# A framework of model predictive control for the safety analysis of an electric power microgrid

F. Han, Ionela Prodan, Enrico Zio

# A Framework of Model Predictive Control for the Safety Analysis of an Electric Power Microgrid

F. Han
*Chair on Systems Science and the Energetic Challenge, Fondation EDF, CentraleSupelec, France*

I. Prodan
*Chair on Systems Science and the Energetic Challenge, Fondation EDF, CentraleSupelec, France*

E. Zio
*Chair on Systems Science and the Energetic Challenge, Fondation EDF, CentraleSupelec, France*
*Department of Energy, Politecnico di Milano, Italy.*

ABSTRACT: This paper investigates system safety within a control perspective. We adopt model predictive control for our safety investigation and consider a microgrid system as case study. We study the satisfaction of consumer demands under different faulty scenarios, and different controllability and observability conditions. By simulations, we show the feasibility of investigating safety in relation to control properties of the system.

## 1 INTRODUCTION

Safety is the absence of catastrophic consequences on the users and the environment (Lussier, Chatila, Ingrand, Killijian, & Powell 2004). Different academic and professional communities have addressed the multi-disciplinary issue of system safety from different points of view. Under a control perspective, system safety is framed as a control "problem" (Leveson 2004), whereby, accidents result from inadequate control or insufficient enforcement of safety-related constraints on the development, design, and operation of the system, leading to their violation and subsequently to accidents.

On these premises, the notions of controllability and observability have been introduced in relation to the problem of accident causation and prevention (Bakolas & Saleh 2011). In (Bakolas & Saleh 2011), for example, the control-theoretic notion of controllability has been expanded as the ability of a system to be brought back to its "safety zone" through inputs, and the idea that an accident sequence can be interrupted through appropriate control inputs has been introduced. Such inputs must be chosen through state feedback, a process that in many practical applications requires state estimation and is, thus, contingent on the system being state-observable (observability is a central concept in Control Theory). In this view, system safety should not be based on output monitoring but state monitoring/estimation and feedback.

In the present paper, we explore quantitatively the above perspective, proposing an empirical approach by numerical simulation to show and investigate the role and effects of observability and controllability properties on system safety.

A microgrid system is considered as case study. Various approaches for energy management within a microgrid are reported in the literature. For example, Jimeno, Anduaga, Oyarzabal, & de Muro (2011), Kuznetsova, Culver, & Zio (2011), Krause, Beck, Cherkaoui, Germond, Andersson, & Ernst (2006), Weidlich & Veit (2008) propose an agent-based modeling approach to model microgrids and to analyze by simulation the interactions between individual intelligent decision-makers. In (Prodan & Zio 2014a), (Prodan & Zio 2014b), an optimization-based control approach is developed. For this kind of system, it is necessary to consider not only exogenous factors (e.g. wind speed, variations of consumer load, etc), but also internal dynamics and structural properties of individual components (e.g. links, storage device, etc.), which may change due to degradation, failure and other factors.

We use model predictive control (MPC), which is a widely used technique in the control community, to manage the dynamics of systems affected by uncertainties in the behavior of their components (see, for instance, (Rawlings & Mayne 2011), (Richalet & O'Donovan 2009) for basic notions about MPC),

due to its ability to handle control and state constraints while offering good performance specifications. Typically, in MPC, the objective (or cost) function penalizes deviations of the states and inputs from their reference values, while the constraints are enforced explicitly (Goodwin, Seron, & De Dona 2005). Recently, MPC is being considered for refrigeration systems (Hovgaard, Larsen, & Jorgensen 2011), for power production plants (Halvgaard, Poulsen, Madsen, & Jorgensen 2012), (Edlund, Bendtsen, & Jørgensen 2011) and transportation networks (Negenborn, De Schutter, & Hellendoorn 2008).

The proposed MPC framework is used to analyze various faulty scenarios, whose consequences are evaluated in terms of consumer power demands not satisfied. We look at the effects of different conditions of observability/controllability on "system safety" (consumer power demands satisfaction).

The original contributions are the following:

- A simulation-based framework for the investigation of the effects of controllability and observability properties on system safety.
- The formulation of an optimization-based model predictive control problem for safety considerations.

The reminder of this paper is organized as follows. Section 2 describes in detail the considered microgrid system, including the dynamic model, the profiles characterizing the system, the constraints and the different types of faults analyzed. Section 3 presents the safety criteria and observability/controllability properties considered for the system, and the formulation of the optimization-based control problem. Simulation results for the different faulty scenarios are presented in Section 4. Conclusions are drawn in Section 5.

## 2 SYSTEM MODELING AND DESCRIPTION

In this section, we present the dynamic models, the profiles of operation, the constraints and the faults considered for the components of the microgrid system in Figure 1.

### 2.1 *Dynamic models*

In the present subsection, we introduce the detailed dynamic model of the microgrid system, which includes a local consumer (e.g., large cooling houses), a renewable generator (e.g., wind turbine) and a storage facility (e.g., battery). The microgrid is connected to the external grid via a transformer.

We consider six components, including various electrical links and the battery operation in Figure 1. The internal dynamics appearing in the scheme lead

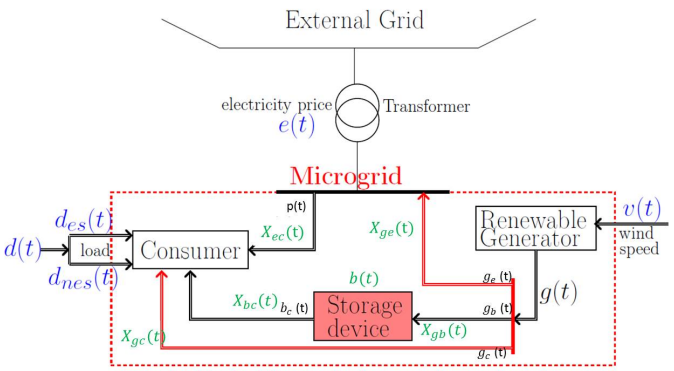



Figure 1: Microgrid

to a 6 components state: 5 describe the power propagation and one, the storage level in the battery element.

