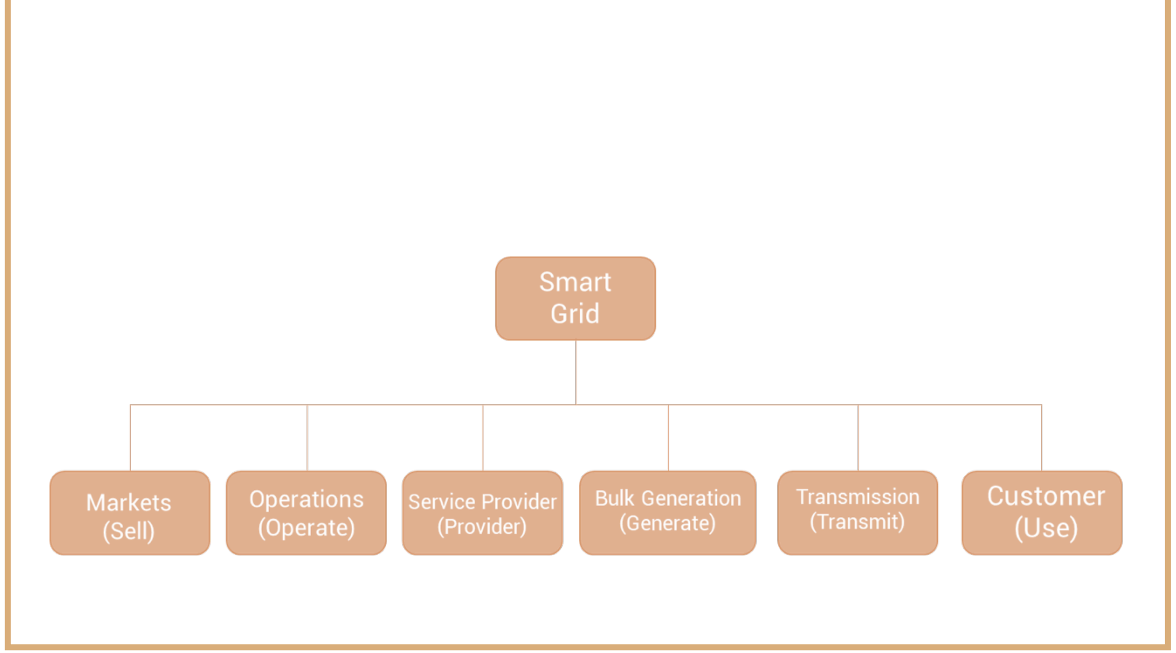
System-Theoretic Process Analysis (STPA) of Demand-Side Load Management in Smart grids

Stylianos Karatzas
Athanasios Chassiakos

UNIVERSITY OF
PATRAS
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

Smart Grid- The concept

A **smart grid** is an electricity network based on digital technology that is used to supply electricity to consumers via two-way digital communication, to provide:



a) ***operational efficiency*** (distributed generation, network optimization, remote monitoring, improved assets utilization, and preventive maintenance)

b) ***energy efficiency*** (reduced system and line losses, improved reactive load control, peak-load shaving)

c) ***customer satisfaction*** (improve the communication between producers and consumers)

