



Project ADVANCE
Grant Agreement 287563
“Advanced Design and Verification Environment for
Cyber-physical System Engineering”



ADVANCE Deliverable D.2.1 (issue 2)
Smart Energy Grid Case Study Definition

Public Document

March 28th, 2013

<http://www.advance-ict.eu>

SMART GRID CASE STUDY DEFINITION

ADVANCE

Approval			
Name	Function	Signature	Date
John Colley	Project Co-Ordinator		28/03/2013
Luke Walsh	Project Manager		28/03/2013

Authors and Contributors			
Name	Contact	Description	Date
Brett Bicknell	bbicknell@critical-software.co.uk	Author	28/03/2013
José Reis	jreis@critical-software.co.uk	Contributor	28/03/2013
Michael Butler	mjb@ecs.soton.ac.uk	Reviewer	28/03/2013

Access List
Internal Access
Project Team, Engineering Department
External Access
Southampton University, ADVANCE project team
The contents of this document are under copyright of Critical Software Technologies. It is released on condition that it shall not be copied in whole, in part or otherwise reproduced (whether by photographic, or any other method) and the contents therefore shall not be divulged to any person other than that of the addressee (save to other authorized offices of his organization having need to know such contents, for the purpose for which disclosure is made) without prior written consent of submitting company.

Revision History			
Issue	Date	Description	Author
1	19/12/2011	First Issue	Brett Bicknell
2		Second Issue – changes made in response to EU review	Brett Bicknell

CRITICAL SOFTWARE TECHNOLOGIES LTD 2 VENTURE ROAD SOUTHAMPTON SCIENCE PARK – CHILWORTH SOUTHAMPTON - SO16 7NP – UNITED KINGDOM	CRITICAL SOFTWARE, S.A. PARQUE INDUSTRIAL DE TAVEIRO, LOTE 48, 3045-504 COIMBRA PORTUGAL
--	--

TABLE OF CONTENTS

1. INTRODUCTION.....	4
1.1 OBJECTIVE.....	4
1.2 AUDIENCE.....	4
1.3 DEFINITIONS AND ACRONYMS.....	4
1.4 REQUIREMENT CLASSIFICATION.....	4
1.5 DOCUMENT STRUCTURE.....	4
2. SCOPE FOR FORMAL METHODS IN SMART GRID SYSTEMS.....	5
2.1 GENERAL REQUIREMENTS FROM A MISSION-CRITICAL PERSPECTIVE.....	5
2.1.1 <i>Distributed databases in the context of smart grids</i>	6
3. MODELLING AND REFINING A SMART GRID ARCHITECTURE.....	7
3.1 REQUIREMENTS.....	8
3.1.1 <i>Assumptions</i>	8
4. SPECIFICATION OF WORK.....	10
4.1 LOW VOLTAGE SUBSTATION MONITORING SYSTEM.....	10
5. SUITABILITY FOR INFLUENCING TOOL DEVELOPMENT.....	14
6. EXPECTED OUTCOMES AND SUCCESS CRITERIA.....	15

1. Introduction

1.1 Objective

This document introduces and defines the Smart Grid case study of the ADVANCE project, including architectural properties, initial models and requirements, the relationship to tool development and success criteria. The case study is part of work package 2 of ADVANCE.

This deliverable focuses on the first stage of the work which is to do with the low-voltage substation monitoring system modelling. The next stages of work are going to be specified in the next set of deliverables.

1.2 Audience

Those involved or interested in the case study, including the ADVANCE consortium.

1.3 Definitions and acronyms

Table 1 presents the list of acronyms used throughout the present document.

Acronyms	Description
SIU	Sensor Interface Unit
WP	Work Package

Table 1: Table of acronyms

1.4 Requirement Classification

Table 2 presents the system of identification for the requirements listed throughout the document.

KEY	Description
SGCS-GEN-FUN-xxx	General (functional) requirements which encompass the entire case study.
SGCS-GEN-NON-xxx	General (non-functional) requirements which encompass the entire case study.
SGCS-GEN-ASM-xxx	Assumptions associated with the general requirements.
SGCS-LVM-FUN-xxx	Functional requirements specific to the low-voltage substation monitoring system.
SGCS-LVM-NON-xxx	Non-functional requirements specific to the low-voltage substation monitoring system.

Table 2: Table of requirement classification

1.5 Document structure

Section 1 introduces the document.

Section 2 presents a more general context of smart grid systems to establish the overall scope and possible properties that can provide focus for the project.