The state vector containing the information regarding the condition of the system is :

$$\mathbf{x}(t) = [x_{ec}(t) \quad x_{ge}(t) \quad x_{gc}(t) \quad x_{gb}(t) \quad x_{bc}(t) \quad b(t)]^T$$

The first 5 components of the state denote the values of energy in the transport wires. We assume first order dynamics to model how the value at one end of the wire propagates to the other end. The sixth state denotes the charge in the storage component. The dynamic models are given in the following.

External grid to consumer:

$$x_{ec}(t+1) = (1-\alpha)x_{ec}(t) + \alpha p(t) \tag{1}$$

Generator to external grid:

$$x_{ge}(t+1) = (1-\alpha)x_{ge}(t) + \alpha g_e(t) \tag{2}$$

Generator to consumer:

$$x_{gc}(t+1) = (1-\alpha)x_{gc}(t) + \alpha g_c(t) \tag{3}$$

Generator to battery:

$$x_{gb}(t+1) = (1-\alpha)x_{gb}(t) + \alpha g_b(t) \tag{4}$$

Battery to consumer:

$$x_{bc}(t+1) = (1-\alpha)x_{bc}(t) + \alpha b_c(t) \tag{5}$$

where $\alpha \in [0,1]$ is a fixed constant, mainly dependent upon the size of the discretization step.

Battery charge:

$$b(t+1) = (1-\tau)b(t) + x_{gb}(t) - b_c(t) + w(t) \tag{6}$$

with the mixed-integer conditions (Prodan & Zio 2014a):

$$\begin{cases} 0 \leq b_c(t) \leq Ma(t), \\ 0 \leq x_{gb}(t) \leq M(1-a(t)), \end{cases} \tag{7}$$

where $\tau$ denotes the hourly self-discharge decay and is equal to $10^{-4}$, $M$ represents an appropriately chosen constraint and $a(t) \in \{0,1\}$ is an auxiliary binary variable, characterizing the battery state of charge: when $a(t) = 1$ the battery is in discharge mode, when $a(t) = 0$ he battery is in charge mode.

Then, we describe the interactions between the independent components of the microgrid:

- $p(t) \in \mathbb{R}$ [W] represents the electrical power transmitted by the external grid to the consumer, at time step $t$.
- $g_e(t) \in \mathbb{R}$ [W] represents the electrical power transmitted by the renewable generator to external grid, at time step $t$.
- $g_b(t) \in \mathbb{R}$ [W] represents the electrical power transmitted by the renewable generator to battery, at time step $t$.
- $g_c(t) \in \mathbb{R}$ [W] represents the electrical power transmitted by the renewable generator to consumer, at time step $t$.
- $b_c(t) \in \mathbb{R}$ [W] represents the electrical power transmitted by the battery to consumer, at time step $t$.

Let $\mathbf{u}(t)$ represent the vector of system control inputs:

$$\mathbf{u}(t) = [p(t) \quad g_e(t) \quad g_c(t) \quad g_b(t) \quad b_c(t)]^T$$

Note that $\mathbf{x}(t)$ represent the amount of energy and the components of the control inputs vector $\mathbf{u}(t)$ are electrical powers, which are multiplied by sampling time $\Delta t = 1$ hour in the dynamic model equations.

We also assume that five states are available via sensors. The system outputs vector is made of:

$$\mathbf{y}(t) = [y_{ec}(t) \quad y_{ge}(t) \quad y_{gc}(t) \quad y_{bc}(t) \quad y_b(t)]^T$$

and contains:

- energy received by the consumer from external grid $y_{ec} \in \mathbb{R}$ [Wh],
- energy received by the external grid from the renewable generator $y_{ge} \in \mathbb{R}$ [Wh].
- energy received by the consumer from the renewable generator $y_{gc} \in \mathbb{R}$ [Wh],
- energy received by the consumer from the battery $y_{bc} \in \mathbb{R}$ [Wh],
- energy stored in the battery $y_b \in \mathbb{R}$ [Wh].

Further, the microgrid can be described by the following global dynamic model:

$$\begin{aligned} \mathbf{x}(t+1) &= \mathbf{A}\mathbf{x}(t) + \mathbf{B}\mathbf{u}(t) \\ \mathbf{y}(t) &= \mathbf{C}\mathbf{x}(t) \end{aligned} \tag{8}$$

where

$$\mathbf{A} = \begin{bmatrix} 1-\alpha & 0 & 0 & 0 & 0 & 0 \\ 0 & 1-\alpha & 0 & 0 & 0 & 0 \\ 0 & 0 & 1-\alpha & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-\alpha & 0 & 0 \\ 0 & 0 & 0 & 0 & 1-\alpha & 0 \\ 0 & 0 & 0 & 1 & 0 & 1-\tau \end{bmatrix},$$

$$\mathbf{B} = \begin{bmatrix} \alpha & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 \\ 0 & 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & 0 & \alpha \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\mathbf{C} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

## 2.2 *Profile construction*

All the microgrid components are characterized by certain profiles of reference: consumer load profile $d(t) \in \mathbb{R}$, wind speed profile $v(t) \in \mathbb{R}$, from which we can obtain the generator power profile $g(t) \in \mathbb{R}$. The numerical data is taken from (Grigg, Wong, Albrecht, Allan, Bhavaraju, Billinton, Chen, Fong, Haddad, & Kuruganty 1999).

- Consumer load profile

Figure 2 depicts the reference consumer load $d(t)$ (based on real numerical data coming from a reliability test system (Grigg, Wong, Albrecht, Allan, Bhavaraju, Billinton, Chen, Fong, Haddad, & Kuruganty 1999)).

