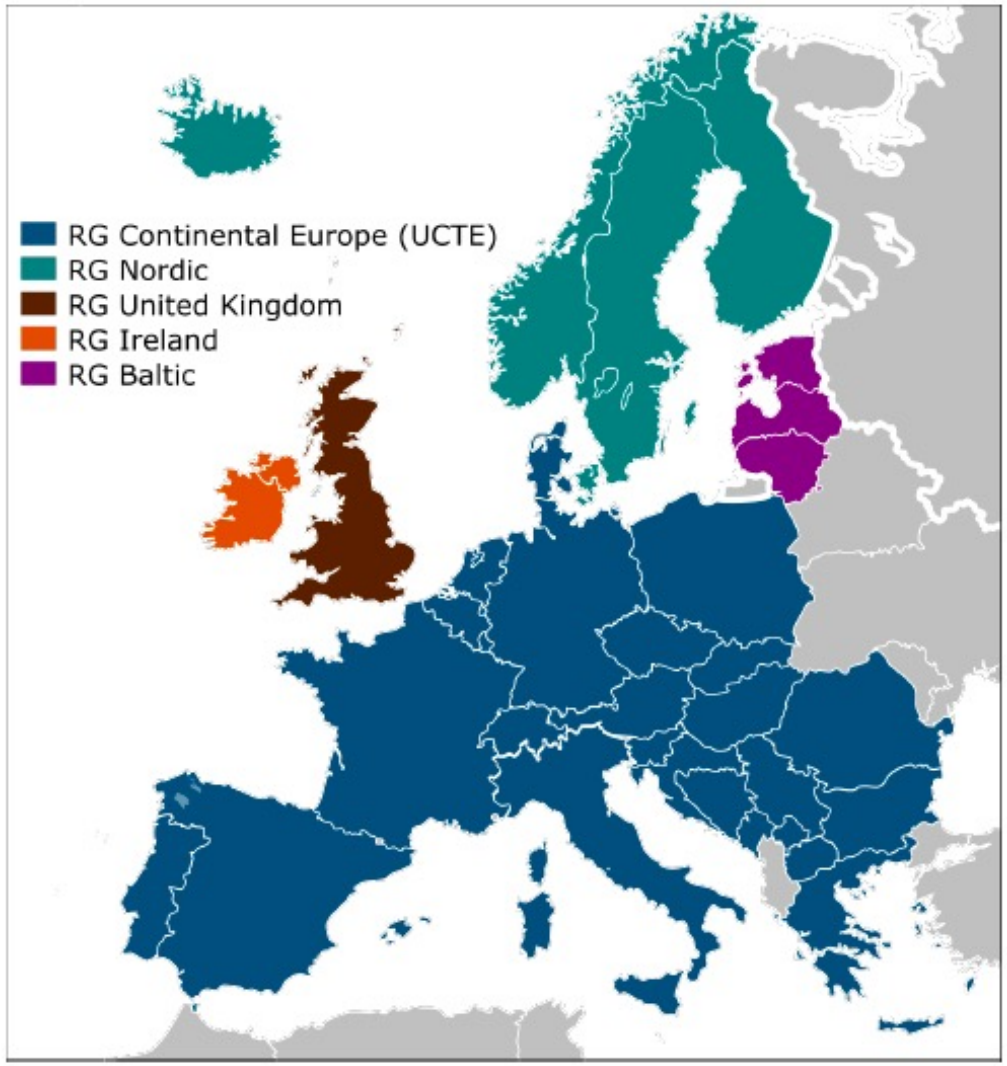
The nature of Electric Power Systems

Schematic view of a generic Electric Power System



Mission: Deliver electricity from producers to consumers, while ensuring high reliability of supply at the lowest possible cost

The European Electric Power System



- A network of $\approx$ 30,000 branches / 20,000 nodes at EH voltage levels (225-400kV)
- About 30 Transmission System Operators (TSOs)
- Coupled energy markets
- Quickly increasing penetration of renewable generation
- Ageing physical infrastructure
- Increasing uncertainties and faster dynamics
- Cost: 20-30% of electricity bill

LIÈGE université

Electric power system reliability

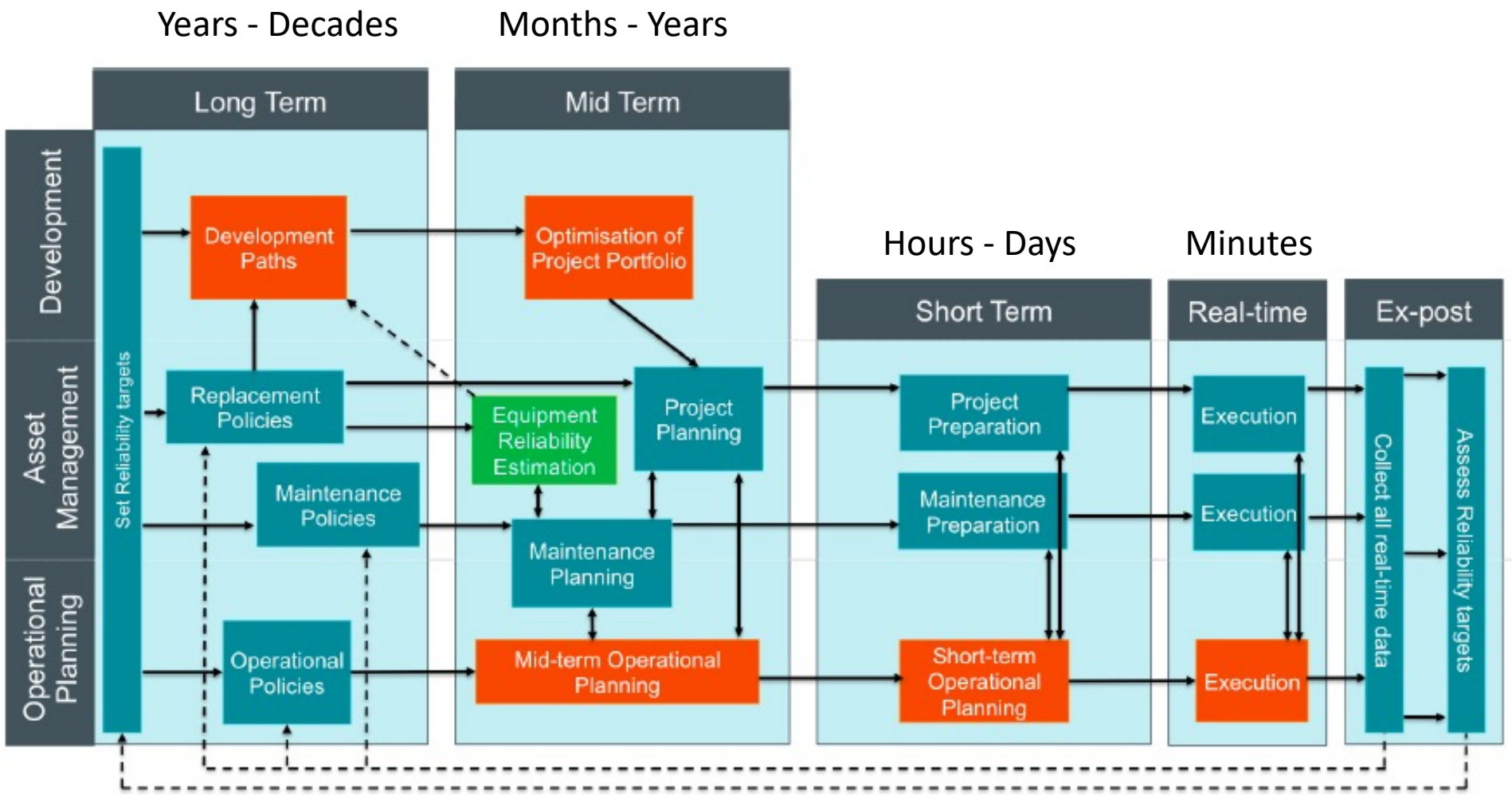
- **Requirement:**
  - At sub-second temporal resolution, balance generation/storage/consumption, under network constraints, in spite of various threats
- **Threats faced:**
  - Variations of generation and demand, weather conditions
  - Component failures, human errors, adversarial attacks
- **Problems to avoid:**
  - Component overloads, voltage or frequency deviations
  - Cascading overloads, instabilities, blackouts
- **Opportunities:**
  - Optimisation and control of flows closer to real-time
  - Preventive maintenance and planning of operation
  - Adaptation of the grid structure to market needs

