This is a repository copy of Engineering Trustworthy Self-Adaptive Software with Dynamic Assurance Cases.

White Rose Research Online URL for this paper: http://eprints.whiterose.ac.uk/120173/

Version: Accepted Version

Article:
Calinescu, Radu Constantin orcid.org/0000-0002-2678-9260, Weyns, Danny, Gerasimou, Simos et al. (3 more authors) (2017) Engineering Trustworthy Self-Adaptive Software with Dynamic Assurance Cases. IEEE Transactions on Software Engineering. pp. 1-30. ISSN 0098-5589

https://doi.org/10.1109/TSE.2017.2738640

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.
Engineering Trustworthy Self-Adaptive Software with Dynamic Assurance Cases

Radu Calinescu, Danny Weyns, Simos Gerasimou, M. Usman Iftikhar, Ibrahim Habli, and Tim Kelly

Abstract—Building on concepts drawn from control theory, self-adaptive software handles environmental and internal uncertainties by dynamically adjusting its architecture and parameters in response to events such as workload changes and component failures. Self-adaptive software is increasingly expected to meet strict functional and non-functional requirements in applications from areas as diverse as manufacturing, healthcare and finance. To address this need, we introduce a methodology for the systematic ENgineering of TRUstworthy Self-adaptive softWare (ENTRUST). ENTRUST uses a combination of (1) design-time and runtime modelling and verification, and (2) industry-adopted assurance processes to develop trustworthy self-adaptive software and assurance cases arguing the suitability of the software for its intended application. To evaluate the effectiveness of our methodology, we present a tool-supported instance of ENTRUST and its use to develop proof-of-concept self-adaptive software for embedded and service-based systems from the oceanic monitoring and e-finance domains, respectively. The experimental results show that ENTRUST can be used to engineer self-adaptive software systems in different application domains and to generate dynamic assurance cases for these systems.

Index Terms—Self-adaptive software systems, software engineering methodology, assurance evidence, assurance cases.

1 INTRODUCTION

Software systems are regularly used in applications characterised by uncertain environments, evolving requirements and unexpected failures. The correct operation of these applications depends on the ability of software to adapt to change, through the dynamic reconfiguration of its parameters or architecture. When events such as variations in workload, changes in the required throughput or component failures are observed, alternative adaptation options are analysed, and a suitable new software configuration may be selected and applied.

As software adaptation is often too complex or too costly to be performed by human operators, its automation has been the subject of intense research. Using concepts borrowed from the control of discrete-event systems [91], this research proposes the extension of software systems with closed-loop control. As shown in Fig. 1, the paradigm involves using an external software controller to monitor the system and to adapt its architecture or configuration after environmental and internal changes. Inspired by the autonomic computing manifesto [67], [73] and by pioneering work on self-adaptive software [71], [86], this research has been very successful. Over the past decade, numerous research projects proposed architectures [54], [76], [124] and frameworks [15], [43], [109], [123] for the engineering of self-adaptive systems. Extensive surveys of this research and its applications are available in [68], [89], [95].

In this paper, we are concerned with the use of self-adaptive software in systems with strict functional and non-functional requirements. A growing number of systems are expected to fit this description in the near future. Service-based telehealth systems are envisaged to use self-adaptation to cope with service failures and workload variations [15], [44], [120], avoiding harm to patients. Autonomous robots used in applications ranging from manufacturing [40], [58] to oceanic monitoring [19], [55] will need to rely on self-adaptive software for completing their missions safely and effectively, without damage to, or loss of, expensive equipment. Employing self-adaptive software in these applications is very challenging, as it requires assurances about the correct operation of the software in scenarios affected by uncertainty.

Assurance has become a major concern for self-adaptive software only recently [25], [30], [36], [37]. Accordingly, the research in the area is limited, and often confined to providing evidence that individual aspects of the self-adaptive software are correct (e.g. the software platform used to execute the controller, the controller functions, or the runtime adaptation decisions). However, such evidence is only one component of the established industry process for the assurance of software-based systems [11], [81], [111]. In real-world applications, assuring a software system requires the provision of an assurance case, which standards such as [112] define as

"a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment".

---

R. Calinescu, S. Gerasimou, I. Habli and T. Kelly are with the Department of Computer Science at the University of York, UK.
D. Weyns is with the Department of Computer Science of the Katholieke Universiteit Leuven, Belgium.
M. U. Iftikhar is with the Department of Computer Science at Linnaeus University, Sweden.

---

Fig. 1. Closed-loop control is used to automate software adaptation
Our work addresses this discrepancy between the state of practice and the current research on assurances for self-adaptive software. To this end, we introduce a generic methodology for the joint development of trustworthy self-adaptive software systems and their associated assurance cases. Our methodology for the ENgineering of TRUstworthy Self-adaptive soFtWare (ENTRUST) is underpinned by a combination of (1) design-time and runtime modelling and verification, and (2) an industry-adopted standard for the formalisation of assurance arguments [60], [102].

ENTRUST uses design-time modelling, verification and synthesis of assurance evidence for the control aspects of a self-adaptive system that are engineered before the system is deployed. These design-time activities support the initial controller enactment and the generation of a partial assurance case for the self-adaptive system. The dynamic selection of a system configuration (i.e., architecture and parameters) during the initial deployment and after internal and environmental changes involves further modelling and verification, and the synthesis of the additional assurance evidence required to complete the assurance case. These activities are fully automated and carried out at runtime.

The ENTRUST methodology is not prescriptive about the modelling, verification and assurance evidence generation methods used in its design-time and runtime stages. This generality exploits the fact that the body of evidence underpinning an assurance case can combine verification evidence from activities including formal verification, testing and simulation. As such, ENTRUST assurance cases can use assurance evidence obtained through a combination of testing, simulation and formal verification, at both design-time and runtime.

ENTRUST supports the systematic engineering and assurance of self-adaptive systems. In line with other research on self-adaptive systems (see e.g. [95], [122]), we assume that the controlled software system from Fig. 1 already exists, and we focus on its enhancement with self-adaptation capabilities through the addition of a high-level monitor-analyse-plan-execute (MAPE) control loop. The components of the controlled software system may already support low-level, real-time adaptation to localised changes. For instance, the self-adaptive embedded system used in one of our case studies is a controlled unmanned vehicle that employs built-in low-level control to maintain the speed selected by its high-level ENTRUST controller. Mature approaches from the areas of robust control of discrete-event systems (e.g. [80], [91], [107], [126]) and real-time systems (e.g. [77], [82]) already exist for the engineering of such low-level control. Thus, real-time control is outside the scope of ENTRUST.

Likewise, established assurance processes are available for the non-self-adaptive aspects of software systems (e.g. [10], [11], [62], [65], [94]). We do not duplicate this work. Using these processes to construct assurance arguments for the correct design, development and operation of the controlled software system, and for the derivation, validity, completeness and formalisation of the requirements from Fig. 1 is outside the scope of our paper. Thus, ENTRUST focuses on the correct engineering of the controller and on the correct operation of self-adaptive system, assuming that the controlled system and its requirements are both correct.

The main contributions of our paper are:

1) The first end-to-end methodology for (a) engineering self-adaptive software systems with assurance evidence for the controller platform, its functions and the adaptation decisions; and (b) devising assurance cases whose assurance arguments bring together this evidence.

2) A novel assurance argument pattern for self-adaptive systems, expressed in the Goal Structuring Notation (GSN) standard [60] that is widely used for assurance case development in industry [102].

3) An instantiation of our methodology whose stages are supported by the established modelling and verification tools UPPAAL [7] and PRISM [79].

These contributions include four significant extensions of complementary results from our previously separate strands of work on developing formally verified control loops [69], runtime probabilistic model checking [20] and dynamic assurance cases [38]. First, the instantiation of the ENTRUST methodology is based on a formally verifiable controller architecture where the controller from [69] was extended to use probabilistic model checking at runtime [20]. Second, we introduce a set of generic properties that ENTRUST controllers must satisfy. Third, we extend our preliminary work from [38] with a realisation of the principles of dynamic assurance case continuity, updatability, proactivity, automation and formality that we suggested in [38]. Fourth, we devise the first assurance argument pattern for self-adaptive systems. In addition, we integrate these extended building blocks into a complete methodology for the engineering of self-adaptive systems.

To ensure the generality of ENTRUST, these contributions are evaluated using two case studies with different characteristics (e.g. types of system, requirements and adaptation actions) and belonging to different application domains (i.e. oceanic monitoring and exchange trade). We chose for these case studies systems that have been used to evaluate related software engineering research [19], [55], [57], [98], as these systems are already known to the research community – one of them as an “exemplar” for the evaluation of new approaches to engineering self-adaptive systems [56].

The remainder of the paper is organised as follows. In Section 2, we provide background information on assurance cases, GSN and assurance argument patterns. Section 3 introduces the self-adaptive systems used in our case studies, and Section 4 describes the generic ENTRUST methodology. Sections 5 and 6 present the tool-supported ENTRUST instance and its use to develop the self-adaptive systems from the two case studies, respectively. Section 7 presents our evaluation results, which show that the methodology can be used for the effective engineering of self-adaptive systems from different domains and for the generation of dynamic assurance cases for these systems. In Section 8, we overview the existing approaches to providing assurances for self-adaptive software systems, and we compare them to ENTRUST. Finally, Section 9 concludes the paper with a discussion and a summary of future work directions.

2 Preliminaries
This section provides background information on assurance cases, introducing the assurance-related terminology and
concepts used in the rest of the paper. We start by defining assurance cases and their components in Section 2.1. Next, we introduce a commonly used notation for the specification of assurance cases in Section 2.2. Finally, we introduce the concept of an assurance argument pattern in Section 2.3.

2.1 Assurance Cases

An assurance case\(^1\) is a report that supports a specific claim about the requirements of a system [10]. As an example, the assurance case in [85] provides documented assurance that the “implementation and operation of North European Functional Airspace Block (NEFAB) is acceptably safe according to ICAO, EC and EUROCONTROL safety requirements.” The documented assurance within an assurance case comprises (1) evidence and (2) structured arguments that link the evidence to the claim [10], possibly through intermediate claims.

Assurance cases are becoming mandatory for software systems used in safety-critical and mission-critical applications [11], [81], [111]. They are used in domains ranging from nuclear energy [113] and medical devices [115] to air traffic control [45] and defence [112]. A growing number of assurance cases from these and other domains are openly available (e.g., [85], [114]).

The development of assurance cases comprises processes carried out at all stages of the system life cycle [111]. Requirements analysis evidence and design evidence demonstrate that system reliability, safety, maintainability, etc. are considered in the early stages of the life cycle. Implementation, validation and verification evidence are then generated as the system is developed. Finally, evidence collected at runtime is used to update assurance cases during system maintenance.

As aptly described in [111], the assurance case must be “a living, cradle-to-grave document.” This is particularly true for self-adaptive software systems. For these systems, existing evidence needs to be continuously combined with adaptation evidence, i.e., evidence that the system will continue to operate safely after self-adaptation activities.

1. Assurance cases developed for safety-critical systems are also called safety cases. In this work, we are concerned with any self-adaptive software systems that must meet strict requirements, and therefore we talk about assurance cases and assurance arguments.

2.2 Goal Structuring Notation

The assurance cases for self-adaptive systems introduced later in the paper are devised in the Goal Structuring Notation (GSN) [72], a community standard [60] widely used for assurance case development in industry [102]. The main GSN elements (Fig. 2) can be used to construct an argument by showing how an assurance claim (represented in GSN by a goal) is broken down into sub-claims (also represented by GSN goals), until eventually it can be supported by GSN solutions (i.e., assurance evidence from verification, testing, etc.). Strategies are used to partition the argument and describe the nature of the inference that exists between a goal and its supporting goal(s). The rationale (assumptions and justifications) for individual elements of the argument can be captured, along with the context (e.g. to describe the operational environment) in which the claims are stated.

In a GSN diagram, claims are linked to strategies, sub-claims and ultimately to solutions using ‘supported by’ connectives, which are rendered as lines with a solid arrowhead and declare inferential or evidential relationships. ‘Supported by’ connectives may be decorated with their multiplicity or marked as optional. The ‘in context of’ connective, rendered as a line with a hollow arrowhead, declares a contextual relationship between a goal or strategy on the one hand and a context, assumption or justification on the other hand.

