

₁ A Unified Modeling Framework to Abstract
₂ Knowledge of Dynamically Adaptive Systems

₃ Ludovic Mouline

₄ April 23, 2019

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 neither present in the model nor not considered by the adaptation process, then the adaptation

1 process may make suboptimal reconfiguration decision.

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

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

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

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

27 **Through this thesis, I argue that this data uncertainty and this delay**
28 **cannot be ignored for all dynamic adaptive systems.** To know if the data un-
29 certainty should be considered, stakeholders should wonder **if this data uncertainty**

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

1 **affects the result of their reasoning process, like adaptation.** Regarding delayed
2 action, they should verify **if the frequency of the monitoring stage is lower than**
3 **the time of action effects to be measurable.** These characteristics are common
4 to smart grids, cloud infrastructure or cyber-physical systems in general.

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

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

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

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

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

26 The language, named Ain'tea, integrates data uncertainty as a first-class concept. It
27 allows developers to attach data with a probability distribution which represents their
28 uncertainty. Plus, it mapped all arithmetic and boolean operators to uncertainty prop-
29 agation operations. And so, developers will automatically propagate the uncertainty

1 of data without additional effort, compared to an algorithm which manipulates certain
2 data.

3 *Validation* Each contribution has been evaluated separately. The language has been
4 evaluated through two axes: its ability to detect errors at development time and its
5 expressiveness. Ain'tea can detect errors in the combination of uncertain data earlier
6 than state-of-the-art approaches. The language is also as expressive as current ap-
7 proaches found in the literature. Moreover, we use this language to implement the load
8 approximation of a smart grid furnished by an industrial partner, Creos S.A.².

9 The context model has been evaluated through the performance axis. The disser-
10 tation shows that it can be used to represent the Luxembourg smart grid. The model
11 also provides an API which enables the execution of query for diagnosis purpose. In
12 order to show the feasibility of the solution, it has also been applied to the use case
13 provided by the industrial partner.

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

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

1 Table of Contents

2	1 Introduction	1
3	1.1 Introduction	2
4	1.2 Use case: Luxembourg smart grid	2
5	1.3 General background	2
6	2 TKM: a temporal knowledge model	3
7	2.1 Introduction	4
8	2.2 Knowledge formalization	6
9	2.2.1 Formalization of the temporal axis	6
10	2.2.2 Formalism	7
11	2.2.3 Application on the use case	12
12	2.3 Modeling the knowledge	16
13	2.3.1 Parent element: <i>TimedElement</i> class	17
14	2.3.2 Knowledge metamodel	17
15	2.3.3 Context metamodel	18
16	2.3.4 Requirement metamodel	19
17	2.3.5 Action metamodel	20
18	Abbreviations	i
19	Glossary	iii
20	Bibliography	v

1

2 Introduction

3 Contents

4	1.1 Introduction	2
5		
6	1.2 Use case: Luxembourg smart grid	2
7		
8	1.3 General background	2
10		

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

1 Introduction

2 Use case: Luxembourg smart grid

3 Should contain: - veg iqu grqaub

4 General background

5 should contain: - MDE / metamodel / model - DAS

TKM: a temporal knowledge model to represent actions, their contexts and their impacts

Contents

2.1 Introduction	4
2.2 Knowledge formalization	6
2.3 Modeling the knowledge	16

Abstract: *Adaptation processes are executed with a high frequency to react to any incidents whereas the execution of their decisions is constrained by the executions of delayed actions. We identified two problems that result from these different paces. First, unfinished actions, together with their expected effects, over time are not considered, leading upcoming analysis phases potentially make suboptimal decisions. Second, explanation of the adaptation process remains 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 through a use case based on the smart grid at Luxembourg. We also demonstrate its scalability both in terms of execution time and consumed memory.*

1 Introduction

2 Adaptive systems have the capabilities of adjusting their behavior to dynamic
3 changes encountered in their environments [?]. To do so, they make adaptation de-
4 cisions, in the form of actions, based on high-level policies. These adaptations are often
5 relevant to achieving a goal or an objective while satisfying a set of constraints [?].
6 One of the successful approaches used to achieve this adaptability is the closed con-
7 trol loop paradigm, in particular, the MAPE-K loop [?]. It consists of monitoring the
8 well-behaving of the system with regards to a set of requirements, either functional or
9 non-functional. Once the system deviates from its normal behavior, the control loop se-
10 lects and executes a set of actions (adaptation tactic) to remediate the system behavior.

11 Faced with growingly complex and large-scale software systems (e.g. smart grid sys-
12 tems), we can all agree that the presence of residual defects becomes unavoidable [?].
13 Even with a meticulous verification or validation process, it is very likely to run into an
14 unexpected behavior that was not foreseen at design time. Alone, existing formal mod-
15 eling and verification approaches may not be sufficient to anticipate these failures [?].
16 As such, complementary techniques need to be proposed to locate the anomalous be-
17 havior and its origin in order to handle it in a safe way.