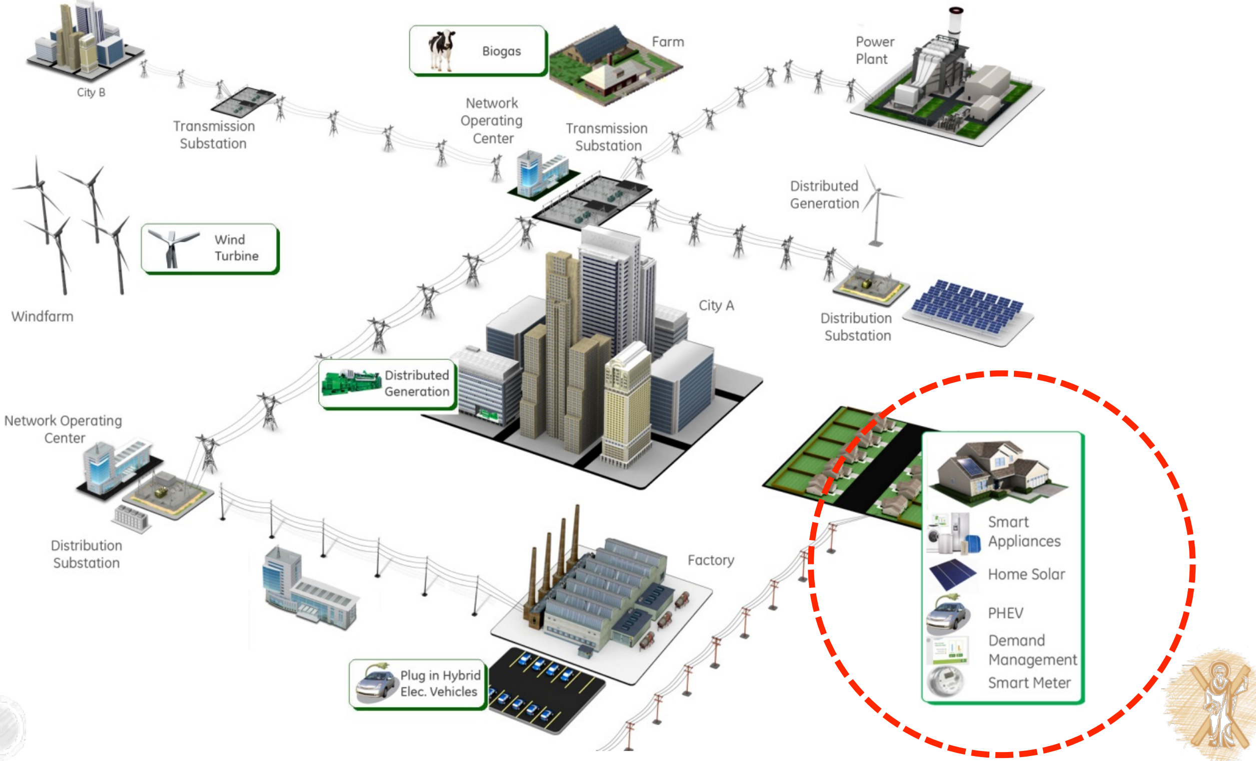
d) ***CO2 emission reduction*** (demand-side load management and integration of renewable energy sources)

Demand-Side Load Management- The Concept

- Electricity demand side management (DSM) refers to the changes in the electricity usage by the end-use customers from their nominal consumption patterns

- After a fault occurs, DSM can be used to increase the restoration capacity and reduce the load interruption duration.

- DSM enable utilities to reduce the overall system demand during emergency times



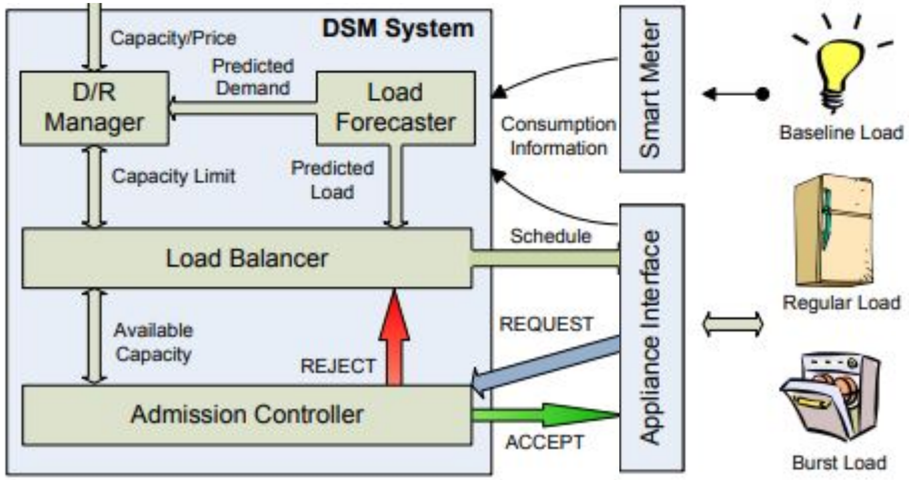
UNIVERSITY OF PATRAS
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

