

The Faculty of Science, Technology and Communication

DISSERTATION

Defence held on ??/??/2019 in Luxembourg

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG ET
DE L'UNIVERSITÉ DE RENNES 1 EN INFORMATIQUE

by

Ludovic MOULINE

TOWARDS A MODELING FRAMEWORK WITH TEMPORAL AND UNCERTAIN DATA FOR ADAPTIVE SYSTEMS

Dissertation defence committee (*Waiting for approval*)

Dr. Jacques KLEIN, chairman

Senior Research Scientist, University of Luxembourg, Luxembourg, Luxembourg

Prof. Dr. Antonio VALLECILLO, vice-chairman & reviewer

Professor, University of Málaga, Málaga, Spain

Prof. Dr. Yves LE TRAON, co-supervisor

Professor, University of Luxembourg, Luxembourg, Luxembourg

Prof. Dr. Olivier BARAIS, co-supervisor

Professor, University of Rennes 1, Rennes, France

Dr. Johann BOURCIER, advisor

Lecturer, University of Rennes 1, Rennes, France

Dr. Franck FLEUREY, member & reviewer

Research Associate, SINTEF, Oslo, Norway

A-Prof. Dr. Ada DIACONESCU, expert

Research Associate, Telecom ParisTech, Paris, France

Dr. François FOUQUET, expert & advisor

CTO, DataThings, Luxembourg, Luxembourg

Abstract

Vision: As state-of-the-art techniques fail to model efficiently the evolution and the uncertainty existing in dynamically adaptive systems, the adaptation process makes suboptimal decisions. To tackle this challenge, modern modeling frameworks should efficiently encapsulate time and uncertainty as first-class concepts.

Context Smart grid approach introduces information and communication technologies into traditional power grid to cope with new challenges of electricity distribution. Among them, one challenge is the resiliency of the grid: how to automatically recover from any incident such as overload? These systems therefore need a deep understanding of the ongoing situation which enables reasoning tasks for healing operations. **Abstraction** is a key technique that provided an illuminating description of systems, their behaviors, and/or their environments alleviating their complexity. **Adaptation** is a cornerstone feature that enables reconfiguration at runtime for optimizing software to the current and/or future situation.

Abstraction technique is pushed to its paramountcy by the model-driven engineering (MDE) methodology. However, information concerning the grid, such as loads, is not always known with absolute confidence. Through the thesis, this lack of confidence about data is referred to as **data uncertainty**. They are approximated from the measured consumption and the grid topology. This topology is inferred from fuse states, which are set by technicians after their services on the grid. As humans are not error-free, the topology is therefore not known with absolute confidence. This data uncertainty is propagated to the load through the computation made. If it is

1 neither present in the model nor not considered by the adaptation process, then the
2 adaptation process may make suboptimal reconfiguration decision.

3 The literature refers to systems which provide adaptation capabilities as dynam-
4 ically adaptive systems (DAS). One challenge in the grid is the phase difference
5 between the monitoring frequency and the time for actions to have measurable effects.
6 Action with no immediate measurable effects are named **delayed action**. On the
7 one hand, an incident should be detected in the next minutes. On the other hand, a
8 reconfiguration action can take up to several hours. For example, when a tree falls
9 on a cable and cuts it during a storm, the grid manager should be noticed in real
10 time. The reconfiguration of the grid, to reconnect as many people as possible before
11 replacing the cable, is done by technicians who need to use their cars to go on the
12 reconfiguration places. In a fully autonomous adaptive system, the reasoning process
13 should consider the ongoing actions to avoid repeating decisions.

14 *Problematic* **Data uncertainty and delayed actions are not specific to smart**
15 **grids.**

16 First, data are, almost by definition, uncertain and developers always work with
17 estimates. Hardware sensors have by construction a precision that can vary according
18 to the current environment in which they are deployed. A simple example is the
19 temperature sensor that provides a temperature with precision to the nearest degree.
20 Software sensors approximate also values from these physical sensors, which increases
21 the uncertainty. For example, CPU usage is computed counting the cycle used by a
22 program. As stated by Intel, this counter is not error-prone¹.

23 Second, it always exists a delay between the moment where a suboptimal state is
24 detected by the adaptation process and the moment where the effects of decisions
25 taken are measured. This delayed is due to the time needed by a computer to process
26 data and, eventually, to send orders or data through networks. For example, migrating
27 a virtual machine from a server to another one can take several minutes.

28 **Through this thesis, I argue that this data uncertainty and this delay**

¹<https://software.intel.com/en-us/itc-user-and-reference-guide-cpu-cycle-counter>

cannot be ignored for all dynamic adaptive systems. To know if the data uncertainty should be considered, stakeholders should wonder **if this data uncertainty affects the result of their reasoning process, like adaptation**. Regarding delayed actions, they should verify **if the frequency of the monitoring stage is lower than the time of action effects to be measurable**. These characteristics are common to smart grids, cloud infrastructure or cyber-physical systems in general.

Challenge These problematics come with different challenges concerning the representation of the knowledge for DAS. The global challenge address by this thesis is: **how to represent the uncertain knowledge allowing to efficiently query it and to represent ongoing actions in order to improve adaptation processes?**

Vision This thesis defends the need for a unified modeling framework which includes, despite all traditional elements, temporal and uncertainty as first-class concepts. Therefore, a developer will be able to abstract information related to the adaptation process, the environment as well as the system itself.

Concerning the adaptation process, the framework should enable abstraction of the actions, their context, their impact, and the specification of this process (requirements and constraints). It should also enable the abstraction of the system environment and its behavior. Finally, the framework should represent the structure, behavior and specification of the system itself as well as the actuators and sensors. All these representations should integrate the data uncertainty existing.

Contributions Towards this vision, this document presents two approaches: a temporal context model and a language for uncertain data.

The temporal context model allows abstracting past, ongoing and future actions with their impacts and context. First, a developer can use this model to know what the ongoing actions, with their expect future impacts on the system, are. Second, she/he can navigate through past decisions to understand why they have been made when they have led to a sub-optimal state.

The language, named Ain'tea, integrates data uncertainty as a first-class citizen. It allows developers to attach data with a probability distribution which represents

1 their uncertainty. Plus, it mapped all arithmetic and boolean operators to uncertainty
2 propagation operations. And so, developers will automatically propagate the uncer-
3 tainty of data without additional effort, compared to an algorithm which manipulates
4 certain data.

5 *Validation* Each contribution has been evaluated separately. The context model has
6 been evaluated through the performance axis. The dissertation shows that it can
7 be used to represent the Luxembourg smart grid. The model also provides an API
8 which enables the execution of query for diagnosis purpose. In order to show the
9 feasibility of the solution, it has also been applied to the use case provided by the
10 industrial partner.

11 The language has been evaluated through two axes: its ability to detect errors at
12 development time and its expressiveness. Ain'tea can detect errors in the combination
13 of uncertain data earlier than state-of-the-art approaches. The language is also as
14 expressive as current approaches found in the literature. Moreover, we use this
15 language to implement the load approximation of a smart grid furnished by an
16 industrial partner, Creos S.A.².

17 **Keywords:** dynamically adaptive systems, knowledge representation, model-
18 driven engineering, uncertainty modeling, time modeling

²Creos S.A. is the power grid manager of Luxembourg. <https://www.creos-net.lu>

Table of Contents

1	Introduction	1
1.1	Context	2
1.2	Problem statement	4
1.3	Challenge	4
1.4	Scope of the thesis	5
1.5	Contribution & Validation	5
1.6	Remainder	5
2	Background	7
2.1	Model-driven engineering	8
2.2	Adaptive systems	8
3	TKM: a temporal knowledge model	9
3.1	Introduction	11
3.1.1	Motivation	12
3.1.2	Background	18
3.1.3	Use case scenario	21
3.2	Knowledge formalization	22
3.2.1	Formalization of the temporal axis	23
3.2.2	Formalism	24
3.2.3	Application on the use case	29
3.3	Modeling the knowledge	33
3.3.1	Parent element: <i>TimedElement</i> class	34

1	3.3.2	Knowledge metamodel	34
2	3.3.3	Context metamodel	35
3	3.3.4	Requirement metamodel	37
4	3.3.5	Action metamodel	38
5	3.4	Validation	39
6	3.4.1	Diagnostic: implementation of the use case	39
7	3.4.2	Reasoning over unfinished actions and their expected effects .	42
8	3.4.3	Performance evaluation	44
9	3.4.4	Discussion	47
10	3.5	Conclusion	49
11	4	State of the art	51
12	4.1	Introduction	52
13		List of publications and tools	i
14		Abbreviations	iii
15		Glossary	v

Introduction

Contents

1.1	Context	2
1.2	Problem statement	4
1.3	Challenge	4
1.4	Scope of the thesis	5
1.5	Contribution & Validation	5
1.6	Remainder	5

Model-driven engineering methodology and dynamically adaptive systems approach are combined to tackle new challenges brought by systems nowadays. After introducing these two software engineering techniques, I give one example of such systems: the Luxembourg smart grid. I will also use this example to highlight two of the problematics: uncertainty of data and delays in actions. Among the different challenges which are implied by them, I present the global one addressed by the vision defended in this thesis: modeling of temporal and uncertain data. This global challenge can be addressed by splitting up in several ones. I present two of them, which are directly tackled by two contributions presented in this thesis.

Context

Utilities introduce more and more Information and Communication Technology (ICT)* in the grid in order to face the new challenges of electricity delivery [farhangi2010path; ipakchi2009grid; DBLP:journals/comsur/FangMXY12]. These novel power grids are referred to as smart grid*.

Among the different features that they possess, the one that will interest us in this document is the **self-healing system*** one. As defined by Jeffrey O. Kephart and David M. Chess [DBLP:journals/computer/KephartC03], a system can be described as a self-healing system* system if it can automatically fix any incident at runtime. For example, a smart grid can automatically optimize the power flow in order to deal with failures of transformers¹ [DBLP:journals/comsur/FangMXY12].

This healing mechanism can be performed only if the smart grid has a deep understanding of itself and its environment. To tame their complexity, a common approach in software engineers is to use an **abstraction** mechanism. Abstractions provide an illuminating description of systems, their behaviors, and/or their environment. For example, Hartmann *et al.*, [DBLP:conf/smartgridcomm/0001FKTPTR14] provide a class diagram that describes the smart grid topology, when it uses power-line communications².

More generally, a self-healing system* is a **self-adaptive system***. Cheng *et al.*, define self-adaptive systems* as “systems that are able to adjust their behaviour in response to their perception of the environment and the system itself” [DBLP:conf/dagstuhl/ChengLGIMABBBCSDFGGGKKKLMMMPSTTWW09]. Jeffrey O. Kephart and David M. Chess [DBLP:journals/computer/KephartC03] laid the groundwork of this approach, based on a IBM white paper [computing2006architectural]. Since then, it has been used in different domain [DBLP:journals/corr/abs-1904-01518] such as cloud infrastructure [DBLP:conf/icac/JavadiG17; OpenStack:Watcher:Wiki DBLP:conf/icse/BarnaKFL17] or Cyber-Physical System (CPS)* [DBLP:conf/icac/Lalanda DBLP:conf/cbse/FouquetMFBPJ12; DBLP:conf/smartgridsec/0001FKNT14]

¹Transformers change the voltage in cables.

²Data are sent through cables that also distribute electricity.

1 **Model-Driven Engineering (MDE)*** uses the abstraction mechanism to facili-
2 tate the development of nowadays software [DBLP:journals/computer/Schmidt06
3 DBLP:conf/itm/Kent02; DBLP:series/synthesis/2017Brambilla]. This method-
4 ology can be applied on the different stages of software development. In this thesis, we
5 focus on one of its paradigm: **models@run.time*** [DBLP:journals/computer/BlairBF09
6 DBLP:journals/computer/MorinBJFS09]. The state of the system and/or its
7 environment as well as its behavior are reflected in a model, used for analysis. Develop-
8 ers can use this paradigm to implement adaptive systems* [DBLP:journals/computer/MorinBJFS09
9 DBLP:conf/smartgridsec/0001FKNT14].

10 Whereas smart grids introduce more and more automation capacity, human
11 interventions are still required. First, information gathered by smart grids is therefore
12 not always known with absolute confidence. Second, smart grids reconfigurations are
13 not immediate and their effects are not instantaneously measured. Third, smart grids
14 behavior is emergent [zio2011uncertainties], *i.e.*, it cannot be perfectly known at
15 design time.

16 Most fuses are manually open and close by technicians rather than automatically
17 modified. Then, technicians manually report the modifications done on the grid. Due
18 to human mistakes, this results in mistakes. The grid topology is thus uncertain.
19 This uncertainty is propagated to the load approximation, used to detect overloads
20 in the grid. Wrong reconfigurations might be triggered, which could be even worse
21 than if no change would have been applied.

22 Reconfiguring a smart grid implied to change the power flow. This is done by
23 connecting or disconnecting specific cables. That is, opening or closing fuses. As said
24 before, a technician need to physically drive to the fuse location to modify its state. In
25 addition, in the case of the Luxembourg smart grid, meters send energy measurement
26 every 15 mins, desynchronously. Between the moment where a reconfiguration of
27 the smart grid is decided and the moment of the effect are measured, a delay of at
28 least 15 mins occurs. On the other hand, an incident should be detected in the next
29 minutes. If the adaptation process does not consider this difference of paces, it can
30 cause repeated decisions.

1 Smart grid behavior is affected by several factors that cannot be controlled by
2 the grid manager. One example is the weather condition. Smart grids rely on an
3 energy production that is distributed over several actors. For instance, users, who
4 were mainly consumers before, now produce energy by adding solar panels on the
5 roof of their houses. The production of such energy depends on the weather and
6 even on the season³. Another example is the increasing adoption of electrical vehicle,
7 which de facto drastically increase the consumption of electricity during the night.
8 Ignoring this characteristic of adaptive system* may result suboptimal situations that
9 can be understood with difficulties.