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

24 Bencomo *et al.*, [?] argue that comprehensive explanation about the system be-
25 havior contributes drastically to the quality of the diagnosis, and eases the task of
26 troubleshooting the system behavior. To enable this, we believe that adaptive software
27 systems should be equipped with traceability management facilities to link the deci-
28 sions made to their **(i) circumstances, that is to say, the history of the system**
29 **states and the targeted requirements, and (ii) the performed actions with**
30 **their impact(s) on the system.** In particular, an adaptive system should keep

1 **a trace of the relevant historical events.** Additionally, it should be able to **trace**
2 **the goals intended to be achieved by the system to the adaptations and**
3 **the decisions that have been made, and vice versa.** Finally, in order to enable
4 developers to interact with the system in a clear and understandable way, appropriate
5 abstraction to **enable the navigation of the traces and their history should also**
6 **be provided.**

7 Existing approaches [?] are accompanied by built-in monitoring rules and do not
8 allow to interact with the underlying system in a simple way. Moreover, they do not
9 keep track of historical changes as well as causal relationships linking requirements to
10 their corresponding adaptations. Only flat execution logs are stored.

11 In this paper, we propose a framework to structure and store the state and behavior
12 of a running adaptive system, together with a high-level API to efficiently perform
13 diagnosis routines. Our framework relies on a temporal model-based solution that
14 efficiently abstracts decisions and their corresponding circumstances. Specifically, based
15 on existing approaches for modeling and monitoring adaptation processes, we identify
16 a set of properties that characterize context, requirements, and actions in self-adaptive
17 systems. Then, we formalize the common core concepts implied in adaptation processes,
18 also referred to as knowledge, by means of temporal graphs and a set of relations
19 that trace decisions impact to circumstances. Finally, thanks to exposing common
20 interfaces in adaptive processes, existing approaches in requirements and goal modeling
21 engineering can be easily integrated into our framework.

22 The rest of the paper is structured as follows. We first describe a guidance example
23 in Section ??, based on the smart grid system at Luxembourg. In Section ??, we
24 summarize core concepts manipulated in adaptation processes and their characteristics.
25 Then, we provide a formal definition of these concepts in Section ??. Later, we describe
26 the proposed data model in Section ??. In Section ??, we demonstrate the applicability
27 of our approach by applying it to the smart grid example. Before concluding the paper
28 in Section ??, we introduce some related work in Section ??.

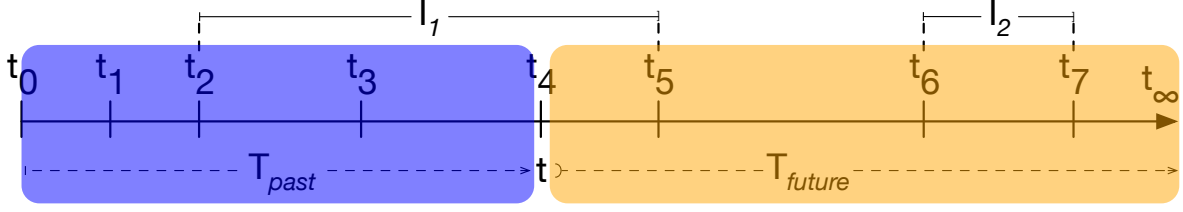


Figure 2.1: Time definition used for the knowledge formalism

Knowledge formalization

As discussed previously, I consider **knowledge** to be the association of **context** information, **requirements**, and **action** information, all in one global and unified 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. The **actions**, on the other hand, are means to reach the goals of the system.

In this section, I 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 seems to be 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, I describe the semantic used for the temporal axis. Then, I exemplify the knowledge formalism using the Luxembourg smart grid use case.

Formalization of the temporal axis

The formalism describe 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 estimated (or predicted data). Second, it should permit the definition of the life cycle of an element

1 of the **knowledge**, which can be seen as a succession of states with a validity period that
 2 should not overlap each other.

3 Time space T is considered as an ordered discrete set of time points non-uniformly
 4 distributed. As depicted in Figure 2.1, this set can be divided into 3 different subsets
 5 $T = T_{past} \cup \{t\} \cup T_{future}$, where:

- 6 • T_{past} is the sub-domain $\{t_0; t_1; \dots; t_{current-1}\}$ representing graph data history start-
 7 ing from t_0 , the oldest point, until current time, t , excluded.
- 8 • $\{t\}$ is a singleton representing the current time point
- 9 • T_{future} is sub-domain $\{t_{current+1}; \dots; t_\infty\}$ representing future time points

10 The three domains depend completely on the current time $\{t\}$ as these subsets slide
 11 as time passes. At any point in time, these domains never overlap: $T_{past} \cap \{t\} = \emptyset$,
 12 $T_{future} \cap \{t\} = \emptyset$, and $T_{past} \cap T_{future} = \emptyset$. The definition of these three subsets reaches
 13 the first goal.