Large or complex sections of the assurance argument can be organised into modules by means of GSN away goals referenced in the main argument and defined separately. Finally, GSN entities can be marked as uninstantiated to indicate that they are placeholders that need to be replaced with a concrete instantiation, and GSN goals can be marked as undeveloped to indicate that they need to be further developed into sub-goals, strategies and solutions.

As an example, Fig. 3 shows a simple GSN assurance argument for the software part of a heating system. Its root goal (Goal 1) claims that the system is safe at all times. This claim is partitioned into sub-claims using a strategy (Strategy 1) that addresses the safety of the two system functions (i.e. control and monitoring) separately through.
Fig. 4. Example of a GSN assurance argument pattern

2.3 Assurance Argument Patterns

To reduce the significant effort required to develop assurance cases, in our previous work on software assurance [62], [64] we collaborated to the creation of a catalog of reusable GSN assurance argument patterns [63]. Each pattern considers the contribution made by the software to system hazards for a particular class of systems and scenarios. The GSN elements of a pattern that are generic to the entire class are fully developed and instantiated, whereas the entities that are specific to each system and scenario within the class are left undeveloped and/or uninstantiated.

As an example, Fig. 4 depicts an assurance argument pattern that is instantiated by the GSN assurance argument from Fig. 3. The elements surrounded by curly brackets ‘{’ and ‘}’ in the pattern must be instantiated for each assurance argument based on the pattern, as further indicated by the triangular ‘uninstantiated’ symbol under the GSN entities that contain them. Goal 2 is marked with both this ‘uninstantiated’ symbol (because it contains elements in curly brackets) and a diamond-shaped ‘undeveloped’ symbol (because, like for the ‘choice’ sub-claims Goal 3 and Goal 4, additional GSN entities must be added underneath to complete the assurance argument); the two symbols are rendered overlapping under Goal 2.

In this paper, we devise a new assurance argument pattern, which is applicable to self-adaptive software systems.

3 Self-adaptive Systems Used in the Case Studies

This section introduces the self-adaptive software systems from the two case studies used to illustrate and evaluate our methodology. To assess the generality of ENTRUST, we chose different types of systems from different domains. The first system, introduced in Section 3.1, is an embedded unmanned underwater vehicle (UUV) system from the oceanic monitoring domain. The second system, presented in Section 3.2, is a service-based system from the foreign exchange (FX) trade domain. Table 1 lists several additional characteristics that differ significantly between the two systems. These characteristics include the types of requirements, sensor data and adaptation actions of the systems, and the types of models whose verification underpins their self-adaptation decisions.

3.1 Unmanned Underwater Vehicle (UUV) System

The self-adaptive UUV embedded system is adapted from [55]. UUVs are increasingly used in a wide range of oceanographic and military tasks, including oceanic surveillance (e.g., to monitor pollution levels and ecosystems), undersea mapping and mine detection. Limitations due to their operating environment (e.g., impossibility to maintain UUV-operator communication during missions and unexpected changes) require that UUV systems are self-adaptive. These systems are often mission critical (e.g., when used for mine detection) or business critical (e.g., they carry expensive equipment that should not be lost).

The self-adaptive system we use consists of a UUV deployed to carry out a data gathering mission. The UUV is equipped with $n \geq 1$ on-board sensors that can measure the same characteristic of the ocean environment (e.g., water current, salinity or temperature). When used, the sensors take measurements with different, variable rates $r_1, r_2, \ldots, r_n$. The probability that each sensor produces measurements that are sufficiently accurate for the purpose of the mission depends on the UUV speed $sp$, and is given by $p_1, p_2, \ldots, p_n$. For each measurement taken, a different amount of energy is consumed, given by $e_1, e_2, \ldots, e_n$. Finally, the $n$ sensors can be switched on and off individually (e.g., to save battery power when not required), but these operations consume an amount of energy given by $e_{on}^1, e_{on}^2, \ldots, e_{on}^n$ and $e_{off}^1, e_{off}^2, \ldots, e_{off}^n$ respectively. The UUV must adapt to changes in the sensor measurement rates $r_1, r_2, \ldots, r_n$ and to sensor failures by dynamically adjusting:

(a) the UUV speed $sp$
(b) the sensor configuration $x_1, x_2, \ldots, x_n$ (where $x_i = 1$ if the $i$-th sensor is on and $x_i = 0$ otherwise)

in order to meet the quality-of-service requirements below:

- **R1 (throughput):** The UUV should take at least 20 measurements of sufficient accuracy for every 10 metres of mission distance.

<table>
<thead>
<tr>
<th>Type</th>
<th>Domain</th>
<th>Requirements</th>
<th>Sensor data</th>
<th>Adaptation actions</th>
<th>Uncertainty modelling</th>
</tr>
</thead>
<tbody>
<tr>
<td>UUV</td>
<td>oceanic monitoring</td>
<td>throughput, resource use, cost, safety</td>
<td>UUV sensor measurement rate</td>
<td>switch sensors on/off, change service instance</td>
<td>continuous-time stochastic model of UUV sensors</td>
</tr>
<tr>
<td>FX</td>
<td>exchange trade</td>
<td>reliability, response time, cost, safety</td>
<td>service response time and reliability</td>
<td>change service instance</td>
<td>discrete-time stochastic model of system</td>
</tr>
</tbody>
</table>

Table 1: Comparison of systems used to assess the generality of ENTRUST
R2 (resource usage): The energy consumption of the sensors should not exceed 120 Joules per 10 surveyed metres.

R3 (cost): If requirements R1 and R2 are satisfied by multiple configurations, the UUV should use one of these configurations that minimises the cost function

\[ \text{cost} = w_1 E + w_2 sp^{-1}, \]

where \( E \) is the energy used by the sensors to survey a 10m mission distance, and \( w_1, w_2 > 0 \) are weights that reflect the relative importance of carrying out the mission with reduced battery usage and completing the mission faster. \(^2\)

R4 (safety): If a configuration that meets requirements R1–R3 is not identified within 2 seconds after a sensor rate change, the UUV speed must be reduced to 0m/s. This ensures that the UUV does not advance more than the distance it can cover at its maximum speed within 2 seconds without taking appropriate measurements, and waits until the controller identifies a suitable configuration (e.g., after the UUV sensors recover) or new instructions are provided by a human operator.

3.2 Foreign Exchange Trading System

The service-based system from the area of foreign exchange trading is taken from our recent work in [57]. This system, which we anonymise as FX for confidentiality reasons, is used by an European foreign exchange brokerage company, the FX system implements the workflow shown in Fig. 5 and described below.

An FX customer (called a trader) can use the system in two operation modes. In the expert mode, FX executes a loop that analyses market activity, identifies patterns that satisfy the trader’s objectives, and automatically carries out trades. Thus, the Market watch service extracts real-time exchange rates (bid/ask price) of selected currency pairs. This data is used by a Technical analysis service that evaluates the current trading conditions, predicts future price movement, and decides if the trader’s objectives are: (i) “satisfied” (causing the invocation of an Order service to carry out a trade); (ii) “unsatisfied” (resulting in a new Market watch invocation); or (iii) “unsatisfied with high variance” (triggering an Alarm service invocation to notify the trader about discrepancies/opportunities not covered by the trading objectives). In the normal mode, FX assesses the economic outlook of a country using a Fundamental analysis service that collects, analyses and evaluates information such as news reports, economic data and political events, and provides an assessment on the country’s currency. If satisfied with this assessment, the trader can use the Order service to sell or buy currency, in which case a Notification service confirms the completion of the trade. We assume that the FX system has to dynamically select third-party implementations for each service from Fig. 5, in order to meet the following system requirements:

2. Cost (or utility) functions that employ weights to combine several performance, reliability, resource use and other quality attributes of software—accounting for differences in attribute value ranges and relative importance—are extensively used in self-adaptive software systems (e.g., [15], [43], [54], [95], [118]).

R1 (reliability): Workflow executions must complete successfully with probability at least 0.9.

R2 (response time): The total service response time per workflow execution must be at most 5s.

R3 (cost): If requirements R1 and R2 are satisfied by multiple configurations, the FX system should use one of these configurations that minimises the cost function:

\[ \text{cost} = w_1 price + w_2 time, \]

where \( price \) and \( time \) represent the total price of the services invoked by a workflow execution and the response time for a workflow execution, respectively, and \( w_1, w_2 > 0 \) are weights that encode the desired trade-off between price and response time.

R4 (safety): If a configuration that ensures requirements R1–R3 cannot be identified within 2s after a change in service characteristics is signalled by the sensors of the self-adaptive FX system, the Order service invocation is bypassed, so that the FX system does not carry out any trade that might be based on incorrect or stale data.

Note that requirements R1–R3 express two constraints and an optimisation criterion that are qualitatively different from those specified by the requirements from our first case study (cf. Section 3.1). Nevertheless, our tool-supported instance of the ENTRUST methodology enabled the development of the self-adaptive FX system as described in Section 6.

4 The ENTRUST METHODOLOGY

The ENTRUST methodology supports the systematic engineering and assurance of self-adaptive systems based on monitor-analyse-plan-execute (MAPE) control loops. This is by far the most common type of control loop used to devise self-adaptive software systems [14], [36], [37], [43], [68], [78], [83], [95]. The engineering of self-adaptive systems based on essentially different control techniques, such as the control theoretical paradigm [97], as for example proposed in [49], is not supported by our methodology.

ENTRUST comprises the tool-supported design-time stages and the automated runtime stages shown in Fig. 6, and is underpinned by two key principles:
Model-driven engineering is essential for developing trustworthy self-adaptive systems and their assurance cases. As emphasised in the previous section, model-based analysis, simulation, testing and formal verification—at design time and during reconfiguration—represent the main sources of assurance evidence for self-adaptive software. As such, both the design-time and the runtime stages of our methodology are model driven. Models of the structure and behaviour of the functional components, controller and environment are the basis for the engineering and assurance of ENTRUST self-adaptive systems.

2) The relevant aspects of the controlled software system and its environment. A combination of structural and behavioural models may be produced, depending on the evidence needed to assemble the assurance case for the self-adaptive system under development. ENTRUST is not prescriptive in this respect. However, we require that these models are verifiable, i.e., that they can be used in conjunction with methods such as model checking or simulation, to obtain evidence that the controller and the self-adaptive system meet their requirements. As an example, finite state transition models may be produced for the controllers of our UUV and FX systems from Section 3, enabling the use of model checking to verify that these controllers are deadlock free.

The verifiable models are application-specific. As illustrated in Fig. 6, their development requires domain knowledge, based on a controlled system specification, and is informed by the system requirements. As in other areas of software engineering, we envisage that tool-supported methods will typically be used to obtain these models. However, their manual development or fully automated synthesis are not precluded by ENTRUST.

In line with the “reuse of artefacts” principle, ENTRUST exploits the fact that the controllers of self-adaptive systems implement the established MAPE workflow, and uses application-independent controller model template(s) to devise the controller model(s). These templates model the generic aspects of the MAPE workflow and contain placeholders for the application-specific elements of an ENTRUST controller.

1) Model-driven engineering is essential for developing trustworthy self-adaptive systems and their assurance cases. As emphasised in the previous section, model-based analysis, simulation, testing and formal verification—at design time and during reconfiguration—represent the main sources of assurance evidence for self-adaptive software. As such, both the design-time and the runtime stages of our methodology are model driven. Models of the structure and behaviour of the functional components, controller and environment are the basis for the engineering and assurance of ENTRUST self-adaptive systems.

The ENTRUST stages and their exploitation of these two principles are described in the remainder of this section.

### 4.1 Design-time ENTRUST Stages

#### 4.1.1 Stage 1: Development of Verifiable Models

In ENTRUST, the engineering of a self-adaptive system with the architecture from Fig. 1 starts with the development of models for:

1) The controller of the self-adaptive system;
Given the environmental and internal uncertainty that characterises self-adaptive systems, only **incomplete system and environment models** can be produced in this ENTRUST stage. These incomplete models may include unknown or estimated parameters, nondeterminism (i.e., alternative options whose likelihoods are unknown), parts that are missing, or some combination of all of these. For example, parametric Markov chains may be devised to enable the runtime analysis of the requirements for our UUV and FX systems detailed in Sections 3.1 and 3.2, respectively, by means of probabilistic model checking or simulation.