Demand Side Load Management – The Architecture

DSM System

HAEM System

Smart Appliances



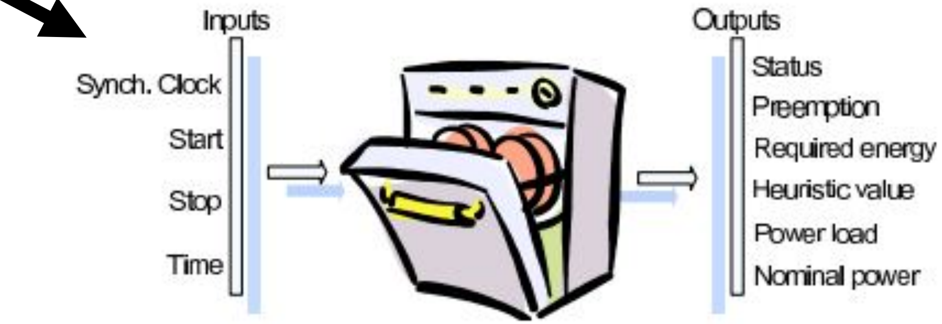
Appliance Status
Off
Ready
Run
Idle
Complete
Fault

Universal Appliances Controller

Comfort Context System

Human comfort Boundaries

User Profiles



UNIVERSITY OF PATRAS
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

The need: Continuously reliable operation of Smartgrids

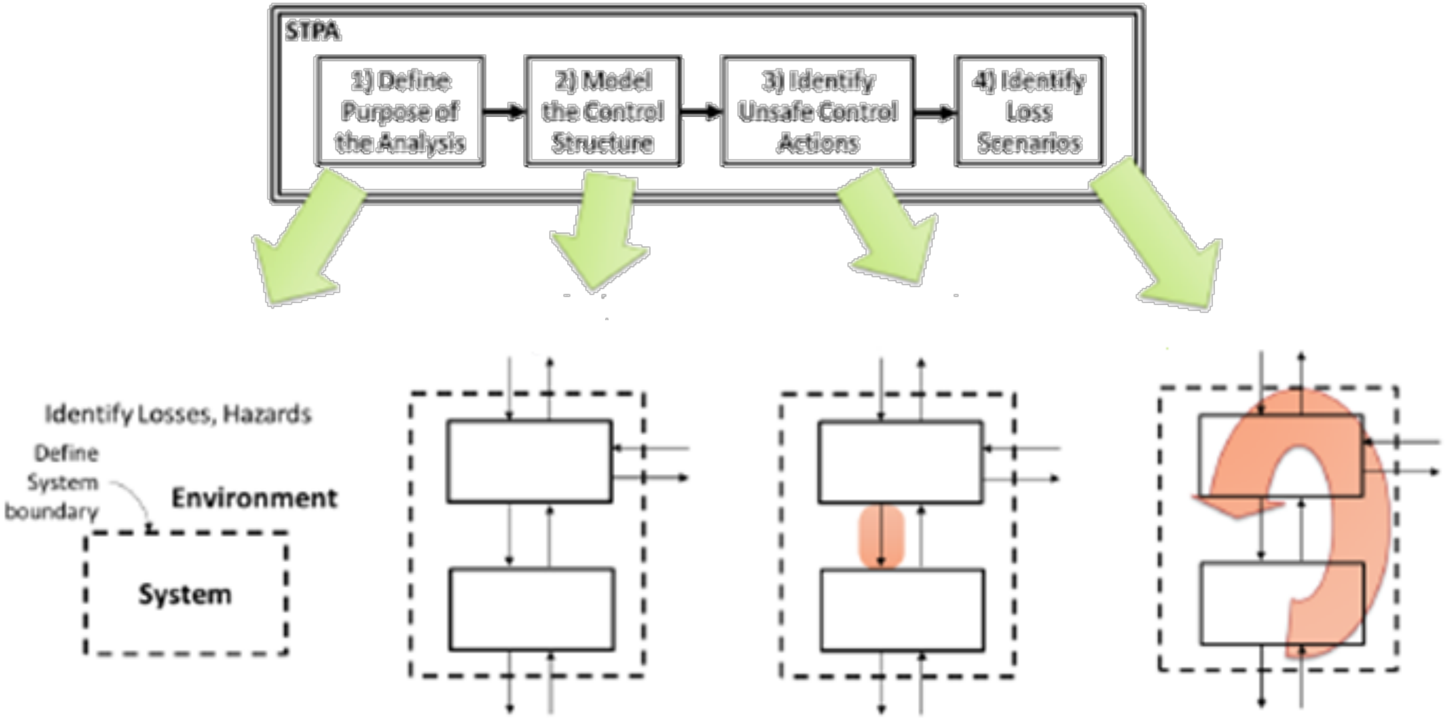
- ➢ increasing complexity of power
- ➢ inelasticity of demand
- ➢ growing demand
- ➢ greater distribution of elements
- ➢ security and efficiency
- ➢ environmental and energy sustainability