14 In addition, there is a right-opened time interval $I \in T \times T$ as $[t_s, t_e)$ where $t_e - t_s > 0$.
 15 In English words, it means that the interval cannot represent a single time point and
 16 should follow the time order. For any $i \in I$, $start(i)$ denotes its lower bound and $end(i)$
 17 its upper bound. As detailed in Section 2.2.2, these intervals are used to define the
 18 validity period for each node of the graph.

19 Figure 2.1 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,
 20 the current time is $t = t_4$. According to the definition of the past subset (T_{past}) and
 21 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
 22 intervals have been defined on T_1 , namely I_1 and I_2 . The first one starts at t_2 and ends
 23 at t_5 and the last one is defined from t_6 to t_7 . As shown with I_1 , an interval could be
 24 defined on different subsets, here it is on all of them (T_{past} , t , and T_{future}).

25 Formalism

26 **Graph definition** First, let K be an adaptive process over a system **knowledge** rep-
 27 resented by a graph such as $K = (N, E)$, comprising a set of nodes N and a set of edges
 28 E . Nodes represent any element of the knowledge (context, actions, *etc.*) and edges
 29 represent their relationships. Nodes have a set of attribute values. An attribute value

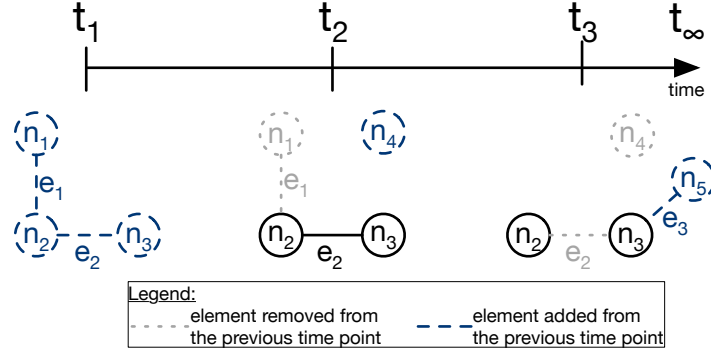


Figure 2.2: Evolution of a temporal graph over time

has a type (numerical, boolean, ...). Every relationship $e \in E$ can be considered as a couple of nodes $(n_s, n_t) \in N \times N$, where n_s is the source node and n_t is the target node.

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

A node is considered valid either until it is removed or until one of its attributes value changes. In the latter case, a new node with the updated value is created. Whilst, an edge is considered valid until either its source node and target node is valid, or until the edge itself is removed. Otherwise, nodes and edges are considered invalid. The temporal validity relation is defined as $V^T : N \cup E \rightarrow I$. It takes as a parameter a node or an edge ($k \in N \cup E$) and returns a time interval ($i \in I$, cf. Section 2.2.1) during which the graph element is valid.

Figure 2.2 shows an example of a temporal graph K_1 with five nodes (n_1, n_2, n_3, 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 way, K_1 equals to $(\{n_1, n_2, n_3, n_4, n_5\}, \{e_1, e_2, e_3\}, V_1^T)$. Let's assume that the graph is created at t_1 . As n_1 is modified at t_2 , its validity period starts at t_1 and ends at t_2 : $V_1^T(n_1) = [t_1, t_2)$. n_2 and n_3 are not modified; their validity period thus starts at t_1 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 , 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 . As

1 n_1 is being modified at t_2 , its validity period goes from t_1 to t_2 : $V_1^T(e_1) = [t_1, t_2)$. e_2 is
2 deleted at t_3 . Its validity period is thus equal to: $V_1^T(e_2) = [t_1, t_3)$.

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

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

13 In order to consider this new relation in the example presented in Figure 2.2, the
14 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 Fig-
15 ure 2.2, let's imagine that n_1 , n_4 , and n_5 represent the same knowledge element k_e .
16 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 node
22 input (n_1 , n_4 , or n_5): $Z_1^T(n_4, t_1) = n_1$. On the other hand, applying the same relation
23 with another node (n_2 or n_3) returns another node. For example, if n_2 and n_3 do not
24 belongs to the same knowledge element, then it will return the node given as input, for
25 example $Z_1^T(n_2, t_1) = n_2$.

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

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

7 Using a high level overview, these processes can be depicted as: taking the knowl-
 8 edge as input, perform task, and modify this knowledge as output. As detailed in the
 9 next two paragraphs, they can be formalized by relations.

10 **Temporal queries for requirements** At the current state, the formalism of the
 11 knowledge K do not contain any information regarding the requirement processes. To
 12 overcome this, system requirements processes R_P are added such as $K = (N, E, V^T, Z^T,$
 13 $R_P)$. R_P is a set of patterns $P_{[t_j, t_k]}(K)$ and queries Q over these patterns: $R_P = P \cup Q$.