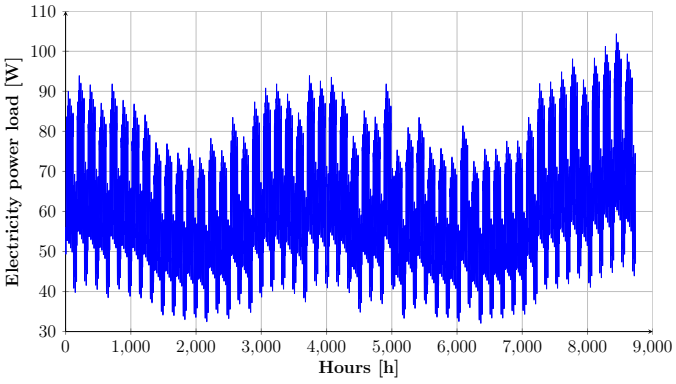



Figure 2: Consumer load profile

- Wind speed and power generator profiles

We also need to specify a profile for the wind power generator output. This depends directly on the wind profile $v(t)$, which has to be estimated from meteorological data and information. Figure 3 depicts the considered wind speed profile.

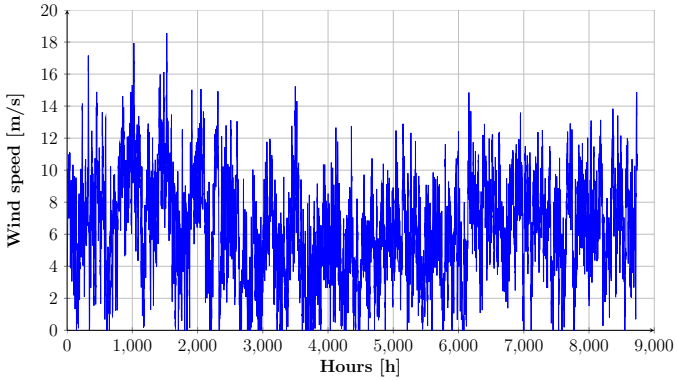



Figure 3: Wind speed profile

More precisely, the wind power generated is, then, given by the following power curve transformation(Justus, Hargraves, & Yalcin 1976):

$$g(t) = \begin{cases} 0, & if\ v < v_{ci}, \\ P_r \cdot \frac{v(t)-v_{ci}}{v_r - v_{ci}} \cdot \Delta t, & if\ v_{ci} \leq v(t) < v_r, \\ P_r \cdot \Delta t, & if\ v_r \leq v < v_{co}, \\ 0, & if\ v > v_{co}, \end{cases} \tag{9}$$

where $v(t)$ [m/s] is the working wind speed at time step $t$ of 1 hour, $v_{ci}$ [m/s], $v_r$ [m/s] and $v_{co}$ [m/s] are the cut-in, rated and cut-off wind speeds, respectively, and $P_r$ [W] is the rated power of the wind turbine.

Figure 4 depicts the power generator profile with the numerical data $P_r = 6000$ W, $v_{ci} = 3$ m/s, $v_r = 12$ m/s, $v_{co} = 20$ m/s.

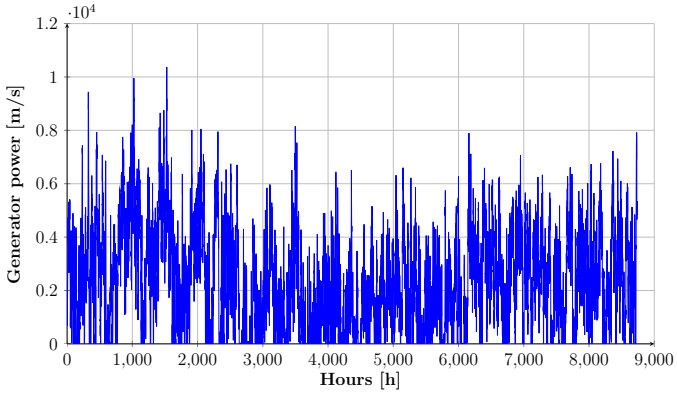



Figure 4: Power generator profile

## 2.3 *Constraints*

A number of constraints are set for the different components of the microgrid system.

- Satisfaction of consumer power demands

The consumer can take electricity from three sources: the external grid, the renewable generator and the battery. Thus, the sum of powers received by the consumer is $y_{ec}(t) + y_{gc}(t) + y_{bc}(t)$. We partition the consumer's demand into two parts: essential demand $d_{es}(t)$ and nonessential demand $d_{nes}(t)$, respectively. Therefore, for a safe energy system it is necessary to ensure that at time $t$ the electricity purchased from these three sources satisfies the following condition:

$$d_{es}(t) \leq y_{ec}(t) + y_{gc}(t) + y_{bc}(t) \leq d_{es}(t) + d_{nes}(t) \tag{10}$$

- Battery storage

The energy stored in the battery at time $t$ needs to remain between some bounds, as well as the rate of the battery charge:

$$B_{min} \leq b(t) \leq B_{max}, \tag{11}$$

$$D_{min} \leq \Delta b(t) \leq D_{max}, \tag{12}$$

where $B_{min} \in \mathbb{R}$, $B_{max} \in \mathbb{R}$, $D_{min} \in \mathbb{R}$, $D_{max} \in \mathbb{R}$.

- Generator

We consider the limitations on the generator power taken by the battery, the consumer and the external grid:

$$0 \leq g_b(t) + g_c(t) + g_e(t) \leq g(t), \tag{13}$$

with $g_b(t) \geq 0$, $g_c(t) \geq 0$, $g_e(t) \geq 0$.

- Link capacities

We consider the physical limits on the energy transfer:

$$\mathbf{u}_{min} \leq \mathbf{u}(t) \leq \mathbf{u}_{max}, \tag{14}$$

where $u(t) \in \mathbb{R}$.