A few examples of blackouts

- 1965 USA Northeast Blackout left 25 million people and 80,000 square miles (207,000 km²) without electricity for up to twelve hours
  - See https://www.youtube.com/watch?v=cdF-CsxqDko
  - See https://en.wikipedia.org/wiki/Northeast_blackout_of_1965
  - It was the 'birth' of power systems control centres

- 2003 USA Northeast Blackout of left 55 million people …
  - https://en.wikipedia.org/wiki/Northeast_blackout_of_2003
- 2003 Italian Blackout
  - https://en.wikipedia.org/wiki/2003_Italy_blackout
- 2006 European Blackout
  - https://en.wikipedia.org/wiki/2006_European_blackout
- 2021 Texas Power Crisis
  - https://en.wikipedia.org/wiki/2021_Texas_power_crisis
- 2021 Europe in extremis situation
  - https://www.bloomberg.com/news/articles/2021-01-27/green-shift-brings-blackout-risk-to-world-s-biggest-power-grid

Types of Reliability Management Activities *vs* Temporal Horizons



Power systems security and its management in the context of power system operation

Notion of ***Power System Security*** (intuitively)

The security of a power system in a given operating state is its capability to functionally survive to any "credible" disturbance that could occur

- Notion of 'operating state'
  - Mainly defined by grid topology, currents, and voltages
  - NB: but depends also on the settings of some automatic devices
- Set of 'credible disturbances'
  - Small disturbances: e.g. variation of load and generation
  - Large disturbances: component outages, short-circuits, trippings
  - NB: meaning of 'credible' may change from one context to another
- Notion of 'functional survival'
  - Continue to operate without service interruptions
  - e.g. no cascades and no dynamic instabilities

LIÈGE université

The ***Security Level*** of a power system depends on

Possible Causes

- System loading and grid topology
- Static and dynamic system behavior
- Types and probabilities of exogenous disturbances

Undesired consequences

- Thermal overloads and/or under/over-voltages
- Nature and size of instability mechanisms
- Operator and protective device heroic interventions

LIÈGE université

How can an operator avoid undesired consequences ?

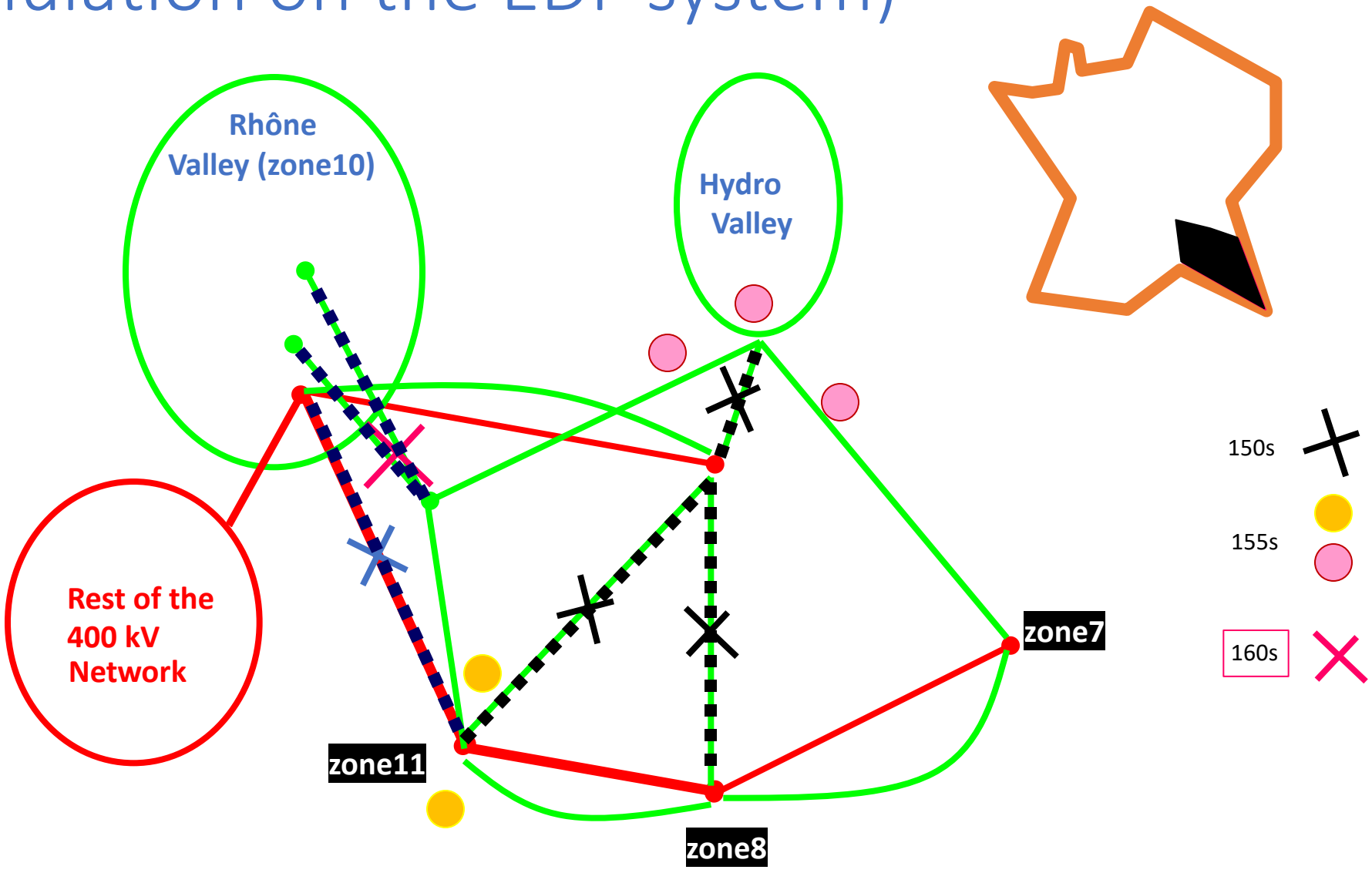
- In preventive mode (i.e. before a disturbance has occurred):
  - Impose operating margins by changing the system topology and/or the generation schedules (P and Q) while minimizing the resulting operating cost
  - So as to limit the potentially negative consequences over a postulated set of 'possible' disturbances