10 Problem statement

11 **Data are uncertain, actions have delayed effects, and the behavior of**
12 **adaptive systems* is emergent.**

13 Data are, almost by definition, uncertain and developers always work with es-
14 timates. This is due to how data are collected. We can identify three different
15 sources. They can **Uncertainty impacts the understanding of the global**
16 **situation**

17 **Actions.... if the frequency of the monitoring stage is lower than the**
18 **time of action effects to be measurable**

19 **Behavior ... The behavior cannot be perfectly known at design time or**
20 **inferred from the set of executed actions.**

21 Challenge

22 **Global challenge:** How to represent the uncertain knowledge allowing to effi-
23 ciently query it and to represent ongoing actions in order to improve adaptation
processes?

³The angle of the sun has an impact on the amount of energy produced by solar panels. This angle varies according to the season.

¹ Scope of the thesis

²

³ **Sub-Challenge #1:** How to diagnose the self-adaption process?

⁴

⁵ **Sub-Challenge #2:** How to enable reasoning over unfinished actions and their expected effects?

⁶

⁷ **Sub-Challenge #3:** How to ease the manipulation of data uncertainty?

⁸ Contribution & Validation

⁹ Remainder

Background

Contents

2.1	Model-driven engineering	8
2.2	Adaptive systems	8

This chapter describes the necessary background to understand this thesis. We first describe the model-driven engineering methodology. Then we detailed the approach referred to as adaptive systems.

¹ **Model-driven engineering**

² **Adaptive systems**

A temporal knowledge meta-model to represent, reason and diagnose decisions, their circumstances and their impacts

Contents

3.1	Introduction	11
3.2	Knowledge formalization	22
3.3	Modeling the knowledge	33
3.4	Validation	39
3.5	Conclusion	49

Adaptation processes are executed with a high frequency to react to any incident whereas the delay for decision applications are constrained by the time to execute the delayed actions. We identified two problems that result from these different paces. First, not considered unfinished actions, together with their expected effects, over time lead upcoming analysis phases potentially make suboptimal decisions. Second, explanations of adaptation processes remain challenging due to the lack of tracing ability of current approaches. To tackle this problem, we first propose a knowledge formalism to define the concept of a decision. Second, we describe a novel temporal knowledge model to represent, store and query decisions as well as their relationship with the knowledge (context, requirements, and actions). We validate our approach

¹ *through a use case based on the smart grid at Luxembourg. We also demonstrate its*
² *scalability both in terms of execution time and consumed memory.*

Introduction

Adaptive systems have proven their suitability to handle the increasing complexity of systems and their ever-changing environment. To do so, they make adaptation decisions, in the form of actions, based on high-level policies. For instance, the OpenStack Watcher project [OpenStack:Watcher:Wiki] implements the MAPE-k loop to assist cloud administrators in their activities to tune and rebalance their cloud resources according to some optimization goals (e.g., CPU and network bandwidth). For readability purpose, we refer to adaptation decision as decision in the remaining part of this document.

Despite the reactivity of adaptation processes, impacts of their decisions can be measurable long after they have been taken. We identified two problematics caused by this difference of paces:

- How to diagnose the self-adaptation process?
- How to enable reasoning over unfinished actions and their expected effects?

To address them, we propose a temporal knowledge model which can trace decisions over time, along with their circumstances and effects. By storing them, the adaptation process could consider ongoing actions with their expected effects, also called impacts. Plus, in case of faulty decisions, developers may trace back their effects to their circumstances. Our current approach is limited to the representation of measurable effects of any decision, and therefore action.

The meta-model allow structuring and storing the state and behavior of a running adaptive system, together with a high-level API to efficiently perform diagnosis routines. Our framework relies on a temporal model-based solution that efficiently abstracts decisions and their corresponding circumstances. Specifically, based on existing approaches for modeling and monitoring adaptation processes, we identify a set of properties that characterize context, requirements, and actions in self-adaptive systems. Then, we formalize the common core concepts implied in adaptation processes, also referred to as knowledge, by means of temporal graphs and a set of relations that trace decisions impact to circumstances. Finally, thanks to exposing

We consider that decision, delayed action, context and knowledge have been defined in the global introduction

1 common interfaces in adaptive processes, existing approaches in requirements and
2 goal modeling engineering can be easily integrated into our framework.

3 The rest of this chapter is structured as follows. In the remaining part of this
4 section, we motivate our approach, we summarize core concepts manipulated in
5 adaptation processes, and we present a use case scenario based on the Luxembourg
6 Smart Grid (*cf.* Chapter). Then, we provide a formal definition of these concepts in
7 Section 3.2. Later, we describe the proposed data model in Section 3.3. In Section 3.4,
8 we demonstrate the applicability of our approach by applying it to the smart grid
9 example. We conclude this chapter in Section 3.5.

10 Motivation

11 Delayed action

12 In this section, we motivate the need to reason over delayed actions. To do so, we
13 first give four examples of these actions. Then we detail why the effects of actions
14 should be considered. Finally, we summarize and motivate the need for incorporating
15 actions and their effects on the knowledge.

16 **Delayed action examples** Until here, we have claimed that adaptation processes
17 should handle delayed actions. In order to show their existence, we give four different
18 examples: two based on our use case, one on cloud infrastructure and a last one on
19 smart homes. From our understanding, three phenomena can explain this delay: the
20 time to execute an action(s) (Example 1), the time for the system to handle the new
21 configuration (Example 3) and the inertia of the measured element (Example 2 and
22 4).

23 **Example 1: Modification of fuse states in smart grids** Even if the Lux-
24 embourg power grid is moving to an autonomous one, not all the elements can be
25 remotely controlled. One example is fuses that still need to be open or closed by a
26 human. Open and close actions in the Luxembourg smart grid both imply technicians
27 who are contacted, drive to fuse places and manually change their states. If several
28 fuses need to be changed due to one decision, only one technician will drive to them,
29 sequentially, and executes the modifications. For example, in our case, our industrial

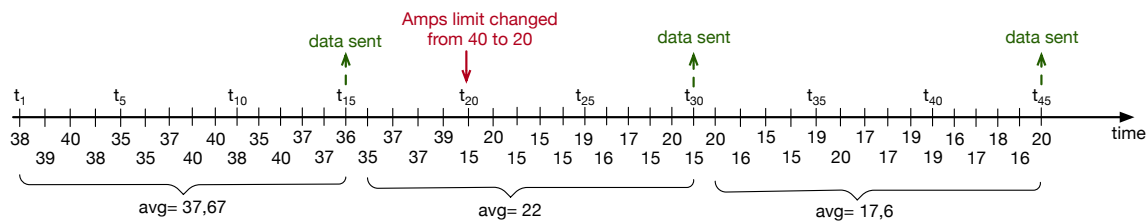


Figure 3.1: Example of consumption measurement before and after a limitation of amps has been executed at t_{20} .

on-amps-limit)

partner asks us to consider that each fuse modification takes 15 min whereas any incident should be detected in the minute. Let's imagine that an incident is detected at 4 p.m. and can be solved by modifying three fuses. The incidents will be seen as resolved by the adaptation process at 4 p.m. + 15 min * 3 = 4:45 p.m. In this case, the delay of the action is due to the execution time that is not immediate.

Example 2: Reduction of amps limit in smart grids¹ In its smart grid project, Creos S.A. envisages controlling remotely amps limits of customers. Customers will have two limits: a fixed one, set at the beginning, and a flexible one, remotely managed. The action to remotely change amps limits will be performed through specific plugs, such as one for electric vehicles. Even if the action is near instant, due to how power consumption is collected, its impacts would not be visible immediately. Indeed, data received by Creos S.A. corresponds to the total energy consumed since the installation. From this information, only the average of consumed data for the last period can be computed.

In Figure 3.1, we depict a scenario that shows the delay between the action is executed and the impacts are measured. Each time point represents one minute, with the consumption at this moment.

Let's imagine a customer who has his or her limit set to 40 amps² and consumes near this limit. We consider that data are sent every 15 min. After receiving data

¹This example is based on randomly generated data. As this action is not yet available on the Luxembourg smart grid, we miss real data. However, it reflects an hypothesis shared with our partner.

²The user cannot consume more than 40 amps at a precise time t_i .

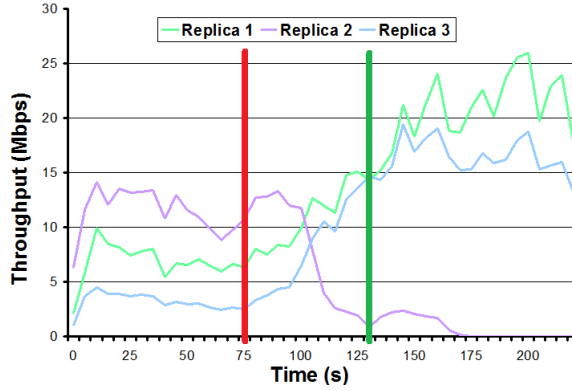


Figure 3.2: Figure extracted from [DBLP:conf/nsdi/WangBR11]. The red bar depicted the moment when Replica 2 stop receiving new connections. The green one represents the moment where all the rules in the load balancer stop considering R2. Despite these two actions, the throughput of the machine does not drop to 0 due to existing and active connections.

sample-load-balancer)

1 sent t_{15} and processing them, the adaptation process detects an overload and decides
2 to reduce the limits to 20 amps for the customer. However, considering the delay for
3 data to be collected and the one to send data³, the action is received and executed
4 at t_{20} . At t_{30} , new consumption data is sent, here equals 22 amps. Here, there are
5 two situations. First, this reduction was enough to fix the overload. Even in this
6 idealistic scenario, the adaptation process must wait at worst 15 min ($t_{30} - t_{15}$) to see
7 the resolution (without considering the communication time). Second, this reduction
8 was not enough - as the adaptation process considered that the consumption data
9 will be at worst 20 amps and here it is 22. Before seeing the incident as solved and
10 knowing that the decision fixed the incident, the adaptation process should wait for
11 new data, sent at t_{45} , *i.e.*, around 30 min ($t_{45} - t_{15}$) after the detection.

12 In this case, the delay of this action can be explained by the inertia in the average
13 of the consumption.

14 **Example 3: Switching off a machine from a load balancer** An example
15 based on cloud infrastructure of delayed actions is to remove a machine from a

³Reminder: the smart grid is not built upon a fast network such a fiber network.

load balancer, for example during a scale down operation. Scale down operations allows cloud managers to reduce allocated resources for a specific task. It is used either to reduce the cost of the infrastructure or to reallocate them to other tasks. In [DBLP:conf/nsdi/WangBR11], Wang *et al.*, present a load-balancing algorithm. In their evaluation, they present the figure depicted in Figure 3.2 that shows the evolution of the throughput after the server Replica 2 (R2) is removing from the load balancer. The red bar shows the moment where R2 stop receiving new connection and the green the moment where it is removed from the load balancer algorithm. However, despite these actions have been taken, R2 should finish the ongoing tasks that it is executing. This explains why the throughput is progressively decreasing to 0 and there is a delay of around 100s between the red bars and the moment where R2 stop being active.

This example shows a delayed action due to the time required by the system to handle the new configuration.

Example 4: Modifying home temperature through a smart home system Smart home systems have been implemented in order to manage remotely a house or to perform automatically routines. For example, it allows users to close or open blinds from their smartphones. Based on instruction temperatures, smart home systems manage the heating or cooling system to reach them at the desired time. However, heating or cooling a house is not immediate, it can take several hours before the targeted temperature is reached. Plus, if the temperature sensor and the heating or cooling system are not placed nearby, the new temperature can take time before being measured. This can be explained due to the temperature inertia plus the delay for the temperature to be propagated.

Through these four examples, we show that delayed actions can be found in different kinds of systems, from CPS to cloud infrastructure. However, not only knowing that an action is running is important but also knowing its expecting effect. We detail this point in the following section.

The need to consider effects In the previous section, we show the existence of delayed actions. One may argue that action statuses are already integrated into

1 the knowledge. For example, the OpenStack Watcher framework stores them in a
2 database⁴, accessible through an API. However, for the best of our knowledge Watcher
3 does not store the expecting effects of each action. While the adaptation process
4 knows what action is running, it does not know what it should expect from them.

5 Considering our example based on the modification of fuses, if the system knows
6 that the technician is modifying fuse states, it does not know what would be the
7 effects. In this case, when the adaptation process analyzes the system context it may
8 wonder: what will be the next grid configuration? How the load will be balanced?
9 Will the future configuration fix all the current incidents? If the effects are not
10 considered by the adaptation process, then it may take suboptimal decisions.

11 Let's exemplify this claim through a scenario based on the fuse example (*cf.*
12 Example 1). As explained before, the overload detected at 4 p.m. takes around 45
13 min to be fixed. The system marks this incident as "being resolved". In addition to
14 this information, the knowledge contains another one saying that it is being solved
15 by modifying three fuses. However, during the resolution stage, a cable is also being
16 overloaded. The adaptation process has two solutions. It can either wait for the
17 end of the resolution of the first incident to see if both overloaded elements will be
18 fixed or it takes other actions without considering the ongoing actions and their
19 impacts. Applying the first strategy may make the resolution of the second incident
20 late, whereas the second one may generate a suboptimal sequence of actions. For
21 example, the second modifications may undo what has been done before or both
22 actions may be conflicting.