14 $P_{[t_j, t_k]}$ denotes a temporal graph pattern, where t_j and t_k are the lower and upper
 15 bound of the time interval respectively. The time interval can be either fixed (absolute)
 16 or sliding (relative). Each element of the pattern should be valid for at least one time
 17 point: $\forall p \in P_{[t_j, t_k]}, V^T(e) \cap [t_j, t_k] \neq \emptyset$. Patterns can be seen as temporal subgraph
 18 of K , with a time limiting constraint coming in the form of a time interval. Temporal
 19 graph queries Q consist commonly of two parts: (i) path description to traverse the
 20 graph nodes, at both structural and temporal dimensions; (ii) arithmetic expressions
 21 on nodes, edges, and attribute values.

22 **Temporal relations for actions** Like for R_P , the knowledge K needs to be aug-
 23 mented with the action processes A_P : $K = (N, E, V^T, Z^T, R_P, A_P)$. Actions processes
 24 A_P can be regarded as a set of relations or isomorphisms mapping a source temporal
 25 graph pattern $P_{[t_j, t_k]}$ to a target one $P_{[t_l, t_m]}$, $A_P : K \times I \rightarrow K \times I$.

26 The left-hand side of the relation depicts the temporal graph elements over which
 27 an action is applied. Every relation may have a set of application conditions. They
 28 describe the circumstances under which an action should take place. These application
 29 conditions are either positive, should hold, or negative, should not hold. Application
 30 conditions come in the form of temporal graph invariants. The side effects of these

1 actions are represented by the right-hand side.

2 Finally, we associate to A_P a temporal function E_{A_P} to determine the time interval
3 at which an action has been executed. Formally, $X : A \rightarrow I$.

4 **Temporal relations for decisions** Finally, the knowledge formalism needs to in-
5 clude the last, but not the least, element: decisions made by the adaptation, $K = (N,$
6 $E, V^T, Z^T, R_P, A_P, D)$ While the source of relations in D represents the state before
7 the execution of an action, the target shows its impact on the **context**. Its intent is
8 **to trace back impacts of actions execution to the decisions they originated**
9 **from**.

10 A decision present in D is defined as a set of executed actions, *i.e.*, a subset of A_P .
11 Formally, $D = \{ A_D \cup R_D \mid A_D \subseteq A_P, R_D \subseteq R_P \}$. We assume that each action should
12 result from one decision: $\forall a \in A, \forall d1, d2 \in D \mid a \in d1 \wedge a \in d2 \rightarrow d1 = d2$.

13 The temporal function E_{A_P} is extended to decision in order to represent the execu-
14 tion time: $E_{A_P} : (A \cup D) \rightarrow I$. For decision, the lower bound of the interval correspond
15 to the lowest bound of the action execution intervals. Following the same principle, the
16 upper bound of the interval correspond to the uppermost bound of the action execu-
17 tion intervals. Formally, $\forall d \in D \rightarrow E_{A_P}(d) = [l, u]$, where $l = \min_{a \in A_d} \{E_{A_P}(a)[start]\}$ and
18 $u = \max_{a \in A_d} \{E_{A_P}(a)[end]\}$.

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

- 21 • N is a set of nodes to represent the different information (context, actions and
22 requirements)
- 23 • E is a set of edges with connect the different nodes,
- 24 • V^T is a temporal relation which defines the temporal validity of each elements,
- 25 • Z^T is a relation to track the history of each knowledge elements,
- 26 • R_P is a relation that define the different requirements processes,
- 27 • A_P is a relation that define the different action processes,
- 28 • D is a set of action processes that result from a same decision.

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

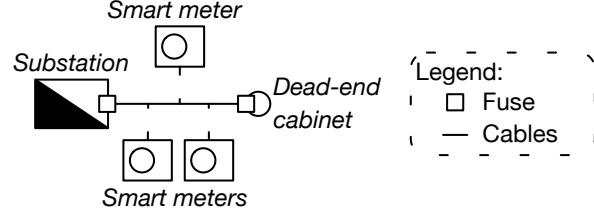


Figure 2.3: Simplified version of a smart grid

Figure 2.4: Representation of the smart grid context depicted in Figure 2.3

Application on the use case

The example presented in Section 1.2 contain too much detail to provide a readable and understandable example of the formalism. Below, an excerpt of it is thus presented in order to overcome this problem.

Excerpt of a smart grid Figure 2.3 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 a fuse. The meters regularly send consumption data at the same time. One requirement is considered for this example: minimizing the number of overloads. To achieve so, among the different actions, two actions are taken into account in this example: decreasing or increasing the amps limits of smart meters.

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 2.4 shows the nodes and edges of this knowledge.

Scenario The system starts at t_0 with the actions, the requirements and the context, which also include initial value for the consumption values. Meters send their values at t_2 and t_3 . Based on these data, the load on cables and substation is computed. On t_2 , an overload is detected on the cable, which break the requirement. At the same time point, the system decides to reduce the load of all smart meters. The impact of these actions will be measured at t_4 , *i.e.*, the cable will not be overloaded from t_4 .