- In corrective mode (i.e. after a disturbance has occurred) :
  - Act quickly on the system behavior to avoid cascades, system splitting, and minimize the eventual loss of load
  - By reacting to the particular disturbance that has actually occurred

A note about ***Protections*** in power systems

- Protection systems: automatic devices that aim at disconnecting certain elements of the system in order to avoid physical dammage to some system components and/or to some human beings
- Taking into account the behavior of protection systems is of paramount importance in the context of power system security management
- Examples
  - Generator under-/over voltage protections
  - Generator under-/over speed protections
  - Over-currents: lines, cables, transformers, rotors
  - Under- frequency, under-voltage: load shedding
  - Distance protections: short-circuits
- Different protections act with different response times (from a few milliseconds to several minutes)

Example of a catastrophic cascading scenario (simulation on the EDF system)



Explanation of the sequence

At t=0s : Loss of a corridor of 400kV lines (assumed exogenous)

⇒Overload, then tripping of three important connections :
- towards Zone 7 (225 kV) : 150 s
- towards Zone 8 (225 kV) : 150 s
- towards Zone 11 (225 kV) : 150 s

⇒Loss of several generators (total of 2500MVA lost):
- Two thermal plants on undervoltage protection : 155 s
- Three hydro plants on overspeed protection : 155 s

⇒Overload, then tripping of the connection towards Zone 10 (225 kV) : 160 s

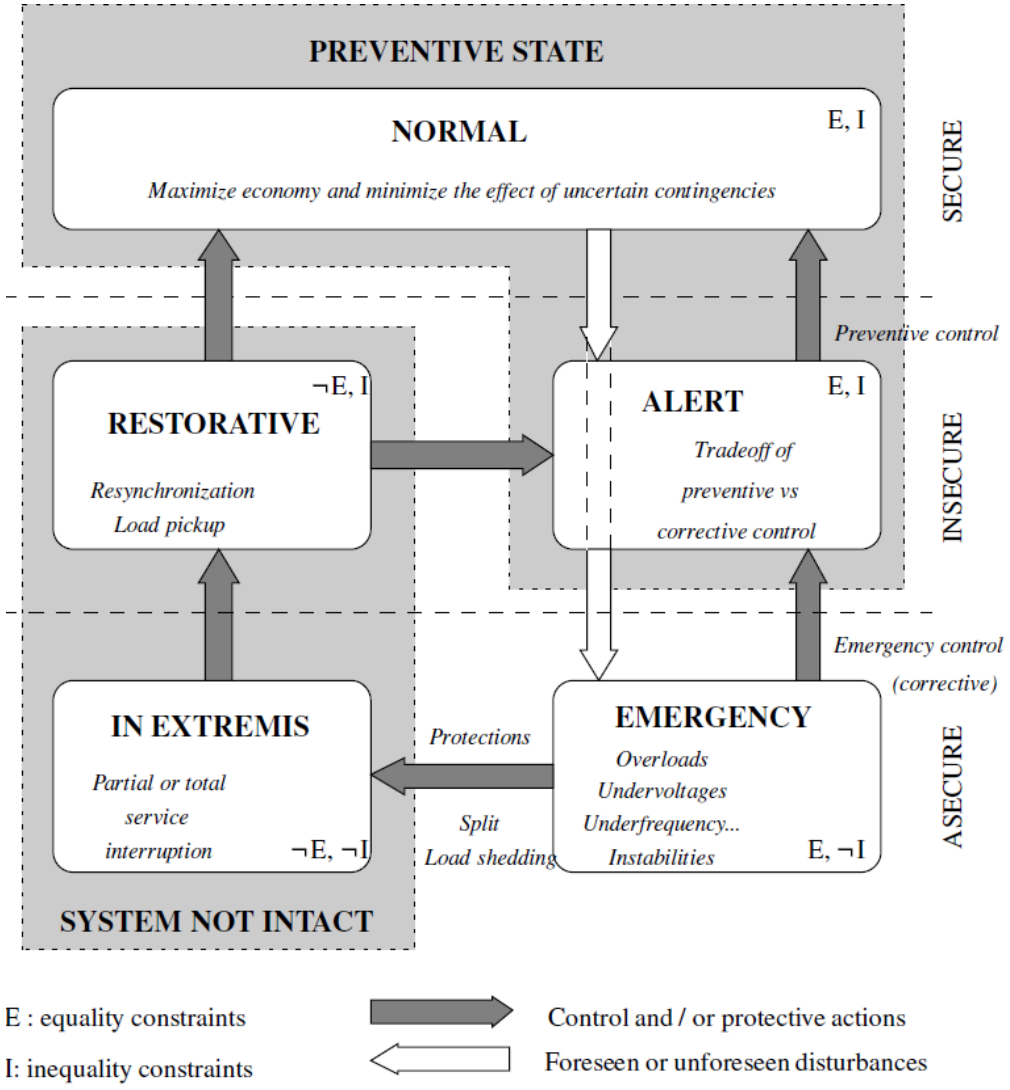
⇒Load shedding in zones 7, 8 and 11 (imporant service interruption)