23 **Conclusion** Actions, like fuse modification in a smart grid or removing a server
24 from a load balancer, generated during by adaptation processes could take time upon
25 completion. Moreover, the expected effects resulting from such action is reflected in
26 the context representation only after a certain delay. One used workaround is the
27 selection, often empirically, of an optimistic time interval between two iterations of
28 the MAPE-K loop such that this interval is bigger than the longest action execution
29 time. However, the time to execute an action is highly influenced by system overload

⁴<https://docs.openstack.org/watcher/latest/glossary.html#watcher-database-definition>

or failures, making such empirical tuning barely reliable. We argue that by enriching context representation with support for past and future planned actions and their expected effects over time, we can highly enhance reasoning processes and avoid empirical tuning.

The research question that motivates our work is thus: how to enable reasoning over unfinished actions and their expected effects?

Fined and rich context information directly influences the accuracy of the actions taken. Various techniques to represent context information have been proposed; among which we find the models@run.time [DBLP:journals/computer/MorinBJFS09; DBLP:journals/computer/BlairBF09]. The models@run.time paradigm inherits model-driven engineering concepts to extend the use of models not only at design time but also at runtime. This model-based representation has proven its ability to structure complex systems and synthesize its internal state as well as its surrounding environment.

Diagnosis support

Faced with growingly complex and large-scale software systems (e.g. smart grid systems), we can all agree that the presence of residual defects becomes unavoidable [DBLP:conf/icse/BarbosaLMJ17; DBLP:conf/icse/MongielloPS15; DBLP:conf/icse/Has]. Even with a meticulous verification or validation process, it is very likely to run into an unexpected behavior that was not foreseen at design time. Alone, existing formal modeling and verification approaches may not be sufficient to anticipate these failures [DBLP:conf/icse/TaharaOH17]. As such, complementary techniques need to be proposed to locate the anomalous behavior and its origin in order to handle it in a safe way.

As there might be many probable causes behind an abnormal behavior, developers usually perform a set of diagnosis routines to narrow down the scope or origin of the failure. One way to do so is by investigating the satisfaction of its requirements and the decisions that led to this system state, as well as their timing [DBLP:conf/iceccs/BencomoWSW12]. In this perspective, developers may set up a set of systematic questions that would help them understand why and how

- 1 the system is behaving in such a way. These questions may comprise:
- 2 • what goal(s) the system was trying to reach by executing a tactic a ?
 - 3 • what were the circumstances used by a decision d and its expected impact on
 - 4 the context?
 - 5 • what decision(s) influenced the system's context at a time t ?

6 Bencomo *et al.*, [DBLP:conf/iceccs/BencomoWSW12] argue that compre-
 7 hensive explanation about the system behavior contributes drastically to the quality
 8 of the diagnosis, and eases the task of troubleshooting the system behavior. To enable
 9 this, we believe that adaptive software systems should be equipped with traceability
 10 management facilities to link the decisions made to their **(i) circumstances, that is**
 11 **to say, the history of the system states and the targeted requirements, and**
 12 **(ii) the performed actions with their impact(s) on the system.** In particular,
 13 an adaptive system should keep a trace of the relevant historical events.
 14 Additionally, it should be able to trace the goals intended to be achieved by
 15 the system to the adaptations and the decisions that have been made, and
 16 vice versa. Finally, in order to enable developers to interact with the system in a
 17 clear and understandable way, appropriate abstraction to enable the navigation of
 18 the traces and their history should also be provided. Unfortunately, suitable
 19 solutions to support these features are under-investigated.

20 Existing approaches [hassel13; DBLP:conf/models/HeinrichSJRMRP14;
 21 DBLP:conf/icac/EhlersHWH11; DBLP:conf/icse/MendoncaAR14; DBLP:conf/icse/C
 22 DBLP:conf/icse/IftikharW14a] are accompanied by built-in monitoring rules and
 23 do not allow to interact with the underlying system in a simple way. Moreover, they do
 24 not keep track of historical changes as well as causal relationships linking requirements
 25 to their corresponding adaptations. Only flat execution logs are stored.

26 Background

27 Before formalizing and modeling decisions and their circumstances, we abstract
 28 common concepts implied in an adaptation process. We refer to these concepts as
 29 the knowledge.

1 General concepts of adaptation process

2 Similar to the definition provided by Kephart [DBLP:journals/computer/KephartC03] IBM defines adaptive systems as “a computing environment with the ability to manage
3 itself and **dynamically adapt** to change in accordance with **business policies and**
4 **objectives**. [These systems] can perform such activities based on **situations they**
5 **observe or sense in the IT environment [...]**” [computing2006architectural].

6 Based on this definition, we can identify three principal concepts involved in
7 adaptation processes. The first concept is *actions*. They are executed in order to
8 perform a dynamic adaptation through actuators. The second concept is **business**
9 **policies and objectives**, which is also referred to as the **system requirements** in
10 the domain of (self-)adaptive systems. The last concept is the observed or sensed
11 **situation**, also known as the **context**. The following subsections provide more
12 details about these concepts.

14 Context

15 In this thesis, we use the widely accepted definition of context provided by
16 Dey [DBLP:journals/puc/Dey01]: “Context is **any information that can be**
17 **used to characterize** the situation of an entity. An entity is a person, place,
18 or object that is considered relevant to the interaction between a user and [the
19 system], including the user and [the system] themselves”. In this section, we list
20 the characteristics of this information based on several works found in the litera-
21 ture [DBLP:conf/pervasive/HenricksenIR02; DBLP:conf/seke/0001FNMKT14
22 DBLP:journals/percom/BettiniBHINRR10; DBLP:journals/comsur/PereraZCG14]
23 We use them to drive our design choices of our Knowledge meta-model (cf. Sec-
24 tion 3.3.2).

25 **Volatility** Data can be either **static** or **dynamic**. Static data, also called frozen,
26 are data that will not be modified, over time, after their creation [DBLP:conf/pervasive/HenricksenIR0
27 DBLP:journals/comsur/MakrisSS13; DBLP:journals/percom/BettiniBHINRR10]
28 For example, the location of a machine, the first name or birth date of a user can be
29 identified as static data. Dynamic data, also referred to as volatile data, are data
30 that will be modified over time.

1 **Temporality** In dynamic data, sometimes we may be interested not only in storing
2 the latest value, but also the previous ones [DBLP:conf/seke/0001FNMKT14;
3 DBLP:conf/pervasive/HenricksenIR02]. We refer to these data as **historical**
4 data. Temporal data is not only about past values, but also future ones. Two kinds
5 of future values can be identified, **predicted** and **planned**. Thanks to machine
6 learning or statistical methods, dynamic data values can be **predicted**. **Planned**
7 data are set by a system or a human to specify planned modification on the data.

8 **Uncertainty** One of the recurrent problems facing context-aware applications is the
9 data uncertainty [DBLP:conf/dagstuhl/LemosGMSALSTVWBBBBBCDDEGGGGIKKI
10 DBLP:conf/pervasive/HenricksenIR02; DBLP:journals/comsur/MakrisSS13
11 DBLP:journals/percom/BettiniBHINRR10]. Uncertain data are not likely to
12 represent the reality. They contain a noise that makes it deviate from its original
13 value. This noise is mainly due to the inaccuracy and imprecision of sensors. Another
14 source of uncertainty is the behavior of the environment, which can be unpredictable.
15 All the computations that use uncertain data are also uncertain by propagation.

16 **Source** According to the literature, data sources are grouped into two main cate-
17 gories, either sensed (measured) data or computed (derived)
18 data [DBLP:journals/comsur/PereraZCG14].

19 **Connection** Context data entities are usually linked using three kinds of connec-
20 tions: conceptual, computational, and consistency [DBLP:conf/pervasive/HenricksenIR02
21 DBLP:journals/percom/BettiniBHINRR10]. The conceptual connection re-
22 lates to (direct) relationships between entities in the real world (e.g. smart meter and
23 concentrator). The computational connection is set up when the state of an entity
24 can be linked to another one by a computation process (derived, predicted). Finally,
25 the consistency connection relates entities that should have consistent values. For
26 instance, temperature sensors belonging to the same geographical area.

27 **Requirement**

28 **Adaptation processes** aim at modifying the system state to reach an optimal
29 one. All along this process, the system should respect the **system requirements**

established ahead. Through this paper, we use the definition provided by IEEE [iso2017systems] “(1) Statement that translates or expresses a need and its associated **constraints** and **conditions**, (2) **Condition or capability that must be met or possessed** by a system [...] to satisfy an agreement, standard, specification, or other formally imposed documents”.

Although in the literature, requirements are categorized as functional or non-functional, in this paper we use a more elaborate taxonomy introduced by Glinz [DBLP:conf/re/Glinz07]. It classifies requirements in four categories: functional, performance, specific quality, and constraint. All these categories share a common feature: they are all temporal. During the life-cycle of an adaptive system, the developer can update, add or remove some requirements [DBLP:conf/icse/ChengA07; pandey2010effective].

Action

In the IEEE Standards [iso2017systems], an action is defined as: “**process of transformation that operates upon data** or other types of inputs to create data, produce outputs, or **change the state** or condition of the subject software”.

Back to adaptive systems, we can define an action as a process that, given the context and requirements as input, adjusts the system behavior. This modification will then create new data that correspond to an output context. In the remainder of this paper, we refer to output context as impacted context, or simply impact(s). Whereas requirements are used to add preconditions to the actions, context information is used to drive the modifications. Actions execution have a start time and a finish time. They can either succeed, fail, or be canceled by an internal or external actor.

Use case scenario

In order to provide a readable and understandable example of the formalism, we give a simplified version of the use case presented in Section ??.

Excerpt of a smart grid Figure 3.3 shows a simplified version of a smart grid with one substation, one cable, three smart meters and one dead-end cabinet. Both the substation and the cabinet have one fuse each. The meters regularly send consumption data at the same timestamp. For this example, we consider one requirement:

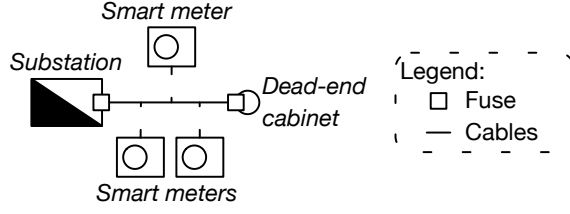


Figure 3.3: Simplified version of a smart grid

1 minimizing the number of overloads. To achieve so, among the different actions, two
 2 actions are taken into account in this example: decreasing or increasing the amps
 3 limits of smart meters.

4 **Adaptation scenario** The system starts at t_0 with the actions, the requirements
 5 and all element of the context that remain fixed: the grid installation. Meters send
 6 their values at t_1 , t_2 and t_3 . Based on these data, the load on cables and substation is
 7 computed. On t_1 , an overload is detected on the cable, which breaks the requirement.
 8 At the same time point, the system decides to reduce the load of all smart meters.
 9 The impact of these actions will be measured at t_2 and t_3 , *i.e.*, the consumption will
 10 slowly reduce until the cable is no longer overloaded from t_3 .

11 **Diagnosis scenario** As all adaptive systems, smart grids are prone to
 12 failures [DBLP:conf/smartgridsec/0001FKNT14]. Using our approach, an engi-
 13 neer could diagnose the system, and determine the adaptation process responsible for
 14 this failure. For instance, considering some reports about regular power cuts during
 15 the last couple of days, in a particular area, a stakeholder may want to interrogate
 16 the system and determine what past decision(s) have led to this suboptimal state.
 17 More concretely, he will ask: did the system make any decisions that could have
 18 impacted the customer consumption? If so, what goal(s) the system was trying to
 19 reach and what were the values used at the time the decision(s) was(were) made?

20 Knowledge formalization

(sec:tkm:k-formalism) As discussed previously, we consider knowledge* to be the association of context*
 22 information, requirements*, and action* information, all in one global and unified

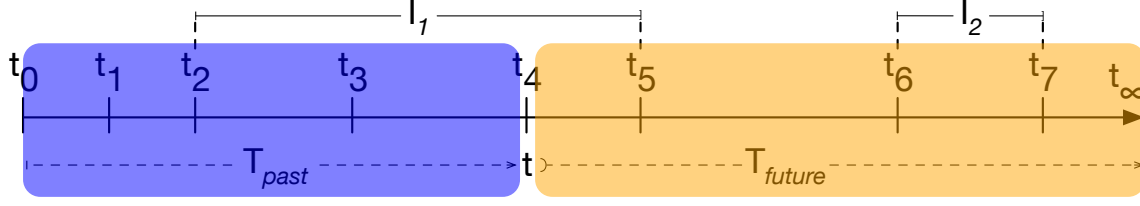


Figure 3.4: Time definition used for the knowledge formalism

model. While context* information captures the state of the system environment and its surroundings, the system requirements* define the constraints that the system should satisfy along the way. Actions*, on the other hand, are meant to reach the goals of the system.

In this section, we provide a formalization of the knowledge* used by adaptation processes based on a temporal graph. Indeed, due to the complexity and interconnectivity of system entities, graph data representation is an appropriate way to represent the knowledge*. Augmented with a temporal dimension, temporal graphs are then able to symbolize the evolution of system entities and states over time. We benefit from the well-defined graph manipulation operations, namely temporal graph pattern matching and temporal graph relations to represent the traceability links between the decisions* made and their circumstances*.

Before describing this formalism, we describe the semantics used for the temporal axis. Then, we exemplify the knowledge formalism using the Luxembourg smart grid use case, detailed in Section 3.1.3.

Formalization of the temporal axis

The formalism described below has been made with two goals in mind. First, the definition of the time space should allow the distinction between past and future. Doing this distinction enable the differentiation between measured data and predicted (or planned data). Second, it should permit the definition of the life cycle of an element of the knowledge*, which can be seen as a succession of states with a validity period that should not overlap each other.