### 4.1.2 Stage 2: Verification of Controller Models

The main role of the second ENTRUST stage is to produce **controller assurance evidence**, i.e., compelling evidence that a controller based on the controller model(s) from Stage 1 will satisfy a set of **generic controller requirements**. These are requirements that must be satisfied in any self-adaptive system (e.g., deadlock freeness) and are predefined in a format compatible with that of the controller model templates and with the method that will be used to verify the controller models. For example, if labelled transition systems are used to model the controller and model checking to establish its correctness as in [40], [41], these generic controller requirements can be predefined as temporal logical formulae.

The controller assurance evidence must include evidence that the system requirements for application-specific failsafe operating mode(s) are always satisfied. In this way, a minimal assurance case is always available for the scenario when the runtime assurance evidence for other system requirements cannot be obtained and the self-adaptive system needs to switch to a degraded, failsafe mode of operation. Several fallback levels as proposed in [40] can also be supported in this way, with only the most degraded fallback level ensured through assurance evidence obtained in this ENTRUST stage. For example, requirements R4 of our UUV and FX systems from Section 3 specify failsafe operating modes for the two systems, so we will need to show that these requirements are always met.

The assurance evidence generated in this stage of the methodology may be obtained using a range of methods that include formal verification, theorem proving and simulation. The methods that can be used depend on the types of models produced in the previous ENTRUST stage, and on the generic controller requirements and system requirements for which assurance is sought. The availability of tool support in the form of model checkers, theorem provers, SMT solvers, domain-specific simulators, etc. will influence the choice of these methods.

Preparing the design-time models, i.e., developing verifiable models and verifying the controller models, comes with a cost. This cost can be reduced by using tool-supported methods and by exploiting reusable application-independent software, as done by the related approaches described in Section 8. Furthermore, these related approaches that only provide a fraction of the assurances that ENTRUST achieves (as detailed when we discuss related work in Section 8) operate with design-time models that require a comparable effort to specify the models and provide the controller assurance evidence.

### 4.1.3 Stage 3: Partial Instantiation of Assurance Argument Pattern

This ENTRUST stage uses the controller assurance evidence from Stage 2 to support the partial instantiation of a generic **assurance argument pattern** for self-adaptive software. As explained in Section 2.3, this pattern is an incomplete assurance argument containing placeholders for the system-specific assurance evidence. A subset of the placeholders correspond to the controller assurance evidence obtained in Stage 2, and are therefore instantiated using this evidence. The result is a **partial assurance argument**, which still contains placeholders for the assurance evidence that cannot be obtained until the uncertainties associated with the self-adaptive system are resolved at runtime.

For example, the partial assurance argument for our UUV and FX systems should contain evidence that their controllers are deadlock free and that their failsafe requirements R4 are always satisfied. These requirements can be verified at design time. In contrast, requirements R1–R3 for the two systems cannot be verified until runtime, when the controller acquires information about the measurement rates of the UUV sensors and the third-party services available for the FX operations, respectively. Assurance evidence that requirements R1–R3 are satisfied can only be obtained at runtime.

In addition to the two types of placeholders, the assurance argument pattern used as input for this stage includes assurance evidence that is application independent. In particular, it includes evidence about the correct operation of the verified controller platform, i.e., the software that implements application-independent controller functionality used to execute the ENTRUST controllers. This **platform assurance evidence** is reusable across self-adaptive systems.

### 4.1.4 Stage 4: Enactment of the Controller

This ENTRUST stage assembles the controller of the self-adaptive system. The process involves integrating the verified controller platform with the application-specific controller elements, and with the sensors and effectors that interface the controller with the controlled software system from Fig. 1.

The application-specific controller elements must be devised from the verified controller models, by using a trusted model-driven engineering method. This can be done using **model-to-text transformation**, a method that employs a trusted model compiler to generate a low-level executable representation of the controller models. Alternatively, the ENTRUST verified controller platform may include a trusted virtual machine capable of directly interpret and run the controller models. The second, **model interpretation** method [101], has the advantage that it eliminates the need to generate controller code and to provide additional assurances for it.

### 4.1.5 Stage 5: Deployment of the Self-Adaptive System

In the last design-time stage, the integrated controller and controlled components of the self-adaptive system are installed, preconfigured and activated by means of an

4. Throughout the paper, the term “virtual machine” refers to a software component capable to interpret and execute controller models, much like a Java virtual machine executes Java code.
application-specific process. The pre-configuration is responsible for setting the deployment-specific parameters and architectural aspects of the system. For example, the pre-configuration of the UUV system from Section 3.1 involves selecting the initial speed and active sensor set for the UUV, whereas for the FX system from Section 3.2 it involves choosing initial third-party implementations for each FX service.

The deployed self-adaptive system will be fully configured and a complete assurance argument will be available only after the first execution of the MAPE control loop. This execution is typically triggered by the system activation, to ensure that the newly deployed self-adaptive system takes into account the current state of its environment as described next.

4.2 Runtime ENTRUST Stages

4.2.1 Stage 6: Self-adaptation

In this ENTRUST stage, the deployed self-adaptive system is dynamically adjusting its parameters and architecture in line with observed internal and environmental changes. To this end, the controller executes a typical MAPE loop that monitors the system and its environment, using the information obtained in this way to resolve the “unknowns” from the incomplete system and environment models. The resulting up-to-date system and environment models enable the MAPE loop to analyse the system compliance with its requirements after changes, and to plan and execute suitable reconfigurations if necessary.

Whenever the MAPE loop produces a reconfigured self-adaptive system, its analysis and planning steps generate adaptation assurance evidence confirming the correctness of the analysis results and of the reconfiguration plan devised on the basis of these results. This assurance evidence is a by-product of analysis and planning methods that may include runtime verification, simulation and runtime model checking. Irrespective of the methods that produce it, the adaptation assurance evidence is essential for the development of a complete assurance argument in the next ENTRUST stage.

4.2.2 Stage 7: Synthesis of Dynamic Assurance Argument

The final ENTRUST stage uses the adaptation correctness evidence produced by the MAPE loop to fill in the placeholders from the partial assurance argument, and to devise the complete assurance case for the reconfigured self-adaptive system. For example, runtime evidence that requirements R1–R3 of the UUV and FX systems from Section 3 are met will be used to complete the remaining placeholders from their partial assurance arguments. Thus, an ENTRUST assurance case is underpinned by a dynamic assurance argument that is updated after each reconfiguration of the system parameters and architecture. This assurance case captures both the full assurance argument and the evidence that justifies the active configuration of the self-adaptive system.

The ENTRUST assurance case versions generated for every system reconfiguration have two key uses. First, they allow decision makers and auditors to understand and assess the present and past versions of the assurance case. Second, they allow human operators to endorse major reconfiguration plans in human-supervised self-adaptive systems. This type of self-adaptive systems is of particular interest in domains where human supervision represents an important risk mitigation factor or may be required by regulations. As an example, UK Civil Aviation Authority regulations [110] permit self-adaptation in certain functions (e.g., power management, flight management and collision avoidance) of unmanned aircraft of no more than 20 kg provided that the aircraft operates within the visual line of sight of a human operator.

5 Tool-Supported Instance of ENTRUST

This section presents an instance of ENTRUST in which the stages described in Section 4 are supported by the modelling and verification tools UPPAAL [7] and PRISM [79]. We start with an overview of this tool-supported ENTRUST instance in Section 5.1, followed by a description of each of its stages in Section 5.2.

5.1 Overview

The ENTRUST methodology can be used with different combinations of modelling, verification and controller enactment methods, which may employ different self-adaptive system architectures and types of assurance evidence. This section presents a tool-supported instance of ENTRUST that uses one such combination of methods. We developed this instance of the methodology with the aim to validate ENTRUST and to ease its adoption.

Our ENTRUST instance supports the engineering of self-adaptive systems with the architecture shown in Fig. 7. The reusable verified controller platform at the core of this architecture comprises:

1) A Trusted Virtual Machine that directly interprets and executes models of the four steps from the MAPE control loop (i.e., the ENTRUST controller models).
2) A Probabilistic Verification Engine that is used to verify stochastic models of the controlled system and its environment during the analysis step of the MAPE loop.

Using the Trusted Virtual Machine for controller model interpretation eliminates the need for a model-to-text transformation of the controller models into executable code, which is a complex, error-prone operation. Not having to devise this transformation and to provide assurance evidence for it are major benefits of our ENTRUST instance. Although we still need assurance evidence for the virtual machine, this was obtained when we developed and verified the virtual machine, and is part of the reusable platform assurance evidence for the ENTRUST instance.

The Probabilistic Verification Engine consists of the verification libraries of the probabilistic model checker PRISM [79] and is used by the analysis step of the MAPE control loop. As such, our ENTRUST instance works with:

5. Hence the controller models are depicted as software components in Fig. 7.
6. This assurance evidence is in the form of a comprehensive test suite and a report describing its successful execution by the virtual machine, both of which are available on our ENTRUST project website at https://www-users.cs.york.ac.uk/simos/ENTRUST/.
Fig. 7. Architecture of an ENTRUST self-adaptive system

1) Stochastic finite state transition models of the controlled system and the environment, defined in the PRISM high-level modelling language. Incomplete versions of these models are devised in Stage 1 of ENTRUST, and have their unknowns resolved at runtime. All types of models that PRISM can analyse are supported, including discrete- and continuous-time Markov chains (DTMCs and CTMCs), Markov decision processes (MDPs) and probabilistic automata (PAs).

2) Runtime-assured system requirements expressed in the appropriate variant of probabilistic temporal logic, i.e., probabilistic computation tree logic (PCTL) for DTMCs, MDPs and PAs, and continuous stochastic logic (CSL) for CTMCs.

This makes our instantiation of the generic ENTRUST methodology applicable to self-adaptive systems whose non-functional (e.g., reliability, performance, resource usage and cost-related) requirements can be specified in the above logics, and whose behaviour related to these requirements can be described using stochastic models. As shown by the recent work of multiple research groups (e.g., [15], [20], [27], [44], [47], [50], [90], [104]), this represents a broad and important class of self-adaptive software that includes a wide range of service-based systems, web applications, resource management systems, and embedded systems.

Also developed in Stage 1 of ENTRUST, the four controller models form an application-specific network of interacting timed automata [2], and are expressed in the modelling language of the UPPAAL verification tool suite [7].

Accordingly, UPPAAL is used in Stage 2 of ENTRUST to verify the compliance of the controller models with the generic controller requirements and with any system requirements that can be assured at design time. These requirements are defined in computation tree logic (CTL) [31].

In Stage 3 of our ENTRUST instance, a partial assurance argument is devised starting from an assurance argument pattern represented in goal structuring notation (GSN) [72].

The controller enactment from Stage 4 involves integrating the timed-automata controller models with our verified controller platform.

In Stage 5 of ENTRUST, the controlled software system and its enacted controller are deployed, together with a Knowledge Repository that supports the operation of the controller. Initially, this repository contains: (i) the partial assurance argument from Stage 3; (ii) the system requirements to be assured at runtime; and (iii) the (incomplete) stochastic system and environment models from Stage 1.

During the execution of the MAPE loop in Stage 6 of ENTRUST, the Monitor obtains information about the system and its environment through Sensors. This information is used to resolve the unknowns from the stochastic models of the controlled system and its environment. Examples of such unknowns include probabilities of transition to ‘failure’ states for a DTMC, MDP or PA, rates of transition to ‘success’ states for a CTMC, and sets of states and transitions modelling certain system behaviours. After each update of the stochastic system and environment models, the Analyzer re-verifies the compliance of the self-adaptive system with its runtime-assured requirements. When the requirements are no longer met, the Analyzer uses the verification results to identify a new system configuration that restores this compliance, or to find out that such a configuration does not exist and to select a predefined failsafe configuration. The step-by-step actions needed to achieve the new configuration are then established by the Planner and implemented by the Executor through the Effectors of the controlled system.