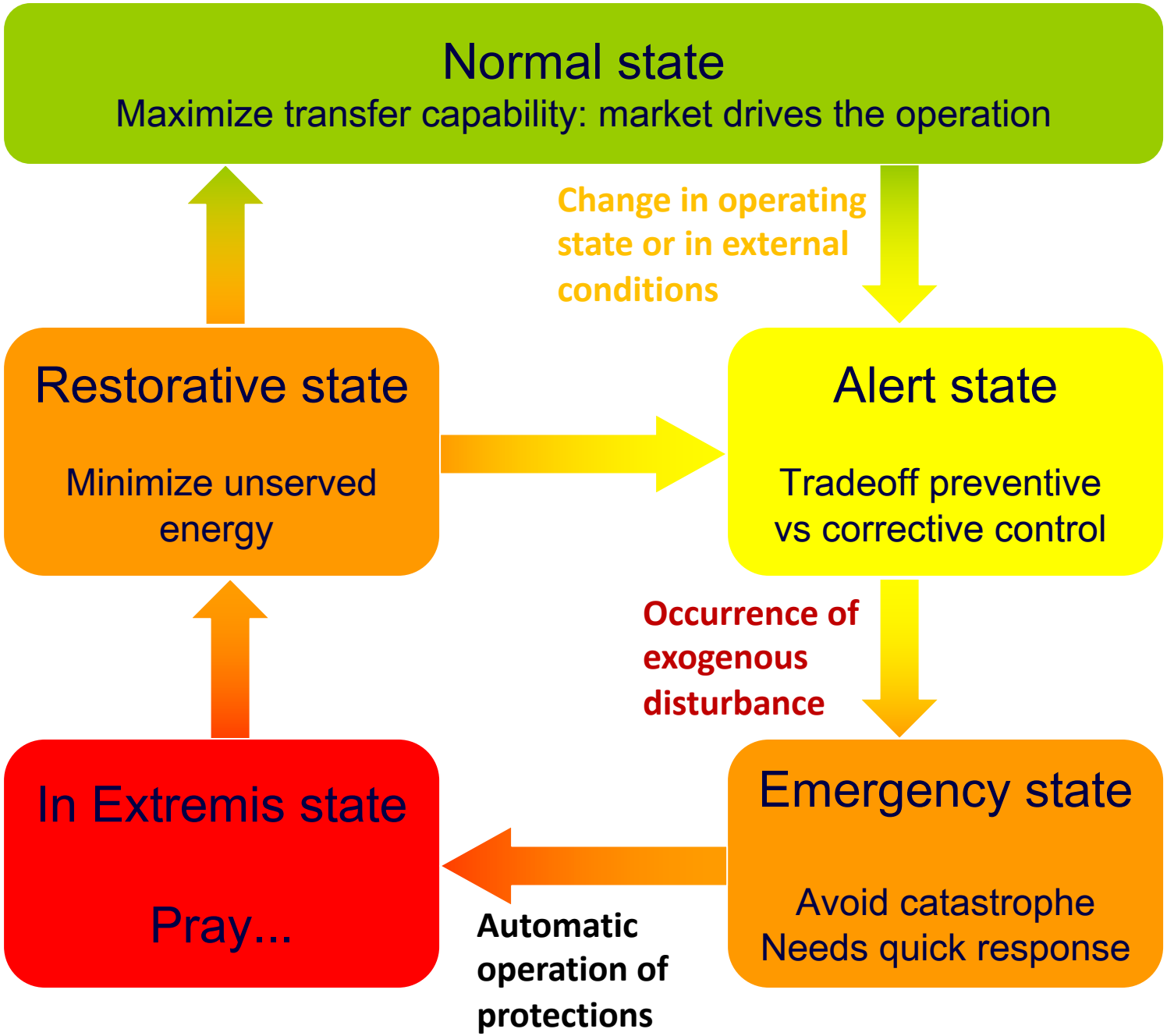
Relevant operating states of a power system

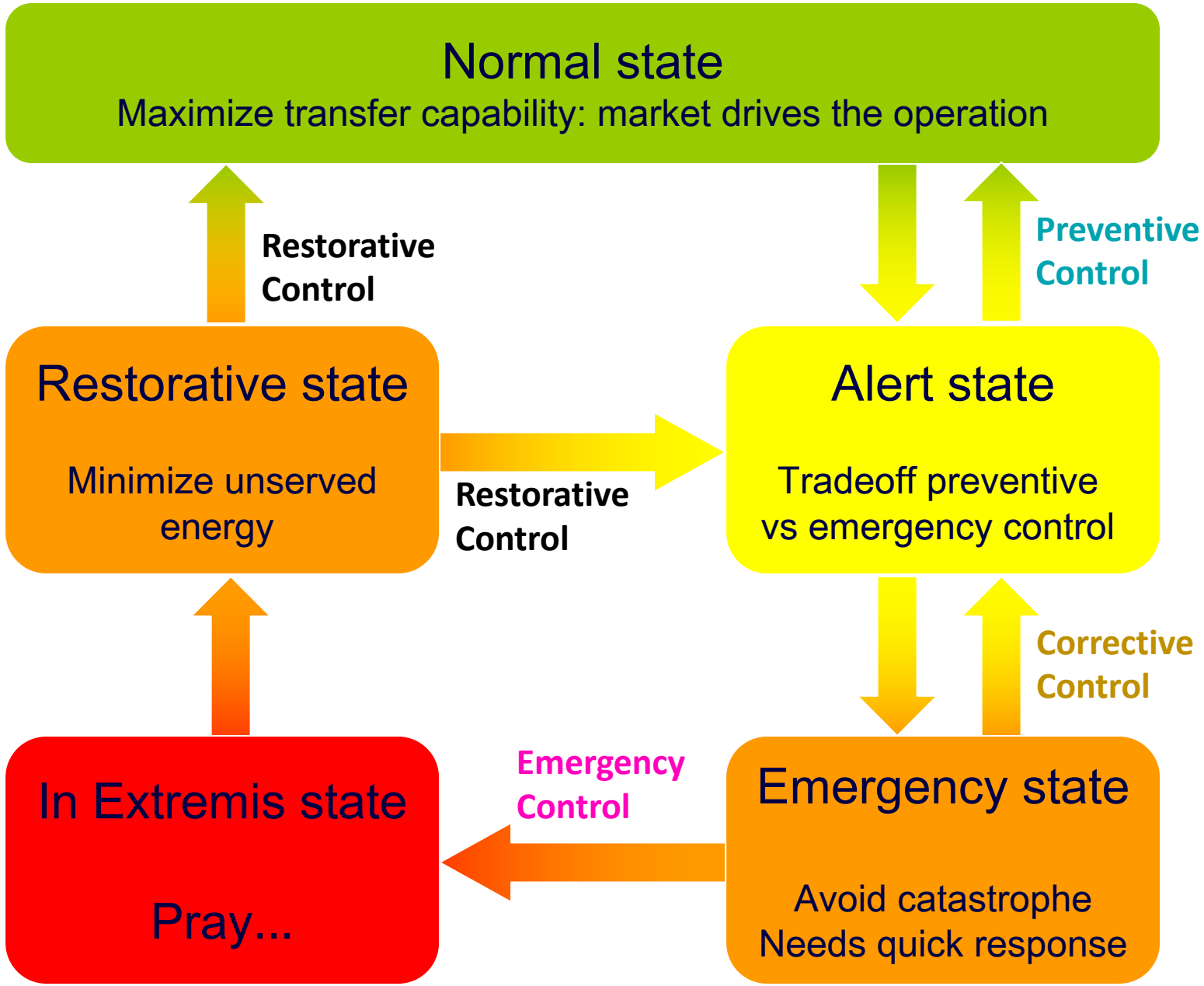
The following diagram was proposed in the 1970's in order to structure security assessment and security control activities in the context of bulk power systems operation.