Time space T is considered as an ordered discrete set of time points non-uniformly

distributed. As depicted in Figure 3.4, this set can be divided into 3 different subsets
 $T = T_{past} \cup \{t\} \cup T_{future}$, where:

- T_{past} is the subdomain $\{t_0; t_1; \dots; t_{current-1}\}$ representing graph data history starting from t_0 , the oldest point, until the current time, t , excluded.
- $\{t\}$ is a singleton representing the current time point
- T_{future} is subdomain $\{t_{current+1}; \dots; t_\infty\}$ representing future time points

The three domains depend completely on the current time $\{t\}$ as these subsets slide as time passes. At any point in time, these domains never overlap: $T_{past} \cap \{t\} = \emptyset$, $T_{future} \cap \{t\} = \emptyset$, and $T_{past} \cap T_{future} = \emptyset$. The definition of these three subsets reaches the first goal.

In addition, there is a right-opened time interval $I \in T \times T$ as $[t_s, t_e)$ where $t_e - t_s > 0$. In English words, it means that the interval should represent at least one time point and should follow the time order. For any $i \in I$, $start(i)$ denotes its lower bound and $end(i)$ its upper bound. As detailed in Section 3.2.2, these intervals are used to define the validity period for each node of the graph (our second goal).

Figure 3.4 displays an example of a time space $T_1 = \{t_0, t_1, t_2, t_3, t_4, t_5, t_6, t_7\}$. Here, the current time is $t = t_4$. According to the definition of the past subset (T_{past}) and the future one (T_{future}), there is: $T_{past1} = \{t_0, t_1, t_2, t_3\}$ and $T_{future1} = \{t_5, t_6, t_7\}$. Two intervals have been defined on T_1 , namely I_1 and I_2 . The first one starts at t_2 and ends at t_5 and the last one is defined from t_6 to t_7 . As shown with I_1 , an interval could be defined on different subsets, here it is on all of them (T_{past} , t , and T_{future}).

Formalism

Graph definition First, let K be an adaptive process over a system knowledge* represented by a graph such as $K = (N, E)$, comprising a set of nodes N and a set of edges E . Nodes represent any element of the knowledge (context, actions, etc.) and edges represent their relationships. Nodes have a set of attribute values: $\forall n \in N, n = (id, P)$, where P is the set of key-value attributes. An attribute value has a type (numerical, boolean, ...). Every relationship $e \in E$ can be considered as a couple of nodes with a label $(n_s, n_t, label) \in N \times N$, where n_s is the source node and n_t is the target node.

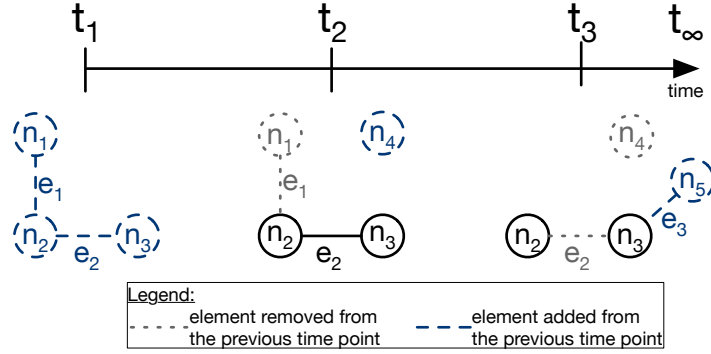


Figure 3.5: Evolution of a temporal graph over time

1 **Adding the temporal dimension** In order to augment the graph with a temporal
2 dimension, the relation V^T is added. So now the knowledge K is defined as a temporal
3 graph such as $K = (N, E, V^T)$.

4 A node is considered valid either until it is removed or until one of its attributes
5 value changes. In the latter case, a new node with the updated value is created.
6 Whilst, an edge is considered valid until either its source node and target node are
7 valid, or until the edge itself is removed. Otherwise, nodes and edges are considered
8 invalid. The temporal validity relation is defined as $V^T : N \cup E \rightarrow I$. It takes as
9 a parameter a node or an edge ($k \in N \cup E$) and returns a time interval ($i \in I$, cf.
10 Section ??) during which the graph element is valid.

11 Figure 3.5 shows an example of a temporal graph K_1 with five nodes ($n_1, n_2, n_3,$
12 $n_4,$ and n_5) and three edges ($e_1, e_2,$ and e_3) over a lifecycle from t_1 to t_3 . In this
13 way, K_1 equals $(\{n_1, n_2, n_3, n_4, n_5\}, \{e_1, e_2, e_3\}, V_1^T)$. Let's assume that the graph is
14 created at t_1 . As n_1 is modified at t_2 , its validity period starts at t_1 and ends at t_2 :
15 $V_1^T(n_1) = [t_1, t_2]$. n_2 and n_3 are not modified; their validity period thus starts at t_1
16 and ends at t_∞ : $V_1^T(n_2) = V_1^T(n_3) = [t_1, t_\infty]$. Regarding the edges, the first one, e_1 ,
17 is between n_1 and n_2 and the second one, e_2 from n_2 to n_3 . Both are created at t_1 .
18 As n_1 is being modified at t_2 , its validity period goes from t_1 to t_2 : $V_1^T(e_1) = [t_1, t_2]$.
19 e_2 is deleted at t_3 . Its validity period is thus equal to: $V_1^T(e_2) = [t_1, t_3]$.

1 **Lifecycle of a knowledge element** One node represents the state of exactly one
2 knowledge element during a period named the validity period. The lifecycle of a
3 knowledge element is thus modeled by a unique set of nodes. By definition, the
4 validity periods of different nodes cannot overlap. A same time period cannot be
5 represented by two different nodes, which could create inconsistency in the temporal
6 graph.

7 To keep track of this knowledge element history, the Z^T relation is added to the
8 graph formalism: $K = (N, E, V^T, Z^T)$. It serves to trace the updates of a given
9 knowledge element at any point in time. This relation can also be seen as a temporal
10 identity function which takes as parameters a given node $n \in N$ and a specific
11 time point $t \in T$, and returns the corresponding node at that point. Formally,
12 $Z^T : N \times T \rightarrow N$.

13 In order to consider this new relation in the example presented in Figure 3.5,
14 the definition of K_1 is modified to $K_1 = (\{n_1, n_2, n_3, n_4, n_5\}, \{e_1, e_2, e_3\}, V_1^T, Z_1^T)$. In
15 Figure 3.5, let's imagine that n_1 , n_4 , and n_5 represent the same knowledge element
16 k_e . The lifecycle of k_e is thus:

- 17 • n_1 for period $[t_1, t_2)$,
- 18 • n_4 for period $[t_2, t_3)$,
- 19 • n_5 for period $[t_3, t_\infty)$.

20 Let t'_1 be a timepoint between t_1 and t_2 . When one wants to resolve the node
21 representing the knowledge element at t'_1 , she or he gets n_1 node, no matter of the
22 node input (n_1 , n_4 , or n_5): $Z_1^T(n_4, t_1) = n_1$. On the other hand, applying the same
23 relation with another node (n_2 or n_3) returns another node. For example, if n_2 and
24 n_3 do not belong to the same knowledge element, then it will return the node given
25 as input, for example $Z_1^T(n_2, t_1) = n_2$.

26 **Knowledge elements stored in nodes** Nodes are used to store the different
27 knowledge elements: context, requirements and actions. The set of nodes N is thus
28 split in three subsets: $N = C \cup R \cup A$ where C is the set of nodes which store context
29 information, R a set of nodes for requirement information and A a set of nodes for
30 action information.

Actions define processes that indirectly impact the context: they will change the behavior of the system, which will be reflected in the context information. Requirements are also processes that are continuously run over the system in order to check the specifications. Here, the purpose of the A and R subset is not to store these processes but to list them. It can be thought as a catalogue of actions and requirements, with their history.

Using a high-level overview, these processes can be depicted as: taking the knowledge as input, perform tasks, and modify this knowledge as output. As detailed in the next two paragraphs, action executions and requirement analysis can be formalized by relations.

Temporal queries for requirements At the current state, the formalism of the knowledge K does not contain any information regarding the requirement analysis. To overcome this, system requirements analysis R_A are added such as $K = (N, E, V^T, Z^T, R_A)$. R_A is a set of couples composed of patterns $P_{[t_j, t_k]}(K)$ and requirements R over these patterns: $R_P = P \cup R$.

$P_{[t_j, t_k]}$ denotes a temporal graph pattern, where t_j and t_k are the lower and upper bound of the time interval respectively. $P_{[t_j, t_k]}$ is the result of a function which takes the knowledge and an interval as input: $P_{[t_j, t_k]} : K \times I$. The time interval can be either fixed (absolute), *i.e.*, both bounds are precisely defined, or sliding (relative), *i.e.*, the upper bound is computed from the lower bound. For example, $P_{[t_0, t_4]}$ is considered as fixed and $P_{[t_0, t_0+4]}$ is considered as relative. Each element of the pattern should be valid for at least one timepoint: $\forall p \in P_{[t_j, t_k]}, V^T(e) \cap [t_j, t_k] \neq \emptyset$. Patterns can be seen as temporal subgraphs of K , with a time limiting constraint coming in the form of a time interval.

Temporal relations for actions Like for R_A , the knowledge K needs to be augmented with action executions A_E : $K = (N, E, V^T, Z^T, R_A, A_E)$. Actions executions A_E can be regarded as a couple (A, A_F) , where A is the action that is executed and A_F a set of relations or isomorphisms mapping a source temporal graph pattern $P_{[t_j, t_k]}$ to a target one $P_{[t_l, t_m]}$, $A_F : K \times I \rightarrow K \times I$.

The left-hand side of the A_F relation depicts the temporal graph elements over

1 which an action is applied. Every relation may have a set of application conditions.
 2 They describe the circumstances under which an action should take place. These
 3 application conditions are either positive, should hold, or negative, should not hold.
 4 Application conditions come in the form of temporal graph invariants. The side
 5 effects of these actions are represented by the right-hand side.

6 Finally, we associate to A_E a temporal function E_{A_E} to determine the time interval
 7 at which an action has been executed. Formally, $E_{A_E} : A_E \rightarrow I$.

8 **Temporal relations for decisions** Finally, the knowledge formalism needs to
 9 include the last, but not the least, element: decisions made by the adaptation,
 10 $K = (N, E, V^T, Z^T, R_A, A_E, D)$ While the source of relations in D represents the
 11 state before the execution of an action, the target shows its impact on the context*.
 12 Its intent is **to trace back impacts of action executions to the decisions they**
 13 **originated from.**

14 A decision present in D is defined as a set of actions executed, *i.e.*, a subset of
 15 A_E , combined with a set of requirement analysis, *i.e.*, a subset of R_A . Formally,
 16 $D = \{ A_D \cup R_D \mid A_D \subseteq A_E, R_A \subseteq R_P \}$. We assume that each action should result
 17 from only one decision: $\forall a \in A, \forall d1, d2 \in D \mid a \in d1 \wedge a \in d2 \rightarrow d1 = d2$.

18 The temporal function E_{A_E} is extended to decisions in order to represent the
 19 execution time: $E_{A_E} : (A \cup D) \rightarrow I$. For decision, the lower bound of the interval
 20 corresponds to the lowest bound of the action execution intervals. Following the
 21 same principle, the upper bound of the interval corresponds to the uppermost bound
 22 of the action execution intervals. Formally, $\forall d \in D \rightarrow E_{A_E}(d) = [l, u]$, where
 23 $l = \min_{a \in A_d} \{E_{A_E}(a)[start]\}$ and $u = \max_{a \in A_d} \{E_{A_E}(a)[end]\}$.

24 **Sum up** Knowledge of an adaptive system can be formalism with a temporal graph
 25 such as $K = (N, E, V^T, Z^T, R_A, A_E, D)$, wherein:

- 26 • N is a set of nodes to represent the different information (context, actions and
 27 requirements)
- 28 • E is a set of edges which connects the different nodes,
- 29 • V^T is a temporal relation which defines the temporal validity of each element,
- 30 • Z^T is a relation to track the history of each knowledge elements,

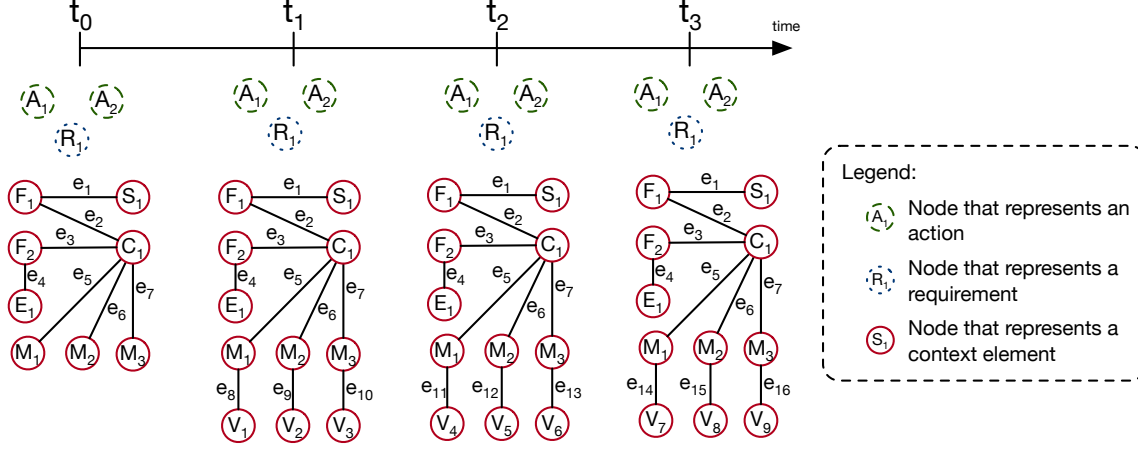


Figure 3.6: Application of the formalism with a temporal graph that represents the knowledge of the smart grid described in Section 3.1.3

- R_A is a relation that defines the different requirements processes,
- A_E is a relation that defines the different action processes,
- D is a set of action executions, which result from the same decision, and requirement analysis.

