



HAL
open science

Model-based analysis support for dependable complex systems in CHES

Alberto Debiasi, Felicien Ihirwe, Pierluigi Pierini, Silvia Mazzini, Stefano Tonetta

► **To cite this version:**

Alberto Debiasi, Felicien Ihirwe, Pierluigi Pierini, Silvia Mazzini, Stefano Tonetta. Model-based analysis support for dependable complex systems in CHES. 9th International Conference on Model-Driven Engineering and Software Development, Feb 2021, Vienna (Online), Austria. hal-03002722

HAL Id: hal-03002722

<https://hal.science/hal-03002722v1>

Submitted on 12 Nov 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Model-based analysis support for dependable complex systems in CHES

Felicien Ihirwe¹, Silvia Mazzini¹, Pierluigi Pierini¹, Stefano Tonetta² and Alberto Debiasi²

¹*Innovation Technology Service Lab, Intecs Solution Spa, Pisa, Italy*

²*Embedded Systems Unit, Fondazione Bruno Kessler (FBK), Povo, Italy*

{felicien.ihirwe,silvia.mazzini,pierluigi.pierini}@intecs.it, {adebiasi,tonettas}@fbk.eu

Keywords: CHES, model driven engineering, complex systems, dependability analysis

Abstract: The challenges related to dependable complex systems are heterogeneous and involve different aspects of the system. On one hand, the decision-making processes need to take into account many options. On the other hand, the design of the system logical architecture must consider various dependability concerns such as safety, reliability, and security. Moreover, in case of high-assurance systems, the analysis of such concerns must be performed with rigorous methods. In this paper, we present the new development of CHES, a cross-domain, model-driven, component-based and open-source tool for the development of high-integrity systems. We focus on the new recently distributed version of CHES, which supports extended model-based development and analyses for safety and security concerns. Finally, we present contributions of CHES to several international research projects.

1 INTRODUCTION

The ever increasing complexity and dependability issues of systems in various domains, such as transportation, space, energy, health, and industrial production, requires effective design and development methods. The complexity and heterogeneity of components requires modeling approaches that spans different technical disciplines and prove effective in the end-to-end engineering of the products. This imply taking into account various requirements such as quality, performance, cost, safety, security, and reliability. Model-based design technologies enable the user to perform beforehand different assurance related activities such as physical architecture exploration, system's behavioral analysis, early verification, and validation.

CHES (Cicchetti et al., 2012) toolset offers a cross-domain modeling and analysis of high-integrity systems providing an integrated framework that helps the modeler (user) to automate different development phases: from the requirements definition, to the architectural modeling of the system's software and hardware, up to its deployment to hardware platform (Cicchetti et al., 2012). CHES follows a component-based approach where the user decouple different functional parts of the system as components that can be modeled, analyzed, verified, stored, reused individually, and be integrated to meet the system's com-

mon goal. CHES supports, among other, schedulability and dependability analysis across the entire projects life cycle. The results of the analysis are back-propagated to the model itself so that the modeler can review and fine-tune the model to satisfy real-time and dependability requirements (Puri et al., 2020).

CHES recently became a full-fledged open-source project, hosted by The Eclipse Foundation (<https://www.eclipse.org/ches/>). The code is developed by various contributors following an open-source approach with public projects for issue tracking, code repository branches, and continuous integration. This paper presents the latest development of CHES to address software's security and safety analysis of the system exploiting the CHES error model to represent faults and attacks. Analysis is completed by the integration with back-end tools such as xSAP (Bittner et al., 2016) and Mobius (Courtney et al., 2009) for the minimal cut sets analysis and Monte-Carlo simulation.

We report on various projects that used CHES to provide evidence for the assurance of complex systems and on the functionalities that have been added for such purpose. So far CHES has been applied in domains such as Avionics (Godard and Nelissen, 2016), Automotive (Bressan et al., 2018), Space (Pace et al., 2014), Telecommunication (Mazzini, 2015), and Petroleum (Gallina et al., 2014)(Montecchi and

Gallina, 2017).

The rest of the paper is arranged into six sections. Sections 2 provides an introduction to the CHESSTM tool building blocks and methodology, Section 3 presents the new major features released under CHESSTM 1.0.0, Section 4 presents some practical applications on different projects, Section 5 discusses the related work with respect to CHESSTM approach. In Section 6 we present the envisioned future extension on CHESSTM and finally Section 7 concludes the paper.

2 CHESSTM IN A NUTSHELL

The CHESSTM modeling tool was released under the Eclipse PolarSys project¹ and recently it was moved from the incubation status to the first major release. CHESSTM is an integrated modelling language profiled from OMG standard languages: UML, SysML and MARTE under the Papyrus modeling environment (Papyrus, 2020). Figure 1 shows the high-level architecture of CHESSTM infrastructure. Not all the features from all the three languages were used, CHESSTM only exploits specific subsets of the them that suits its perspective. There are different tools, plugins, and languages that were integrated into CHESSTM to support model validation, model checking, realtime and dependability analysis.

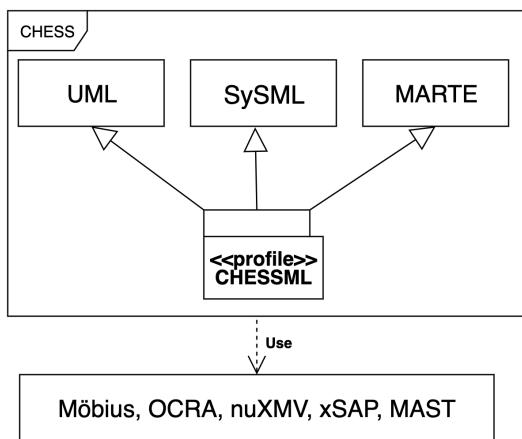


Figure 1: CHESSTM high level structure

In this section, we are going to look at different core aspects of CHESSTM methodology, development features, and implementation mechanisms. We will also look in depth at different analysis mechanisms that are being performed in CHESSTM and how they link together to enhance system correctness.