For further reading:

"Operating under stress and strain", LH Fink and K Carlsen, IEEE Spectrum March 1978, pp 48-53



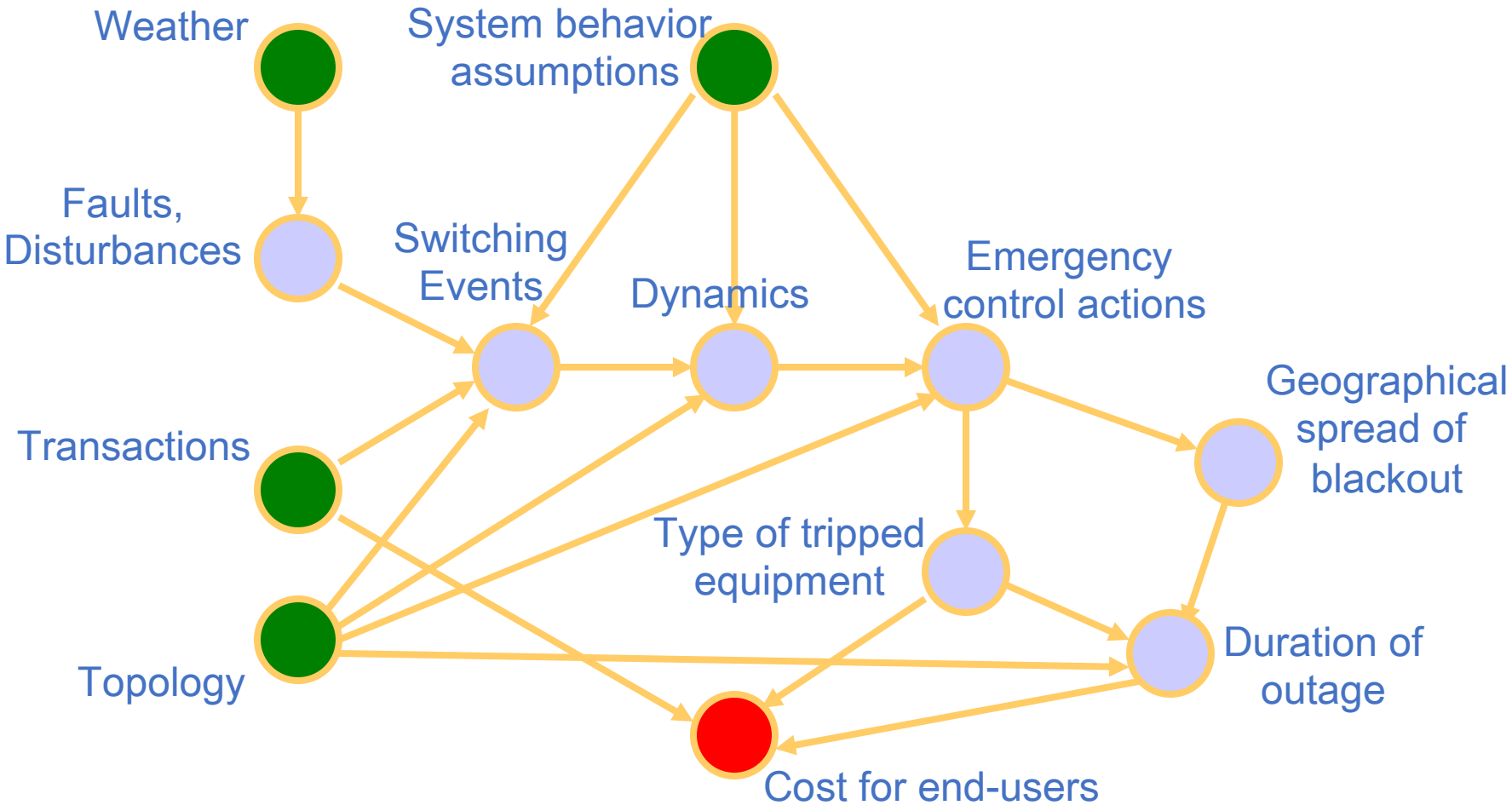

Normal state
Maximize transfer capability: market drives the operation
Change in operating state or in external conditions
Alert state
Tradeoff preventive vs corrective control
Occurrence of exogenous disturbance
Emergency state
Avoid catastrophe
Needs quick response
Automatic operation of protections
In Extremis state
Pray...
Restorative state
Minimize unserved energy


Normal state
Maximize transfer capability: market drives the operation
Restorative Control
Preventive Control
Restorative state
Minimize unserved energy
Restorative Control
Alert state
Tradeoff preventive vs emergency control
Corrective Control
In Extremis state
Pray...
Emergency Control
Emergency state
Avoid catastrophe
Needs quick response

Security assessment

- Determine in which operating regime (mainly normal vs alert) the system is and what are the most dangerous threats
- Can be achieved by
  - Postulating a set of possible disturbances and a physical behavior model of the system in the form of a ‘simulator’
  - Using the information of the system operating state as input, simulating the impact of various disturbances
  - Analyse, summarize and visualize the simulations’ results
- The list of disturbances used is also called the **‘list of contingencies’**

Influences in security assessment of power systems



Security - Decomposition into physical sub-problems

- Steady-state behavior: static security
  - See if currents, voltages, and frequency, remain within limits defined by component ratings, in the post-disturbance steady-state regime

- Dynamic behavior: dynamic security
  - See if the dynamic response to a disturbance leads to a stable trajectory towards a post-disturbance steady-state
    - local (small perturbations)
    - global (large perturbations)
    - Mechanisms: rotor-angles vs voltages

In principle we need both static and dynamic security

This decomposition is still very useful from a practical point of view. Different tools are indeed used, e.g. to assess dynamic and static security.