Decisions D can allow adaptation processes to reason over ongoing and future executions of decisions. Moreover, it allows tracing the state of the knowledge before and after the decision has been or is executed, thanks to its A_D component. Plus, it represents which action has been used for this. Thanks to the R_A relation, one can access the requirements at the root of the decision and the state of the knowledge used by this requirement.

In the next section, we exemplify this formalism over our case study.

Application on the use case

In this section we apply the formalism described on the use case presented in Section 3.1.3.

Let K_{SG} be the temporal graph that represents the knowledge of this adaptive system: $K_{SG} = (N_{SG}, E_{SG}, V_{SG}^T, Z_{SG}^T, R_{P_{SG}}, A_{P_{SG}}, D_{SG})$. Figure 3.6 shows the nodes and edges of this knowledge.

1 **Description of N_{SG}** N_{SG} is divided into three subsets: C_{SG} , R_{SG} and A_{SG} . R_{SG}
2 contains one node, R_1 in Figure 3.6, which represents the requirement of this example
3 (minimizing the number of overloads): $R_{SG} = \{R_1\}$. Two nodes, A_1 and A_2 , belong to
4 A_{SG} : $A_{SG} = \{A_1, A_2\}$. They represent the two actions of this example, respectively
5 decreasing and increasing amps limits. Regarding the context C_{SG} , there are three
6 nodes to represent the three smart meters (M_1 , M_2 , and M_3), one for the substation
7 (S_1), two for the fuses (F_1 and F_2), one for the dead-end cabinet (E_1), one for the
8 cable (C_1) and one node per consumption value received (V_i): $C_{SG} = \{M_1, M_2, M_3,$
9 $S_1, F_1, F_2, E_1, C_1\} \cup \{V_i | i \in [1..9]\}$.

10 According to the scenario, except for nodes to store consumption values, the other
11 nodes are created at t_0 and are never modified. Therefore, their validity period starts
12 at t_0 and never ends: $\forall n \in A_{SG} \cup R_{SG} \cup \{M_1, M_2, M_3, S_1, F_1, F_2, E_1, C_1\}, V_{SG}^T(n) = [t_0,$
13 $t_\infty)$. Considering the consumption values, all the nodes represent the history of the
14 values for the three smart meters. In other words, there are three knowledge elements:
15 the consumption measured for each meter. Let C_i notes the consumption measured
16 by the smart meter M_i . As shown in Figure ??, there is:

- 17 • C_1 of M_1 is represented by $\{V_1, V_4, V_7\}$,
- 18 • C_2 of M_2 is represented by $\{V_2, V_5, V_8\}$,
- 19 • C_3 of M_3 is represented by $\{V_3, V_6, V_9\}$.

20 Taking C_2 as an example, V_2 is the initial consumption value, replaced by V_5 at t_2 ,
21 itself replaced by V_8 at t_3 . Applying the V_{SG}^T on these different values, results are
22 thus:

- 23 • $V_{SG}^T(V_2) = [t_1, t_2)$,
- 24 • $V_{SG}^T(V_5) = [t_2, t_3)$,
- 25 • $V_{SG}^T(V_8) = [t_3, t_\infty)$.

26 These validity periods are shown in Figure 3.7a. As meters send the new consumption
27 values at the same time, this example can also be applied to C_1 and C_3 .

28 From these validity periods, the Z_{SG}^T can be used to navigate to the different
29 values over time. Let's continue with the same example, C_2 . In order to get the
30 evolution of the consumption value C_2 , given the initial one, one will use the Z_{SG}^T
31 relation:

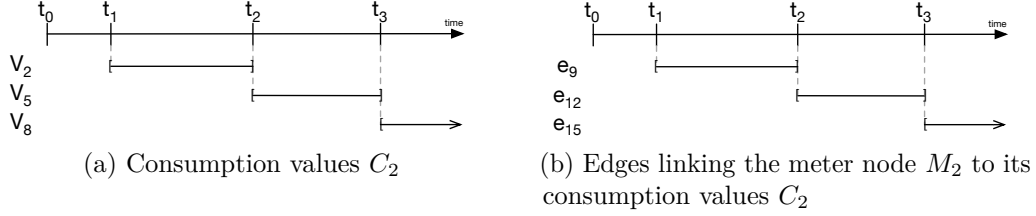


Figure 3.7: Validity periods of consumption values and their edges to the smart meter M_2

- 1 • $Z_{SG}^T(V_2, t_{s1}) = \emptyset$, where $t_0 \leq t_{s1} < t_1$
- 2 • $Z_{SG}^T(V_2, t_{s2}) = V_2$, where $t_1 \leq t_{s2} < t_2$
- 3 • $Z_{SG}^T(V_2, t_{s3}) = V_5$, where $t_2 \leq t_{s3} < t_\infty$.
- 4 • $Z_{SG}^T(V_2, t_{s4}) = V_8$, where $t_2 \leq t_{s4} < t_\infty$.

5 **Description of E_{SG}** In this example, edges are used to store the relationships
6 between the different context elements. For example, the edge between the substation
7 S_1 and the fuse F_1 allow representing the fact that the fuse is physically inside the
8 substation. Another example, edges between the cable C_1 and the meters M_1 , M_2
9 and M_3 represent the fact that these meters are connected to the smart grid through
10 this cable.

11 One may consider that relations (validity, Z^T , decisions, action executions and
12 requirements analysis) will be stored as edges. But this decision is let to the imple-
13 mentation part of this formalism.

14 In our model, only consumption values (V_i nodes) are modified over time. Plus,
15 since the scenario does not imply any edge modifications, only those between meters
16 and values are modified. The edge set contains thus sixteen edges: $E_{SG} = \{e_i \mid i \in$
17 $[1..16]\}$.

18 By definition, the unmodified edges have a validity period starting from t_0 and
19 never ends: $\forall i \in [1..7], V_{SG}^T(e_i) = [t_0, t_\infty)$. The history of the three knowledge
20 elements that represent consumption values do not only impact the nodes which
21 represent the values but also the edges between those nodes and the meters ones:

- 22 • C_1 impacts edges between M_1 and V_1 , V_4 , and V_7 , i.e., $\{e_8, e_{11}, e_{14}\}$,

- 1 • C_2 impacts edges between M_2 and V_2 , V_5 , and V_8 , *i.e.*, $\{e_9, e_{12}, e_{15}\}$,
- 2 • C_3 impacts edges between M_3 and V_3 , V_6 , and V_9 , *i.e.*, $\{e_{10}, e_{13}, e_{16}\}$.

3 Continuing with C_2 as an example, the initial edge value is e_9 from t_1 , which is
 4 replaced by e_{12} from t_2 , itself replaced by e_{15} from t_2 . The validity relation, applied
 5 to these edges, thus returns:

- 6 • $V_{SG}^T(e_9) = [t_1, t_2) = V_{SG}^T(V_2)$,
- 7 • $V_{SG}^T(e_{12}) = [t_2, t_3) = V_{SG}^T(V_5)$,
- 8 • $V_{SG}^T(e_{15}) = [t_3, t_\infty) = V_{SG}^T(V_8)$,

9 These validity periods are depicted in Figure 3.7b. As they are driven by those of
 10 consumption values (V_2 , V_5 , and V_8), they are equal.

11 As for nodes, the Z_{SG}^T relation can navigate over time through these values. For
 12 example, to get the history of the edges between the consumption value C_2 and the
 13 meter represented by M_2 , one can apply the Z_{SG}^T relation as follows:

- 14 • $Z_{SG}^T(e_9, t_{s1}) = \emptyset$, where $t_0 \leq t_{s1} < t_1$
- 15 • $Z_{SG}^T(e_9, t_{s2}) = e_9$, where $t_1 \leq t_{s2} < t_2$,
- 16 • $Z_{SG}^T(e_9, t_{s3}) = e_{12}$, where $t_2 \leq t_{s3} < t_3$,
- 17 • $Z_{SG}^T(e_9, t_{s4}) = e_{15}$, where $t_3 \leq t_{s4} < t_\infty$.

18 **Description of D_{SG} , A_{ESG} , and R_{ASG}** As described in the scenario (cf. Sec-
 19 tion 3.1.3), the requirement analysis detects that t_1 the requirement is broken. The
 20 adaptation process will thus apply the “decreasing amps limits” action on the three
 21 meters. Following Example 2 detailed in Section 3.1.1, we consider that the action
 22 will impact the consumption values on the next two measurements: t_2 and t_3 .

23 In the knowledge, we thus have one decision: $D_{SG} = D_1$. This decision has
 24 been taken after one requirement analysis, R_{ASG1} , that detects no respect of the
 25 requirement R_1 . To determine if there is an overload, this analysis needs to know
 26 the topology and the consumption values. The pattern is thus defined by all nodes
 27 related to the grid network and consumption values at $t1$: $P_{1[t_1, t_1+1]} = \{S_1, F_1, F_2, C_1,$
 28 $E_1, M_1, M_2, M_3, V_1, V_2, V_3\}$. So we have: $R_{ASG1} = \{R_1, P_{1[t_1, t_1+1]}\}$.

29 The knowledge also includes the three action executions: A_{ESG1} , A_{ESG2} , and A_{ESG3} .
 30 These actions have been executed on, respectively, M_1 , M_2 , and M_3 . Following the

definition, they all contain the action A_1 and similar relation which linked the circumstances to the impacts. The circumstances are the state of the knowledge at t_0 , which contain all information of the grid network and the consumption values. We denote them $P_{2[t_1, t_1+1]}$, $P_{3[t_1, t_1+1]}$, and $P_{4[t_1, t_1+1]}$, all equal $P_{1[t_1, t_1+1]}$. The impact contains all consumption values received at t_2 and t_3 . Each action impacts the consumption value of the meter that it modifies. For example, A_{ESG2} only impacts values of meter M_2 . For this action, the output pattern is thus : $P_{5[t_2, t_3]} = \{V_5, V_8\}$. In summary, A_{ESG1} , A_{ESG2} , and A_{ESG3} are defined as follows:

- for the action executed on M_1 : $A_{ESG1} = (A_1, A_{F1})$, with $A_{F1} : P_{2[t_1, t_1+1]} \rightarrow \{V_4, V_7\}$,
- for the action executed on M_2 : $A_{ESG2} = (A_1, A_{F2})$, with $A_{F2} : P_{3[t_1, t_1+1]} \rightarrow \{V_5, V_8\}$,
- for the action executed on M_3 : $A_{ESG3} = (A_1, A_{F3})$, with $A_{F3} : P_{4[t_1, t_1+1]} \rightarrow \{V_6, V_9\}$,

The decision described in the scenario is thus equal to: $D_1 = \{R_{ASG1}, A_{ESG1}, A_{ESG2}, A_{ESG3}\}$. At t_2 , this decision will still be valid. The adaptation process can thus include it in the adaptation process to reason over the ongoing actions. If at t_3 the cable remains overloaded, then one may use this element to check if the system tried to fix it, how and based on which information.

Modeling the knowledge

In order to simplify the diagnosis of adaptive systems, this thesis proposes a novel metamodel* that combines, what we call, design elements and runtime elements. Design elements abstract the different elements involved in knowledge* information to assist the specification of the adaptation process. Runtime elements instead, represent the data collected by the adaptation process during its execution. In order to maintain the consistency between previous design elements and newly created ones, instances of design elements (*e.g.*, actions) can be either added or removed. Modifying these elements would consist in removing existing elements and creating new ones. Combining design elements and runtime elements in the same model helps not only to acquire the evolution of system but also the evolution of its structure and

1 specification (e.g. evolution of the requirements of the system). Design time elements
2 are depicted in gray in the Figures 3.8– 3.11. Note that, this thesis does not address
3 how runtime information is collected.

4 For the sake of modularity, the metamodel* has been split into four packages:
5 Knowledge, Context, Requirement and Action. All the classes of these packages have
6 a common parent class that adds the temporality dimension: *TimedElement* class.
7 Before describing the Knowledge (core) package, we detail this element. Then, we
8 introduce in more details the other three packages used by the Knowledge package:
9 Context, Requirement, and Action. In below sections, we use "*Package::Class*"
10 notation to refer to the provenance of a class. If the package is omitted, then the
11 provenance package is this one described by the figure or text.

12 **Parent element: *TimedElement* class**

13 we assume that all the classes in the different packages extend a *TimedElement*
14 class. This class contains three methods: *startTime*, *endTime*, and *modificationsTime*.
15 The first two methods allow accessing the validity interval bounds defined by the
16 previously discussed V^T relation. The last method resolves all the timestamps at
17 which an element has been modified: its history. This method is the implementation
18 of the relation Z^T described in our formalism (cf. Section 3.2.2).

19 **Knowledge metamodel**

20 In order to enable interactive diagnosis of adaptive systems, traceability links
21 between the decisions made and their circumstances should be organized in a well-
22 structured representation. In what follows, we introduce how the knowledge*
23 metamodel* helps to describe decisions*, which are linked to their goals and their
24 context (input and impact). Figure 3.8 depicts this metamodel*.

25 Knowledge package is composed of a *context**, a set of *requirements**, a set of
26 *strategies*, and a set of *decisions**. A decision* can be seen as the output of the
27 Analyze and Plan steps in the Monitor, Analyze, Plan, and Execute over knowledge
28 (MAPE-k)* loop.