¹<https://projects.eclipse.org/projects/polarsys.chesstm>

2.1 Component-based methodology

CHESSTM language supports a component-based development methodology. Emphasis is given to *separation of concerns* between the functional and the non-functional dimensions, such as safety, security, reliability, performance, and robustness (Mazzini et al., 2015).

In CHESSTM, components at design level encompass functional concerns only (i.e., they are devoid of any constructs pertaining to tasking and specific computational model). The specification of non-functional attributes is then used for the automated generation of the container, enforcing the realization of the non-functional attributes declared for the component to be wrapped.

This CHESSTM component-based approach enforces two main aspects of modeling: “Compositionality” and “Composability”. Compositionality implies that all the properties of the whole system are determined as the collection of the properties of the constituting components and its execution environment. Composability is achieved when the individual components’ properties are preserved from its definition, development, and deployment on the target platform (Mazzini et al., 2015). These two component’s properties are conceived through the whole development process to support the “composition with guarantee” property, which in turn, gets verified through analysis results.

The CHESSTM methodology follows the “Correctness by Construction” practice which enforces (1) the use of formal and precise tools and notations for the development and the verification of all product items; (2) say things only once to avoid contradictions and repetitions; (3) the design of software components that are easy to verify, by e.g., using safer language subsets, and to implement, by using appropriate coding styles and design patterns. (Panunzio and Vardanega, 2014).

2.2 Multi-view modeling approach

The CHESSTM tool provides a set of design views to uphold the “separation of concern”, the “correctness by construction” and the other methodological principles introduced before. Six main views (requirement, component, system, deployment, analysis and instance views) are defined to support The CHESSTM modeling approach. Throughout the development process, each view has its own underlined constraints that enforce its specific privileges on model entities and properties that can be manipulated. Depending on the current stage of the design process, CHESSTM sub-views are adopted to enhance certain de-

sign properties or stages of the process. Figure 2 shows the high level architecture of CHES views and their inter-relations.

2.2.1 Requirement view

Originally adopted from the SysML requirement diagram, the requirement view is used to define system requirements and track their verification. In CHES, requirements are part of the model and play a central role in the system development life cycle. The system elements are associated with the technical requirements they satisfy, which are, in turn, traced to higher-level requirements, up to system-level requirements (Mazzini et al., 2015). This association technique enhances the traceability while evaluating the correctness and consistency of the modeled system. In this way, the change's impact can be better evaluated and faithful model verification evidence can be provided according to the requirements.

2.2.2 System view

It provides a suitable frame for system-level design activities. In the System view, the system entities are initially designed into blocks and then hierarchically decomposed. The system view supports contract-based design and several functional and dependability analysis. CHESML inherits from SysML the specification of the block hierarchies and their internal decomposition, i.e. a block definition diagram can describe a system structure by means of a set of blocks and each block may have its own dedicated internal block diagram describing its sub-blocks decomposition and interfaces.

2.2.3 Component view

This view is used for software design work and logic of the intended model. The component view is composed of two sub-views, **Functional View** which is enabled by default, and the **Extra-Functional View** which is enabled manually in the tool. The **Functional View** is used to model system functional specifications using diagrams such as class, composite structure, state machine, activity, and sequence diagrams. On the other hand, the **Extra-Functional View** is used to compose the system's extra-functional specifications such as the real-time and dependability attributes. Recall that all views have a dedicated palette depending on their requirements, for instance, the extra-functional view has no access to the activity diagram and has the palette with entries exclusively related to extra-functional concerns.

2.2.4 Deployment view

This view is used to model for software design the hardware structure of the system and permits the allocation of their corresponding software component instances. Through the use of class and composite structure diagrams, the user can model the type of deployment on either single or multi-core processor. In this view, each hardware resource is allocated to a specific memory partition and can only access and change its own memory space. Regarding the software to hardware resources allocation, all software components are allocated to cores.

2.2.5 Analysis view

This is used to capture all the activities and diagrams related to analysis in CHES. The analyses performed in CHES are real-time analysis, quantitative dependability analysis, failure propagation analysis, and so on. We will discuss further on analysis in section 2.3.

2.2.6 Instance view

CHES provides a dedicated view to visualize and model the Platform Specific Model (PSM) as a combination of hardware and software instances generated from the deployment and component views respectively through the composite structure diagrams. This is a novel approach to facilitate the analysis between model instances. These instances are automatically generated when the BuildInstance command is invoked. In the generated instance model each component's property and connector are mapped onto a dedicated *InstanceSpecification*.

2.3 Model-based Analysis and verification

CHES provides the capability to perform several kinds of analysis depending on the specific requirements (functional, timing, dependability). Many of these functionalities have been added to the new release of CHES and are further explained in the next section.

Functional Verification by means of model checking is supported by the integrated *nuXmv* model checker (Cavada et al., 2014). System and component properties, derived from requirements, can be formalized into linear temporal logic properties, then they can be verified on top of the system's or component's behavioral models developed using state machines.