Section 3 details the typical architecture of a smart grid system and how it can be modelled. Also presented are the broader requirements that the case study will seek to validate along with any related assumptions that will need to be made.

Section 4 consists of the details and plan of work with the industrial partner, and how this provides a suitable ground for achieving the aims of the case study.

Section 5 lists how the case study will influence and provide feedback to the tool development process.

Section 6 provides the success criteria and related goals for the case study.

2. Scope for formal methods in smart grid systems

The differentiating factor of a smart grid in comparison to existing energy grids is the two-way communication between the consumer and supplier. This presents the opportunity for the consumer to have a more dynamic role in managing their energy use; by having access to up-to-date energy records and the option to switch between different rates and energy plans. It also allows for a more efficient and intelligent system on the supplier side; which can work around high demand and power outages by constantly updating the price and availability by considering the activity on the rest of the grid. The result is a reduction in the cost and waste of energy for both parties.

The proposition of this case study is to verify the security and reliability of the communication infrastructure which defines a smart grid system. The aspect that will have to be modelled in this case is the data interchange between the consumers, suppliers and other native devices in the network. Formal methods present an ideal means of achieving this goal and establishing a best practice as the technology surrounding smart grid systems is still fairly loosely defined and attracts high development costs throughout the life cycle due to the traditional development methods used.

The importance lies in the fact that the data interchange will have the ability to affect the operation of consumer devices in this type of system. For example: with the ability for the consumer to pick and choose preferred energy suppliers and tariffs, the corresponding information will have to be stored, updated dynamically and used to determine the power supply - all by devices in the network. This in turn leads to the possibility of tariffs which impose particular constraints on the energy usage; and even in the future controlling other appliances around the home or workplace. Thus the resulting behaviour from this data becoming lost or incorrectly managed could include smart meters cutting off or limiting power where it has not been requested that they do so.

The security and reliability of the data interchange can be considered critical in two separate cases:

- Firstly from a **safety-critical perspective**: when installing devices in hospitals or elsewhere where a fault could result in a loss of equipment or life – where in theory such devices have the power to directly change or stop the energy supply – it is imperative that the system is reliable enough that it cannot change the supply to a damaging effect during normal operation either by fault or human mistake, and that it is secure enough that malicious devices cannot breach into the network and change these parameters. Although at first glance it seems that that the latter point is a problem associated mainly with the details of the encryption of the network, the details are not important at the higher level: it will still be necessary to define which devices have (or can be assigned with when they join the network) certain encryption and authorisation levels.
- A perspective which has broader implications is that from a **mission-critical perspective**: the system must operate correctly when providing consumer functions otherwise it will not be successful. The corresponding requirements are detailed in section 2.1.

2.1 General requirements from a mission-critical perspective

The main areas of concern surrounding smart grids are:

- **Security**: as mentioned above the security of the devices is imperative in a safety-critical environment, but it will also be a major concern in a mission-critical environment, i.e. including all regular consumers.
- **Privacy**: the privacy of customer data must be well managed. The stored profile of the energy use that will be built up has the potential to reveal the daily routines and

dependencies of the customer. If outside agencies can access this data they could in theory use it for targeted marketing: for example, a customer who turns the lights on frequently during the night would be offered sleeping remedies. It will likely be possible to identify which household appliance is being used at which time by looking at the individualistic voltage 'trace' that it leaves.

- **Volume of data:** each meter will be sending and receiving frequent updates and with the potential of eventually installing meters in most households the data latency could have a significant impact on how frequently these updates can be successfully sent. It is important that these limits are factored into the specification from the onset.
- **Record Accuracy:** the choices that the consumer makes and the charges that apply to particular tariffs at particular times must have a clear correspondence. This has the potential to be a significant problem in a smart grid system as consumers may eventually be offered the ability to change suppliers or rates on an hour-by-hour or even minute-by-minute basis (whether this is manual or via a pre-set program in the meter which constantly switches to the cheapest, most green, etc rate). In a large network the data latency will be high, and if the energy companies are also constantly updating the rates that they are offering there will be a limit to how responsive the meters can be. If a consumer makes a choice with the most current version of the tariff prices they have on the meter, yet in the meantime the energy company has updated the prices but the information hasn't got through the network yet, the consumer and supplier will have different details for the same point in time so the consumer could be incorrectly charged for that period. The limit imposed by this process and the associated error margins that can be accepted must be specified and catered for from the start.
- **Data Distribution and Synchronisation:** the data for each meter could be distributed or copied throughout the network in the communication process. The meter and sub-station(s) responsible for that meter will also have to store separate versions of the same data which will be updated at certain times. The data system then essentially becomes a **distributed database**, and has all of the problems associated with this. Those particularly relevant to a smart grid system are listed in the next section.