1 **Description of N_{SG}** N_{SG} is divided into three subset: C_{SG} , R_{SG} and A_{SG} . R_{SG}
2 contains one node, R_1 in Figure 2.4, which represents the requirement of this example:
3 $R_{SG} = \{R_1\}$ Two nodes, A_1 and A_2 , belong to A_{SG} : $A_{SG} = \{A_1, A_2\}$. They represent
4 represent the two actions of this example, respectively decreasing and increasing amps
5 limits. Regarding the context C_{SG} , there is three nodes to represent the three smart
6 meters (M_1 , M_2 , and M_3), one for the substation (S_1), two for the fuses (F_1 and F_2),
7 one for the dead-end cabinet (D_{C_1}) and one node per consumption value received (V_i):
8 $C_{SG} = \{M_1, M_2, M_3, S_1, F_1, F_2, D_{C_1}\} \cup \{V_i | i \in [1..9]\}$.

9 According to the scenario, all nodes are created at t_0 and are never modified, except
10 for nodes to store consumption values. Therefore, their validity period starts at t_0
11 and never ends: $\forall n \in A_{SG} \cup R_{SG} \cup \{M_1, M_2, M_3, S_1, F_1, F_2, D_{C_1}\}, V_{SG}^T(n) = [t_0, t_\infty)$.
12 Considering the consumption values, all the nodes represent the history of the values
13 for the three smart meters. In other words, there is three knowledge element: the
14 consumption measured for each meter. Let C_i notes the consumption measured by the
15 smart meter M_i . As shown in Figure 2.4, there is:

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

19 Taking C_2 as example, V_2 is the initial consumption value, replaced by V_5 at t_1 , itself
20 replaced by V_8 at t_2 . Applying the V_{SG}^T on these different values, results are thus:

- 21 • $V_{SG}^T(V_2) = [t_0, t_1)$,
- 22 • $V_{SG}^T(V_5) = [t_1, t_2)$,
- 23 • $V_{SG}^T(V_8) = [t_2, t_\infty)$.

24 These validity periods are shown in Figure 2.5a. As meters send the new consumption
25 values at the same time, this example can be also applied to C_1 and C_3 .

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

- 29 • $Z_{SG}^T(V_2, t_{s1}) = V_2$, where $t_0 \leq t_{s1} < t_1$

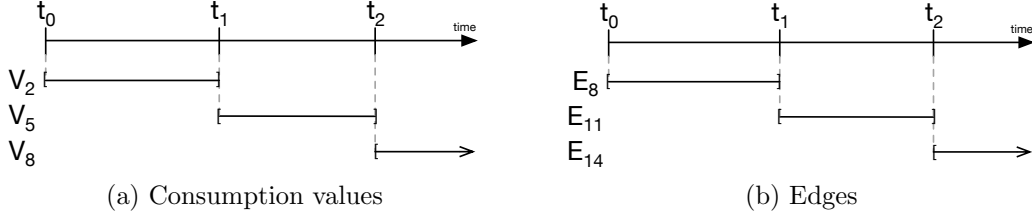


Figure 2.5: Validity periods of the consumptions values and their edges to the smart meter M_2

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

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

8 One may consider that relations (validity, Z^T , decisions, action processes and re-
9 quirements processes) will be stored as edges. But, this decision is let to the implemen-
10 tation part of this formalism.

11 In our model, only consumption values (V_i nodes) are modified. Plus, since the
12 scenario do not imply other edges modifications, only those between meters and values
13 are modified. The edge set contains thus sixteen edges: $E_{SG} = \{E_i \mid i \in [1..16]\}$.

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

- 18 • C_1 impacts edges between M_1 and V_1 , V_4 , and V_7 , *i.e.*, $\{E_8, E_{11}, E_{14}\}$,
- 19 • C_2 impacts edges between M_2 and V_2 , V_5 , and V_8 , *i.e.*, $\{E_9, E_{12}, E_{15}\}$,
- 20 • C_3 impacts edges between M_3 and V_3 , V_6 , and V_9 , *i.e.*, $\{E_{10}, E_{13}, E_{16}\}$.

21 Continuing with C_2 as example, the initial edge value is E_8 from t_0 , which is replaced

by E_{11} from t_1 , itself replaced by E_{14} from t_2 . The validity relation, applied on these edges, thus returns:

- $V_{SG}^T(E_8) = [t_0, t_1) = V_{SG}^T(V_2)$,
- $V_{SG}^T(E_{11}) = [t_1, t_2) = V_{SG}^T(V_5)$,
- $V_{SG}^T(E_{14}) = [t_2, t_\infty) = V_{SG}^T(V_8)$,

These validity periods are depicted in Figure 2.5b. As they are driven by those of consumption values (V_2 , V_5 , and V_8), they are equals.

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

- $Z_{SG}^T(E_8, t_{s1}) = E_8$, where $t_0 \leq t_{s1} < t_1$,
- $Z_{SG}^T(E_8, t_{s2}) = E_8$, where $t_1 \leq t_{s1} < t_2$,
- $Z_{SG}^T(E_8, t_{s3}) = E_8$, where $t_2 \leq t_{s1} < t_\infty$.