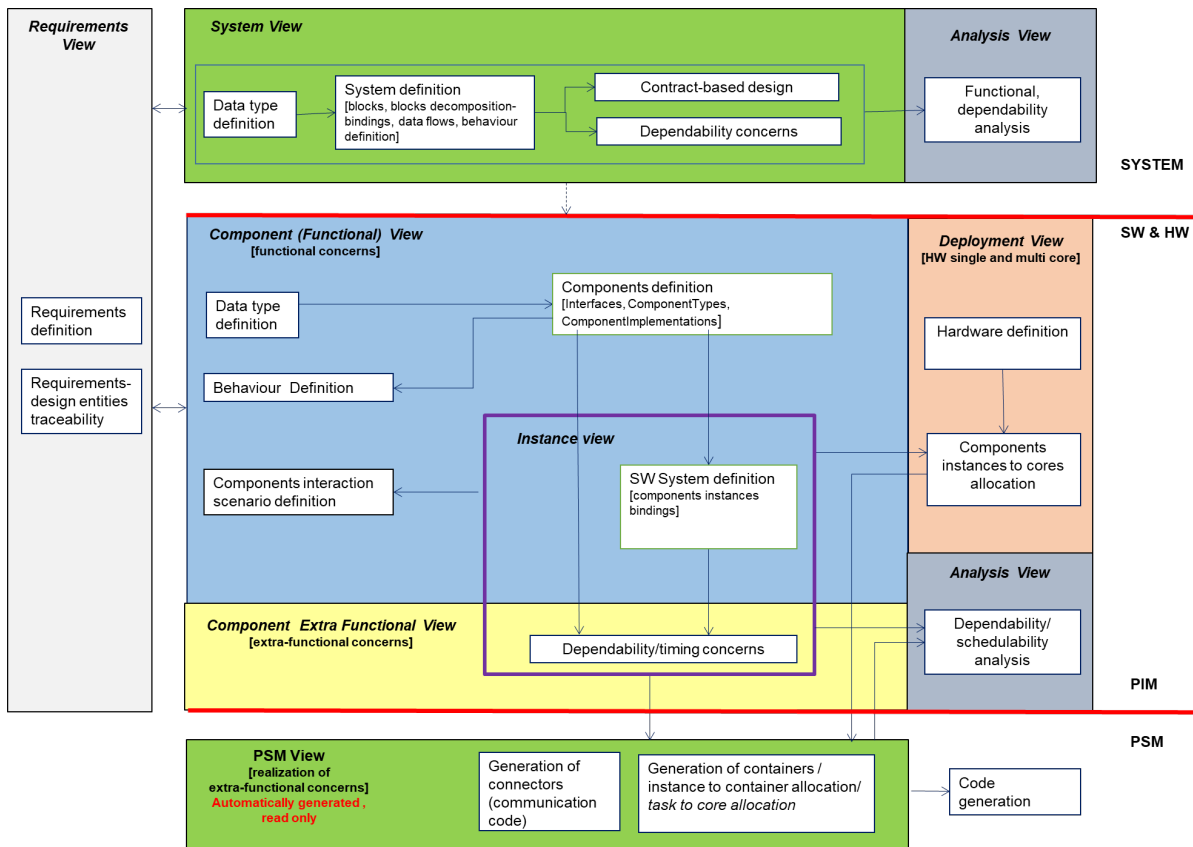


Figure 2: CHESV views architecture,

Contract-Based Analysis is built on top of the OCRA tool support (Cimatti et al., 2013). Component formal properties are structured in terms of contracts, comprised of an assumption and a guarantee pairs. The assumption is a restriction on the component’s environment or usage, and the guarantee is a property that must be satisfied by the component - provided that the environment satisfies the assumption (Mazzini et al., 2016).

Timing Analysis is built on top of the MAST² analysis tool. It is invoked to perform analysis such as schedulability and end-to-end response time analysis. Schedulability analysis is performed by taking input from the annotated PSM model and the computed partition schedule on each available processing unit. Then, the response-time analysis calculates the worst-case response time of each task (Godard and Nelissen, 2016) assessing the schedulable tasks complying with the given timing constraints. The end-to-end analysis is done by utilizing the component sequence diagram. Applying MARTE timing stereotypes, the tool evaluates the hardware component’s responsiveness. This analysis facilitates “early end-to-end response time

²<https://mast.unican.es/>

verification”, giving a sense of any possible refinement of the model before deployment (Mazzini et al., 2015).

Model validation exploits several types of methods to assess the software system on its target platform. We can mention: (1) *Model core constraints validation* is performed to enforce the CHESV model constraints including specific preconditions as required by the schedulability analysis. (2) *Validate model for state-based analysis*, (3) *Validate model for model checking*, (4) *Validate model for criticality specification* and finally (5) *Validate model for Automotive 26262 compliance* (only specific for automotive domain) checks the system correctness of Automotive Safety Integrity Level (ASIL) inheritance and decomposition according to the ISO 26262 standard.

3 NEW SYSTEM-LEVEL ANALYSIS SUPPORT

In this section, we present the new major features released in CHESV 1.0.0. The new release includes the extension support for system-level safety

and security analysis. CHESMML dependability profile which normally supports different techniques for safety and dependability analysis has been extended to model fault injection and threats. Other new features include contract validations, parameter-based architectures, and document generation. This new release can be accessed at <https://www.eclipse.org/chess/>

3.1 Fault Injection and Model-Based Safety Analysis with xSAP

The new release supports the conduct of Fault Tree Analysis (FTA) and Fault Mode Effect Analysis (FMEA). FTA is a deductive technique for identifying, evaluating, and modeling the interrelationship between events leading to a failure or an undesired state. FMEA is a highly structured approach through which all potential failure modes of a system and their effects can be identified, evaluated, and prioritized (Bozzano and Villaforita, 2013).

Once the system model is defined in CHESM, through components definition and their nominal behavioral model, the faulty behavior is expressed through a specific state machine called "Error Model". The Error Model extends the nominal state machine with information about the effect upon a property of the component, and consequently on its nominal behavior. The next figure represents an example of an error model that, in case of an internal fault, moves the related component in an error state where the property "energy" is stuck at 0 value. The optional probability assigned to that transition is 5×10^{-2} . Once the error model is defined, the FTA or

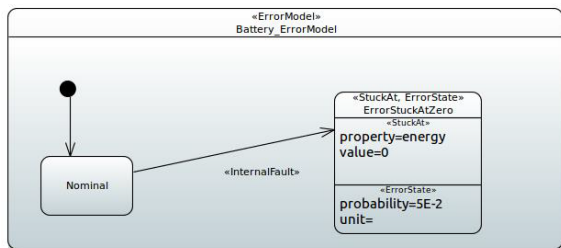


Figure 3: State machine modeling faulty behavior

FMEA can be done by invoking the xSAP symbolic model checker through the CHESM environment.

The xSAP approach is based on the library-based fault injection (i.e., an extension of a behavioral model with the definition of faults taken from a library of faults) and the use of model-based routines to generate safety artifacts.