Demand Side Management (DSM) to exploit demand flexibility

⇩

Assess the potential risks and hazards in a systematic way

STPA – Application

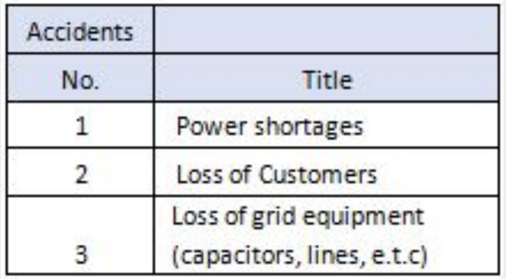

STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
Identify Losses, Hazards
Define System boundary
Environment
System

Overview of the basic STPA Method

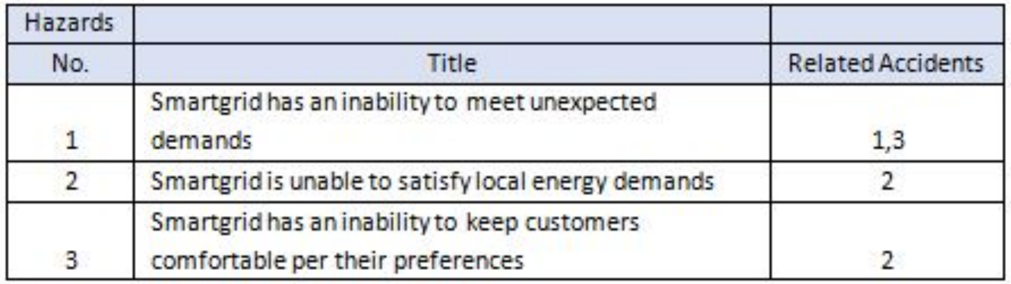
Purpose of the Analysis

Identify Accidents

Accident *: an undesired or unplanned event that results in a loss, including loss of system operation, property damage, environmental pollution, etc*



Accidents	
No.	Title
1	Power shortages
2	Loss of Customers
3	Loss of grid equipment (capacitors, lines, e.t.c)



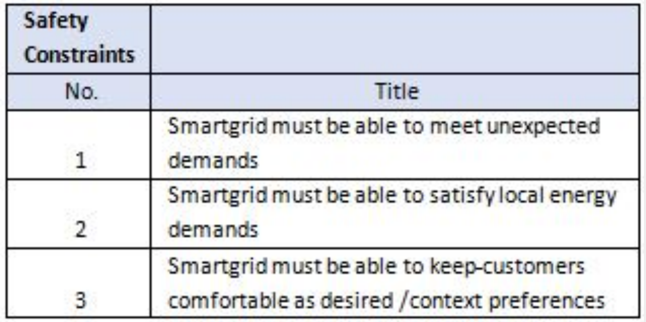
Hazards		
No.	Title	Related Accidents
1	Smartgrid has an inability to meet unexpected demands	1,3
2	Smartgrid is unable to satisfy local energy demands	2
3	Smartgrid has an inability to keep customers comfortable per their preferences	2

Identify System-level Hazards

Hazards*: system states or conditions that lead to a system accident under a specific set of worst-case context conditions.*

Identify system-level safety constraints

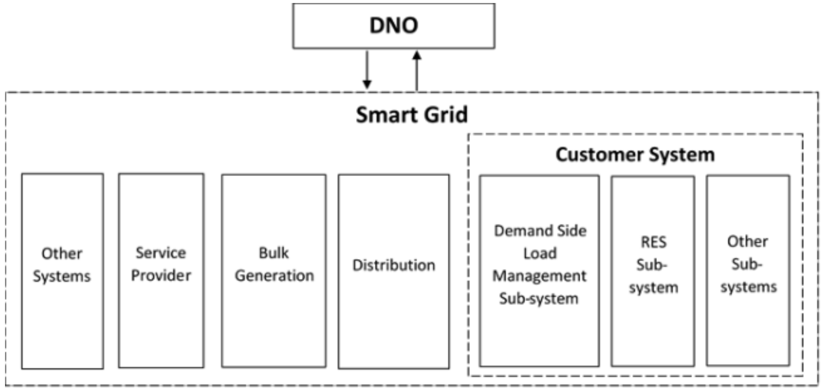
Once the system-level hazards are identified, it is straightforward to identify system-level constraints that must be enforced.