LIÈGE université

Static security assessment

- It is about the existence of a sound post-disturbance equilibrium state that can be sustained (is viable, without service interruption) for a sufficiently long period to allow the operator to again trade-off preventive and corrective controls
- For example:
  - If the disturbances consists of tripping (disconnecting) a line, what about the new steady state currents in the remaining lines, and what about the voltage magnitudes at the different buses.
  - Could be checked by running a power flow computation, while disconnecting the considered line

Dynamic security assessment

- Rotor-angle stability:
  - compute critical clearning times of a credible set of short-circuits
- Voltage stability:
  - compute post-disturbance load power margins, for different contingencies and areas of the system
- Small-signal stability:
  - compute eigenvalues and their sensitivities
- …

(Static and/or Dynamic) Security control

- If the security level of the system is not sufficient, then the operators must apply preventive controls and/or ensure suitable corrective controls
- This is a ‘decision making problem’ under uncertainties, much more complex than the ‘security assessment problem’
- It is only very partially solved today, by calling a lot on human expertise and judgment
- To frame this problem in a suitable way for computer applications, one can to formalize it as an ‘optimization problem’ under ‘security constraints’.
- Further, coordination among different TSOs is necessary to agree on ‘security targets’ for each subsystem

Notion of N-k security and use of N-1 as a security management standard among TSOs

Notion of *N-k* preventive static security (*k =0, 1, 2…*)

- The system in a certain operating state is said to be in *N-k* preventive static security
  - If any contingency consisting of tripping simultaneously up to *k* different system components leads to an acceptable post-contingency steady-state, without requiring any manual corrective control action
  - 'Acceptable' means here (at least) that all bus voltages and branch currents are within their permanent limits

- E.g. *N-0*: means that …
- E.g. *N-1*: means that …, and implies *N-0*

- In general: *N-k* implies *N-(k-1)*, for *k = 1, 2, …*

LIÈGE université

Original rationale of the N-1 criterion

- **Primary target:** ensure continuity of service of the power system
- **Sensible proxy:** avoid cascading outages subsequent to any 'next contingency'

- **Practically:**
  1. define set of **'considered next contingencies'**
  2. define notion of **'acceptable contingency response'**
  3. choose decisions optimizing **'an economic objective',** while complying with **1** and **2**.

LIÈGE université

Present use of the N-1 criterion

(in Real-Time operation)

- **Contingencies explicitly covered:**
  - all **N-1** events (+ possibly some common mode N-k events)
- **Acceptable contingency response:**
  - simulated response within steady-state (and stability) limits, for each and every contingency in the list.
- **Economic objective:**
  - Minimize operating costs: e.g. a combination of TSOs costs and congestion costs

- **NB: Ahead of real-time** (e.g. D-1 operation planning, asset management, grid development …):
  - Take decisions so as **to make N-1 criterion compliance feasible** at later stages, along the forecasted trajectories, and so as to give the best room for economic optimization

LIÈGE université

Security constrained optimal power flow

Security control

- If the security level of the system is not sufficient, then the operator must apply preventive control and/or plan for corrective control
- This is a ‘decision making problem’ under uncertainties, much more complex than the ‘security assessment problem’
- It is only very partially solved today, by calling a lot on human expertise and judgment
- To frame this problem in a suitable way for computer applications, one needs to formalize it as an ‘optimization problem’ under ‘security constraints’.
- Further, coordination among different TSOs needs to agree on ‘security targets’

SCOPF problem statement and its variations

$$\min_{\mathbf{x}_0,\ldots,\mathbf{x}_c,\mathbf{u}_0,\ldots,\mathbf{u}_c} f_0(\mathbf{x}_0,\mathbf{u}_0) \quad (1)$$

subject to:

$$\mathbf{g}_0(\mathbf{x}_0,\mathbf{u}_0) = \mathbf{0} \quad (2)$$

$$\mathbf{h}_0(\mathbf{x}_0,\mathbf{u}_0) \leq \mathbf{L}_l \quad (3)$$

Classical OPF equations,
With preventive control

SCOPF problem statement and its variations

$$\min_{\mathbf{x}_0,\ldots,\mathbf{x}_c,\mathbf{u}_0,\ldots,\mathbf{u}_c} f_0(\mathbf{x}_0,\mathbf{u}_0) \quad (1)$$

subject to:

Classical OPF equations,
With preventive control

$$\mathbf{g}_0(\mathbf{x}_0,\mathbf{u}_0) = \mathbf{0} \quad (2)$$

$$\mathbf{h}_0(\mathbf{x}_0,\mathbf{u}_0) \leq \mathbf{L}_l \quad (3)$$

$$\mathbf{g}_k^s(\mathbf{x}_k^s,\mathbf{u}_0) = \mathbf{0} \quad k = 1,\ldots,c \quad (4)$$

$$\mathbf{h}_k^s(\mathbf{x}_k^s,\mathbf{u}_0) \leq \mathbf{L}_s \quad k = 1,\ldots,c \quad (5)$$

Short term viability, after contingency k, but before corrective control is applied

$$\mathbf{g}_k(\mathbf{x}_k,\mathbf{u}_k) = \mathbf{0} \quad k = 1,\ldots,c \quad (6)$$

$$\mathbf{h}_k(\mathbf{x}_k,\mathbf{u}_k) \leq \mathbf{L}_m \quad k = 1,\ldots,c \quad (7)$$

$$|\mathbf{u}_k - \mathbf{u}_0| \leq \overline{\Delta\mathbf{u}_k} \quad k = 1,\ldots,c \quad (8)$$