The result of the FTA is the fault tree that is automatically shown in a dedicated panel in the front-

end; see Figure 3 for an example. If fault probabilities have been specified during the configuration of the error model, the fault tree will report their combination. The fault tree can be examined for the minimal cut-set, identifying the basic fault conditions which can lead to the top-level failure. This is ad-

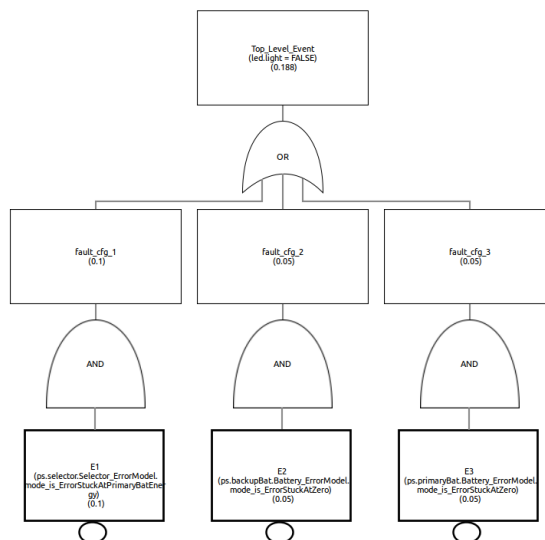


Figure 4: A fault tree visualized in the CHESM Editor View; note the probabilities associated to the top and basic events

ditional to the already existing analysis techniques in CHESM such as Failure Logic Analysis (CHESM-FLA) (Gallina et al., 2014) and State Based Quantitative Dependability Analysis (CHESM-SBA) (Montecchi et al., 2013).

3.2 Reliability Analysis with Mobius

Möbius³ is a software tool for modeling the behavior of complex systems, by allowing the study of the reliability, availability, security, and performance for large-scale discrete-event systems (Courtney et al., 2009). Many reliability analysis results can be obtained with probabilistic models built with Mobius using the stochastic activity networks (SAN) formalism, solved via Monte-Carlo simulation⁴. The CHESM profile for dependability is used to enrich functional models of the system with information regarding the behavior with respect to faults and failures, thus allowing properties like reliability, availability, and safety to be documented and analyzed.

The new release supports the modeling of security concerns which helps in threat identification at

³<https://www.mobius.illinois.edu/>

⁴<https://www.investopedia.com/terms/m/montecarlosimulation.asp>

the early stages of the development and facilitates the exploiting of the Mobius capabilities for analysis of reliability. Specific extensions are related to the modelling of Cyber-Attacks aspects and models transformations from CHES to the Mobius tool to run the analysis of SANs.

As a results the implemented a methodology allows modeling of a system security threat and a data corruption threat, which may result in a service corruption. An example of a system security threat can be a cyber-security attack, i.e. an unauthorized access of the system, halting services. Figure 5 depict the



Figure 5: Process of Security breach

process of a security breach that leads to the violation of the security-related properties. A *threat* event, initiated by a threat source agent, able to exploit a *vulnerability* of an asset (e.g. a component/system) may result in a loss to the confidentiality, integrity, and/or availability of the asset. Vulnerabilities could be represented as a pre-defined enumeration collected through different sources (e.g. personal competence, standards, results of previous threat analysis, etc.). Finally, the consequences could be modeled using pre-defined effects, which refers to the loss of Confidentiality, Integrity and Availability (CIA).

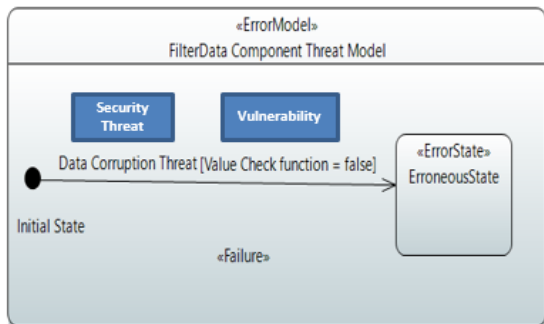


Figure 6: Erroneous state transition due to security threat event and vulnerability

An <<ErrorModel>>-tagged state machine is used when modeling the security breach. The failure, internal fault, and effect are extended to include security threats, vulnerability, and consequences respectively. Figure 6 illustrates an example of an error model, where a cyber-security attack initiates a data corruption threat. The vulnerability was modeled exploiting the value check function which is set to false. In this case, the system transits to an erroneous state

leading to component failure. Note that a component could have multiple instances of <<ErrorModel>>-tagged state machines, attached to it. Each instance would provide the elaboration of input/output failure behavior addressing a specific concern.

The generation of the Mobius SAN model process is done by performing an automatic model-to-model transformation from a model instance to the SAN model recognized by Mobius for reliability analysis.

The new release facilitates the exploiting of the Mobius analysis capabilities for safety and security co-engineering needs, according to the scenario addressed envisaged in (Popov, 2017). Editing Mobius models cannot be trivial. To this purpose we have extended the CHES profile and therefore the CHES modelling language capabilities and user-friendly editor as front-end to fully support the modelling of system architectures taking in consideration safety and security co-engineering, and using automatic transformations to SAN model for reliability analysis with MOBIUS. This approach provides a smooth integration, guarantees the consistency among SysML and SAN models, and drastically reduce the effort required to construct an appropriate SAN analysis model.

This extension has been developed in the context of the AQUAS project, as result of a collaborative effort among Intecs and City University of London, and applied across different use cases, in the ATM and Industrial Drive domain.

3.3 Improved support for contract-based design analysis and model checking

In the contract-based paradigm, the properties of each component may be restricted to its interfaces. The contracts are pairs of properties representing an assumption and a guarantee of the component. In addition, CHES tool supports the contract refinement analysis for composite components. The contract of a composite component is defined by the assumption of the composite component itself and the guarantee ensured by the contracts of its sub-components, considering their interconnection as described by the architecture and and that the assumption of each sub-component is ensured by the contracts of the other sibling sub-components.

The new CHES release has improved the contract-based analysis aspects by integrating CHES with V&V tools such as OCRA, nuXmv, and xSAP. In this regard, the new additional analysis includes:

- (1) *Model checking*, i.e. the behavioral models,

that describe how the internal state of a component and the output ports are updated, can be verified against some formal properties in different temporal logics. The formal properties can represent some requirements (e.g., functional or safety-related requirements) or some validation queries such as the reachability of states.