Safety Constraints	
No.	Title
1	Smartgrid must be able to meet unexpected demands
2	Smartgrid must be able to satisfy local energy demands
3	Smartgrid must be able to keep-customers comfortable as desired /context preferences

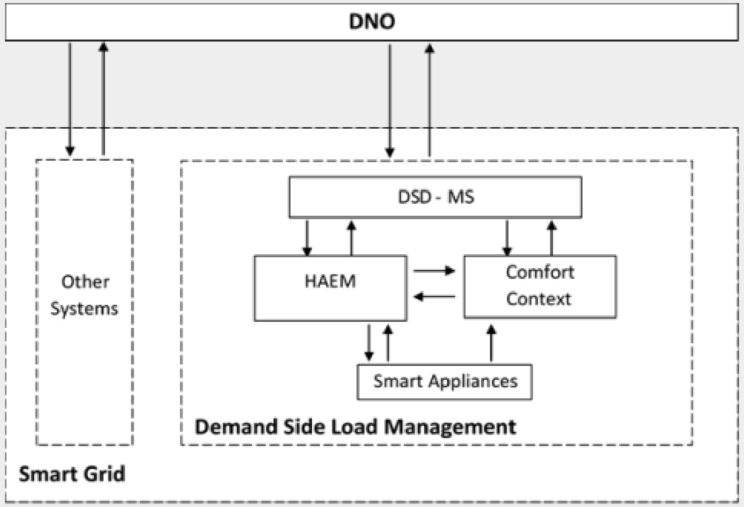
Modeling the Control Structure

Abstract Control Structure



The basic subsystems are identified in order to enforce the constraints and prevent the hazards identified earlier.