## 2.4 *Fault description*

In the present work, we consider three types of faults, corresponding to variations of matrix A, B and C in the system dynamic model (8), respectively:

- Internal faults: faults affecting the internal dynamics of the system (i.e. the states), corresponding to variations of matrix **A**;

- Actuator faults: faults occurring in the control inputs, corresponding to variations of matrix **B**;

- Sensor faults: faults affecting the measurement of states (i.e. the outputs), corresponding to variations of matrix **C**.

## 3 SAFETY ANALYSIS

### 3.1 *Safety specification*

For the purpose of the present safety analysis, we define that the system is safe if it ensures the satisfaction of the consumers essential demands. If one of the previously described fault occurs, the nonessential part of the consumers demands can be safely cut, while the essential part must be always covered, as specified in equation (10).

### 3.2 *Controllability and observability properties*

Controllability and observability are two central concepts in Control Theory (Chen 1995). In this work, we investigate their role and effects on system safety, as just defined in the previous subsection.

A dynamical system is controllable if, with a suitable choice of inputs, it can be driven from any initial state to any desired final state within finite time, which is possible if and only if the controllability matrix has full rank (Kalman 1963):

$$rank[B \quad AB \quad ... \quad A^{n-1}B] = n$$

where $n$ is the number of states of the system.

This represents the mathematical condition for controllability and it is called Kalman's controllability rank condition. Within the system safety perspective, controllability is the ability to guide a system's behavior towards a desired state through the appropriate manipulation of a few input variables (Liu, Slotine, & Barabási 2011). Let us consider a system transitioning from a safe to an unsafe mode of operation due to a discrete change or event (e.g. failure of a component). If the system is controllable, there exists at least one decision/action that could steer the system back to the safe mode of operation. If, however, the system is not controllable, there are no guarantees that the system, having exhibited an accident initiating event, can be brought back to the "safety zone" in its state-space or that the accident sequence can be interrupted through appropriate inputs.

The question is how to choose a control input to achieve a desired system behavior or a state transition from an initial state $x_0$ to a final state $x_f$, for ensuring safety. To achieve this requires full knowledge of the internal state of the system **x** at every instance to the controller/operator, who then compares with an output feedback. It is, thus, contingent on the system being state-observable. Observability is a measure of how well the internal states of the system can be inferred from knowledge of its external outputs. A system is said to be observable if, for any possible sequence of state and control vectors, the current state can be determined in finite time using only the outputs. The mathematical condition is that the observability matrix has full rank (Kalman 1963):

$$rank \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{bmatrix} = n$$

### 3.3 *Optimization-based control for system safety*

We solve an optimization problem in order to find the appropriate control inputs that minimize the difference between the consumer power demanded and received, subject to a set of constraints and following the predicted profiles.

The objective function is:

$$\min_{[\mathbf{u}(t)]_{t=k:k+N_p}} \sum_{t=k}^{k+N_p} C(t)$$

where, $C(t) = d_{es}(t) + d_{nes}(t) - d_a(t)$,$d_a(t) = y_{ec}(t) + y_{gc}(t) + y_{bc}(t)$, with the set of constraints defined in equations: (7) - (14).

## 4 SIMULATION RESULTS

In this section, we proceed with the safety analysis by considering the components faults described in Section 2 (faults affecting the states, control inputs and outputs) and their combinations, and generating the corresponding faulty scenarios of system level. For these scenarios, we check the controllability/observability properties of the microgrid and verify the satisfaction of the safety criteria.

The numerical values of the parameters used for the simulations are presented in Table 1 in Appendix A. All the simulation results are presented in Table 2 and Table 3 in Appendix B.

### 4.1 *Fault-free functioning*

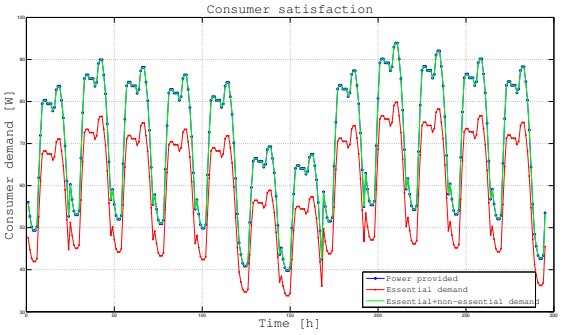
We first consider the case of nominal functioning, i.e. fault-free. We verify the observability and controllability of the system:

$$rank \begin{bmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{bmatrix} = 6$$

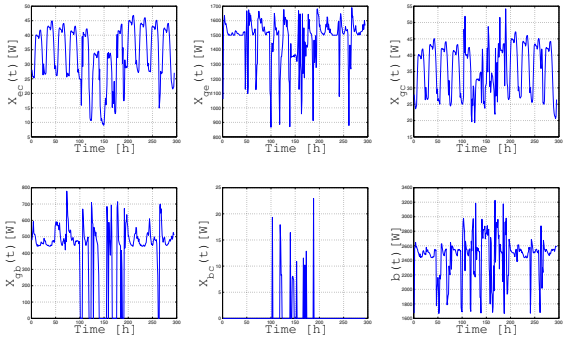
$$rank[B \quad AB \quad ... \quad A^{n-1}B] = 6$$

Thus, the system is, indeed, observable and controllable.

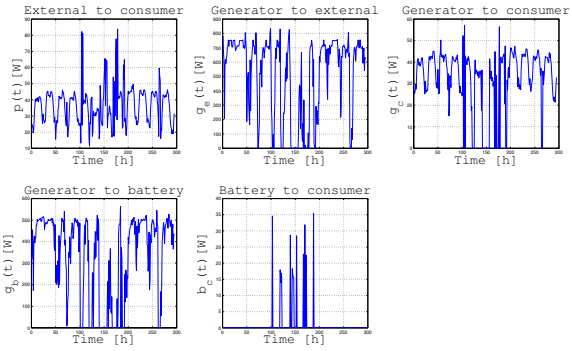
Figure 5 shows the satisfaction of consumer demand, the state evolution and the values of the control inputs, in the nominal case.