(2) *Contract-based compositional verification of state machines* is performed on composite components. The local state machine of each sub-component is verified separately against its local contract. The correctness of the composite component is implicitly derived by the correctness of the contract refinement and the successful verification of local state machines.

(3) *Contract-based safety analysis*, i.e. identify the component failures as the failure of its implementation in satisfying the contract. When the component is composite, its failures can be caused by a failure of one or more sub-components and/or a failure of the environment in satisfying the assumption. As result, the analysis produces a fault tree in which each intermediate event represents the failure of a component or its environment, linked to a Boolean combination of other nodes. The top-level event is the failure of the system component. The basic events are the failures of the leaf sub-components, in addition to the failure of the environment (see (Bozzano et al., 2014) for more details).

3.4 Support for parameterized architecture and trade-off analysis

In a parameterized architecture the number of components, the number of ports, the connections, and the static attributes of components depends on a (possibly infinite) set of parameters. In the new release, it is possible to define a parameterized architecture, setting the multiplicity of FlowPorts and sub-components to express a list of elements with the same type. This can be very helpful when modeling a system with a large number of similar nodes. The modeling of the parameterized architecture is followed by its instantiation. In this phase the user sets the values of the parameters, defining the configuration of the architecture. OCRA takes in input the parameterized architecture and one or more configurations. Then, OCRA produces the instances of the architecture, and for each of them, performs a list of contract-based verifications. The output is the result derived from the contract-based verifications described in Section 3.3.

This new release also supports Tradeoff analysis which allows to execute a certain check such as safety,

security, performance analysis on selected configurations (instances) and get the results in a view that simplifies the comparison between them. This makes it easy to visually get an idea of how the intended model instances perform with respect to the selected configurations. Figure 7 shows the sample result of a trade-

Check	Contract Refinement	Contract1Type	Contract2Type	Contract3Type	Contract4Type
Concerns	safety	security/performance	unspecified	unspecified	
InstantiateArc_1	Success	Success	Success	NOT OK	
InstantiateArc_2	Success	Success	Success	NOT OK	

Figure 7: Trade-off Analysis results sample

off analysis made on two instances by looking at different concerns specified by the assumption/guarantee formal properties of each contract.

3.5 Automatic generation of diagrams and documentation

The traditional way of editing a model is by adding an element in a diagram but changes made in the model are not reflected in the diagrams. The new CHESS release offers the possibility of generating a diagram from the model which reflects the data in the model on the fly. The supported diagrams are Block Definition Diagram(BDD) and Internal Block diagram(IBM). Multiple diagrams can be generated on a single component in the model. The generated diagram elements will be automatically aligned but the user can rearrange by moving elements manually or by invoking **“layout selection command.”**

The new release also supports the generation of the model architecture and the report on various analyses executed on the model in an HTML document or a LaTeX source code. The report is divided into two sections. The first describes the structure of the model which includes diagrams and the associated components while the second includes the report lists of the results of the validation and verification (V&V) analyses results. There are many types of V&V results such as *property validation*, *assume/guarantee properties results*, *contract checks results*, *model checking*, *FTA*, *FMEA*, and so on. Figure 8 gives the sample of the report page that can be generated by the tool.

4 CHESS TOOL IN PRACTICE

Throughout different phases of extending CHESS, CHESS was involved in many projects, research communities, and academies. CHESS has been used for teaching and extending it for research purposes. CHESS has conducted more than 10 international

Components		Validation and Verification Results	
<ul style="list-style-type: none"> Model <ul style="list-style-type: none"> System BSCU SubBSCU Select_Switch_Impl Hydraulic 			
V&V Results <ul style="list-style-type: none"> Property Validation Results Assume/Guarantee Properties Validation Results Check Contract Refinement Results Check Contract Composite Implementation Results Contract-based Fault Tree Analysis Results Model Checking Results Fault Tree Analysis Results Failure Modes and Effects Analysis Results 			
		Properties Validation Results:	
		Main class: System Type of validation: consistency Selected component: ALL Selected properties: ALL	
	Property		Status
	[System.all]		Success
	[BSCU.all]		Success
	[Select_Switch_Impl.all]		Success
	[SubBSCU.all]		Success
		Main class: System Type of validation: possibility Selected component: BSCU Selected properties: BSCU_CMD_Time.NORM_GUARANTEE, BSCU_Safety_AS Conditions: FALSE	
	Property		Status
	[input_validation_prop]		Unknown
		Assume/Guarantee Properties Validation Results:	
		Main class: System Type of validation: possibility Selected component: System Selected properties: System_Brake_Time.NORM_GUARANTEE, bscuBSCU_CA Conditions: TRUE	
	Property		Status
	[input_validation_prop]		Success
		Main class: System Type of validation: entailment Selected component: Select_Switch_Impl Selected properties: Select_Switch_Self_Time ASSUMPTION, Select_Switch_Select_Switch_Set_Time.NORM_GUARANTEE Conditions: FALSE	
	Property		Status
	[input_validation_prop]		NOT OK

Figure 8: Generated report sample

recognized research and development projects in the frame of 8 years⁵. Following we list a brief extent on the projects through which the CHES tool played a major role.

4.1 ARTEMIS JU-CHESS

ARTEMIS JU-CHESS⁶ is the originating project that developed the CHES tool. The project aimed to improve model-driven engineering practices and technologies to better address safety, reliability, performance, robustness, and other non-functional concerns. This was achieved while guaranteeing the correctness and composition of components under development in the embedded systems domain. From this point, the various project was initiated to extend CHES to a new level by adding more functionalities and incorporate other domains.