Description of R_{PSG} The requirement calls for minimizing overloads. It means that when the system detects at least one overload, for example in cables, it will take counter actions. As the system has prediction capabilities, it will not only check is there is one at the current time t but also if one will come in the next hour. The pattern will be defined as follow: $P_{[t, t+15min]}$. To determine if there is an overload, the system needs to know: the current and future consumption, the current and future topology. The last one is used to compute the loads from the consumption (cf. Section 1.2).

Let's consider that time points are regular and there is one every 15 minutes and that current time is t_0 . The pattern, $P_{[t_0, t_1]}$, will thus contain all nodes that are valid between t_0 and t_1 (included):

- all topology nodes between: $\{S_1, C_1, F_1, F_2, D_{C_1}, M_1, M_2, M_3\}$
- all consumption values between: $\{V_i \mid i \in [1..6]\}$,
- all edges that connected these nodes: $\{E_i \mid i \in [1..13]\}$

From these values, the loads is computed and the system checks that none will exceed the capacity of the infrastructure (cables, substations, cabinets).

1 **Description of $A_{P_{SG}}$** Now, let us assume that the execution of $R_{P_{SG}}$ detects an
2 overload on the cable (C_1) at t_0 . The system decides to reduce the amps limits, and
3 thus the load, on the three meters. The action A_1 (decreasing amps limits) is thus
4 executed three times: one time per meter. For each of these action, the input context
5 will correspond to the pattern used by the requirement relation: $P_{[t_0, t_1]}$. The output
6 context will contain the predicted values after the actions have been executed. Here, the
7 actions are executed in parallel and their execution time is in seconds. So the impact
8 will be visible from t_1 . So the output pattern contain the three values at t_1 : $P_{[t_1, t_1]}$. In
9 summary:

- 10 • Action 1: $A_{P_1} : P_{[t_0, t_1]} \rightarrow P_{[t_1, t_1]}$,
- 11 • Action 1: $A_{P_2} : P_{[t_0, t_1]} \rightarrow P_{[t_1, t_1]}$,
- 12 • Action 1: $A_{P_3} : P_{[t_0, t_1]} \rightarrow P_{[t_1, t_1]}$.

13 **Description of D_{SG}** Following the scenario, there is one decision, D_{SG_1} , which try
14 to achieve the requirement R_1 by executing the actions A_1 : A_{P_1} , A_{P_2} , and A_{P_3} . Then,
15 here the decision is equals to: $D_{SG_1} = \{R_1, A_{P_1}, A_{P_2}, A_{P_3}\}$.

16 **Summrarize** Through this section, I explified how the formalism can be used to
17 define an adaptation decision on a smart grid system. As the decision contains infor-
18 mation about the circumstances and the impact, one may use it to debug the process
19 and/or try to explain the behavior of such systems.

20 Modeling the knowledge

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

1 the evolution of system but also the evolution of its structure and specification (e.g.
2 evolution of the requirements of the system). Design time elements are depicted in gray
3 in the Figures 2.6– 2.9. Note that, this thesis does not address how runtime information
4 is collected.

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

13 Parent element: *TimedElement* class

14 I assume that all the classes in the different packages extend a *TimedElement* class.
15 This class contains three methods: *startTime*, *endTime*, and *modificationsTime*. The
16 first two methods allow accessing the validity interval bounds defined by the previously
17 discussed V^T relation. The last method resolves all the timestamps at which an element
18 has been modified: its history. This method is the implementation of the relation Z^T
19 described in our formalism (cf. Section 2.2.2).

20 Knowledge metamodel

21 In order to enable interactive diagnosis of adaptive systems, traceability links be-
22 tween the decisions made and their circumstances should be organized in a well-structured
23 representation. In what follows, I introduce how the **knowledge metamodel** helps to de-
24 scribe **decisions**, which are linked to their goals and their context (input and impact).
25 Figure 2.6 depicts this **metamodel**.