29 Decisions comprise target *goals* and trigger the execution of one *tactic* or more.

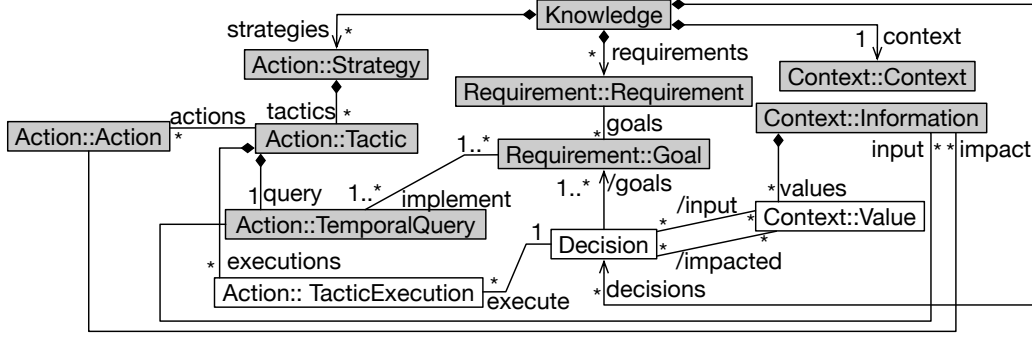


Figure 3.8: Excerpt of the knowledge metamodel

:knowledge-mm)

1 A decision has an *input* context and an *impacted* context. The context impacted
 2 by a decision (*Decision.impact*) is a derived relationship computed by aggregating
 3 the impacts of all actions belonging to a decision (see Fig. 3.11). Likewise, the *input*
 4 relationship is derived and can be computed similarly. In the smart grid example, a
 5 decision can be formulated (in plain English) as follows: since the district D is almost
 6 overloaded (*input context*), we reduce the amps limit of greedy consumers using the
 7 “*reduce amps limit*” action in order to reduce the load on the cable of the district
 8 (*impact*) and satisfy the “*no overload*” policy (*requirement*).

9 As all the elements inherit from the *TimedElement*, we can capture the time at
 10 which a given decision and its subsequent actions were executed, and when their impact
 11 materialized, *i.e.*, measured. Thanks to this metamodel representation, a developer
 12 can apprehend the possible causes behind malicious behavior by navigating from the
 13 context values to the decisions that have impacted its value (*Property.expected.impact*)
 14 and the goals it was trying to reach (*Decision.goals*). In Section 3.1.3, we present an
 15 example of interactive diagnosis queries applied to the smart grid use case.

16 Context metamodel

17 Context models structure context information acquired at runtime. For example,
 18 in a smart-grid system, the context model would contain information about smart-grid
 19 users (address, names, etc.) resource consumption, etc.

20 An excerpt of the context model is depicted in Figure 3.9. we propose to rep-

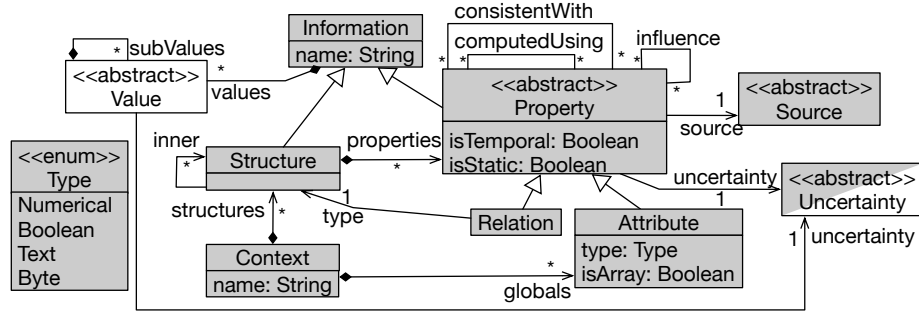


Figure 3.9: Excerpt of the context metamodel

<fig:context-model>

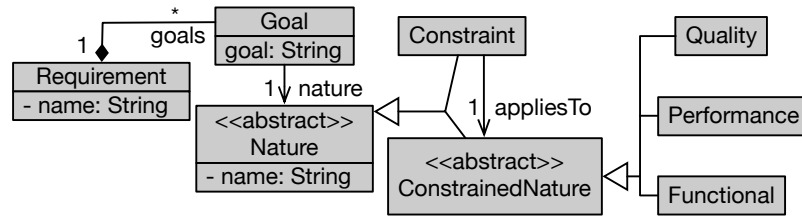


Figure 3.10: Requirement metamodel

ig:requirement-model>

- 1 represent the context as a set of structures (*Context.structures*) and global attributes
- 2 (*Context.globals*). A structure can be viewed as a C-structure with a set of properties
- 3 (*Property*): attributes (*Attribute*) or relationships (*Relation*). A structure may contain
- 4 other nested structures (*Structure.inner*). Structures and properties have values.
- 5 They correspond to the nodes described in the formalization section (*cf.* Section 3.2.2).
- 6 The connection feature described in Section 3.1.2 is represented thanks to three recur-
- 7 sive relationships on the Property class: *consistentWith*, *computedUsing* and *influence*.
- 8 Additionally, each property has a source (*Source*) and an uncertainty (*Uncertainty*).
- 9 It is up to the stakeholder to extend data with the appropriate source: measured,
- 10 computed, provided by a user, or by another system (*e.g.*, weather information coming
- 11 from a public API). Similarly, the uncertainty class can be extended to represent the
- 12 different kinds of uncertainties. Finally, a property can be either historic or static.

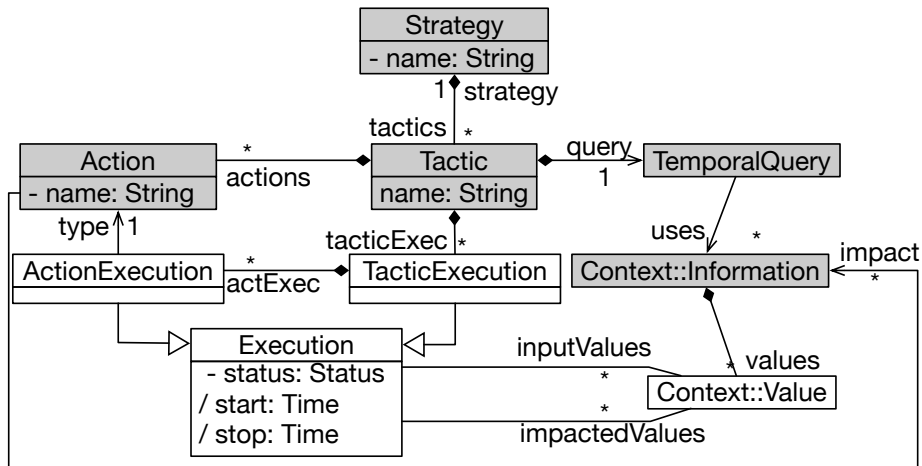


Figure 3.11: Excerpt of the action metamodel

 $\text{fig:action-mm}\rangle$

1 Requirement metamodel

As different solutions to model system requirements exist (*e.g.*, KAOS [DBLP:journals/scp/Dardenne01], i* [yu2011modelling] or Tropos [DBLP:journals/aamas/BrescianiPGGM04]), in this metamodel, we abstract their shared concepts. The requirement model, depicted in Figure 3.10, represents the *requirement* as a set of *goals*. Each goal has a *nature* and a textual specification. The nature of the goals adheres to the four categories of requirements presented in Section 3.1.2. One may use one of the existing requirements modeling languages (*e.g.*, RELAX) to define the semantics of the requirements. Since the requirement model is composed solely of design elements, we may rely on static analysis techniques to infer the requirement model from existing specifications. The work of Egyed [DBLP:conf/icse/Egyed01] is one solution among others. This work is out of the scope of the paper and envisaged for future work.

In the guidance example, the requirement model may contain a **balanced resource distribution** requirement. It can be split into different goals: (i) *minimizing overloads*, (ii) *minimizing production lack*, (iii) *minimizing production loss*.

1 Action metamodel

?⟨sec:action-mm⟩?

2 Similar to the requirements metamodel, the actions metamodel also abstracts main
3 concepts shared among existing solutions to describe adaptation processes and how
4 they are linked to the context. Figure 3.11 depicts an excerpt of the action metamodel.
5 we define a strategy as a set of tactics (*Strategy*). A tactic contains a set of actions
6 (*Action*). A tactic is executed under a precondition represented as a temporal query
7 (*TemporalQuery*) and uses different data from the context as input. In future work, we
8 will investigate the use of preconditions to schedule the executions order of the actions,
9 similarly to existing formalisms such as Stitch [DBLP:journals/jss/ChengG12].
10 The query can be as complex as needed and can navigate through the whole knowledge
11 model. Actions have impacts on certain properties, represented by the *impacted*
12 reference.

13 The different executions are represented thanks to the *Execution* class. Each
14 execution has a status to track its progress and links to the impacted context
15 values(*Execution.impactValues*). Similarly, input values are represented thanks to
16 the *Execution.inputValues* relationship. An execution has *start* and *end* time. Not
17 to confuse with the *startTime* and *endTime* of the validity relation V^T . Whilst the
18 former corresponds to the time range in which a value is valid, the *start* and *stop* time
19 in the class execution correspond to the time range in which an action or a tactic
20 was being executed. The start and stop attributes correspond to the relation E_{AE}
21 (see Section 3.2.2). These values can be derived based on the validity relation. They
22 correspond to the time range in which the status of the execution is “*RUNNING*”.
23 Formally, for every execution node e , $E_{AE}(e) = (V(e) \mid e.status = \text{“RUNNING”})$.

24 Similarly to requirement models, it is possible to automatically infer design
25 elements of action models by statically analyzing actions specification. Since acquiring
26 information about tactics and actions executions happens at runtime, one way to
27 achieve this is by intercepting calls to actions executions and updating the appropriate
28 action model elements accordingly. This is out of the scope of this paper and planned
29 for future work.

Validation

To validate and evaluate our approach, we implemented a prototype publicly available online⁵. This implementation leverages the GreyCat framework⁶, more precisely the modeling plugin, which allows designing a metamodel using a textual syntax. Based on this specification, GreyCat generates a Java and a JavaScript API to create and manipulate models that conform to the predefined metamodel. The GreyCat framework handles time as a built-in concept. Additionally, it has native support of a lazy loading mechanism and an advanced garbage collection. This is achieved by dynamically loading and unloading model elements from the main memory when necessary.

The validation of our approach has been driven by the two research questions formulated in the introduction section:

- How to diagnose the self-adaptation process?
- How to enable reasoning over unfinished actions and their expected effects?

To address the first one, we describe how one can use our approach to represent the knowledge of an adaptation process for a smart grid system. Then, we present a code to extract the circumstances and the goals of a decision. For the second one, we present a scenario where a developer can use our approach to reason over unfinished actions and their expected effects. The presented code shows how information can be extracted from our model to enable any reasoning algorithm. Finally, we present a performance evaluation to show the scalability of our approach.

Diagnostic: implementation of the use case

In what follows, we explain how a stakeholder, Morgan, can apply our approach to a smart grid system in order to, first, abstract adaptive system concepts, then, structure runtime data, and finally, query the model for diagnosis purpose. The corresponding object model is depicted in Figure 3.12. Due to space limitation, we only present an excerpt of the knowledge model. An elaborate version is accessible in the tool repository.

⁵<https://github.com/lmouline/LDAS>

⁶<https://github.com/datathings/greycat>

1 **Abstracting the adaptive system** At design time (t_d), either manually or using
2 an automatic process, Morgan abstracts the different tactics and actions available
3 in the adaptation process. Among the different tactics that Morgan would like to
4 model is “*reduce amps limit*”. It is composed of three actions: sending a request to
5 the smart meter (*askReduce*), checking if the new limit corresponds to the desired
6 one (*checkNewLimit*), and notifying the user by e-mail (*notifyUser*). Morgan assumes
7 that the *askReduce* action impacts consumption data (*csmpt*). This tactic is triggered
8 upon a query (*tempQ*) that uses meter (*mt*), consumption (*csmpt*) and customer
9 (*cust*) data. The query implements the “*no overload*” goal: the system shall never
10 have a cable overload. Figure 3.12 depicts a flattened version of the temporal model
11 representing these elements. The tag at upper-left corner of every object illustrates
12 the creation timestamp. All the elements created at this stage are tagged with t_d .

13 **Adding runtime information** The adaptation process checks if the current sys-
14 tem state fulfills the requirements by analyzing the context. To perform this, it
15 executes the different temporal queries, including *tempQ*. For some reasons, the
16 *tempQ* reveals that the current context does not respect the “*no overload*” goal. To
17 adapt the smart grid system, the adaptation process decides to start the execution
18 of the previously described tactic (*exec1*) at t_s . As a result, a decision element is
19 added to the model along with a relationship to the unsatisfied goal. In addition,
20 this decision entails the planning of a tactic execution, manifested in the creation
21 of the element *exec1* and its subsequent actions (*notifyU*, *checkLmt*, and *askRed*). At
22 t_s , all the actions execution have an IDLE status and an expected start time. All
23 the elements created at this stage are tagged with the t_s timestamp in Figure 3.12.