Using the Probabilistic Verification Engine enables the Analyzer and Planner to produce assurance evidence justifying their selection of new configurations and of plans for transitioning the system to these configurations, respectively. This adaptation assurance evidence is used to synthesise a fully-fledged, dynamic GSN assurance argument in Stage 7 of our ENTRUST instance. As indicated in Fig. 7, versions of the adaptation assurance evidence and of the dynamic assurance argument justifying each reconfiguration of the self-adaptive system are stored in the Knowledge Repository.

The implementation of the ENTRUST stages in our tool-supported instance of the methodology is summarised in Table 2 and described in further detail in Section 5.2.

5.2 Stage Descriptions

5.2.1 Development of Verifiable Models

Controller models. We devised two types of templates for the four controller models from Fig. 7: (i) event triggered, in which the monitor automaton is activated by a sensor-generated signal indicating a change in the managed system or the environment; and (ii) time triggered, in which the monitor is activated periodically by an internal clock. The event-triggered automaton templates are shown in Fig. 8 using the following font and text style conventions:
Finally, signals in angle brackets ‘⟨⟩’ are placeholders for application-specific signal names, and guards and actions decorated with brackets ‘()’ represent application-specific C-style functions.

TABLE 2

<table>
<thead>
<tr>
<th>Stage</th>
<th>Type</th>
<th>Description</th>
<th>Supporting tool(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>tool supported</td>
<td>Timed automata controller models developed from UPPAAL templates</td>
<td>UPPAAL PRISM</td>
</tr>
<tr>
<td>2</td>
<td>tool supported</td>
<td>Controller models verified to obtain controller assurance evidence</td>
<td>UPPAAL</td>
</tr>
<tr>
<td>3</td>
<td>manual</td>
<td>Partial assurance argument devised from GSN assurance argument pattern</td>
<td>–</td>
</tr>
<tr>
<td>4</td>
<td>manual</td>
<td>Controller enacted by integrating the verified controller models and platform</td>
<td>–</td>
</tr>
<tr>
<td>5</td>
<td>manual</td>
<td>Controlled system, controller and knowledge repository deployed</td>
<td>–</td>
</tr>
<tr>
<td>6</td>
<td>automated</td>
<td>MAPE control loop continually executed to ensure the system requirements</td>
<td>PRISM &amp; ENTRUST controller platform</td>
</tr>
<tr>
<td>7</td>
<td>automated</td>
<td>GSN dynamic assurance argument generated</td>
<td>ENTRUST controller platform</td>
</tr>
</tbody>
</table>

Stage Type Description Supporting tool(s)

1 tool supported Timed automata controller models developed from UPPAAL templates UPPAAL PRISM
2 tool supported Controller models verified to obtain controller assurance evidence UPPAAL
3 manual Partial assurance argument devised from GSN assurance argument pattern –
4 manual Controller enacted by integrating the verified controller models and platform –
5 manual Controlled system, controller and knowledge repository deployed –
6 automated MAPE control loop continually executed to ensure the system requirements PRISM & ENTRUST controller platform
7 automated GSN dynamic assurance argument generated ENTRUST controller platform

Fig. 8. Event-triggered MAPE model templates

- Sans-serif font is used to annotate states with the atomic propositions (i.e., boolean properties) that hold in those states, e.g., PlanCreated from the Planner automaton;
- *Italic text* is used for the guards that annotate state transitions with the conditions which must hold for the transitions to occur, e.g., time ≤ MAX_TIME from the Analyzer automaton;
- State transitions are additionally annotated with the actions executed upon taking the transitions, and these actions are also shown in sans-serif font, e.g., time = 0 to initialise a timer in the Monitor automaton;
- **Bold text** is used for the synchronisation channels between two automata—these channels are specified as pairs comprising a ‘!’-decorated sent signal and a ‘?’-decorated received signal with the same name, e.g., startAnalysis! and startAnalysis? from the monitor and analyzer automata, respectively. The two transitions associated with a synchronisation channel can only be taken at the same time.

Finally, signals in angle brackets ‘⟨⟩’ are placeholders for application-specific signal names, and guards and actions decorated with brackets ‘()’ represent application-specific C-style functions.

To specialise these model templates for a particular system and application, software engineers need: (a) to replace the signal placeholders with real signal names; (b) to define the guard and action functions; and (c) to devise the automaton regions shaded in Fig. 8. For example, for the monitor automaton the engineers first need to replace the signal placeholders (sensorSignal1?), . . . , (sensorSignaln?) with sensor signals announcing relevant changes in the managed system. They must then implement the functions process(), analysisRequired() and monitorCleanup(), whose roles are to process the sensor data, to decide if the change specified by this data requires the “invocation” of the analyzer through the startAnalysis! signal, and to carry out any cleanup that may be required, respectively. Details about the other automata from Fig. 8 are available on our project website, which also provides implementations of these MAPE model templates in the modelling language of the UPPAAL verification tool suite [7].

**Parametric stochastic models.** These models used by the ENTRUST control loop at runtime are application specific, and need to be developed from scratch. Their parameters correspond to probabilities or rates of transition between model states, and are continually estimated at runtime, based on change information provided by the sensors of the controlled system. As such, the verification of these models at runtime enables the ENTRUST analyzer to identify
MAPE models were devised. This involves completing the isfies them is possible only after its application-specific verifying that an ENTRUST controller sat-

generic properties that we assembled for the current version specific properties. Table 4 shows a non-exhaustive list of ness properties that include both generic and application-

during this ENTRUST stage, a trusted model checker is used to verify the network of MAPE automata devised in

5.2.2 Verification of Controller Models

During this ENTRUST stage, a trusted model checker is used to verify the network of MAPE automata devised in the previous section. This verification yields evidence that the MAPE models satisfies a set of key safety and liveness properties that include both generic and application-specific properties. Table 4 shows a non-exhaustive list of generic properties that we assembled for the current version of ENTRUST. Although these properties are application-independent, verifying that an ENTRUST controller satisfies them is possible only after its application-specific MAPE models were devised. This involves completing the application-specific parts of the planner and executor automata, and implementing the functions for the guards and actions from all the model templates.

Additionally, automata that simulate the controller sensors, runtime probabilistic verification engine and effectors from Fig. 7 need to be defined to enable this verification. The sensors, verification engine and effectors automata have to synchronise with the relevant monitor, analyzer and executor signals, respectively. The sensors automaton and verification automaton also have to exercise the possible paths through the monitor, analyzer and planner automata (and indirectly the executor automaton). To this end, they can nondeterministically populate the knowledge repository with data that satisfies all the different guard combinations. Alternatively, a finite collection of the two automata can be used to verify subsets of all possible MAPE paths, as long as the union of all such subsets covers the entire behaviour space of the MAPE network of automata.

5.2.3 Partial Instantiation of Assurance Argument Pattern

We used the Goal Structuring Notation (GSN) introduced in Section 2.2 to devise a reusable assurance argument pattern (cf. Section 2.3) for self-adaptive software. Unlike all existing assurance argument patterns [63], our new pattern captures the fact that for self-adaptive software the assurance process cannot be completed at design time. Instead, it is a continual process where some design features and code elements are dynamically reconfigured and executed during self-adaptation. As such, the detailed claims and evidence for meeting the system requirements must vary with self-adaptation, and thus ENTRUST assurance cases must evolve dynamically at runtime.

The ENTRUST assurance argument pattern is shown in Fig. 9. Its root goal, ReqsSatisfied, states that the system requirements are satisfied at all times. These requirements are typically allocated to the software from the higher-level system analysis process, so the justifications of their derivation, validity and completeness are addressed as part of the overall system assurance case (which is outside the scope of the software assurance case). ReqsSatisfied is supported by a sub-claim based on (i.e. in the context of) the current configuration (ReqsConfiguration) and by a reconfiguration sub-claim (Reconfig). That is, the pattern shows that we are guaranteeing that the current configuration satisfies the requirements (in the absence of changes) and that the ENTRUST controller will plan and execute a reconfiguration that will satisfy these requirements (should a change occur).

The pattern justifies how the system requirements are achieved for each configuration by using a sub-goal Rx-Achieved for each requirement Rx. Further, a new configuration has the potential to introduce erroneous behaviours (e.g., deadlocks). The justification for the absence of these errors is provided via the away goal NoErroneousBehaviour (described below). The pattern concludes with the goals RxVerified and ReqsPreservedByPlatform, which justify the verification and the implementation of the formalised requirements, respectively. The away goal ReqsPreservedByPlatform confirms that the controlled system handles correctly the reconfiguration commands received through effectors. This away goal is obtained using standard assurance processes, which are outside the scope of this paper.

As shown Fig. 10, the NoErroneousBehaviour away goal is supported by two sub-claims. The FMsManaged

<table>
<thead>
<tr>
<th>Type of stochastic model</th>
<th>Non-functional requirement specification logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrete-time Markov chains [15], [23], [44], [46], [47], [59]</td>
<td>PCTL, LTL, PCTL, PCTL, PCTL</td>
</tr>
<tr>
<td>Markov decision processes [50]</td>
<td>PCTL, LTL, PCTL, PCTL</td>
</tr>
<tr>
<td>Probabilistic automata [21], [70]</td>
<td>PCTL, LTL, PCTL, PCTL</td>
</tr>
<tr>
<td>Continuous-time Markov chains [19], [22], [55]</td>
<td>CSL</td>
</tr>
<tr>
<td>Stochastic games [26], [27]</td>
<td>rPATL</td>
</tr>
</tbody>
</table>

*Probabilistic Computation Tree Logic [9], [61]*
*Linear Temporal Logic [88]*
PCTL, LTL, PCTL, PCTL, PCTL

Table 3: Stochastic models supported by the ENTRUST instance, with citations of representative research that uses them in self-adaptive systems
TABLE 4
Generic properties that should be satisfied by an ENTRUST controller

<table>
<thead>
<tr>
<th>ID</th>
<th>Informal description</th>
<th>Specification in computation tree logic (CTL) [31]</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>The ENTRUST controller is deadlock free.</td>
<td>$\Box \neg \text{not deadlock}</td>
</tr>
<tr>
<td>P2</td>
<td>Whenever analysis is required, the Analyser eventually carries out this action.</td>
<td>$\Box (\text{Monitor.StartAnalysis} \rightarrow A \Diamond \text{Analyzer.Analyse})$</td>
</tr>
<tr>
<td>P3</td>
<td>Whenever the system requirements are violated, a stepwise reconfiguration plan is eventually assembled.</td>
<td>$\Box (\text{Analyzer.Adapt} \rightarrow A \Diamond \text{Planner.PlanCreated})$</td>
</tr>
<tr>
<td>P4</td>
<td>Whenever a stepwise plan is assembled, the Executor eventually implements it.</td>
<td>$\Box (\text{Planner.PlanCreated} \rightarrow A \Diamond \text{Executor.PlanExecuted})$</td>
</tr>
<tr>
<td>P5</td>
<td>Whenever the Monitor starts processing the received data, it eventually terminates its execution.</td>
<td>$\Box (\text{Monitor.ProcessSensorData} \rightarrow A \Diamond \text{Monitor.Finished})$</td>
</tr>
<tr>
<td>P6</td>
<td>Whenever the Analyser begins the analysis, it eventually terminates its execution.</td>
<td>$\Box (\text{Analyzer.Analyse} \rightarrow A \Diamond \text{Analyzer.AnalysisFinished})$</td>
</tr>
<tr>
<td>P7</td>
<td>A plan is eventually created, each time the Planner starts planning.</td>
<td>$\Box (\text{Planner.Plan} \rightarrow A \Diamond \text{Planner.PlanCreated})$</td>
</tr>
<tr>
<td>P8</td>
<td>Whenever the Executor starts executing a plan, the plan is eventually executed.</td>
<td>$\Box (\text{Executor.Execute} \rightarrow A \Diamond \text{Executor.PlanExecuted})$</td>
</tr>
<tr>
<td>P9</td>
<td>Whenever adaptation is required, the current configuration and the best configuration differ.</td>
<td>$\Box (\text{Analyzer.Adapt} \rightarrow \text{currentConfig} \neq \text{newConfig})$</td>
</tr>
</tbody>
</table>

Fig. 9. ENTRUST assurance argument pattern.

sub-claim uses the goals FMsIdentified and ReqsDerived to state that the relevant “failure modes” for the self-adaptive system have been identified and that the system requirements fully address these failure modes. We leave the two goals undeveloped, as they are achieved using standard requirements engineering and assurance practices. The EngErrorsAbsent sub-claim states that the engineering of the self-adaptive system does not introduce errors in the context of the ENTRUST reusable artefacts (i.e., of our trusted virtual machine and probabilistic verification engine) and of the generic properties that an ENTRUST controller has to satisfy. EngErrorsAbsent is in turn supported by two sub-goals, NoProcessError and NoController&SystemError. The former sub-goal is obtained through using suitable software engineering processes (via the away goal SuitableSoftEngProcess, which also covers the use of the methods mentioned in Section 5.2.1 to ensure the accuracy of the ENTRUST stochastic models) and through avoiding methodological errors by using the ENTRUST methodology. The latter sub-goal, NoController&SystemError, is achieved by claims about:

1) The absence of controller errors. This is supported by (i) the controller verification evidence from Stage 2 of ENTRUST; and (ii) the reusable platform assurance evidence, which includes (testing) evidence about the correct operation of the model checkers UPPAAL and PRISM, based on their long track record of successful adoption across multiple domains and on our own experience of using them to develop self-adaptive systems.