Permanent response wrt to contingency k when using corrective control

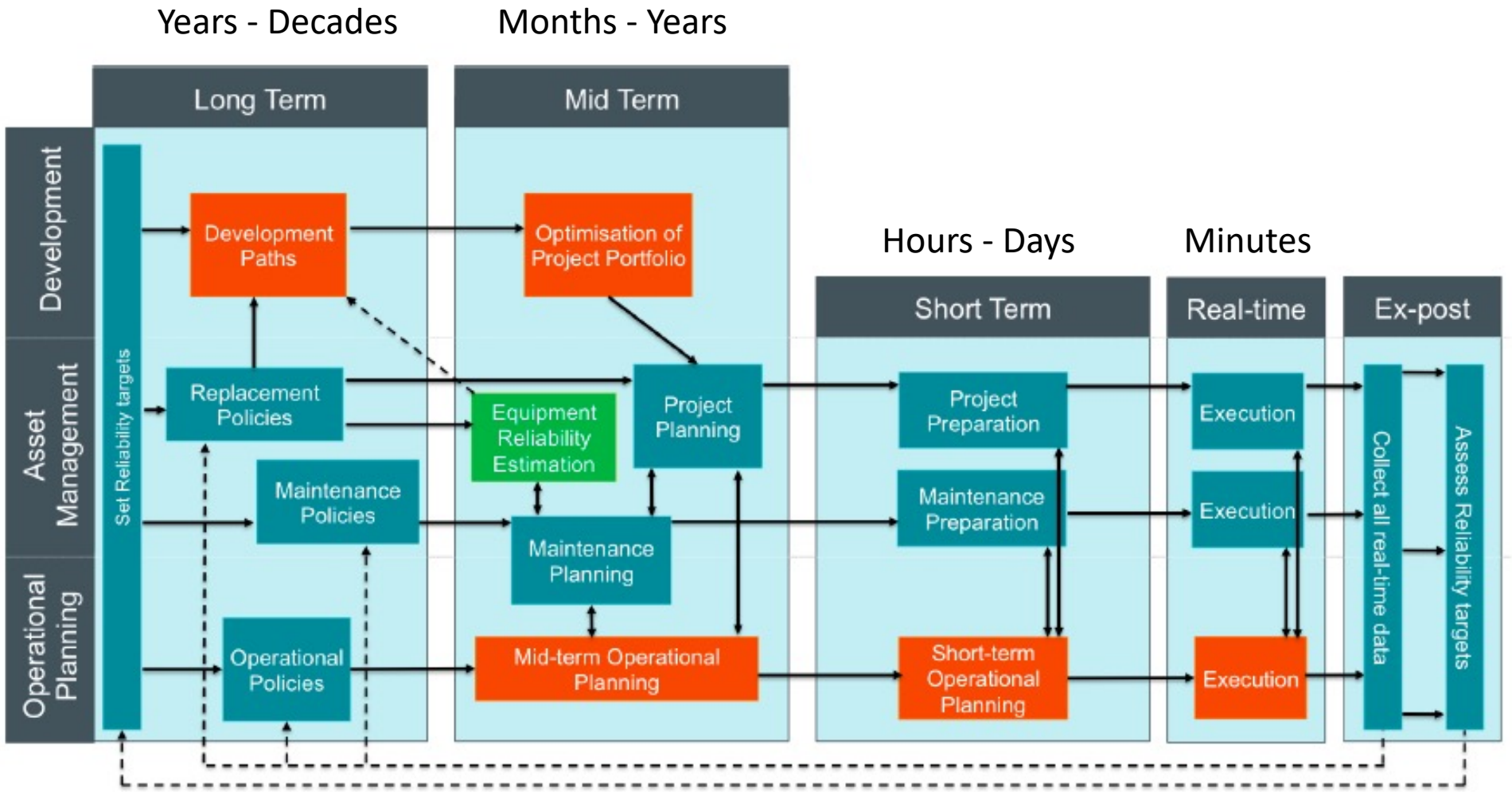
LIÈGE université

SCOPF algorithms & current research

- In general, the SCOPF is a very large scale non-convex and typically mixed discrete/continuous optimization problem
- In the context of real-time operation, we look for near-optimal and feasible solutions, and therefore want to be able to take advantage of all potentially useful types of preventive and corrective controls
- The computational tools should be robust and fast enough, and provide practically exploitable decision support to the operator
- Machine learning methods can be used in combination with numerical optimization techniques to create more effective tools

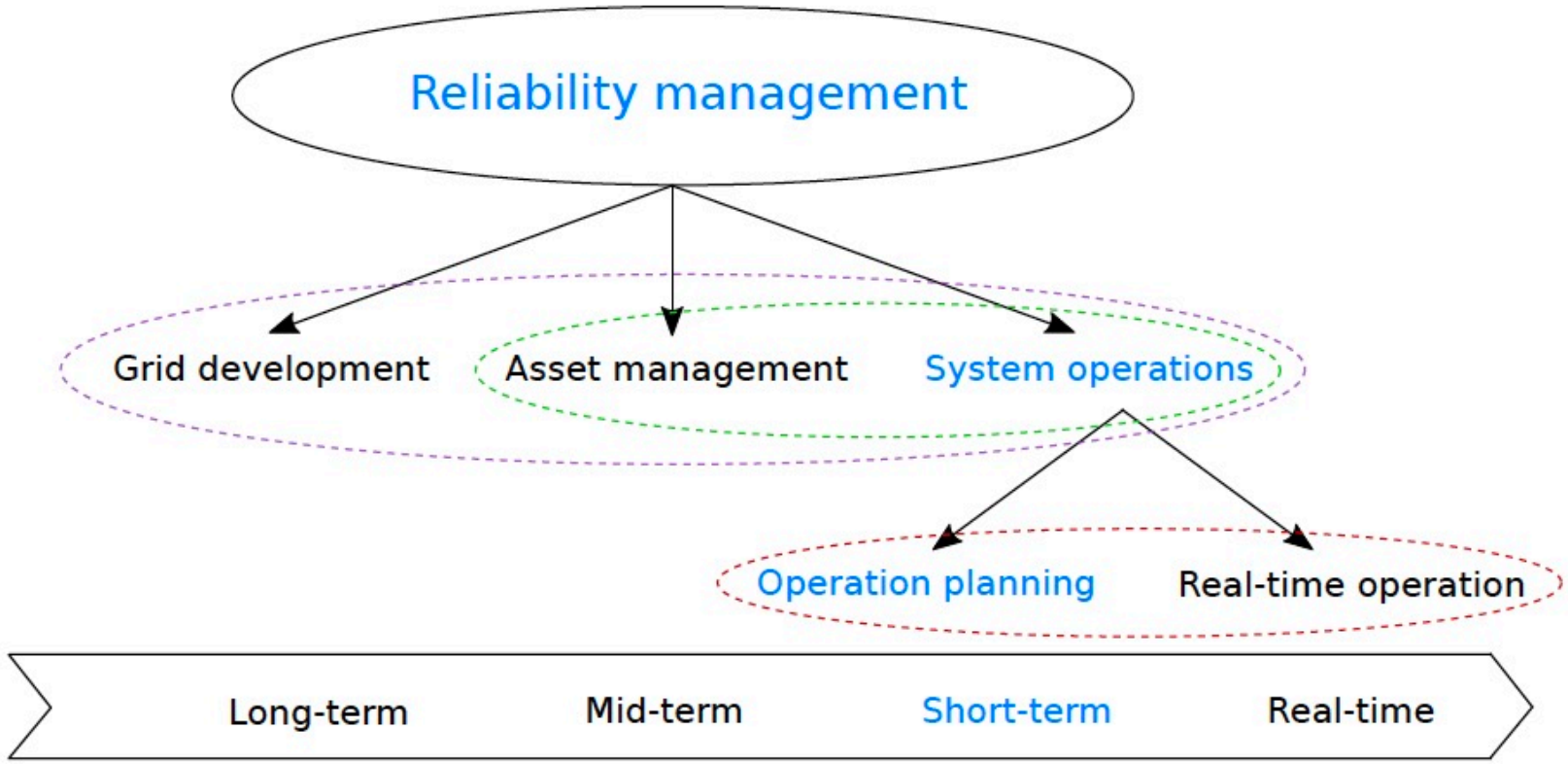
Implications for operation planning, asset management, and system development