Refined Control Structure

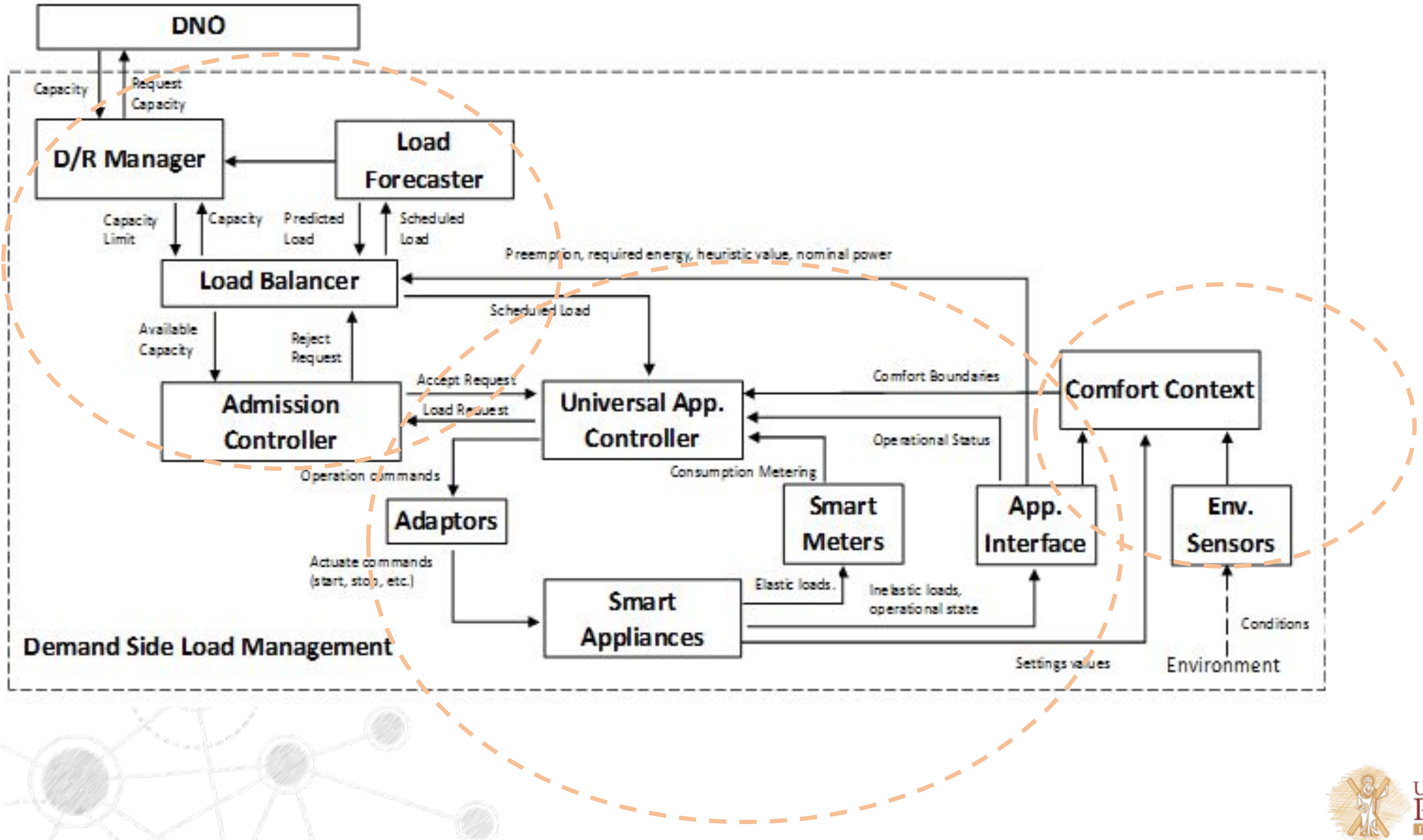


System components of the system (controllers, actuators, sensors, and controlled processes) are defined

Modeling the Control Structure

Responsibilities	Process	Feedback	Control Action Description
DRM asks for excess capacity from the DNO	Excess capacity is required	Excess capacity	excess capacity demand
DRM informs LB about the capacity limits	Capacity is adjusted	Available capacity Predicted demand	provide the capacity limits
LF provides load forecasts	Loads are forecasted	Load schedule, Energy required, preemption, power load	predict required loads
AC manages incoming requests from UAC	AC manage incoming requests from UAC	AC manages incoming requests from UAC	AC manages incoming requests from UAC
LB schedules loads request	Loads are scheduled	rejected requests, heuristic value, dependency matrix,	accept load request

Modeling the Control Structure



Identifying Unsafe Control Actions

Control Action	Not Given	Provided Incorrectly	Wrong Timing or order	Stopped too soon or applied too long
excess capacity demand	DRM does not demand excessive capacity while there is a need to cover more loads [2,3] [UCA1]	DRM demands more excessive capacity than the actual required capacity for appliances to operate in the defined time horizon ahead [1] **[UCA2]** DRM demands less excessive capacity than the actual required capacity for appliances to operate in the defined time horizon ahead [2,3] [UCA5] DRM demands excessive capacity while the appliances can operate sufficiently in the defined time horizon ahead[[1] [UCA6]	DRM demand excessive capacity too late (>TBD) after request [2,3] [UCA3]	DRM stops demanding for excessive capacity while overload still remains [2,3] [UCA4]

Identifying Unsafe Control Actions

Control Action	Not Given	Provided Incorrectly	Wrong Timing or order	Stopped too soon or applied too long
predict required loads	LF does not provide accurate load prediction while there is a change to the load schedule [2, 3] [UCA 9]	LF makes an innacurate load prediction while appliances operation requirements can be met sufficiently according to the schedule [1] **[UCA 10]**	LF provides a load prediction too late (>TBD) after the change on the load schedule [2,3] **[UCA11]**	

Identifying Unsafe Control Actions

Control Action	Not Given	Provided Incorrectly	Wrong Timing or order	Stopped too soon or applied too long
schedule load requests		LB schedules a load that cannot be covered by the capacity at the specific defined time [2, 3] **[UCA 16]** Each appliance load is scheduled in an operation period in such a way that appliance is operated for less than the required time to complete an operational cycle [2, 3] **[UCA 17]** Each load is scheduled more than one time [1] [**UCA 18]**	LF provides a load prediction too late (>TBD) after the change on the load schedule [2, 3] **[UCA11]**	