(a) Consumer's satisfaction




(b) State evolution




(c) Control inputs

Figure 5: Fault-free functioning

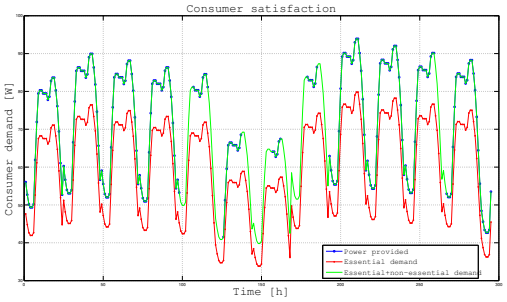
## 4.2 *Internal fault*

The fault considered in this scenario is the total loss of link capacity. The faulty dynamics of the microgrid becomes:

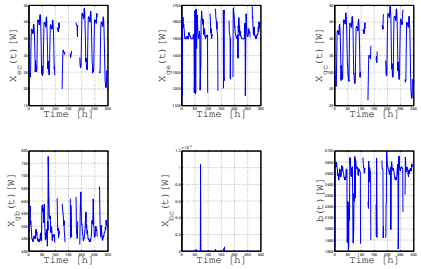
$$\begin{aligned} \mathbf{x}(t+1) &= \mathbf{A}_f\mathbf{x}(t) + \mathbf{B}\mathbf{u}(t) \\ \mathbf{y}(t) &= \mathbf{C}\mathbf{x}(t) \end{aligned} \tag{15}$$

where $\mathbf{A}_f$ is equal to matrix $\mathbf{A}$ described in (8), except that the column corresponding to the faulty link is $[0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]^T$.

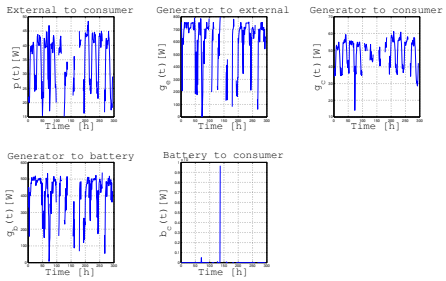
As an example, let us consider the case of a fault in the link from generator to consumer (i.e. $x_{gc}$). Both observability and controllability still hold.




(a) Consumer's satisfaction




(b) State evolution




(c) Control inputs

Figure 6: Internal fault $x_{gc}(t)$

Figure 6 shows the (non-)satisfaction of consumer demand, the state evolution and the values of the control inputs in this faulty scenario. As we can see in Figure 6(a), the essential demand is not always satisfied throughout the time horizon considered, which means that safety is not always ensured. And if we compare the simulation results with the wind power profile as in Figure 4, we note that periods of demand non-satisfaction correspond to periods where wind power is very low (near zero). Compared to the curves in Figures 5(b) and 5(c), we also note that the values of $x_{bc}$ and $b_c$ decrease a lot, while others do not change much.

For the internal faults $x_{ge}$, $x_{gc}$ and $x_{gb}$ for which the scenarios are such that safety is not ensured throughout the time horizon considered (the essential demand is not always satisfied), the values of $x_{bc}$ (and $b_c$) are very low compared to nominal case, while the values of $x_{ec}$ do not change much. By comparing the sim-

ulation results with the wind power profile, we can always find that periods of demand non-satisfaction correspond to periods where wind power is close to zero. Then, the power received from the external grid is not enough to compensate the loss of power transmitted from the battery: thus, the essential demand is not satisfied during these periods.

From the analysis of this faulty scenario, we would conclude that observability and controllability are not sufficient conditions for safety.

### 4.3 *Actuator fault*

The faulty dynamics of the microgrid in this scenario in which an actuator is faulty becomes:

$$\begin{aligned} \mathbf{x}(t+1) &= \mathbf{A}\mathbf{x}(t) + \mathbf{B}_f\mathbf{u}(t) \\ \mathbf{y}(t) &= \mathbf{C}\mathbf{x}(t) \end{aligned} \tag{16}$$

where $\mathbf{B}_f$ equals to matrix $\mathbf{B}$ described in (8), except that the column corresponding to the faulty actuator is $[0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]^T$.

For example, we consider $g_c(t)$ (electrical power transmitted by the renewable generator to consumer) as the faulty control input. Observability still holds, while controllability does not due to modification of matrix $\mathbf{B}$:

$$rank[B_f \quad AB_f \quad \dots \quad A^{n-1}B_f] = 5$$

Figure 7 shows the satisfaction of the consumer demand, the state evolution and the values of the control inputs in this faulty scenario.

From the analysis of this faulty scenario, we would conclude that controllability is not a necessary condition for safety.

### 4.4 *Sensor Fault*

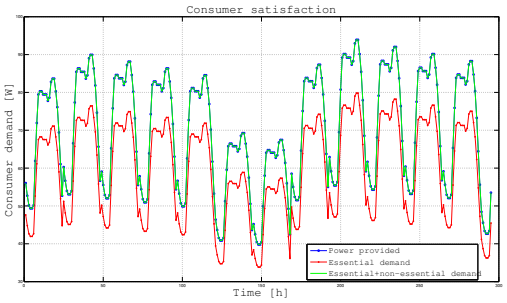
We now consider the fault in a sensor in the microgrid system, such that its measurement drops to zero and stays there all the time. The faulty dynamics of the microgrid becomes:

$$\begin{aligned} \mathbf{x}(t+1) &= \mathbf{A}\mathbf{x}(t) + \mathbf{B}\mathbf{u}(t) \\ \mathbf{y}(t) &= \mathbf{C}_f\mathbf{x}(t) \end{aligned} \tag{17}$$

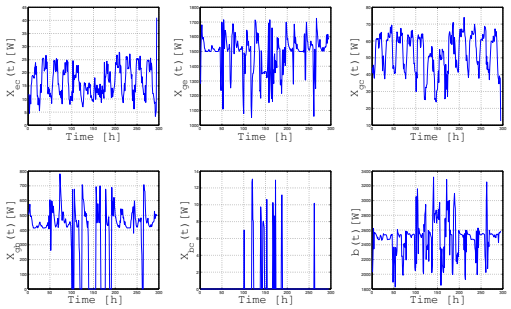
where $\mathbf{C}_f$ equals to matrix $\mathbf{C}$ described in (8) , except that the column corresponding to the faulty sensor is $[0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]$.