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

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

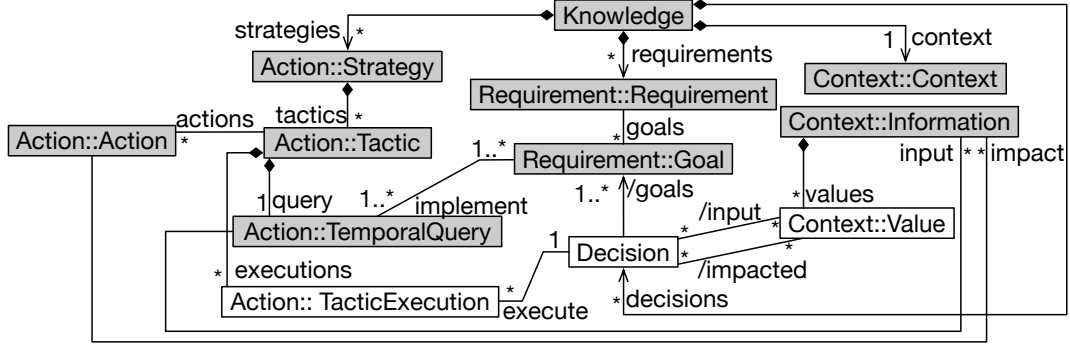


Figure 2.6: Excerpt of the knowledge metamodel

1 decision has an *input* context and an *impacted* context. The context impacted by a deci-
 2 sion (*Decision.impact*) is a derived relationship computed by aggregating the impacts
 3 of all actions belonging to a decision (see Fig. 2.9). Likewise, the *input* relationship is
 4 derived and can be computed similarly. In the smart grid example, a decision can be
 5 formulated (in plain English) as follows: since the district D is almost overloaded (*input*
 6 *context*), we reduce the amps limit of greedy consumers using the “*reduce amps limit*”
 7 *action* in order to reduce the load on the cable of the district (*impact*) and satisfy the
 8 “*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 can
 12 apprehend the possible causes behind malicious behavior by navigating from the context
 13 values to the decisions that have impacted its value (*Property.expected.impact*) and the
 14 goals it was trying to reach (*Decision.goals*). In Section **TODO: add reference**, we
 15 present an 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.

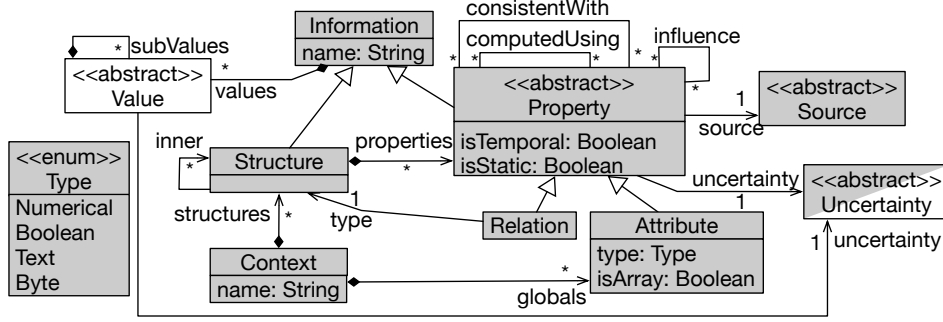


Figure 2.7: Excerpt of the context metamodel

1 An excerpt of the context model is depicted in Figure 2.7. I propose to repre-
 2 sent the context as a set of structures (*Context.structures*) and global attributes (*Con-*
 3 *text.globals*). A structure can be viewed as a C-structure with a set of properties
 4 (*Property*): attributes (*Attribute*) or relationships (*Relation*). A structure may con-
 5 tain other nested structures (*Structure.inner*). Structures and properties have values.
 6 They correspond to the nodes described in the formalization section (cf. Section 2.2.2).
 7 The connection feature described in Section ?? is represented thanks to three recur-
 8 sive relationships on the Property class: *consistentWith*, *computedUsing* and *influence*.
 9 Additionally, each property has a source (*Source*) and an uncertainty (*Uncertainty*). It
 10 is up to the stakeholder to extend data with the appropriate source: measured, com-
 11 puted, provided by a user, or by another system (e.g., weather information coming
 12 from a public API). Similarly, the uncertainty class can be extended to represent the
 13 different kinds of uncertainties. Finally, a property can be either historic or static.

14 Requirement metamodel

15 As different solutions to model system requirements exist (e.g., KAOS [?], i* [?] or
 16 Tropos [?]), in this metamodel, we abstract their shared concepts. The requirement
 17 model, depicted in Figure 2.8, represents the *requirement* as a set of *goals*. Each goal
 18 has a *nature* and a textual specification. The nature of the goals adheres to the four
 19 categories of requirements presented in Section ?. One may use one of the existing
 20 requirements modeling languages (e.g., RELAX) to define the semantics of the require-