4.2 CONCERTO

CONCERTO⁷ project aimed to deliver a reference multi-domain architectural framework for complex, highly concurrent, and multi-core systems, where non-functional properties (including real-time, dependability, and energy management) was established

⁵<https://projects.eclipse.org/projects/polarsys.chess/releases/1.0.0/review>

⁶<http://www.chess-project.org/>

⁷<http://www.concerto-project.org/>

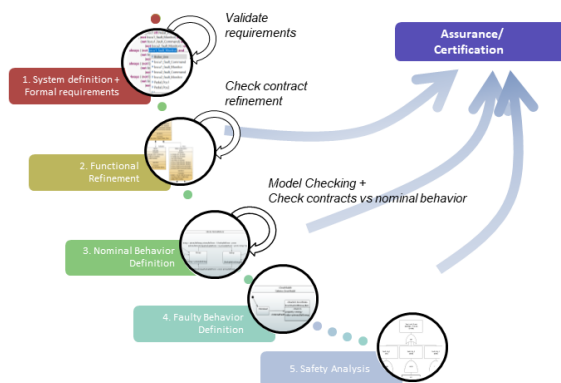


Figure 9: The main workflow supported by CHES in AMASS

for individual components. CONCERTO framework was built on top of the CHES framework developed in 4.1, as well as the results of several other related projects. The project enforced the modeling of multi-core processors among the possible target platforms, with the same level of correctness and guarantees as for traditional single-core processor targets (Baracchi et al., 2016).

4.3 AMASS

AMASS⁸ (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) project aim was to create and consolidate the de-facto European-wide open tool platform, ecosystem, and self-sustainable community for assurance and certification of Cyber-Physical Systems (CPS) in the largest industrial vertical markets (Alaña and Herrero, 2018). In this project, CHES played a role in system architecture modeling assurance, patterns library management assurances, contract-based assurances, and verification and validation (V&V) based assurances through its extension with some tools such as OCRA, nuXmv, and xSAP. For future consultation, the contributor offers free training accessible at <https://www.amass-ecsel.eu/content/training> which includes video tutorials and documentation. Figure 9 shows the main workflow supported by CHES in the context of AMASS. The workflow included the definition of the system and their formal requirements, the functional refinement of the system, the definition of the nominal and faulty behaviors, and finally, the safety analysis.

⁸<https://www.amass-ecsel.eu/>

4.4 AQUAS

AQUAS⁹(Aggregated Quality Assurance in Systems) project aims was to improve on how the non-functional requirements of safety, security, performance (SSP) are dealt with during the product life cycle for embedded computer systems. AQUAS approach was based on two main principles. First, apply the methods for combined analyses of project artifacts from the viewpoints of safety, security, performance. Second, limit the overhead cost of these combined analyses by only applying them at a limited number of points in the product life-cycle, called interaction points (Popov et al., 2020).

The main CHESSE's contribution to the project was to support the modeling of the software architecture of the several use cases. CHESSE was used to enrich the system and software architecture model with information related to safety, security and performance co-engineering, and support of automated toolchains and traceability for combined analysis among the product. In particular, the tool was used to perform performance analysis and support dependability analyses with SANs, exploiting new capabilities presented in section 3.2.

4.5 SESAMO

SESAMO¹⁰ project aimed to develop a methodology to reduce interdependencies between safety and security mechanisms. This was achieved by constructing a tool-chain that uses the constructive elements and integrated analysis procedures to ensure the safety and security characteristics of the system are maintained. The CHESSE contribution to the project was (1) the introduction of the concept of components and reusability into the modelling process. (2) the definition of safety and security as non-functional properties, within the CHESSE component model perspective. (3) provide separation of concerns for the modelling of safety and security in a single model enabling joint verification and analysis (SESAMO, 2014).

4.6 MEGAMART

MegaM@Rt¹¹ is an open-sourced project with the ambition to create a framework which incorporate methods and tools for continuous development and validation. This project leverages the advantages in scalable model-based methods to provide benefits in

⁹<https://aquas-project.eu/>

¹⁰<http://sesamo-project.eu/>

¹¹<https://megamart2-ecsel.eu/>

significantly improved productivity, quality, and predictability of large and complex industrial systems. Employing its rich model-driven toolchain, CHESSE

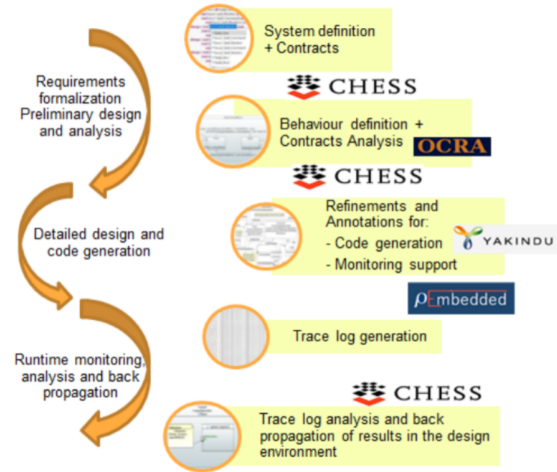


Figure 10: CHESSE fit in MegaM@Rt Tekne case study

served in the design and the development of high-integrity systems with a focus on non-functional properties (Afzal et al., 2018). In this project, CHESSE was used in the design and analysis of the Tekne case study. This was an ultra-wideband (UWB) mobile network technology with a short-range communication, indoor positioning, and tracking capabilities (Cruz et al., 2020).

Figure 10 shows the process of modeling the Tekne case study. In this project, requirement modeling, traceability, contract-based design approach, component real-time behavior analysis exploit and demonstrate the CHESSE potential. In addition, the collected run-time logs were analyzed by CHESSE to capture non-functional constraint violations. The results are back-propagated to the design environment for further model refinement (Cruz et al., 2020).

5 RELATED WORK

Several commercial tools provide similar functionalities of CHESSE. One of the most popular is **Matlab/Simulink** (Mathwork, 2020). Although Matlab/Simulink facilitates the modelling and analysis of complex systems, its simulation efficiency might be an important disadvantage. Being based on a single Model of Computation and Communication (MoCC) is another limitation. **CoFluent** is another commercial tool extended to model IoT systems (Intel, 2020). Although supporting more interaction models than Matlab/Simulink, it is also limited in the way com-

ponents may interact among them.

Another tendency is to overcome the UML lacks in semantic content, required in some application domains, towards a proliferation of DSLs (Brambilla et al., 2012). Among the available DSLs, UML/MARTE is the standard language for real-time and embedded systems design, while SysML is the standard language for system modeling. Several modelling environments like **Papyrus** (Papyrus, 2020) support UML/MARTE. Nevertheless, its flexibility and semantic richness requires the definition of efficient modelling methodologies.