For example, we consider the measurement of the link from generator to consumer (i.e. $y_{gc}$) as the faulty sensor output, i.e. $y_{gc}(t) = 0$. Now, the microgrid system is still controllable but no longer observable:

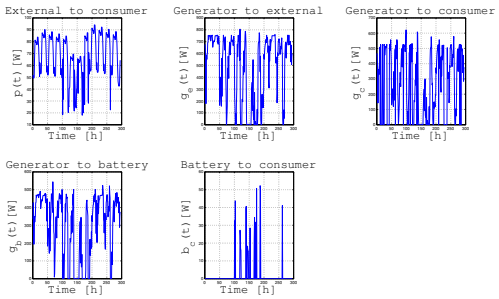
$$rank \begin{bmatrix} C_f \\ C_fA \\ C_fA^2 \\ \vdots \\ C_fA^{n-1} \end{bmatrix} = 5$$




(a) Consumer's satisfaction




(b) State evolution




(c) Control inputs

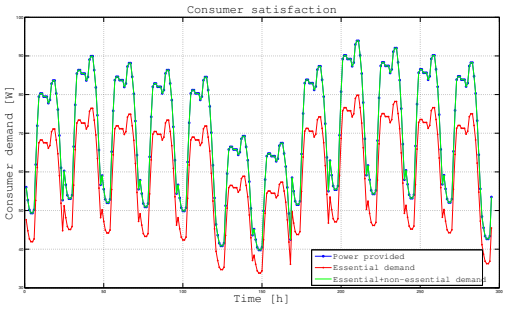
Figure 7: Actuator fault $g_c(t)$

Figure 8 shows the satisfaction of consumer demand, the state evolution and the values of the control inputs in this faulty scenario. The power received by the consumer is $y_{ec} + y_{gc} + y_{bc}$, which should equal to the value of $x_{ec} + x_{gc} + x_{bc}$, but in this case it equals to only $x_{ec} + x_{bc}$. We note that $x_{gc}$ is actually very high. This means that the consumer receives much more than what is measured: since the observability is lost, we cannot have the real information on the internal conditions of the system.

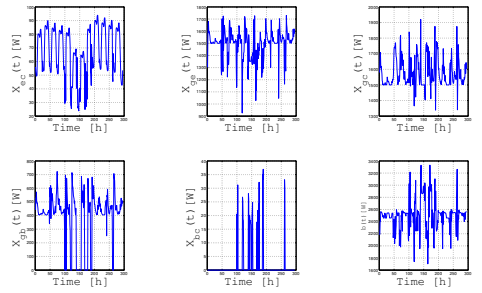
From the analysis of this faulty scenario, we would conclude that observability is not a necessary condition for safety.

### 4.5 *Multi-fault scenarios*

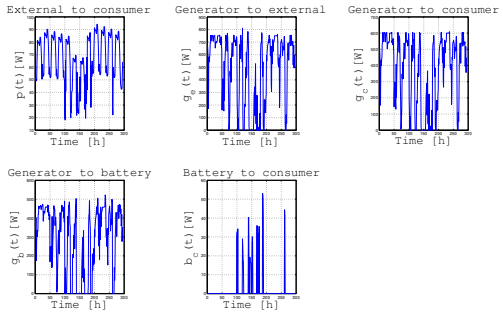
Now we consider scenarios where both observability and controllability are lost. According to previous




(a) Consumer's satisfaction




(b) State evolution




(c) Control inputs

Figure 8: Sensor fault $y_{gc}(t)$

simulation results, a single fault does not influence both of them; thus, we consider the combination of faults.

By analyzing the matrix A, B and C, we can see that:

- Single internal faults have no influence on observability, except for the fault of the links from the renewable generator to the battery ($x_{gb}$).

- Single internal faults have no influence on controllability.

- Internal fault of the link from the renewable generator to the battery ($x_{gb}$) affects observability.

- If any of the links from the renewable generator to the battery ($x_{gb}$) or from the battery to consumer ($x_{bc}$) or the battery ($b$) works normally, controllability holds.

- Any single actuator fault renders the system uncontrollable, but has no influence on observability.

- Any single sensor fault renders the system unobservable, but has no influence on controllability.

Thus, we consider the following categories of multi-fault scenarios:

- One actuator fault and one sensor fault - 25 combinations

- The internal fault of the link from the renewable generator to the battery ($x_{gb}$) and one actuator fault - 5 combinations

- The internal faults of the link from the renewable generator to the battery ($x_{gb}$), the link from the battery to consumer ($x_{bc}$) and the battery ($b$) - 1 combination

The simulation results of the 31 scenarios considered are presented in Table 3 in Appendix, with reference to the consequences in terms of safety specification satisfaction. Among the 31 scenarios, we have 5 where safety is not satisfied and when a fault occurs in the battery, the system does not work at all. For the rest of the scenarios, the consumer demand is satisfied. Analogously to the single fault cases, variations are observed in the values of the states and control inputs, which are the consequences of the combinations of the faults occurred in the multi-fault scenario.

A single actuator fault or sensor fault does not render the system unsafe (according to our previous simulation results), and most of their combinations do not either. But we also notice that the combination of actuator fault $b_c$ and sensor fault $y_{ec}$ renders the system unsafe, because the fault of $b_c$ results in no supply from the battery to the consumer, and the fault of $y_{ec}$ means that the consumer receives nothing from the external grid, so that, the only source would be the renewable generator which is not capable to provide all the power demanded. Besides, the internal fault of the link from the renewable generator to the battery ($x_{gb}$) itself makes the system unsafe; however, its combination with the actuator fault $g_b$ actually keeps the system safe, because the fault of $x_{gb}$ leads to a low level of $b$ (the battery) and $x_{bc}$ (energy from battery to consumer), while the fault of $g_b$ leads to the increase of power in the link from the generator to the consumer $x_{gc}$, which compensates the loss from the battery which was curing the system failure.