Safety Constraints

No.	Unsafe Control Actions	Resulting Safety Constraints
2	DRM demands more excessive capacity than the actual required for appliances to operate in the defined time horizon ahead	DRM must demand the exact capacity required for the consumption of the appliances to operate efficiently in the defined time frame
10	LF does not make new load prediction while there is a change to the load schedule	LF must adjust load predictions when there is a load schedule change
11	LF make an inaccurate load prediction at the specific requirement operational conditions	LF must deliver accurate load predictions considering appliances consumption according to the schedule
16	LB schedules a load that cannot be covered by the capacity at the specific defined time	LB must not schedule a load that cannot be covered by the available capacity at this time
17	LB schedules appliance load in an operation period in such a way that appliance is operated for less than the sufficient time in order to complete the working cycle before the deadline.	LB must not schedule each appliances load in an operation period in such a way that appliance operate for less than the sufficient time in order to complete a working cycle before the deadline
18	LB schedules each load more than one time	LB must schedule a load only once for a timeframe

Loss Scenarios

Unsafe Controller Behaviour

UCA-10: LF does not make new load prediction while there is a change to the load schedule.

Scenario 1: The LF controller is not trained to meet requirements and fails to provide a load forecast during a change on schedule. As a result, less capacity may be required from the DNO which can lead Smart grid not meet local energy demand [H-1].

UCA-17: LB schedules the appliance operation in such a way that appliance operates for less than the enough time to complete the working cycle before the deadline.

Scenario 1: The UAC asks for a task to complete in a certain time slack which is smaller than the task’s operation time, in this case, even with availability of sufficient capacity, the LB fails in scheduling, which may lead to not satisfactory local energy demand or customer preferences [H-2, H-3]

UCA-18: LB schedules each load more than one time.

Scenario 1: The LB algorithm incorrectly considers that a load request has been rejected, and the corresponding task is scheduled again. As a result, the available capacity is not accurate and the requirement for more capacity may lead Smart grid to operate outside the capacity limits [H-1].

Loss Scenarios
Inadequate feedback and information

UCA-2: DRM demands more excessive capacity than the actual required capacity for appliances to operate in the defined time horizon ahead.

Scenario 1: The load request rate of rejection is inappropriately measured due to inefficient information about the number of rejected request from LB (provide higher number of rejected requests). Thus, DRM to improve Quality of Service and avoid customer discomfort, demands excessive capacity from the Smartgrid. As a result, the network may operate out of the capacity limits.

UCA-11: LF makes an excessive load prediction while appliances operation requirements can be met sufficiently according to the schedule.

Scenario 1: The LF forecasting model used unreliable data input which lead to excessive load predictions, and as a result to higher required capacity needs and lead Smartgrid to operate outside the capacity limits [H-1].

UCA-16: LB schedules a load that cannot be covered by the capacity at the specific defined time

Scenario 1: LB receives for an appliance a ‘READY’ state assigned to the variable ‘Nominal Power’ while it is operating in ‘RUN’ state, where the load consumption is higher. This may cause insufficient capacity to meet local demand or satisfy customer preferences [H-2, H-3]

Scenario 2: LB retrieves unrealistic and inaccurate information of local forecasts, and the load cannot be covered. As a result, the local network may not be able to meet current local needs.

Scenario 3: LB retrieves unrealistic and inaccurate information about the available capacity. As a result, the local network may not be able to meet current local needs

Conclusions

Smartgrids

- Too complex for complete analysis
- *Separation into (interacting) subsystems distorts the results*
- *The most important properties are emergent*
- Especially in the building energy sector, the application of risk management methodologies is limited or incomplete

STPA ability to handle with:

- *Component interaction accidents*
- *Systemic factors (affecting all components and barriers)*
- *System design errors*
- *Indirect or non-linear interactions and complexity*

The research study proves:

STPA applicability in Smartgrids case

STPA is a solution

UNIVERSITY OF PATRAS
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

Plans for future work

- Deep evaluation of STPA as a hazards identification and analysis methodology with focus on energy applications. Next steps involve

a) comparison of the results from STPA with traditional hazard analysis methodologies and further evaluation of results

b) further expansion of the methodology to address additional risk and hazards with focus also on smart building environment and smart grids as well.

- Self-consumption optimization in a local network as the case to maximize RES generation absorption at local level is an interesting business scenario.

- The reason for promoting self-consumption is to lessen the burden on regional and low voltage grids as energy is consumed at the same location where it is generated and no longer has to be transported over the grid.

Thank You

UNIVERSITY OF
PATRAS
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