2) The absence of controlled system errors, covered by the ControlledSystem away goal.

The away goals SuitableSoftEngProcess and ControlledSystem are obtained following existing software assurances processes, and thus we do not describe them here.

The partial instantiation of the assurance argument pattern in the last design-time stage of ENTRUST produces a partially-developed and partially-instantiated assurance argument [38]. This includes placeholders for items of evidence that can only be instantiated and developed based on operational data, i.e., the runtime verification evidence that is generated by the analysis and planning steps of the ENTRUST controller.

5.2.4 Enactment of the Controller

In this stage, the controller from Fig. 7 is assembled by integrating the MAPE controller models discussed in Sec-
5.2.6 Self-Adaptation

In this ENTRUST stage, the deployed self-adaptive system is dynamically adjusting its configuration in line with the observed internal and environmental changes. The use of continual verification within the ENTRUST control loop produces assurance evidence that underpins the dynamic generation of assurance cases in the next stage of our ENTRUST instance.

5.2.7 Synthesis of Dynamic Assurance Argument

The ENTRUST assurance case evolves in response to the results of the MAPE process, e.g., time-triggered and event-triggered outputs of the monitor, the outcomes of the analyzer, the mitigation actions developed by the planner and their realisation by the executor. This offers a dynamic approach to assurance because the full instantiation of the ENTRUST assurance argument pattern is left to runtime, i.e., the only stage when the evidence required to complete the argument becomes available. As such, the assurance case resulting from this stage captures the full argument and evidence for the justification of the current configuration of the self-adaptive system.

6 APPLYING THE ENTRUST METHODOLOGY

6.1 Development of Verifiable Models

6.1.1 UUV System

Controller models. We instantiated the ENTRUST model templates for the UUV system from Section 3.1, obtaining the automata shown in Fig. 11. The signal newRate? is the only sensor signal that the monitor automaton needs to deal with, by reading a new UUV-sensor measurement rate (in process()) and checking whether this rate has changed to such extent that a new analysis is required.
inaccurate, the transition probability s_i \rightarrow s_{i+1} \text{ is active this operation is repeated, as modelled by the transition } s_5 \rightarrow s_1. The model is augmented with two reward structures. A “measure” structure, shown in a dashed rectangular box, associates a reward of 1 to each accurate measurement taken. An “energy” structure, shown in solid rectangular boxes, associates the energy used to switch the sensor on (\epsilon_i^{on}) and off (\epsilon_i^{off}) and to perform a measurement (\epsilon_i) with the transitions modelling these events. The model M of the n-sensor UUV is given by the parallel composition of the n sensor models: M = M_1 || \ldots || M_n and the QoS system requirements are specified using CSL as follows:

R1: \quad R_{\text{measure}} = \frac{\sum_{x=0}^{10} E(x)}{\text{sensor}} = \frac{\sum_{x=0}^{10} E(x)}{\text{sensor}} = \frac{\sum_{x=0}^{10} E(x)}{\text{sensor}} \leq 10/\text{sp}.

R2: \quad R_{\text{energy}} = \frac{\sum_{x=0}^{10} E(x)}{\text{sensor}} = \frac{\sum_{x=0}^{10} E(x)}{\text{sensor}} = \frac{\sum_{x=0}^{10} E(x)}{\text{sensor}} \leq 120/\text{sp}.

R3: \quad \text{minimise } (w_1 E + w_2 s^{-1}), \text{ where } E = \frac{\sum_{x=0}^{10} E(x)}{\text{sensor}} \leq 10/\text{sp}.

where 10/sp is the time taken to travel 10m at speed sp. As requirement R4 is a failsafe requirement, we verify it at design time as explained in Section 6.2.1, so it is not encoded into CSL.

6.1.2 FX System

Controller models. We specialised our event-triggered MAPE model templates for the FX system. The resulting MAPE models are shown in Fig. 13, where the shaded areas in Planner and Executor automata indicate the FX-specific steps for assembling a plan and executing the adaptation, respectively. The implementations of all guards and actions decorated with brackets ‘()’ (which represent application-specific C-style functions, as explained in Section 5.2.1) are available on our project website.

Parametric stochastic models. To model the runtime behaviour of the FX system, we used the parametric discrete-time Markov chain (DTMC) depicted in Fig. 14. In this DTMC, constant transition probabilities derived from system logs are associated with the branches of the FX work-
dynamic selection by the ENTRUST controller .

... where $\tau$ time $\leq 5$.

... represents the reliability (i.e. success probability), the response time and the price, respectively, of the implementations used for the MW, TA, . . . system services.

The final version of record is available at http://dx.doi.org/10.1109/TSE.2017.2738640
which represents the CTL encoding of requirement R4. To carry out this verification, we defined simple sensors, verification engine and effectors automata as described above. We used a simple one-state effectors automaton with transitions returning to its single state for each of the received signals sensorON?, sensorOFF? changeSpeed? and planExecuted?, and a finite collection of sensor–verification engine automata pairs that together exercised all possible paths of the MAPE automata from Fig. 11. These auxiliary UPPAAL automata are available on the project website.

6.2.2 FX System

We used the model checker UPPAAL to verify that the MAPE automata network from Fig. 13 satisfies the generic CSL property corresponding to the failsafe requirement R4 of the FX system:

\[
R4: \text{A} \Box (\text{Analyzer.Analyse} \land \text{Analyzer.time} > 2) \rightarrow \text{A} \Diamond \text{Planer.Plan} \land \text{newConfig.Order} == \text{NoSvc},
\]

where ‘newConfig.Order = NoSvc’ signifies that no service is used to implement the Order operation (i.e., the operation is skipped).

6.2.3 Discussion

The availability of a set of generic properties that must be satisfied by all ENTRUST controllers (cf. Table 4) meant that an additional CSL property was only needed for the application-specific failsafe requirement. For both systems, this additional property corresponds to the scenario where a suitable new configuration cannot be obtained timely, suggesting that using a property template may be feasible for this and potentially for other types of failsafe requirements.

6.3 Partial Instantiation of Assurance Argument Pattern

6.3.1 UUV System

Fig. 15 shows the partially-instantiated assurance argument pattern for the self-adaptive UUV system, in which we shaded the (partially) instantiated GSN elements. To keep the diagram clear, we only show the expansion for requirements R1 and R4, leaving R2 and R3 undeveloped. The goal R1Achieved (which needs to be further instantiated when the system configuration is dynamically selected) is supported by: (a) sub-claim R1Verified, whose associated solution placeholder R1Result remains uninstantiated and should constantly be updated by the ENTRUST controller at runtime; and (b) the away goal ReqsPreservedByPlatform described earlier in this section. The undeveloped and partially instantiated goals R2Achieved and R3Achieved have the same structure as R1Achieved. In contrast, the (failsafe) goal R4Achieved is fully instantiated because the solution R4Result, comprising UPPAAL verification evidence that R4 is achieved irrespective of the configuration of the self-adaptive system, was obtained in the second ENTRUST stage (verification of controller models), cf. Section 6.2.1.

6.3.2 FX System

We partially instantiated the ENTRUST assurance argument pattern for our self-adaptive FX system, as shown in Fig. 16.

6.3.3 Discussion

As shown in Figs. 15 and 16, roughly the top half of the partially instantiated assurance argument pattern comes from ENTRUST assurance pattern in Fig. 9. This part of the assurance argument captures assurance elements generic to all self-adaptive systems, allowing the developers of a self-adaptive system to focus on the application-specific elements, which they are often more familiar with.

6.4 Enactment of the Controller

6.4.1 UUV System

To assemble an ENTRUST controller for the UUV system, we implemented Java classes that extend the functionality of the abstract Sensors, Effectors and VerificationEngine classes from the ENTRUST distribution. In addition to synchronising with the relevant application-specific signals from the MAPE automata (e.g., newRate?), the specialised sensors and effectors invoke the relevant API methods of our UUV simulator. The specialised verification engine instantiates the parametric sensor models \( M_i \) from Fig. 12, \( 1 \leq i \leq n \), and verifies the CSL-encoded requirements from Section 6.1.1.

6.4.2 FX System

To assemble the ENTRUST controller for the FX system, we combined the controller and stochastic models from
6.4.3 Discussion

The controller enactment comprises typical software development (i.e. specialisation of Java classes) and integration tasks. A considerable part of the required functionality is application-independent, and already provided by the reusable abstract Java classes available with ENTRUST.

6.5 Deployment of the Self-Adaptive System

6.5.1 UUV System

We used the open-source MOOS-IvP\textsuperscript{7} platform (oceanai.mit.edu/moos-ivp) for the implementation of autonomous applications on unmanned marine vehicles \cite{8} to develop a fully-fledged three-sensor UUV simulator that is available on the ENTRUST website. We then exploited the publish-subscribe architecture of MOOS-IvP to interface the ENTRUST sensors and effectors (and thus the controller from Section 6.4.1) with the UUV simulator, we installed the controller and the controlled system on a computer with a similar spec to that of the payload computer of a mid-range UUV, and we preconfigured the system to start with zero speed and all its sensors switched off. We chose this configuration, corresponding to initial UUV parameter values $(x_1, x_2, x_3, s_p) = (0, 0, 0, 0)$, to ensure that the system started with a configuration satisfying its failsafe requirement R4 (cf. Section 3.1).\textsuperscript{8}

6.5.2 FX System

We implemented a prototype version of the FX system using Java web services deployed in Tomcat/Axis, and a Java FX workflow that we integrated with the ENTRUST controller from Stage 4. Our self-adaptive FX system (whose code is available on our project website) could select from two functionally equivalent web service implementations for each of the six FX services from Fig. 5, i.e. from 12 web services with the initial characteristics shown in Table 5. For simplicity and without loss of generality, we installed the components of the self-adaptive FX system on a single computer with the characteristics detailed in Section 7.1, and we preconfigured the system to start by using the first web service implementation available for each service (i.e. MW\textsubscript{0}, TA\textsubscript{0}, etc.), except for the Order service. For Order, NoSvc\textsubscript{0} was selected initially, to ensure that the failsafe requirement R4 was satisfied until a configuration meeting requirements R1–R3 was automatically selected by the first execution of the MAPE loop, shortly after the system started.

6.5.3 Discussion

This stage involved a typical deployment of the managed systems and of their controllers, except that both self-adaptive systems were preconfigured to start with a configuration satisfying their failsafe requirement. Note that such a configuration always exists because the compliance of the two systems with their failsafe requirements was formally verified in the second ENTRUST stage (cf. Section 6.2).

6.6 Self-Adaptation

6.6.1 UUV System

The dynamic reconfiguration of the self-adaptive UUV system is described in detail in Section 7.1.1. Here we illustrate the process by considering a scenario in which the UUV system comprises $n = 3$ sensors with: initial measurement $(x_1, x_2, x_3, s_p) = (0, 0, 0, 0)$, to ensure that the system

\textsuperscript{7} Mission-Oriented Operating Suite – Interval Programming

\textsuperscript{8} The use of a failsafe initial configuration is our recommended approach for ENTRUST self-adaptive systems. When this is not possible, an execution of the MAPE loop must be initiated as part of the system start-up, to ensure that an initial configuration meeting the system requirements is selected.