2.1.1 Distributed databases in the context of smart grids

The well-established issues with distributed databases are equally relevant to smart grid systems:

- Data may be replicated when corresponding data sets are merged, incurring extra charge for consumers.
- There is also the potential to lose changes to one set of data during the merging process.
- Each site cannot have instantaneous information of the actions being carried out at the other sites; so the data used to calculate the bill will not necessarily be the most recent version. Again limits will need to be specified concerning the maximum time in the past allowed to be 'missing' from the bill for that date.
- On the event of a failure or disconnection in the network the distributed database must be able to recover the information that was recorded by the smart meter(s) affected during that time.

These are all aspects which will need to be set in requirements in order to prove the accuracy of the data interchange.

3. Modelling and refining a smart grid architecture

In this section the possibilities for modelling general smart grid architectures are discussed. This will not reflect exactly on the initial format of the case study but it will become more relevant as the case study progresses and the systems scale.

It will be important to keep in mind a larger, more general, scope of the system even if each constituting component is not subject to finer modelling. This will be present in the highest level abstraction anyway as each device will be, by definition of a smart grid, in frequent contact with the overall network; whether this is modelled as several components, a single component, or just as part of the environment. By keeping in mind the overall scope it will also be easier to assess if the methods developed could be applicable to smart grid systems in general and not just the particular examples that the case study will focus on.

When looking at the overall smart grid architecture it will most likely be suitable to start with a set of identical meters, one or more 'stations' (which act as the point of contact for the energy suppliers) and the connections between them. As the specifics of the case study are initially limited to looking at a single device (see section 4) then at first the rest of the inputs from the network can just be specified as part of the environment; but it seems beneficial from a wider perspective and also from a simulation viewpoint that the other entities in the network have some modelling, even if this is at an abstract level.

The possibilities for refinement in terms of the architecture (if deemed appropriate to the progression of the work as detailed in section 4) include that:

- More than two tiers can be added to the model of the network by including sub-stations, different types of smart meter or more overarching command systems.
- The simplest model of the architecture only requires that each meter is connected to a single station. There is the possibility to expand this so that each meter can connect to more than one station (as a precaution in case of an area of the network failing) and so that each device can also connect to other devices of its own type (to allow for each part of the network to become more informed of - and be able to react to - behaviour in the rest of the network).
- Some or all meters could also function as 'stations', storing and relaying data from other meters.
- It is likely that in the abstract model there will be a defined list of devices. Eventually the possibility to add new and remove existing devices from the network in real-time will need to be included.
- The ability for the smart grid to intelligently react to failures and work around power surges could be factored in - tying into the idea of devices in establishments such as hospitals that cannot lose power - whereas the initial aim is just verifying that the smart grid software itself cannot change the state of such devices through error, rather than how it reacts to failures of the physical network.

If deemed the best course of action it will be possible to model the system with state machines. However the starting point cannot be a single state machine representing the abstract model of the system as there are no global states which are applicable to the entire network. Instead it is more feasible to start with each smart meter, sub-station, etc as a state machine (each type having globally defined states) and the connections between them as a relation within the Event-B model.

Decomposition will be ideal as the model becomes more complex so that each type of device can be modelled independently. This will also involve defining the set of connections between the devices as a component itself which represents the network structure (this can then be decomposed further if necessary). In combination this will allow for the device

relevant to the section of the case study and the network protocols to be refined and developed separately.

3.1 Requirements

The broader requirements of a smart grid architecture that the case study will attempt to verify consist of:

	Description
SGCS-GEN-FUN-001	There shall be a set of devices which are guaranteed to supply constant power at all times.
Notes:	This is necessary in a safety-critical environment.

	Description
SGCS-GEN-FUN-002	It shall be possible to include the addition and removal of meters and stations to and from the network without compromising the other requirements.
Notes:	This shall be possible without compromising the security or reliability of the network.

	Description
SGCS-GEN-NON-003	There shall be levels of authorisation within the system.
Notes:	Only with certain authorisation level(s) can a device change the power supplied to a meter, read the data from a meter, and so on.

	Description
SGCS-GEN-NON-004	The model shall be verified regardless of how the smart grid scales.
Notes:	

3.1.1 Assumptions

There will be a number of assumptions that will, at least initially, need to be made in order for the above requirements to be valid. These will consist of two types: firstly, the assumptions that will be made at the abstract level but with which there will be the opportunity to encapsulate into the model through refinement:

	Description
SGCS-GEN-ASM-001	Each meter and each station is identical.
Notes:	

	Description
SGCS-GEN-ASM-002	Any damage to the physical network is ignored.
Notes:	An example of damage to the physical network is a broken power line. Later on it may be possible for faults of this manner to be injected into the system during simulation.