24 At t_{s+1} , the planned tactic starts being executed by running the action *askReduce*.
25 The status of this action turns from *IDLE* to *RUNNING*. Later, at t_{s+2} , the execution
26 of *askReduce* finishes with a *SUCCEED* status and triggers the execution of the
27 actions *notifyUser* and *checkNewLimit* in parallel. The status of *askReduce* changes
28 to *SUCCEED* while the status of *notifyUser* and *checkNewLimit* turns to *RUNNING*.
29 The first action successfully ends at t_{s+3} while the second ends at t_{s+4} . As all actions
30 terminates with a *SUCCEED* status at t_{s+4} , accordingly, the final status of the tactic

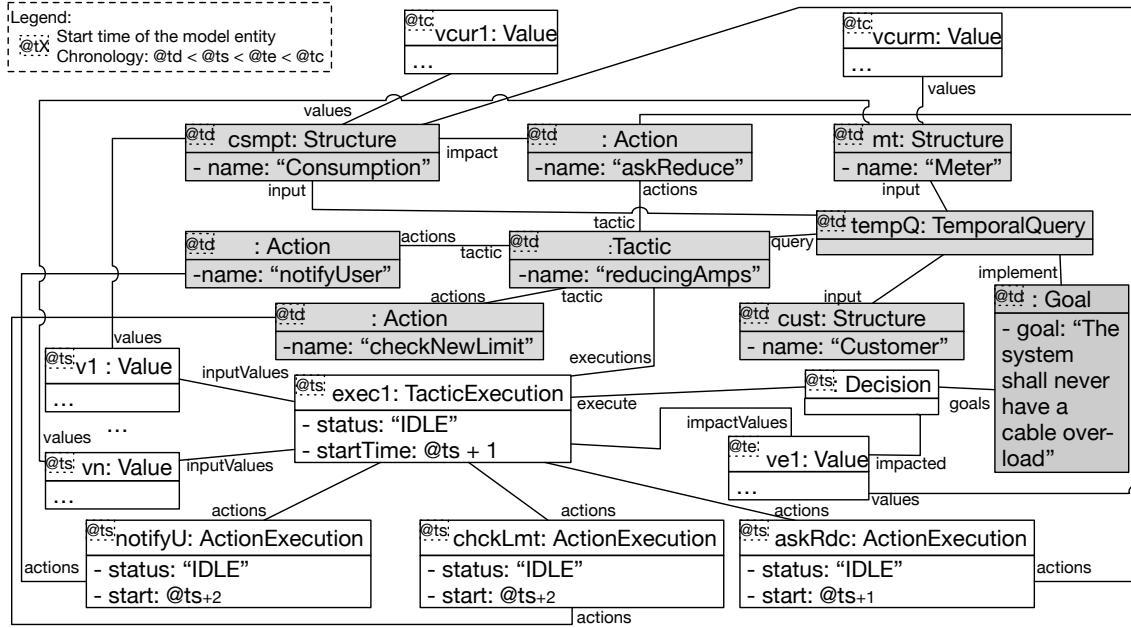


Figure 3.12: Excerpt of the knowledge object model related to our smart grid example

- 1 is set *SUCCEED* and the *stop* attribute value is set to t_e .
- 2 **Interactive diagnosis query** After receiving incident reports concerning regular
- 3 power cuts, and based on the aforementioned knowledge model, Morgan would be
- 4 able to query the system's states and investigate why such incidents have occurred.
- 5 As described in Section 3.1.3, she/he will interactively diagnose the system by
- 6 interrogating the context, the decisions made, and their circumstances.
- 7 The first function, depicted in Listing 3.1, allows to navigate from the currently
- 8 measured values (*vcur1*) to the decision(s) made. The for-loop and the if-condition are
- 9 responsible for resolving the measured data for the past two days. Past elements are
- 10 accessed using the *resolve* function that implements the Z^T relation (*cf.* Section 3.2.2).
- 11 After extracting the decisions leading to power cuts, Morgan carries on with the
- 12 diagnosis by accessing the circumstances of this decision. The code to perform this
- 13 task is depicted in Listing 3.1, the second function (*getCircumstances*). Note that
- 14 the relationship *Decision.input* is the aggregation of *Decision.execute.inputValues*.

```

15 // extracting the decisions
16

```

```

1 Decision [] impactedBy(Value v) {
2   Decision [] respD
3   for( Time t: v.modificationTimes() ):
4     if ( t >= v.startTime() - 2 day)
5       Value resV = resolve(v,t)
6       respD.addAll(from(resV).navigate(Value.impactd))
7   return respD
8 }
9 // extracting the circumstances of the made decisions
10 Tuple<Value [], Goal[]> getCircumstance(Decision d) {
11   Value [] resValues = from(d).navigate(Decision.input)
12   Goal [] resGoals = from(d).navigate(Decision.goals)
13   return Tuple<>(resValues, resGoals)
14 }
15 }

```

Listing 3.1: Get the goals used by the adaptation process from executed actions

Reasoning over unfinished actions and their expected effects

By associating the action model to the knowledge model, we aim at enhancing adaptation processes with new abilities to reason. In this section, we present an example of a reasoning algorithm which considers the impacts of running actions. This example is based on our use case (*cf.* Section ??).

Let's imagine that the adaptation process detects overloaded cables in the smart grid. To fix this situation, it takes several countermeasures, among which there are fuse state modifications. As detailed in Section 3.1.1, this action is considered as delayed action. Later, another incident is detected, for example, a substation is being overloaded. Before taking any actions, the adaptation process can, thanks to our solution, verify if the running actions will be sufficient to solve this new incident. If not, it can either take additional actions or replan the running one. The algorithm to reschedule current actions or to compute additional actions is out of the scope of this thesis. Here, we present the code to extract the required information from our model.

Checking if the running actions will be sufficient to solve all current issues can also be thought as: will the issue remain with the new context, *i.e.*, after each action have been executed. In our case, it is like verifying if the second overload will still remain with the new topology, which is coming. The adaptation process, therefore, needs to extract the context in the future. To do so, the adaptation process should know the

1 latest timepoint at which the impact will be measured. Listing 3.2 shows the code
2 to get this timepoint. Running, idle and finished actions are accessed thanks to the
3 first two nested loops with the if-condition. We consider that failed and canceled
4 actions have no effects. As finished actions may still have effects, we also consider
5 them. Then we navigate through all impacted values to get their start time, *i.e.*, the
6 beginning of their validity period (V^T relation, *cf.* Section 3.2.2). Doing so, we are
7 sure to get the latest timepoint at which an impact will be measurable.

```

8 latest-impact
9 Time latestImpact(Knowledge k) {
10     Time latestTime = CURRENT_TIME
11
12     for(Decision d: from(k).navigate(decisions))
13         for(TacticExecution te: from(d).navigate(execute))
14             if(te.status == "RUNNING" || te.status == "IDLE" || te.status == "SUCCEED")
15                 for(Value v: from(te).navigate(impactedValues))
16                     if(v.startTime() > latestTime)
17                         latestTime = v.startTime()
18
19     return latestTime
20 }

```

Listing 3.2: Get latest timepoint at which the impact will be measured

22 Using this timepoint, then the adaptation process can then compute how the
23 grid should be after the actions have been executed. If the system has no prediction
24 mechanism, then the adaptation process can verify how the power will be balanced
25 over the new topology. Otherwise, it can use this prediction feature to compute the
26 expected loads with the coming topology. Using this information, it can verify if all
27 current incidents will be solved by the ongoing actions or not. If not, it may take
28 additional actions or reschedule them.

29 Listing 3.3 depicts the code to extract all running actions. The nested loops
30 allow accessing all executions made by decision. Then, we filter only those with the
31 “RUNNING” status. The resulting collection should then be given to the scheduling
32 algorithm, which will decide if rescheduling is possible and how.

```

33 d:extract-act
34 TacticExecution[] runningActions(Knowledge k) {
35     TacticExecution[] resA
36     for(Decision d: k.decisions) {
37         for(TacticExecution te: d.execute) {

```

```

1      if(te.status == Status.RUNNING) {
2          resA.add(te)
3      }
4  }
5  }
6  return resA
7  }

```

Listing 3.3: Extract ongoing actions and their effects

Using our model, developers have two solutions to model a rescheduling operation. Either they modify the actions, which may delete the history of the previous decision, or they mark all running and idle actions as “CANCELED” and create a new decision, with new actions, which update the circumstances and re-use the same requirements.

Performance evaluation

GreyCat stores temporal graph elements in several key/value maps. Thus, the complexity of accessing a graph element is linear and depends on the size of the graph. Note that in our experimentation we evaluate only the execution performance of diagnosis algorithms. For more information on I/O performance in GreyCat, please refer to the original work by Hartmann *et al.*, [DBLP:conf/seke/0001FJRT17; DBLP:phd/basesearch/Hartmann16].

```

20  MATCH (input)-[*4]->(output)
21  WHERE input.id IN [randomly generated set]
22  RETURN output
23  LIMIT O
24
25

```

Listing 3.4: Traversal used during the experimentations

We consider a diagnosis algorithm to be a graph navigation from a set of nodes (input) to another set of nodes (output). Unlike typical graph algorithms, diagnosis algorithms are simple graph traversals and do not involve complex computations at the node level. Hence, we believe that three parameters can impact their performance (memory and/or CPU): the global size of the graph, the size of the input, and the number of traversed elements. In our evaluation, we altered these parameters and report on the behavior of the main memory and the execution time. The code of

our evaluation is publicly available online⁷. All experiments reporting on memory consumption were executed 20 times after one warm-up round. Whilst, execution time experiments were run 100 times after 20 warm-up rounds. The presented results correspond to the mean of all the iterations. We randomly generate graph with sizes (N) ranging from 1 000 to 2 000 000. At every execution iteration, we follow these steps: (1) in a graph with size N , we randomly select a set of I input nodes, (2) then traverse M nodes in the graph, (3) and we collect the first O nodes that are at four hops from the input element. Listing 3.4 describes the behavior of the traversal using Cypher, a well-known graph traversal language.

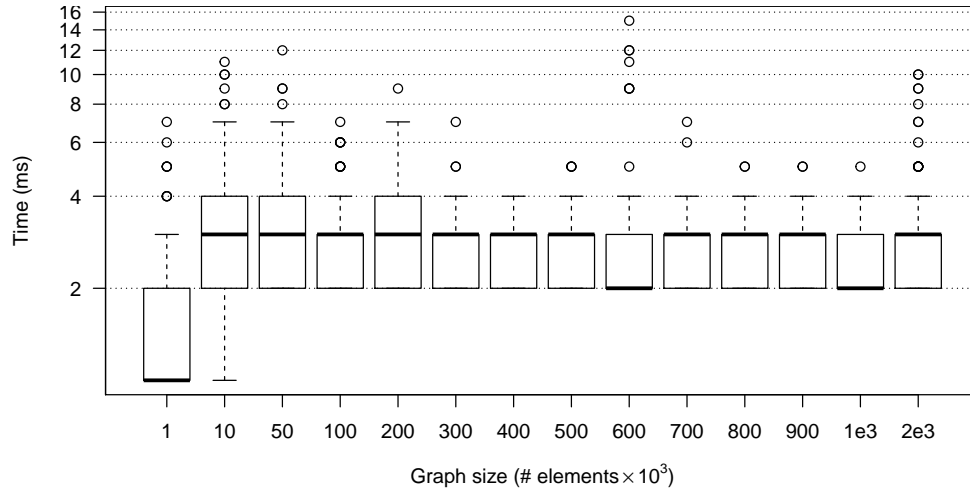
We executed our experimentation on a MacBook Pro with an Intel Core i7 processor (2.6 GHz, 4 cores, 16GB main memory (RAM), macOS High Sierra version 10.13.2). We used the Oracle JDK version 1.8.0_65.

How performance is influenced by the graph size N ? This experimentation aims at showing the impact of the graph size (N) on memory and execution time while performing common diagnosis routines. We fix the size of I to 10. To assure that the behavior of our traversals is the same, we use a seed value to select the starting input elements. We stop the algorithm when we reach 10 elements. Results are depicted in Figure 3.13.

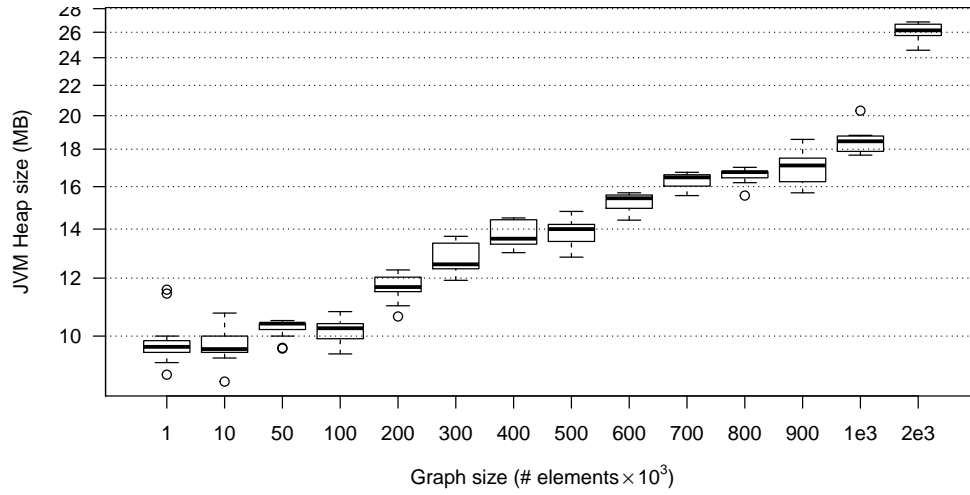
As we can notice, the graph size does not have a significant impact on the execution time of diagnosis algorithms. For graphs with up to 2,000,000 elements, execution time remains between 2 ms and four 4 ms. We can also notice that the memory consumption insignificantly increases. Thanks to the implementation of a lazy loading and a garbage collection strategy by GreyCat, the graph size does not influence memory or execution time performance. The increase in memory consumption can be due to the internal indexes or stores that grow with the graph size.