Table 5

<table>
<thead>
<tr>
<th>Operation: Service ID:</th>
<th>Market Watch MW₀</th>
<th>MW₁</th>
<th>Technical Analysis TA₀</th>
<th>TA₁</th>
<th>Fundam. Analysis FA₀</th>
<th>FA₁</th>
<th>Alarms A₀</th>
<th>A₁</th>
<th>Order Or₀</th>
<th>Or₁</th>
<th>Notification No₀</th>
<th>No₁</th>
</tr>
</thead>
<tbody>
<tr>
<td>response time [s]</td>
<td>0.5</td>
<td>0.5</td>
<td>0.6</td>
<td>1.0</td>
<td>1.6</td>
<td>0.7</td>
<td>0.6</td>
<td>0.9</td>
<td>0.6</td>
<td>1.3</td>
<td>1.8</td>
<td>0.5</td>
</tr>
<tr>
<td>reliability</td>
<td>0.976</td>
<td>0.995</td>
<td>0.988</td>
<td>0.985</td>
<td>0.998</td>
<td>0.995</td>
<td>0.995</td>
<td>0.995</td>
<td>0.95</td>
<td>0.99</td>
<td>0.99</td>
<td></td>
</tr>
<tr>
<td>price</td>
<td>5</td>
<td>10</td>
<td>6</td>
<td>4</td>
<td>23</td>
<td>25</td>
<td>15</td>
<td>9</td>
<td>25</td>
<td>20</td>
<td>5</td>
<td>8</td>
</tr>
</tbody>
</table>

Fig. 17. Verification results for requirement (a) R1, (b) R2, and (c) cost of the feasible configurations; 21 speed values between 1 m/s and 5 m/s are considered for each of the seven combinations of active sensors, corresponding to 21 × 7 = 147 alternative configurations. The best configuration (circled) corresponds to x₁ = x₂ = x₃ = 1, i.e., UUV using only its first two sensors; and sp = 3.2 m/s, and the shaded regions correspond to requirement violations.

9. Note that R1 and R2 are “conflicting” requirements, in the sense that the configurations that satisfy R1 by the widest margin violate R2, and the other way around. In such scenarios, ENTRUST supports the selection of configurations based on trade-offs between the conflicting requirements, as specified by a cost (or utility) function. If either requirement became much stricter (e.g., if R1 required over 50 measurements per every 10 m), no configuration would satisfy both R1 and R2. In this case, ENTRUST would choose the configuration specified by the failsafe requirement R₄, i.e., would reduce the UUV speed to 0 m/s, and would record the probabilistic model checking evidence showing the lack of a suitable non-failsafe configuration.

6.6.2 FX System

In this stage, the self-adaptive FX system dynamically reconfigures in response to observed changes in the characteristics of the web services it uses. Several such reconfigurations are described later in the paper, in Section 7.1.2 and in Fig. 22. To illustrate this process in detail, consider the system configuration immediately after change C from Fig. 22, where the FX workflow uses the services MW₁, TA₀, FA₀, A₀, Or₀, and No₁. This configuration is reached after the FX services, initially operating with the characteristics from Table 5, experience degradations in the reliability of MW₀ (pr⁰MW₀ = 0.9, change B in Fig. 22) and in the response time of FA₁ (time⁰FA₁ = 1.2 s, change C in Fig. 22). With the FX system in this configuration, suppose that the Market Watch service MW₀ recovers, i.e., pr⁰MW₀ = 0.976 as in Table 5. Under these circumstances, which correspond to change D from Fig. 22, the ENTRUST controller receives the updated characteristics of MW₀ via its monitor. As the new service characteristics differ from those in the knowledge repository, the guard analysisRequired() returns true and the startAnalysis! signal is sent. Upon receiving the signal, the analyser invokes the probabilistic verification engine, whose analysis results for requirements R1–R3 are depicted in Fig. 17. The analyse() action filters the results as follows: configurations that violate requirements R₁ or R₂, i.e., the shaded areas from Fig. 17a and Fig. 17b, respectively, are discarded.

invokes the planner to assemble a stepwise reconfiguration plan with which i) sensor 1 is switched on; ii) next, sensor 3 is switched off; and iii) finally the speed is adjusted to 3.2 m/s. Once the plan is assembled, the executor is enforcing this plan to the UUV system. The adaptation results from Fig. 17 provide the evidence required for the generation of the assurance case as described in Section 6.7.1.
configurations (corresponding to six services each provided by two implementations) is shown in Fig. 18. As part of this analysis, configurations that violate requirements R1 or R2 (i.e., those from the shaded areas in Fig. 18a and Fig. 18b, respectively) are discarded. The remaining configurations are feasible, so their cost is calculated (for $w_1 = 1$ and $w_2 = 2$) as shown in Fig. 18c. The feasible configuration using services $MW_0$, $TA_0$, $FA_0$, $Al_1$, $Or_0$, and $No_1$ has the lowest cost and is thus selected as the best system configuration. Since the best and the current configurations differ, the guard adaptationRequired() holds and the analyser invokes the planner through the startPlanning! signal to assemble a stepwise reconfiguration plan through which: (i) $MW_0$ replaces $MW_1$; and (ii) $Al_1$ replaces $Al_0$. Once the plan is ready, the executor automaton receives the startExecuting? signal and is ensuring the implementation of this plan by sending the signal changeService! to the system effectors.

6.6.3 Discussion

Both self-adaptive systems reconfigured in response to application-specific changes (more of which are described in Section 7). Selecting the new configurations involved the runtime probabilistic model checking of different types of stochastic models, to generate assurance evidence that system requirements were satisfied after each change.

6.7 Synthesis of Dynamic Assurance Argument

6.7.1 UUV System

In this stage, the partially-instantiated assurance argument pattern for the UUV system (Fig. 15) is fully instantiated after every selection of a new UUV configuration by the ENTRUST controller. For instance, after the ENTRUST controller activities described in Section 6.6.1 conclude with the selection of the UUV configuration $(x_1, x_2, x_3, sp) = (1, 1, 0, 3.2)$ and the generation of runtime verification evidence that this configuration satisfies requirements R1–R3, this partially-instantiated assurance argument pattern is fully instantiated as shown in Fig. 19.

6.7.2 FX System

The partially instantiated FX assurance pattern from Fig. 16 is updated into a full assurance argument after each selection of a new configuration by the ENTRUST controller. This involves using the new evidence generated by the runtime probabilistic verification engine to complete the
instantiation of the assurance pattern. As an example, Fig. 20 shows the complete assurance pattern synthesised as part of the configuration change that we used to illustrate the previous stage of ENTRUST in Section 6.6.2.

6.7.3 Discussion

For both the UUV system and the FX system, integrating the dynamically generated assurance evidence required the updating of only a few uninstantiated GSN ‘solutions’ from the partially instantiated assurance arguments. In contrast, instantiating the current system configurations in the two assurance arguments involved multiple but small updates of ‘context’, ‘strategy’ and ‘goal’ GSN elements. The rightmost branches of the assurance arguments ensure the goals associated with the failsafe requirements of the two systems, and therefore remained unchanged in this ENTRUST stage.

7 Evaluation

To evaluate the effectiveness and generality of ENTRUST, we used our methodology to engineer the self-adaptive software systems from Section 3. The two systems were developed as described in Section 6, and were deployed in a realistic environment seeded with simulated changes specific to their application domains. Finally, we examined the correctness and efficiency of the adaptation and of the assurance cases produced by ENTRUST in response to each of these unexpected environmental changes. The aim of our evaluation was to answer the following research questions.

RQ1 (Correctness): Are ENTRUST self-adaptive systems making the right adaptation decisions and generating valid assurance cases?

RQ2 (Efficiency): Does ENTRUST provide design-time and runtime assurance evidence with acceptable overheads for realistic system sizes?

RQ3 (Generality): Does ENTRUST support the development of self-adaptive software systems and dynamic assurance cases across application domains?

As the focus of our evaluation was the ENTRUST methodology and its tool-supported instance, we necessarily made a number of assumptions. In particular, we assumed that established assurance processes could be used to construct assurance arguments for all aspects of the controlled systems from our case studies, including their correct design, development, operation, ability to respond to effector requests, and any real-time considerations associated with achieving the new configurations decided by the ENTRUST controller. As such, these aspects are outside the scope of ENTRUST and are not covered in our evaluation. We further assumed that the derivation, validity, completeness and formalisation of the self-adaptive system requirements are addressed as part of the overall system assurance cases for the two case studies, and therefore also outside the scope of our evaluation of ENTRUST.

The experiments carried out to address the three research questions are described in Sections 7.1–7.3, and the main threats to validity are discussed in Section 7.4.

7.1 RQ1 (Correctness)

To answer the first research question, we carried out experiments that involved running the UUV and FX systems in realistic environments comprising (simulated) unexpected changes specific to their domains. For the UUV system, the experiments were seeded with failures including sudden degradation in the measurement rates of sensors and complete failures of sensors, and with recoveries from these problems. For the FX system, we considered variations in the response time and the probability of successful completion of third-party service invocation. All the experiments were run on a MacBook Pro with 2.5 GHz Intel Core i7 processor, and 16 GB 1600 MHz DDR3 RAM.

7.1.1 UUV System

For the UUV system, we described a concrete change scenario and the resulting self-adaptation process and generation of an assurance case in Sections 6.6.1 and 6.7.1. The complete set of change scenarios we used in this experiment is summarised in Fig. 21, which depicts the changes in the sensor rates and the new UUV configurations selected by the ENTRUST controller. The labels A–H from Fig. 21 correspond to following key events:

A) The UUV starts with the initial state and configuration from Section 6.6.1;
Sensors 2 and 3 resume operation at nominal rates and
G) Sensor 3 recovers and the initial configuration is re-
lines depict the services selected at each point in time.

Fig. 22. Change scenarios for the self-adaptive FX system, with the initial services characteristics shown in Table 5. The thick continuous

F) As a result of a reliability degradation in the Order service \( \text{Or}_0 \) \( (p_{\text{new}} = 0.91) \) and recovery of the Technical Analysis service \( \text{TA}_0 \), the FX system replaces services \( \text{MW}_0, \text{TA}_1, \text{FA}_1 \) and \( \text{Or}_0 \) with \( \text{MW}_1, \text{TA}_0, \text{FA}_0 \) and \( \text{Or}_1 \), respectively;

G) All the degraded services recover, so the initial configuration \( \text{MW}_0, \text{TA}_0, \text{FA}_0, \text{Al}_1, \text{Or}_0 \) and \( \text{No}_1 \) is reinstated.

As in the case of the UUV system, a non-adaptive FX version will fail to meet the system requirements for extended periods of time. For example, choosing to always use the initial FX configuration from Fig. 22 would lead to a violation of the reliability requirement R1 while service \( \text{MW}_0 \) experiences a significant reliability degradation in the time interval B–D. While using service \( \text{MW}_1 \) instead of \( \text{MW}_0 \) would avoid this violation, \( \text{MW}_1 \) is more expensive but no faster than \( \text{MW}_0 \) (cf. Table 5) so its choice would increase the cost (2), thus violating the cost requirement R3 in the time interval A–B.

7.1.3 Discussion

For each change scenario from our experiments within the two case studies (cf. Figs. 21 and 22), we performed two checks. For the former check, we confirmed that the ENTRUST controller operated correctly. To this end, we established that the change was accurately reported by the sensors and correctly processed by the monitor, leading the analyzer to select the right new configuration, for which a correct plan was built by the planner and implemented by the executor.