From the analysis of these scenarios, we can conclude that the loss of both controllability and observability does not necessarily imply system safety, as defined in our case study.

## 5 CONCLUSIONS

In this work, we have adopted the control perspective of safety. We have developed a simulation-based framework of model predictive control for the investigation of the controllability and observability properties of a microgrid system and their effects on system safety. We have implemented an optimization-based control for safety. Results show that, for this specific case of the microgrid, different types of faults have different effects on the system controllability/observability properties, and on system safety. We have proved the feasibility of quantitatively investigating safety in relation to the control properties of a system. However, based on the results of the case study, we cannot give conclusive indications on how controllability and observability (here defined in classical control theory terms) affect safety, as in some of the scenarios investigated the fact of having controllability and observability does not guarantee safety (satisfaction of consumer essential demand) and in some others safety is achieved even without system controllability or observability.

## REFERENCES


Bakolas, E. & J. H. Saleh (2011). Augmenting defense-in-depth with the concepts of observability and diagnosability from control theory and discrete event systems. *Reliability Engineering & System Safety 96*(1), 184–193.

Chen, C.-T. (1995). *Linear system theory and design*. Oxford University Press, Inc.

Edlund, K., J. Bendtsen, & J. Jørgensen (2011). Hierarchical model-based predictive control of a power plant portfolio. *Control Engineering Practice 19*(10), 1126–1136.

Goodwin, G., M. Seron, & J. De Dona (2005). *Constrained control and estimation: an optimisation approach*. Springer Verlag.

Grigg, C., P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, & S. Kuruganty (1999). The ieee reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee. *Power Systems, IEEE Transactions on 14*(3), 1010–1020.

Halvgaard, R., N. K. Poulsen, H. Madsen, & J. Jorgensen (2012). Economic model predictive control for building climate control in a smart grid. In *IEEE PES Innovative Smart Grid Technologies (ISGT)*, pp. 1–6. IEEE.

Hovgaard, T., L. Larsen, & J. Jorgensen (2011). Robust economic mpc for a power management scenario with uncertainties. In *Proceedings of the 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, pp. 1515–1520. IEEE.

Jimeno, J., J. Anduaga, J. Oyarzabal, & A. de Muro (2011). Architecture of a microgrid energy management system. *European Transactions on Electrical Power 21*(2), 1142–1158.

Justus, C., W. Hargraves, & A. Yalcin (1976). Nationwide assessment of potential output from wind-powered generators. *Journal of Applied Meteorology 15*(7), 673–678.

Kalman, R. E. (1963). Mathematical description of linear dynamical systems. *Journal of the Society for Industrial & Applied Mathematics, Series A: Control 1*(2), 152–192.

Krause, T., E. Beck, R. Cherkaoui, A. Germond, G. Andersson, & D. Ernst (2006). A comparison of nash equilibria analysis and agent-based modelling for power markets. *International Journal of Electrical Power & Energy Systems 28*(9), 599–607.

Kuznetsova, E., K. Culver, & E. Zio (2011). Complexity and vulnerability of smartgrid systems. In *Proceedings of the European Safety and Reliability Conference*, pp. 2474–2482.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety science 42*(4), 237–270.

Liu, Y.-Y., J.-J. Slotine, & A.-L. Barabási (2011). Controllability of complex networks. *Nature 473*(7346), 167–173.

Lussier, B., R. Chatila, F. Ingrand, M.-O. Killijian, & D. Powell (2004). On fault tolerance and robustness in autonomous systems. In *Proceedings of the 3rd IARP-IEEE/RAS-EURON Joint Workshop on Technical Challenges for Dependable Robots in Human Environments*.

Negenborn, R., B. De Schutter, & J. Hellendoorn (2008). Multi-agent model predictive control for transportation networks: Serial versus parallel schemes. *Engineering Applications of Artificial Intelligence 21*(3), 353–366.

Prodan, I. & E. Zio (2014a). A model predictive control framework for reliable microgrid energy management. *International Journal of Electrical Power & Energy Systems 61*, 399–409.

Prodan, I. & E. Zio (2014b). On the microgrid energy management under a predictive control framework. In *Control Applications (CCA), 2014 IEEE Conference on*, pp. 861–866. IEEE.

Rawlings, J. & D. Mayne (2011). Postface to model predictive control: Theory and design.

Richalet, J. & D. O'Donovan (2009). *Predictive Functional Control: Principles and Industrial Applications*. Springer.

Weidlich, A. & D. Veit (2008). A critical survey of agent-based wholesale electricity market models. *Energy Economics 30*(4), 1728–1759.

## A NUMERICAL DATA

Table 1: Numerical data for the microgrid components

| | |
|---|---|
| **Battery parameters** | |
| $\tau$ | $13 \cdot 10^{-4}$ |
| $M$ | $9 \cdot 10^3$ |
| $B_{min}$ $[Wh]$ | $1.2 \cdot 10^3$ |
| $B_{max}$ $[Wh]$ | $6 \cdot 10^3$ |
| $D_{min}$ $[W]$ | $-1.5 \cdot 10^3$ |
| $D_{max}$ $[W]$ | $1.5 \cdot 10^3$ |
| **Power generator parameters** | |
| $P_r$ $[W]$ | $6 \cdot 10^3$ |
| $V_{cr}$ $[m/s]$ | 3 |
| $V_r$ $[m/s]$ | 12 |
| $V_{cv}$ $[m/s]$ | 20 |
| **Control input constraints** | |
| $U_{min}$ | $[0 \quad 0 \quad 0 \quad 0 \quad 0]^T$ |
| $U_{max}$ | $[1.2 \quad 1.5 \quad 1.2 \quad 1.5 \quad 1.5]^T \cdot 10^3$ |
| **Prediction horizon** | |
| $N_p$ | 5 |