Capella (Capella, 2020) is an open-source comprehensive and extensible Eclipse system modelling tool. It is inspired to the SysML principles and it supports the **ARCADIA** methodology that is successfully deployed in a wide variety of industrial contexts (Bonnet et al., 2015). ARCADIA provides architectural descriptions for functional analysis, structural analysis, interfaces and behavior modeling, structured in five perspectives according to major system engineering activities and concerns.

COMPASS (Bozzano et al., 2019) supports model checking, model-based safety, reliability, and performance analysis and shares with CHES some of the tools used as backend for such analyses. Differently from CHES, it targets a variant of AADL and does not support traceability and code generation.

MapleSim¹² is a modeling tool for multi-domain engineering systems built on top of **Modelica** modeling language (Elmqvist et al., 1998). MapleSim features an integrated environment in which the system equations can be automatically generated and analyzed (Cao and Wu, 2013).

Although we see some approaches able to tackle modeling challenges, no tool or approach has been able to fit in our methodology with such analysis and verification functionalities. Which makes CHES a novel approach for implementing component-based modeling methodology for real-time and dependable systems by taking care of non-functional properties and enforces the correctness at all the stages of the development process.

6 FUTURE WORK

CHES is a very huge toolset with more sophisticated and powerful functionality to meet user needs. However, there is still a gap for improvement, to cover more and more domains such as the Internet of Things (IoT) in a more concrete way. Note that we are not

¹²<https://www.maplesoft.com/products/maplesim/>

concluding that it is not capable to perform some basic modeling of IoT related scenarios but we aspire to make it more IoT specific. This extension will follow CHES's component-based methodology and it will also follow already existing modeling approaches present in CHES.

The envisioned approach will be achieved by improving the CHESML metamodel with a set of specific stereotypes, contracts, communications, and operations profiled for IoT. The new proposed approach will also take in use of already existing dependability analysis infrastructure such as Fault Mode Effect Analysis, Fault Logic Analysis, Fault Tree Analysis, and so on. We also plan to export IoT models developed with CHES to external consumers. Finally, we plan to exploit the current CHES's code generation support for Ada language, integrated with the open-source ThingML framework, for IoT code generation.

7 CONCLUSIONS

Dependable complex system design and development present several challenges, the well-known canonical approach is to divide complex systems into smaller chunks (or subsystems), build them separately, and later integrate them. In this paper, we presented the current state of the CHES tool to tackle design, analysis, and verification of real-time dependable complex systems. We walked through the CHES tool architecture and we highlighted its component-based and multi-view modeling approaches. We have also presented the new system-level extensions and capabilities of the tool released under the CHES1.0.0 version. Finally, we introduced the different projects and contributions where CHES was used either in the industry and academia at large and presented the future envisioned extension strategy.

ACKNOWLEDGEMENTS

This work has received funding from the Low-comote project under European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement n813884. We would like to acknowledge also different projects funding leading to the mature realization of CHES which include the CHES¹³, CONCERTO¹⁴,

¹³<http://www.ches-project.org/>

¹⁴<http://www.concerto-project.org/>

SESAMO¹⁵ under ARTEMIS Joint Undertaking initiative, and AMASS¹⁶, and AQUAS¹⁷ under ECSEL Joint Undertaking initiative. We would like to acknowledge the main contributors to the development of the CHESS toolset, in particular Stefano Puri, Nicholas Pacini, Luca Cristoforetti and Pietro Braghieri. Finally, we would like to acknowledge also Prof. Davide Di Ruscio for the assistance on drafting this paper.