For the latter check, we determined the suitability of the ENTRUST assurance cases. We started from the guidelines set by safety and assurance standards, which highlight the importance of demonstrating, using available evidence, that an assurance argument is compelling, structured and valid [34], [81], [112]. Also, we considered the fact that ENTRUST has been examined experimentally but has not been tested in real-world scenarios to generate the industrial evidence necessary before approaching the relevant regulator. However, our preliminary results show, based on formal design-time and runtime evidence, that the primary claim of EN-TRUST assurance cases is supported by a direct and robust argument. Firstly, the argument assures the achievement of the requirements either based on a particular active configuration or through reconfiguration, while maintaining a failsafe mechanism. Secondly, the argument and patterns are well-structured and conform to the GSN community standard [60]. Thirdly, ENTRUST provides rigorous assessments of validity not only at design time but also throughout-life, by means of monitoring and continuous verification that assess and challenge the validity of the assurance case based on actual operational data. This continuous assessment of validity is a core requirement for safety standards, as highlighted recently for medical devices [93]. As such, our approach satisfies five key principles of dynamic assurance cases [38]:

- continuity and updatability, as evidence is generated and updated at runtime to ensure the continuous validity of the assurance argument (e.g. the formal evidence for solution \( \text{R1Result} \) from the UUV argument in Fig. 19, which satisfies a system requirement given the current configuration);
- proactivity, since the assurance factors that provide the basis for the evidence in the assurance argument are proactively identified (e.g. the ConfigDef context from the UUV argument in Fig. 19, which captures the parameters of the current configuration);
- automation, because the runtime evidence is dynamically synthesised by the MAPE controller;
- formality, as the assurance arguments are formalised using the GSN standard.

In conclusion, subject to the limitations described above, our experiments provide strong empirical evidence that ENTRUST self-adaptive systems make the right adaptation decisions and generate valid assurance cases.

7.2 RQ2 (Efficiency)

To assess the efficiency of the ENTRUST generation of assurance evidence, we measured the CPU time taken by (i) the design-time UPPAAL model checking of the generic controller properties from Table 4; and (ii) the runtime probabilistic model checking performed by the ENTRUST analyzer. Fig. 23 shows the time taken to verify the generic controller properties from Table 4 for a three-sensor UUV system, and for an FX system comprising two third-party implementations for each workflow service. With typical CPU times of several minutes per property and a maximum below 12 minutes, the overheads for this design-time, once-only verification of all controller properties are entirely acceptable.

The CPU times required for the runtime probabilistic model checking of the QoS requirements for alternative configurations of the two systems (Fig. 24) have values below 1.5s and 2s, respectively. These runtime overheads, which correspond to under 10ms for the verification of a UUV configuration and under 30ms for the verification of an FX configuration, are acceptable because ENTRUST is intended for scenarios where:

1) failures and other changes requiring system reconfigurations are, on average, much less frequent than the
frequency with which the runtime verification can be executed (i.e. every 1.5–2s for our two systems); 2) failsafe configurations can be temporarily assumed if needed during the infrequent re-verifications of the ENTRUST stochastic models.

These assumptions ensure that, most of the time, ENTRUST adaptation decisions are reached before new changes occur and can be applied. They also ensure that any time spent in failsafe configurations is small compared to the time when the system employs “useful” configurations.

As shown in Fig. 24, we also ran experiments to assess the increase in runtime overhead with the system size and number of alternative configurations, by considering UUVs with up to six sensors, and FX system variants with up to five implementations per service. Typical for model checking, the CPU time increases exponentially with these system characteristics. This makes the current implementation of our ENTRUST instance suitable for self-adaptive systems with up to hundreds of configurations to analyse and select from at runtime. However, our recent work on compositional [21], incremental [70], caching-lookahead [55] and distributed [19] approaches to probabilistic model checking and on metaheuristics for probabilistic model synthesis [57] suggests that these more efficient model checking approaches could be used to extend the applicability of our ENTRUST instance to much larger configuration space sizes. As an example, in [55] we used caching of recent runtime probabilistic model checking results and anticipatory verification of likely future configurations (i.e. lookahead) to significantly reduce the mean time required to select new configurations for a variant of our self-adaptive UUV system (by over one order of magnitude in many scenarios). Integrating ENTRUST with these approaches is complementary to the purpose of this paper and represents future work.

7.3 RQ3 (Generality)

We used ENTRUST to develop an embedded system from the oceanic monitoring domain, and a service-based system from the exchange trade domain. As previously mentioned in Section 3 and summarised in Table 1, self-adaptation within these systems was underpinned by the verification of continuous- and discrete-time Markov chains, respectively; and the requirements and types of changes for the two systems differed. Finally, the ENTRUST assurance arguments for the two systems were based on assurance evidence obtained using multiple verification techniques:

1) testing evidence for the correct operation of trusted virtual machine;
2) model checking evidence for the correctness of the MAPE controller and the failsafe system requirements;
3) probabilistic model checking evidence for the remaining system requirements.

Although evaluation in additional areas is needed, these results indicate that our ENTRUST instance can be used across application domains.

To assess the overall generality of ENTRUST, we note that probabilistic model checking can effortlessly be replaced with simulation in our experiments, because the probabilistic model checker PRISM can be configured to use discrete-event simulation instead of model checking techniques. Using this PRISM configuration requires no change to the Markov models or probabilistic temporal logic properties we analysed at runtime. As for any simulation, the analysis results would be approximate, but would be obtained with lower overheads than those from Fig. 24.

The uncertainties that affect self-adaptive systems are often of a stochastic nature, and thus the use of stochastic models and probabilistic model checking to analyse the behaviour of these systems is very common (e.g. [15], [20], [27], [44], [47], [50], [90], [104]). As such, our ENTRUST instance is applicable to a broad class of self-adaptive systems.

Nevertheless, other methods have been used to synthesise MAPE controllers and to support their operation. Many such methods (e.g. based on formal proof, traditional model checking, other simulation techniques and testing) are described in Section 8. Given the generality of ENTRUST, these methods could potentially be employed at design time and/or at runtime by alternative instantiations of ENTRUST, supported by different modelling paradigms, requirement specification formalisms, and tools. For example, the use of the (non-probabilistic) graph transformation models or dynamic tests proposed in [6] and [51], respectively, in the self-adaptation ENTRUST stage is not precluded by any of our assumptions (cf. Section 4.2.1), although the method chosen for this stage will clearly constrain the types of requirements for which assurance evidence can be provided at runtime.
7.4 Threats to Validity

Construct validity threats may be due to the assumptions made when implementing our simple versions of the UUV and FX systems, and in the development of the stochastic models and requirements for these systems. To mitigate these threats, we implemented the two systems using the well-established UUV software platform MOOS-IvP and (for FX) standard Java web services deployed in Tomcat/Axis. The model and requirements for the UUV system are based on a validated case study that we are familiar with from previous work [55], and those for the FX system were developed in close collaboration with a foreign exchange expert.

Internal validity threats can originate from how the experiments were performed, and from bias in the interpretation of the results due to researcher subjectivity. To address these threats, we reported results over multiple independent runs; we worked with a team comprising experts in all the key areas of ENTRUST (self-adaptation, formal verification and assurance cases); and we made all experimental data and results publicly available to enable replication.

External validity threats may be due to the use of only two systems in our evaluation, and to the experimental evaluation having been done by only the authors’ three research groups. To reduce the first threat, we selected systems from different domains with different requirements. The evaluation results show that ENTRUST supports the development of trustworthy self-adaptive solutions with assurance cases for the two different settings. To reduce the second threat, we based ENTRUST on input from, and needs identified by, the research community [25], [30], [36], [37]. In addition, we fine-tuned ENTRUST based on feedback from industrial partners involved in the development of mission-critical self-adaptive systems, and these partners are now using our methodology in planning future engineering activities. Nevertheless, additional evaluation is required to confirm generality for domains with characteristics that differ from those in our evaluation (e.g., different timing patterns and types of requirements and disturbances) and usability by a larger number of users.

8 Related Work

Given the uncertain operating conditions of self-adaptive systems, a central aspect of providing assurances for such systems is to collect and integrate evidence that the requirements are satisfied during the entire lifetime. To this end, researchers from the area of self-adaptive systems have actively studied a wide variety of assurance methods and techniques applicable at design time and/or at runtime [30], [36], [84], [108], [119], [122], [128]. Tables 6 and 7 summarise the state of the art, partitioned into categories based on the main method used to provide assurances, e.g., formal proof, model checking or simulation. We consider as the main method of a study from our analysis the method that the study primarily focuses on; the approaches from these studies may implicitly use additional methods, such as testing of their platforms and tools, but this is not emphasised by their authors. We summarise the representative approaches included in each category according to their:

1) Assurances evidence, comprising separate parts for the methods used to provide assurance evidence for: (i) the correctness of the platform used to execute the controller, (ii) the correctness of the controller functions, and (iii) the correctness of the runtime adaptation decisions;

2) Methodology, comprising three parts: the engineering process (i.e., a methodical series of steps to provide the assurances), tool support (i.e., tools used by engineers to provide evidence at design time and tools used at runtime by the controller, e.g., during analysis or planning), and other reusable components (i.e., third-party libraries and purpose-built software components used as part of the controller, and other artefacts that can be used at design time or at runtime, including models, templates, patterns, algorithms).

Providing assurances for self-adaptive systems with strict requirements requires covering all these aspects, as well as an assurance argument that integrates the assurance evidence into a compelling, comprehensible and valid case that the system requirements are satisfied. Unlike ENTRUST (Table 8), the current research disregards this need for an assurance argument. We discuss below the different approaches and point out limitations that we overcome with ENTRUST.

Formal proof establishes theorems to prove properties of the controller or the system under adaptation. Proof was used to provide evidence for safety and liveness properties of self-adaptive systems with different semantics (one-point adaptation, overlap adaptation, and guided adaptation) [127]. Formal proof was also used to provide evidence for properties of automatically synthesised controllers, e.g., the completeness and soundness of synthesised behavioral models that satisfy an expressive subset of liveness properties [42] and correctness and deadlock free adaptations performed by automatically synthesised controllers [74]. Finally, formal proof was used to demonstrate the correctness of adaptation effects, e.g., proofs for safety, no deadlock, and no starvation of system processes as a result of adaptation [13], and guarantees for the required qualities of adaptations, e.g., proofs for optimised resource allocation, while satisfying quality of service constraints [1]. The focus of all these approaches is on providing assurance evidence for particular aspects of adaptation. All of them offer reusable components, however, these solutions require complete specifications of the system and its environment, and—unlike ENTRUST—cannot handle aspects of the managed system and its environment that are unknown until runtime.

Model checking enables verifying that a property holds for all reachable states of a system, either offline by engineers and/or online by the controller software. Model checking was used to ensure correctness of the adaptation functions that are modeled as interacting automata, with the verified models directly interpreted during execution by a thoroughly tested virtual machine [69]. Model checking was also used to provide guarantees for automatic controller synthesis and enactment, e.g., to assure that a synthesised controller and reusable model interpreter have no anomalies [12]. Model checking has extensively been used to provide guarantees for the effects of adaptation actions on the managed system, e.g., for safety properties of the transitions of a managed system that is modeled as
TABLE 6
Overview of related research on assurances for self-adaptive systems - part I

<table>
<thead>
<tr>
<th>Approach</th>
<th>Assurance evidence</th>
<th>Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Controller platform</td>
<td>Controller functions</td>
</tr>
<tr>
<td></td>
<td>Formal proof</td>
<td></td>
</tr>
<tr>
<td>Adaptation semantics [127]</td>
<td>Proof of safety and liveness of adaptive programs and program compositions</td>
<td></td>
</tr>
<tr>
<td>Synthesis of behavioral models [42]</td>
<td>Proof of completeness and soundness of synthesized behavioral models</td>
<td></td>
</tr>
<tr>
<td>Controller synthesis [74]</td>
<td>Proof that controller synthesis algorithm generates controllers that guarantee correct and deadlock free adaptations</td>
<td>Controller synthesis process only</td>
</tr>
<tr>
<td>Correctness adaptation effects [13]</td>
<td>Proof of safety, no deadlock, and no starvation of system processes as a result of adaptation</td>
<td></td>
</tr>
<tr>
<td>Guaranteed qualities [1]</td>
<td>Proof of optimizing resource allocation under QoS constraints</td>
<td></td>
</tr>
<tr>
<td>Correct adaptation functions [69]</td>
<td>Thoroughly tested virtual machine used to interpret and run controller models</td>
<td>Synthesized controller that is guaranteed not to be anomalous</td>
</tr>
<tr>
<td>Controller synthesis and enactment [12]</td>
<td>Synthesized controller model</td>
<td>Tool used for controller synthesis</td>
</tr>
<tr>
<td>Safe adaptation configurations [6]</td>
<td>Verification of safety properties of system transitions using a graph transformation model</td>
<td></td>
</tr>
<tr>
<td>Guaranteed qualities [18]</td>
<td>Probabilistic model checking of continually updated stochastic models of the controlled system and the environment to ensure non-functional requirements</td>
<td>PRISM verification library for analysis of stochastic system and environment models</td>
</tr>
<tr>
<td>Resilience to controller failures [24]</td>
<td>Probabilistic model checking of resilience properties of synthesized Markov models of the managed system</td>
<td>Procedure to check resilience to controller failures</td>
</tr>
</tbody>
</table>

a graph transformation system [6], to ensure non-functional requirements by runtime verification of continually updated stochastic models of the controlled system and the environment [18], and to provide evidence for resilience properties of synthesized Markov models of the managed system [24]. Again, the focus of all the approaches is on providing assurance evidence for particular aspects of adaptation. The ENTRUST instance presented in Section 5 uses two of these techniques (i.e., [69] and [18]) to verify the correctness of the MAPE logic at design time and to obtain evidence that adaptation decisions are correct at runtime, respectively. In addition, ENTRUST offers a process for the systematic engineering of all components of the self-adaptive system, which includes employing an industry-adopted standard for the formalization of assurance arguments.