## B SIMULATION RESULTS

Table 2: Simulation results for single fault scenarios

| **No.** | **Faulty Component** | **Observability** | **Controllability** | **Consequences** (on safety specifications) |
|---|---|---|---|---|
| 1 | Link: external grid to consumer $x_{ec}$ | Y | Y | - |
| 2 | Link: generator to external grid $x_{ge}$ | Y | Y | Not satisfied |
| 3 | Link: generator to consumer $x_{gc}$ | Y | Y | Not satisfied |
| 4 | Link: generator to the battery $x_{gb}$ | Y | Y | Not satisfied |
| 5 | Link: battery to consumer $x_{bc}$ | Y | Y | - |
| 6 | Battery $b$ | Y | Y | No supply |
| 7 | Actuator: external grid to consumer $p$ | Y | N | - |
| 8 | Actuator: generator to external grid $g_e$ | Y | N | - |
| 9 | Actuator: generator to battery $g_b$ | Y | N | - |
| 10 | Actuator: generator to consumer $g_c$ | Y | N | - |
| 11 | Actuator: battery to consumer $b_c$ | Y | N | - |
| 12 | Sensor: external grid to consumer $y_{ec}$ | N | Y | - |
| 13 | Sensor: generator to external grid $y_{ge}$ | N | Y | - |
| 14 | Sensor: generator to consumer $y_{gc}$ | N | Y | - |
| 15 | Sensor: battery to consumer $y_{bc}$ | N | Y | - |
| 16 | Sensor: battery $y_b$ | N | Y | - |

Table 3: Simulation results for multi-fault scenarios

| **No.** | **Faulty Components** | **Observability** | **Controllability** | **Consequences** (on safety specifications) |
|---|---|---|---|---|
| 1 | Actuator: external grid to consumer $p$<br>Sensor: external grid to consumer $y_{ec}$ | N | N | - |
| 2 | Actuator: external grid to consumer $p$<br>Sensor: generator to external grid $y_{ge}$ | N | N | - |
| 3 | Actuator: external grid to consumer $p$<br>Sensor: generator to consumer $y_{gc}$ | N | N | - |

| | | | | |
|---|---|---|---|---|
| 4 | Actuator: external grid to consumer $p$<br>Sensor: battery to consumer $y_{bc}$ | N | N | Not satisfied |
| 5 | Actuator: external grid to consumer $p$<br>Sensor: battery $y_b$ | N | N | - |
| 6 | Actuator: generator to external grid $g_e$<br>Sensor: external grid to consumer $y_{ec}$ | N | N | - |
| 7 | Actuator: generator to external grid $g_e$<br>Sensor: generator to external grid $y_{ge}$ | N | N | - |
| 8 | Actuator: generator to external grid $g_e$<br>Sensor: generator to consumer $y_{gc}$ | N | N | - |
| 9 | Actuator: generator to external grid $g_e$<br>Sensor: battery to consumer $y_{bc}$ | N | N | - |
| 10 | Actuator: generator to external grid $g_e$<br>Sensor: battery $y_b$ | N | N | - |
| 11 | Actuator: generator to battery $g_b$<br>Sensor: external grid to consumer $y_{ec}$ | N | N | - |
| 12 | Actuator: generator to battery $g_b$<br>Sensor: generator to external grid $y_{ge}$ | N | N | - |
| 13 | Actuator: generator to battery $g_b$<br>Sensor: generator to consumer $y_{gc}$ | N | N | - |
| 14 | Actuator: generator to battery $g_b$<br>Sensor: battery to consumer $y_{bc}$ | N | N | - |
| 15 | Actuator: generator to battery $g_b$<br>Sensor: battery $y_b$ | N | N | - |
| 16 | Actuator: generator to consumer $g_c$<br>Sensor: external grid to consumer $y_{ec}$ | N | N | - |
| 17 | Actuator: generator to consumer $g_c$<br>Sensor: generator to external grid $y_{ge}$ | N | N | - |
| 18 | Actuator: generator to consumer $g_c$<br>Sensor: generator to consumer $y_{gc}$ | N | N | - |
| 19 | Actuator: generator to consumer $g_c$<br>Sensor: battery to consumer $y_{bc}$ | N | N | - |
| 20 | Actuator: generator to consumer $g_c$<br>Sensor: battery $y_b$ | N | N | - |
| 21 | Actuator: battery to consumer $b_c$<br>Sensor: external grid to consumer $y_{ec}$ | N | N | - |
| 22 | Actuator: battery to consumer $b_c$<br>Sensor: generator to external grid $y_{ge}$ | N | N | - |
| 23 | Actuator: battery to consumer $b_c$<br>Sensor: generator to consumer $y_{gc}$ | N | N | - |
| 24 | Actuator: battery to consumer $b_c$<br>Sensor: battery to consumer $y_{bc}$ | N | N | - |
| 25 | Actuator: battery to consumer $b_c$<br>Sensor: battery $y_b$ | N | N | - |
| 26 | Link: generator to the battery $x_{gb}$<br>Sensor: external grid to consumer $y_{ec}$ | N | N | Not satisfied |
| 27 | Link: generator to the battery $x_{gb}$<br>Sensor: generator to external grid $y_{ge}$ | N | N | Not satisfied |
| 28 | Link: generator to the battery $x_{gb}$<br>Sensor: generator to consumer $y_{gc}$ | N | N | Not satisfied |
| 29 | Link: generator to the battery $x_{gb}$<br>Sensor: battery to consumer $y_{bc}$ | N | N | - |
| 30 | Link: generator to the battery $x_{gb}$<br>Sensor: battery $y_b$ | N | N | - |
| 31 | Link: generator to the battery $x_{gb}$<br>Link: battery to consumer $x_{bc}$<br>Battery $b$ | N | N | No supply |