How performance is influenced by the input size (I)? The second experiment aims to show the impact of the input size (I) on the execution of diagnosis algorithms. We fix the size of N to 500 000 and we variate I from 1 000 nodes to 100 000, *i.e.*, from 0.2% to 20% of the graph size. The results are depicted in Figure 3.14 (straight

⁷<https://bitbucket.org/ludovicpapers/icac18-eval>



(a) Execution time evolution



(b) Memory evolution

`<fig:exp1>` Figure 3.13: Experimentation results when the knowledge based size increases

lines).

Unlike to the previous experiment, we notice that the input size (I) impacts the performance, both in terms of memory consumption and execution time. This is because our framework keeps in memory all the traversed elements, namely the input elements. The increase in memory consumption follows a linear trend with regards to N . As it can be noticed, it reaches 2GB for $I=100\,000$. The execution time also shows a similar curve, while the query response time takes around 60ms to run for $I=1\,000$, it takes a bit more than 4 seconds to finish for $I=100\,000$. Nonetheless, these results remain very acceptable for diagnosis purposes.

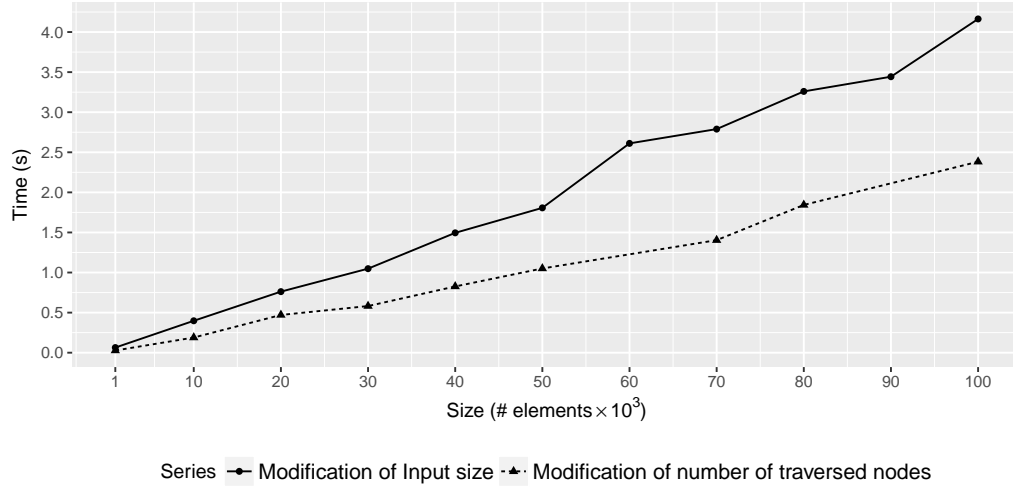
How performance is influenced by the number of traversed elements (M)?

For the last experiment, we aim to highlight the impact of the number of traversed elements (M). For this, we fix I and O to 1, and randomly generate a graph with sizes ranging from 1 000 to 100 000. Our algorithm navigates the whole model ($M=N$). We depict the results in Figure 3.14 (dashed curve). As we can notice, the memory consumption increases in a quasi-linear way. The memory footprint to traverse $M = 100\,000$ elements is around 0.9GB. The progress of the execution time curve behaves similarly, in a quasi-linear way. Finally, the execution time of a full traversal over the biggest graph takes less than 2.5 seconds.

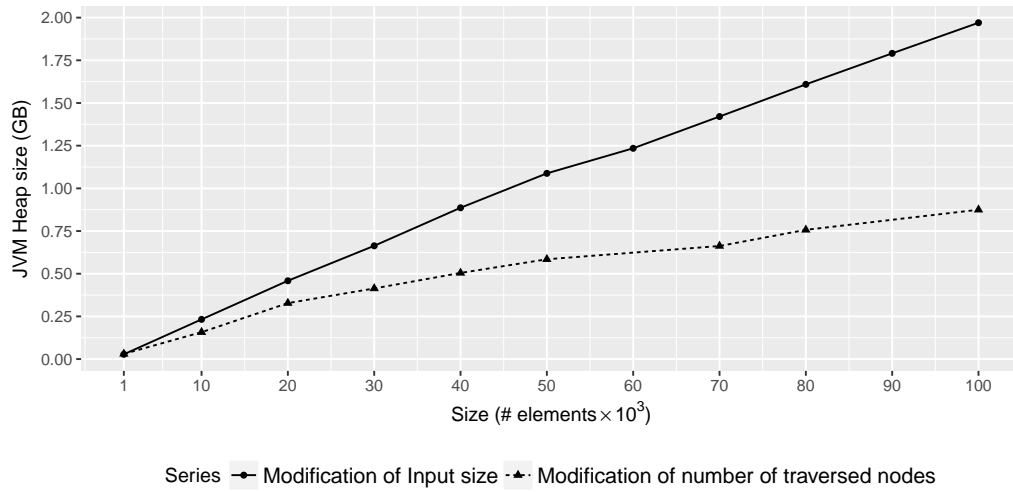
Discussion

By linking context, actions, and requirements using decisions, data extraction for explanation or fault localization can be achieved by performing common temporal graph traversal operations. In the detailed example, we show how a stakeholder could use our approach to define the different elements required by such systems, to structure runtime data, finally, to diagnose the behavior of adaptation processes.

Our implementation allows to dynamically load and release nodes during the execution of a graph traversal. Using this feature, only the needed elements are kept in the main memory. Hence, we can perform interactive diagnosis routines on large graphs with an acceptable memory footprint. However, the performance of our solution, in terms of memory and execution time, is restricted by the number of traversed elements and the number of input elements. Indeed, as shown in our



(a) Evolution of the execution time



(b) Evolution of the memory consumption

Figure 3.14: Results of experiments when the number of traversed or input elements increases
(fig:exp-res)

1 experimentation, both the execution time and the memory consumption grow linearly.

2 In the Luxembourg smart grid, a district contains approximatively 3 data con-
3 centrators and 227 meters⁸. Counting the global datacenter, the network is thus
4 composed of 231 elements. Each meter sends the consumption value every 15 min,
5 being 908 every hours. Plus, there is from 0 to 273 topology modifications in the
6 network. In total, the system generates from 908 to 1,181 new values every hour. If we
7 consider that we have one model element per smart grid entity and one model element
8 per new value, 100,000 model elements correspond thus from $((100,000 - 231) * 1H) / 1,$
9 $181 = 84,5H$ ($\sim 3,5$ days) to $((100,000 - 231) * 1H) / 908 = 109,9H$ ($\sim 4,6$ days) of
10 data. In other word, our approach can efficiently interrogate up to ~ 5 days history
11 data in 2.4s of one district.

12 Conclusion

km:conclusion> 13 Adaptive systems are prone to faults given their evolving complexity. To enable
14 interactive diagnosis over these systems, we proposed a temporal data model to
15 abstract and store knowledge elements. We also provided a high-level API to specify
16 and perform diagnosis algorithms. Thanks to this structure, a stakeholder can
17 abstract and store decisions made by the adaptation process and link them to their
18 circumstances –targeted requirements and used context– as well as their impacts.
19 In our evaluation, we showed that our solution can efficiently handle up to 100 000
20 elements, in a single machine. This size is comparable to 5 days history of one district
21 in the Luxembourg smart grid.

22 Throughout this work, we assumed that designers are able to link actions with
23 their expected impacts at design time. However, this is not always true. Some
24 impacts cannot be known in advance. In this perspective, in addition to the future
25 plans already mentioned throughout the paper, we will investigate techniques to
26 identify unknown impacts on the context model, for instance, by studying the use
27 of machine learning techniques. In order to improve the accuracy and correctness

⁸Previously, our studies uses the data described in [DBLP:conf/smartgridcomm/0001FKTPTR14] which corresponded to the all Luxembourg at this date. Since 2014, the smart grid has been more and more deployed. Numbers present in this paper now correspond more to one district.

1 of diagnosis routines, another aspect to be considered for future work is handling
2 uncertainty in self-adaptive systems. Understanding the effect of uncertainty on the
3 development of self-adaptive systems and their diagnosis is still an open question.
4 We plan to explore this research direction by answering the following questions: How
5 to represent and express uncertainty in self-adaptive systems at design time? How to
6 efficiently interrogate data with uncertainty in self-adaptive systems, for instance, for
7 troubleshooting purpose?

1

2 **State of the art**

3 **Contents**

4	4.1 Introduction	52
---	-----------------------------------	-----------

5
6
7
8

9 *This chapter reviews work related to the one presented in this dissertation.*

1 Introduction

2 **Delayed actions** General research question:

3 **RQ1:** Do current state of the art solutions allow modeling and reasoning over
4 delayed actions?

5 Sub research questions:

- 6 • **RQ1.1:** How current approaches model the evolution of the context and/or the
7 evolution of the behavior of systems over time?
- 8 • **RQ1.2:** Do these solutions model actions, their circumstances and their effects?
- 9 • **RQ1.3:** What are the solutions that enable the reasoning over the evolving
10 context and/or behavior of systems?

11 **Uncertainty** Snowballing approach [DBLP:conf/ease/Wohlin14]

12 Inclusion criteria

- 13 • **IC1:** The paper has been published before the May 31 2019
- 14 • **IC2:** The paper is available online and written in English
- 15 • **IC3:** The paper describes a modeling approach that abstract the context or
16 behavior of a system or an approach that enables to reason or navigate through
17 a temporal model.

18 Exclusion criteria

- 19 • **EC1:** The paper has at most 4 pages (short paper).
- 20 • **EC2:** The paper presents a work in progress (workshop papers), a poster, a
21 vision, a position, doctoral studies or the paper is a Bachelor, Master or PhD
22 dissertation.
- 23 • **EC3:** The paper describes a secondary study (*e.g.*, literature reviews, lessons
24 learned).
- 25 • **EC4:** The document has not been published in a venue with a peer-review
26 process. For example, technical and research report or white papers.
- 27 • **EC5:** The document is an introduction to the proceedings of a venue or a
28 special issue or it is a guest paper.

₁ However, the references of papers rejected are considered for the snowballing
₂ iteration.

List of publications and tools

Papers included in the dissertation

- 2018
 - DBLP:conf/icac/MoulineBFBB18
 - DBLP:conf/sac/MoulineB0FBMB18
- in the process of submission
 - insubmission:2019:comlan:datauncertainty

Papers not included in the dissertation

- 2017
 - DBLP:conf/models/Benelallam0MFBB17
 - DBLP:conf/programming/Mouline0FTBB17
- 2018
 - DBLP:conf/mobiquitous/GuineaBMT18

Tools included in the dissertation

- Ain'tea: a language which integrated data uncertainty as a first-class citizen
 - <https://github.com/lmouline/aintea>
- LDAS: a meta-model of knowledge for adaptive systems
 - <https://github.com/lmouline/LDAS>

1 Abbreviations

2 **CPS** Cyber-Physical System. 2

3 **ICT** Information and communication technology. 2

4 **MAPE-k** Monitor, Analyze, Plan, and Execute over knowledge. 33, *Glossary:*

5 MAPE-k

6 **MDE** Model-Driven Engineering. 3

Glossary

- action** In this document, I use the definition provided by IEEE Standards [iso2017systems]: “Process that, given the context* and requirements* as input, adjusts the system behavior”. 21, 22
- adaptive system** In this document, I modified the definition of self-adaptive systems provided by Cheng *et al.*, in [DBLP:conf/dagstuhl/ChengLGIMABBBCSDFGGGKKKLMMMP]: Adaptive systems are able to have their behavior adjusted in response to the perception of the environment and the system themselves. If a system perform this adjustment on itself, the literature refers to it as self-adaptive system.. 3, 4
- circumstance** State of the knowledge* when a decision* has been taken. 22
- context** In this document, I use the definition provided by Anind K. Dey [DBLP:journals/puc/Dey01]: “Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and [the system], including the user and [the system] themselves”. 21, 22, 27, 33
- decision** A set of actions* taken after comparing the state of the knowledge* with the requirement*. 22, 33
- knowledge** The knowledge of an adaptive system gathers information about the context*, actions* and requirements*. 21–23, 32, 33
- MAPE-k** A theoretical model of the adaptation process proposed by Kephart and Chess [DBLP:journals/computer/KephartC03]. It divides the process in four

1 stages: monitoring, analysing, planning and executing. These four stages share a
2 knowledge*. 33, *Abbreviation*: MAPE-k

3 **metamodel** In this document, I use the definition provided by Ed Seidewitz [DBLP:journals/softw
4 “A metamodel is a specification model for a class of [system under study] where
5 each [system under study] in the class is it-self a valid model expressed in a certain
6 modeling language”. 32, 33

7 **models@run.time** In this document, I use the definition provided by Blair *et*
8 *al.*, [DBLP:journals/computer/BlairBF09]: “A model@run.time is a causally
9 connected self-representation of the as-sociated system that emphasizes the structure,
10 behavior, or goals of the system from a problem space perspective”. 3

11 **requirement** In this document, I use the definition provided by IEEE Standards [iso2017systems]
12 “(1) Statement that translates or expresses a need and its associated constraints
13 and conditions, (2) Condition or capability that must be met or possessed by a
14 system [...] to satisfy an agreement, standard, specification, or other formally imposed
15 documents”. 21, 22, 33

16 **self-adaptive system** See adaptive system*. 2

17 **self-healing system** In this document, I use the definition provided by Jeffrey
18 O. Kephart and David M. Chess [DBLP:journals/computer/KephartC03]: “[A
19 self-healing] system automatically detects, diagnoses, and repairs localized software
20 and hardware problems”. 2

21 **smart grid** In this document, I use the definition provided by the National Institute of
22 Standards and Technology (NIST)* [NIST:SmartGrid:Def:What]: “a modernized
23 grid that enables bidirectional flows of energy and uses two-way communication and
24 control capabilities that will lead to an array of new functionalities and applications.”.

25 2