Simulation approaches provide evidence by analysing the output of the execution of a model of the system. Simulation was used to evaluate novel self-adaptation approaches, e.g., to ensure the scalability and robustness to node failures and message loss of a self-assembly algorithm [106], and to support the design of self-adaptive systems, e.g., to check if the performance of a latency-aware adaptation algorithm falls within predicted bounds [27]. Recently some efforts have been made to let the controller exploit simulation at runtime to support analysis, e.g. runtime simulation of stochastic models of managed system and environment has been used to ensure non-functional requirements with certain level of confidence [121]. The primary focus of simulation approaches has been on providing assurance evidence for the adaptation actions (either as a means to check the controller effects or to make a prediction of the expected effects of different adaptation options). The approaches typically rely on established simulators.

Testing is a standard method for assessing if a software system performs as expected in a finite number of scenarios. Testing was used to test the effectiveness of adaptation frameworks, e.g. checking whether a self-repair framework applied to a client-server system keeps the latencies of clients within certain bounds when the network is overloaded [54]. Testing was used to provide evidence for the robustness of controllers by injecting invalid inputs at the controller’s interface and use the responses to classify robustness [24]. Several studies have applied testing at runtime, e.g. to validate safe and correct adaptations of the managed system based on adapt test cases generated in response to changes in the system and environment [51]. While simulation and testing approaches can be employed within the generic ENTRUST methodology to obtain
### TABLE 7
Overview of related research on assurances for self-adaptive systems - part II

<table>
<thead>
<tr>
<th>Approach</th>
<th>Assurance evidence</th>
<th>Methodology</th>
<th>Other reusable components</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Controller platform</td>
<td>Controller functions</td>
<td>Engineering process</td>
</tr>
<tr>
<td>Evaluation novel approach [106]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adaptation decisions</td>
<td>Tool support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Other reusable components</td>
</tr>
<tr>
<td>Support for design [27]</td>
<td>Offline simulation to ensure the scalability and robustness to node failures and message loss</td>
<td>OMNeT++ simulator for checking algorithm performance</td>
<td></td>
</tr>
<tr>
<td>Runtime analysis [121]</td>
<td>Offline simulation to check if the performance of a latency-aware adaptation algorithm falls within predicted bounds</td>
<td>UPPAAL-SMC used for online simulation of stochastic system and environment models</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Runtime simulation of stochastic models of managed system and environment to ensure non-functional requirements with certain level of confidence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test effectiveness of adaptation framework [54]</td>
<td>Offline stress testing in client-server system, showing that self-repair significantly improves system performance</td>
<td>Rainbow framework to realise self-adaptation</td>
<td></td>
</tr>
<tr>
<td>Test controller robustness [24]</td>
<td>Robustness testing of controller by injecting invalid inputs at the controller’s interface and employ responses to classify robustness</td>
<td>Probabilistic response specification patterns for robustness testing</td>
<td></td>
</tr>
<tr>
<td>Runtime testing [51]</td>
<td>Dynamic tests to validate safe and correct adaptation of system using test cases adapted to changes in the system and environment</td>
<td>One-stage process for test case adaptation</td>
<td></td>
</tr>
<tr>
<td>Other approaches</td>
<td>Control-theoretic guarantees for one goal (setpoint) used automatically synthesised controller at runtime</td>
<td>ARPE tool to build online a first-order model of the system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controller guarantees for stability, overshoot, settling time and robustness of system operating under disturbances</td>
<td>Kalman filter and change point detection procedure for model updates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Online verification of the probability that a temporal property is satisfied given a sample execution trace</td>
<td>TRACE-CONTRACT tool used for trace analysis</td>
<td></td>
</tr>
<tr>
<td>Sanity checks [116]</td>
<td>Sanity checks evaluate the correctness of resource sharing decisions made by a reasoning engine</td>
<td>CHAMELEON tool providing performance guarantees</td>
<td></td>
</tr>
</tbody>
</table>

### TABLE 8
Comparison of ENTRUST to related research on assurances for self-adaptive systems

<table>
<thead>
<tr>
<th>Approach</th>
<th>Assurance evidence</th>
<th>Methodology</th>
<th>Other reusable components</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Controller platform</td>
<td>Controller functions</td>
<td>Engineering process</td>
</tr>
<tr>
<td></td>
<td>Adaptation decisions</td>
<td></td>
<td>Tool support</td>
</tr>
<tr>
<td></td>
<td>Assurance argument</td>
<td></td>
<td>Other reusable components</td>
</tr>
<tr>
<td>Generic ENTRUST methodology</td>
<td>Reuse of verified application-independent controller functionality</td>
<td>Verification of controller models to ensure generic controller requirements and some system requirements</td>
<td>Development of partial assurance argument at design time, and synthesis of dynamic assurance argument during self-adaptation</td>
</tr>
<tr>
<td>Tool-supported ENTRUST instance</td>
<td>UPPAAL model checking of interacting timed automata models to ensure controller deadlock-freeness, liveness, etc. and functional system requirements</td>
<td>UPPAAL model checking of continually updated stochastic models of the Controlled system and the environment to ensure non-functional requirements</td>
<td>Assurance argument synthesised using the industry-adopted Goal Structuring Notation (GSN) standard</td>
</tr>
</tbody>
</table>
assurance evidence for particular aspects of self-adaptive systems, they need to be complemented by assurances for other components of a self-adaptive system and integrated in a systematic process as provided by ENTRUST.

Other approaches. We highlight some other related approaches that have been used to provide assurances for self-adaptive systems. Recently, there has been a growing interest in applying control theory to build “correct by construction” controllers [97]. The approach was used to automatically synthesise controllers at runtime, providing control-theoretic guarantees for stability, overshoot, setting time and robustness of system operating under disturbances [49]. Although promising, this research is at an early stage, and its potential to deliver solutions for real-world systems and scenarios has yet to be confirmed. In contrast, ENTRUST relies on proven software engineering techniques for modelling and analysing software systems and assuring their required properties. Runtime verification is a well-studied lightweight verification technique based on extracting information from a running system to detect whether certain properties are violated. For example, sequences of events can be modeled as observation sequences of a Hidden Markov Model allowing to verify the probability that a temporal property is satisfied by a run of a system given a sampled execution trace [103]. Sanity checks are another approach to check the conformance of requirements of adaptive systems. Sanity checks have been used to evaluate the correctness of resource sharing decisions made by a reasoning engine [116]. Approaches such as runtime verification and sanity checks are often supported by established tools. However, these approaches provide only one piece of evidence. Such approaches can also be used by our generic ENTRUST methodology, which supports the integration of assurance evidence from multiple sources in order to continuously generate an assurance case.

Another line of related research (not specifically targeting self-adaptation and thus not included in Table 7) is runtime certification, proposed in [94] and further developed in [75], [96]. Runtime certification involves the proactive runtime monitoring of the assumptions made in the assurance case, thereby providing early warnings for potential failures. ENTRUST goes beyond the mere monitoring of assumptions, to evolving the arguments and evidence dynamically based on the runtime verification data, particularly for self-adaptive software assurance. ENTRUST also extends existing work on assurance argument patterns [39] by enabling runtime instantiation.

The ENTRUST methodology and the other research summarised in this section also build on results from the areas of configurable software, configuration optimisation, and performance tuning. For instance, symbolic evaluation has been used to understand the behaviour of configurable software systems [92], dedicated support to automatically verify the correctness of dynamic updates of client-server systems has been proposed [66], and specification languages have been devised to help program library developers expose multiple variations of the same API using different algorithms [35]. Research in this area has been applied to realise self-adaptive software systems. For example, it has been used to deal with the problem of configurability of multi-tenant cloud settings by using a game theoretic approach that maximises tenants’ preferences satisfaction [53], to find workarounds and add configuration guards to prevent particular failures [105], and to model the variability of cloud systems and identify reconfigurations that meet given criteria using temporal constraints and reconfiguration operations [99]. While these approaches address adaptation of highly configurable systems at runtime, they provide only specific pieces of evidence. Runtime testing as mentioned above (e.g. [51]) is one interesting approach to ensure that such systems continue to execute in a safe and correct manner when adapting to handle changing environmental conditions. Such an approach could be integrated in the generic ENTRUST methodology as part of the analysis phase to provide guarantees about the runtime decision making process of self-adaptation.

Finally, assurance cases and GSN in particular are related to goal modeling. Several approaches exist that provide alternative means to specify goal models for self-adaptive systems; we discuss a representative selection. RELAX offers a textual language that allows requirements to be temporarily relaxed to deal with uncertainty in adaptation [125]. RELAX has been integrated with traditional goal modeling using KAOS [29]. FLAGS provides both crisp goals specified in linear temporal logic and fuzzy goals specified in fuzzy temporal language [5]. Adaptations are triggered by violated goals and the goal model is modified accordingly to maintain a coherent view of the system and enforce adaptation on the running system. Other researchers specify requirements for adaptive systems as two complementary types: awareness requirements and evolution requirements [100]. Awareness requirements indicate the situations that require adaptation and evolution requirements prescribe what to do in these situations. The development of GSN was influenced by the research on goal modeling. Similar to the approaches discussed above, the notation is used to represent and decompose system goals, but in addition to that explicitly incorporate rationale arguments for the decomposition.

The sparsity of Tables 6 and 7 makes clear that existing approaches are confined to providing correctness evidence for specific aspects of the self-adaptive software. In contrast to existing work on assurances for self-adaptive systems, Table 8 shows that ENTRUST offers an end-to-end methodology for the development of trustworthy self-adaptive software systems. Unique to our approach, this includes the development of assurance arguments. The upper part of Table 8 shows how the generic ENTRUST methodology covers the whole spectrum of aspects that are required to provide assurances for self-adaptive systems with strict requirements. The lower part of Table 8 shows a concrete tool-supported instantiation of ENTRUST and summarises how the various assurances aspects are covered for this instance. Details about the information summarised in the table are provided in Sections 4 and 5.

9 Conclusion

We introduced ENTRUST, the first end-to-end methodology for the engineering of trustworthy self-adaptive software systems and the dynamic generation of their assurance cases. ENTRUST and its tool-supported instance presented
in the paper include methods for the development of verifiable controllers for self-adaptive systems, for the generation of design-time and runtime assurance evidence, and for the runtime instantiation of an assurance argument pattern that we devised specifically for these systems.

The future research directions for our project include evaluating the usability of ENTRUST in a controlled experiment, extending the runtime model checking of system requirements to functional requirements, and reducing the runtime overheads by exploiting recent advances in probabilistic model checking at runtime [19], [21], [46], [55], [70]. In addition, we are planning to explore the applicability of ENTRUST to other systems and application domains.

References