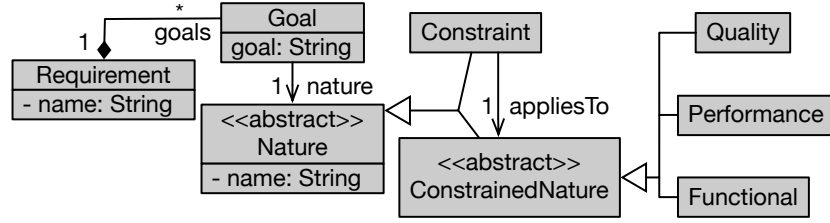


Figure 2.8: Requirement metamodel

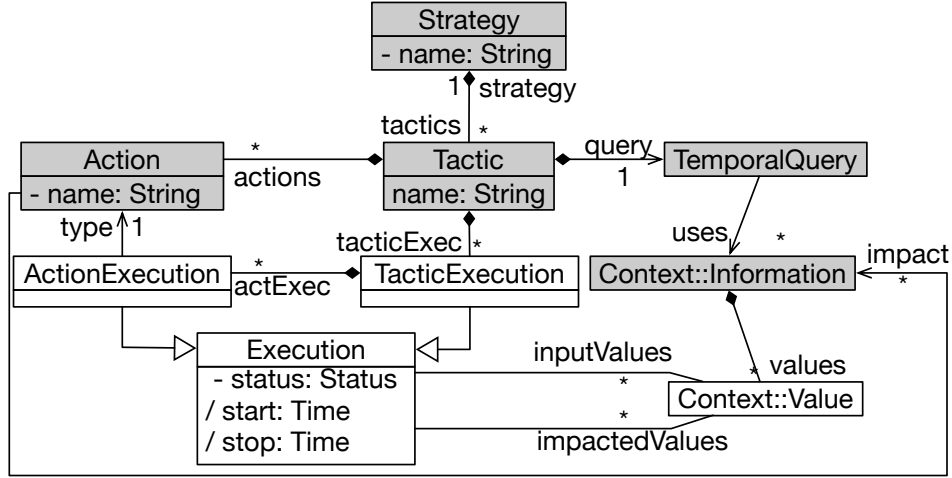


Figure 2.9: Excerpt of the action metamodel

ments. 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 [?] 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) *no overload*, (ii) *no production lack*, (iii) *no production loss*.

Action metamodel

Similar to the requirements metamodel, the actions metamodel also abstracts main concepts shared among existing solutions to describe adaptation processes and how

1 they are linked to the context. Figure 2.9 depicts an excerpt of the action metamodel.
2 I define a strategy as a set of tactics (*Strategy*). A tactic contains a set of actions
3 (*Action*). A tactic is executed under a precondition represented as a temporal query
4 (*TemporalQuery*) and uses different data from the context as input. In future work, we
5 will investigate the use of preconditions to schedule the executions order of the actions,
6 similarly to existing formalisms such as Stitch [?]. The query can be as complex as
7 needed and can navigate through the whole knowledge model. Actions have impacts
8 on certain properties, represented by the *impacted* reference.

9 The different executions are represented thanks to the *Execution* class. Each ex-
10 ecution has a status to track its progress and links to the impacted context val-
11 ues(*Execution.impactedValues*). Similarly, input values are represented thanks to the
12 *Execution.inputValues* relationship. An execution has *start* and *end* time. Not to con-
13 fuse with the *startTime* and *endTime* of the validity relation \mathcal{V}^T . Whilst the former
14 corresponds to the time range in which a value is valid, the *start* and *stop* time in the
15 class execution correspond to the time range in which an action or a tactic was being
16 executed. The start and stop attributes correspond to the relation \mathcal{X} (see Section ??).
17 These values can be derived based on the validity relation. They correspond to the
18 time range in which the status of the execution is "RUNNING". Formally, for every
19 execution node e , $\mathcal{X}(e) = (\mathcal{V}(e) \mid e.status = "RUNNING")$.

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

¹ Abbreviations

² **MAPE-k** Monitor, Analyze, Plan, and Execute over knowledge. ¹⁷, *Glossary*: **MAPE-**
³ **k**

Glossary

action “Process that, given the **context** and **requirements** as input, adjusts the system behavior”, IEEE Standards [III17]. 6

circumstance State of the **knowledge** when a **decision** has been taken. 6

context In this document, I use the definition provided by Anind K. Dey [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”. 6, 11, 17

decision A set of **actions** taken after comparing the state of the **knowledge** with the **requirement**. 6, 17

knowledge The knowledge of an adaptive system gathers information about the **context**, **actions** and **requirements**. 6, 7, 16, 17

MAPE-k A theoretical model of the adaptation process proposed by Kephart and Chess [KC03]. It divides the process in four stages: monitoring, analysing, planning and executing. These four stages share a **knowledge**. 17, *Abbreviation: MAPE-k*

metamodel Through this thesis, I use the definition of Seidewitz: “A metamodel is a specification model for a class of [system under study] where each [system under study] in the class is it-self a valid model expressed in a certain modeling language.” [Sei03]. 16, 17

requirement “(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”, IEEE Standards [III17]. 6, 17

Bibliography

- [Dey01] Anind K. Dey. Understanding and using context. *Personal and Ubiquitous Computing*, 5(1):4–7, 2001. URL: <https://doi.org/10.1007/s007790170019>, doi:10.1007/s007790170019. [Cited on page iii]
- [III17] ISO, IEC, and IEEE. Systems and software engineering – vocabulary. In *ISO/IEC/IEEE 24765: 2017 (E)*, pages 1–536. 2017. URL: <https://doi.org/10.1109/IEEESTD.2017.8016712>, doi:10.1109/IEEESTD.2017.8016712. [Cited on pages iii and iv]
- [KC03] Jeffrey O. Kephart and David M. Chess. The vision of autonomic computing. *IEEE Computer*, 36(1):41–50, 2003. URL: <https://doi.org/10.1109/MC.2003.1160055>, doi:10.1109/MC.2003.1160055. [Cited on page iii]
- [Sei03] Ed Seidewitz. What models mean. *IEEE Software*, 20(5):26–32, 2003. URL: <https://doi.org/10.1109/MS.2003.1231147>, doi:10.1109/MS.2003.1231147. [Cited on page iii]