REFERENCES

- Afzal, W., Bruneliere, H., Di Ruscio, D., Sadovykh, A., Mazzini, S., Cariou, E., Truscan, D., Cabot, J., Gómez, A., Gorroñoigoitia, J., Pomante, L., and Smrz, P. (2018). The MegaM@Rt2 ECSEL project: MegaModelling at Runtime – Scalable model-based framework for continuous development and runtime validation of complex systems. *Microprocessors and Microsystems: Embedded Hardware Design (MICPRO)*, 61:86 – 95.
- Alaña, E. and Herrero, J. (2018). Design and safety assessment of on-board software applications using the amass platform. In *EUROSPACE DASIA 2018*.
- Baracchi, L., Mazzini, S., Puri, S., and Vardanega, T. (2016). Lessons learned in a journey toward correct-by-construction model-based development. In Bertogna, M., Pinho, L. M., and Quiñones, E., editors, *Reliable Software Technologies – Ada-Europe 2016*, pages 113–128, Cham. Springer International Publishing.
- Bittner, B., Bozzano, M., Cavada, R., Cimatti, A., Gario, M., Griggio, A., Mattarei, C., Micheli, A., and Zampedri, G. (2016). The xSAP Safety Analysis Platform. In Chechik, M. and Raskin, J., editors, *Tools and Algorithms for the Construction and Analysis of Systems - 22nd International Conference, TACAS 2016, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2016, Eindhoven, The Netherlands, April 2-8, 2016, Proceedings*, volume 9636 of *Lecture Notes in Computer Science*, pages 533–539. Springer.
- Bonnet, S., Voirin, J.-L., Normand, V., and Exertier, D. (2015). Implementing the mbse cultural change: Organization, coaching and lessons learned. *INCOSE International Symposium*, 25(1):508–523.
- Bozzano, M., Bruintjes, H., Cimatti, A., Katoen, J., Noll, T., and Tonetta, S. (2019). COMPASS 3.0. In Vojnar, T. and Zhang, L., editors, *Tools and Algorithms for the Construction and Analysis of Systems - 25th International Conference, TACAS 2019, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2019, Prague, Czech Republic, April 6-11, 2019, Proceedings, Part I*, volume 11427 of *Lecture Notes in Computer Science*, pages 379–385. Springer.
- Bozzano, M., Cimatti, A., Mattarei, C., and Tonetta, S. (2014). Formal safety assessment via contract-based design. In *International Symposium on Automated Technology for Verification and Analysis*, pages 81–97. Springer.
- Bozzano, M. and Villafiorita, A. (2013). Safety critical systems. In *Encyclopedia of Software Engineering*. CRC Press (Taylor & Francis Group).
- Brambilla, M., Cabot, J., and Wimmer, M. (2012). *Model-Driven Software Engineering in Practice*, volume 1.
- Bressan, L., de Oliveira, A. L., Montecchi, L., and Gallina, B. (2018). A systematic process for applying the chess methodology in the creation of certifiable evidence. In *2018 14th European Dependable Computing Conference (EDCC)*, pages 49–56.
- Cao, J. M. and Wu, T. (2013). Multi-domain modeling simulation and application based on maplesim. In *Mechatronics and Intelligent Materials III*, volume 706 of *Advanced Materials Research*, pages 1894–1897. Trans Tech Publications Ltd.
- Capella (2020). An open source solution for model-based systems engineering. Last Accessed: July 2020.
- Cavada, R., Cimatti, A., Dorigatti, M., Griggio, A., Mariotti, A., Micheli, A., Mover, S., Roveri, M., and Tonetta, S. (2014). The nuXmv Symbolic Model Checker. In Biere, A. and Bloem, R., editors, *Computer Aided Verification - 26th International Conference, CAV 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 18-22, 2014. Proceedings*, volume 8559 of *Lecture Notes in Computer Science*, pages 334–342. Springer.
- Cicchetti, A., Ciccozzi, F., Mazzini, S., Puri, S., Panunzio, M., Zovi, A., and Vardanega, T. (2012). CHESS: a model-driven engineering tool environment for aiding the development of complex industrial systems. In *2012 Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering*, pages 362–365.
- Cimatti, A., Dorigatti, M., and Tonetta, S. (2013). OCRA: A tool for checking the refinement of temporal contracts. In Denney, E., Bultan, T., and Zeller, A., editors, *2013 28th IEEE/ACM International Conference on Automated Software Engineering, ASE 2013, Silicon Valley, CA, USA, November 11-15, 2013*, pages 702–705. IEEE.
- Courtney, T., Gaonkar, S., Keefe, K., Rozier, E. W. D., and Sanders, W. H. (2009). Möbius 2.3: An extensible tool for dependability, security, and performance evaluation of large and complex system models. In *2009 IEEE/IFIP International Conference on Dependable Systems Networks*, pages 353–358.
- Cruz, J. G., Sadovykh, A., Truscan, D., Bruneliere, H., Pierini, P., and Muñoz, L. L. (2020). Megam@rt2 eu project: Open source tools for mega-modelling at runtime of cpss. In Ivanov, V., Kruglov, A., Masyagin, S., Sillitti, A., and Succi, G., editors, *Open Source Systems*, pages 183–189, Cham. Springer International Publishing.

¹⁵<http://sesamo-project.eu/>

¹⁶<https://www.amass-ecsel.eu/>

¹⁷<https://aquas-project.eu/>

- Elmqvist, H., Mattsson, S. E., and Otter, M. (June, 1998). Modelica- the new object oriented modeling language. *The 12th European Simulation Multiconference*.
- Gallina, B., Sefer, E., and Refsdal, A. (2014). Towards safety risk assessment of socio-technical systems via failure logic analysis. In *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, pages 287–292.
- Gallina, B., Sefer, E., and Refsdal, A. (2014). Towards safety risk assessment of socio-technical systems via failure logic analysis. In *Proceedings of the 2014 IEEE International Symposium on Software Reliability Engineering Workshops*, pages 287–292.
- Godard, W. and Nelissen, G. (2016). Model-based design and schedulability analysis for avionic applications on multicore platforms. *37:157–163*.
- Intel, C. (2020). Solution for simulation and modeling of systems. Last Accessed: July 2020.
- Mathwork (2020). Simulation and model-based design. Last Accessed: July 2020.
- Mazzini, S. (2015). The concerto project: An open source methodology for designing, deploying, and operating reliable and safe cps systems. *Ada User Journal*, 36:264–267.
- Mazzini, S., Favaro, J., and Baracchi, L. (2015). A model-based approach across the IoT lifecycle for scalable and distributed smart applications. In *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, pages 149–154.
- Mazzini, S., Favaro, J. M., Puri, S., and Baracchi, L. (2016). CHESS: an open source methodology and toolset for the development of critical systems. In *EduSymp/OSS4MDE@MoDELS*.
- Montecchi, L. and Gallina, B. (2017). Safeconcert: A metamodel for a concerted safety modeling of socio-technical systems. In Bozzano, M. and Papadopoulos, Y., editors, *Model-Based Safety and Assessment*, pages 129–144, Cham. Springer International Publishing.
- Montecchi, L., Lollini, P., and Bondavalli, A. (2013). A reusable modular toolchain for automated dependability evaluation. In *Proceedings of the 7th International Conference on Performance Evaluation Methodologies and Tools*, ValueTools '13, page 298–303, Brussels, BEL. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
- Pace, L., Pasquinelli, M., Gerbaz, D., Fuchs, J., Basso, V., Mazzini, S., Baracchi, L., Puri, S., Lassalle, M., and Viitaniemi, J. (2014). Model-based approach for the verification enhancement across the lifecycle of a space system. In *INCOSE Italian Chapter Conference on Systems Engineering (CIISE2014)*.
- Panunzio, M. and Vardanega, T. (2014). A component-based process with separation of concerns for the development of embedded real-time software systems. *Journal of Systems and Software*, 96:105 – 121.
- Papyrus (2020). Eclipse papyrus modeling environment. Last Accessed: July 2020.
- Popov, P. (2017). Models of reliability of fault-tolerant software under cyber-attacks. In *2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE)*, pages 228–239.
- Popov, P., Strigini, L., Hunt, S., and et al (2020). Deliverable 3.3: Combined analysis of safety, security and performance. Technical report, City, University of London and AQUAS team.
- Puri, S., Mazzini, S., and Pachini, N. (May 2020). CHESS toolset user guide, toolset release 1.0.0.
- SESAMO, T. (2014). *D4.2 – Integrated Design and Evaluation Methodology Version 01*.