Types of decision making activities versus temporal horizons

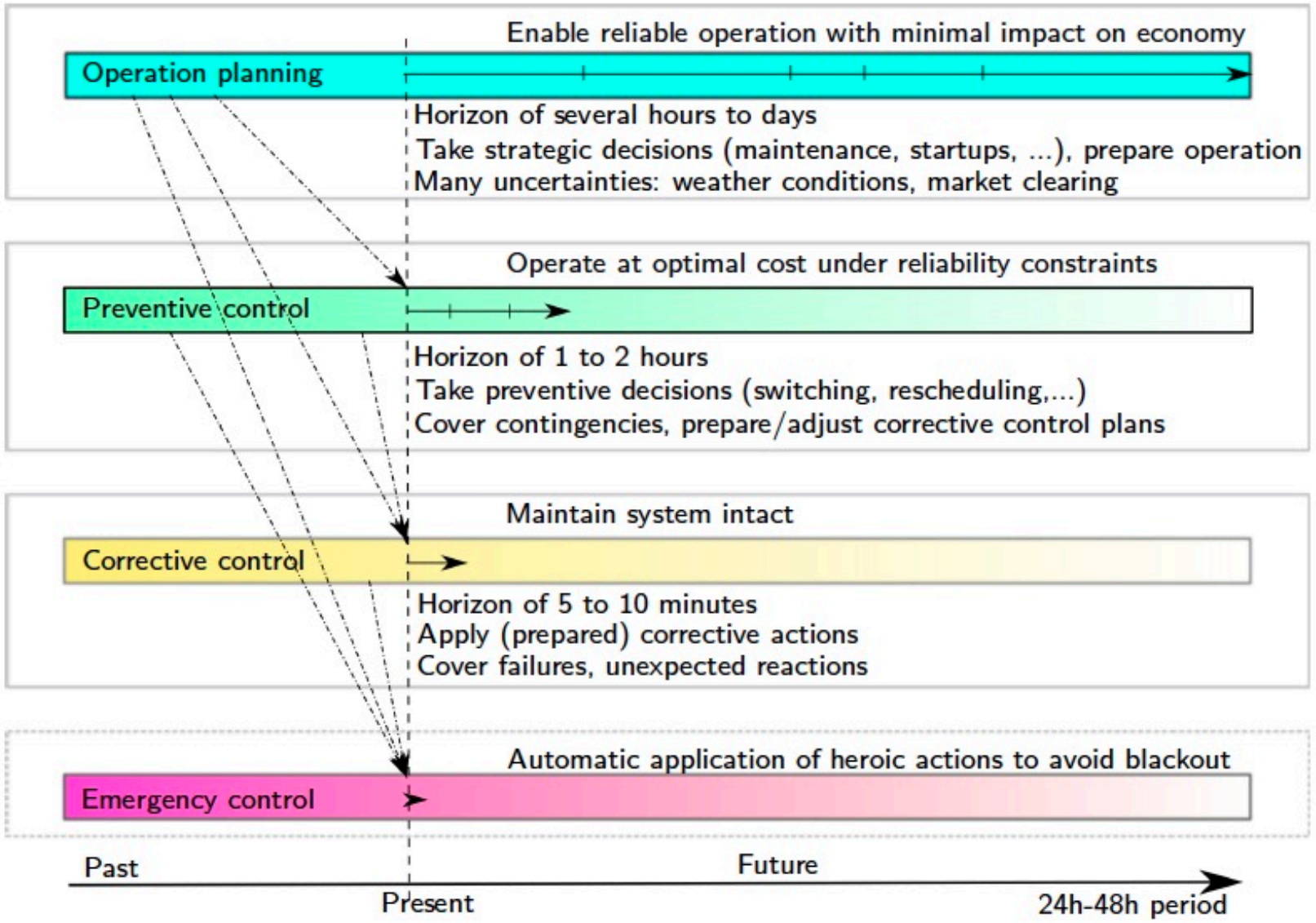


Reliability management (objective)

Taking decisions in order to ensure the reliability of the system while minimizing socio-economic costs



Operation planning, operation, and automatic control



Present use of the N-1 criterion

(in Real-Time operation)

- **Contingencies explicitly covered:**
  - all **N-1** events (+ possibly some common mode N-k events)
- **Acceptable contingency response:**
  - simulated response within steady-state (and stability) limits, for each and every contingency in the list.
- **Economic objective:**
  - Minimize operating costs: e.g. a combination of TSOs costs and congestion costs

- **NB: Ahead of real-time** (e.g. D-1 operation planning, asset management, grid development …):
  - Take decisions so as **to make N-1 criterion compliance feasible** at later stages, along the forecasted trajectories, and so as to give the best room for economic optimization

LIÈGE université

Further Reading

- “Operating under stress and strain”, LH Fink and K Carlsen, *IEEE Spectrum*, March 1978, pp 48-53
- “Power systems ‘2000’: hierarchical control strategies”, FC Schweppe, *IEEE Spectrum*, July 1978, pp 42-47
- “A Vision to enhance transmission security – The case of Switzerland’s Power System”, E Vrettos, M Hohmann, M Zima, *IEEE Power & Energy Magazine*, March-April 2021, pp 56-68
- “State-of-the-art, challenges, and future trends in security constrained optimal power flow”, F Capitanescu et al., *Electric Power Systems Research* 81.8 2011, pp 1731-1741