	Description
SGCS-GEN-ASM-003	When verifying properties (such as the requirement that devices in safety-critical environments cannot be cut off or have their supply inadvertently changed) only the potential faults or limitations within the software system itself are considered, and not any changes to the physical devices and network or the overall power supply in the network (power blackouts, etc).
Notes:	Later this will be an important point to consider in the context of a cyber-physical system.

Secondly, the assumptions which will be necessary due to the limitations imposed from the type of properties that can be verified in the Event-B language:

	Description
SGCS-GEN-ASM-004	The security of the network will be validated assuming that the devices already present will not be modified or reprogrammed in any way.
Notes:	

	Description
SGCS-GEN-ASM-005	The software and network protocols are well enough protected or encrypted on each device that they cannot be replicated by outside agencies.
Notes:	

4. Specification of work

The case study will be produced in collaboration with an industrial partner, the name of which cannot be stated due to confidentiality issues. There will be the opportunity to work with the partner on multiple smart grid related products that they are developing, as mentioned below.

It has been decided that the bulk of the case study will be split into multiple stages, each stage increasing the scope and scale of the models. This has been deemed necessary as there is not a single case study that could be provided which spans the entire period whilst providing a suitably diverse base for testing. It also lends well to giving the case study a natural progression in scope and complexity.

The first stage will concern a low-voltage substation monitoring system, as detailed in section 4.1. There is the opportunity to follow the development process from the start and provide requirements analysis using formal modelling. Initially just the high-level requirements for the abstract model will be provided; with the more detailed requirements necessary for each refinement given as the project progresses. The likely focus will be on the system of authorisation and secure identification - feeding into the security and privacy issues detailed in section 2 – along with the main elements of the normal operation of the system, but this can evolve depending on the requirements found to be suited to formal modelling and the progression of the product.

During the second stage there is the opportunity for the focus to shift to a smart building maintenance system. In this case the motivation will be more geared towards verifying the reliability of the system - in that the system will always display correct and up-to-date information about the condition of the various products so that it can notify users as to when a product will need replacing – addressing the data distribution and accuracy issues in section 2. As each device in the network will be constantly sending and receiving updates it provides an excellent opportunity to model the type of communication and data exchange that will be present in a smart grid. On top of this the hospital setting lends itself to the addition of safety-analysis into the requirements.

The work after the initial stage concerning the low-voltage monitoring system will be flexible and dependent on the successes of the earlier work, but it is planned to implement a gradual progression towards larger systems more representative of an actual smart grid. As the case study progresses this will involve introducing higher level properties concerned with, for instance, the secure data interchange between customer and supplier (as described in section 3). I.e. the modelling will start with a single device, and move on to networks of devices; the networks and systems becoming larger and more complex at each stage. The modelling performed during the initial stage will provide the groundwork for the later stages, where the multi-simulation and code generation tools will be applied. As the work progresses, there will also be the opportunity to work with standards relevant to the smart grid, such as IEC 61850 and IEEE 1547-2003.

4.1 Low voltage substation monitoring system

The intention of the first system to be modelled is to fit onto existing low voltage substations (without need for intrusion) and monitor the activity; providing data, status information and warnings. As shown in fig.1 the SIU (Sensor Interface Unit) is provided readings from a number of sensors attached to the low voltage station and in turn sends out the data over the air to the data centre. The requirements analysis and modelling will be focused primarily on the SIU, with the possibility of simulating inputs from both the sensors and data centre for verification.

The abstract requirements that it will likely be necessary to validate from the specification and purpose of the unit (this may change when the final top-level requirements are given; although it is assumed they will remain similar) consist of:

The system shall permit future expansion by allowing for additional sensors to be added:

	Description
SGCS-LVM-FUN-001	It shall be possible for new sensors to be added to the system after initial setup without disrupting the normal operation of the system.
Notes:	

	Description
SGCS-LVM-FUN-002	It shall be possible for existing sensors to be removed or replaced without disrupting the normal operation of the system.
Notes:	

	Description
SGCS-LVM-NON-003	There shall be a secure identification system for adding new sensors such that only sensors approved by the supplier can be added.
Notes:	

	Description
SGCS-LVM-NON-004	There shall be a maximum number of sensors that system can use; after this has been reached no more sensors should be added.
Notes:	

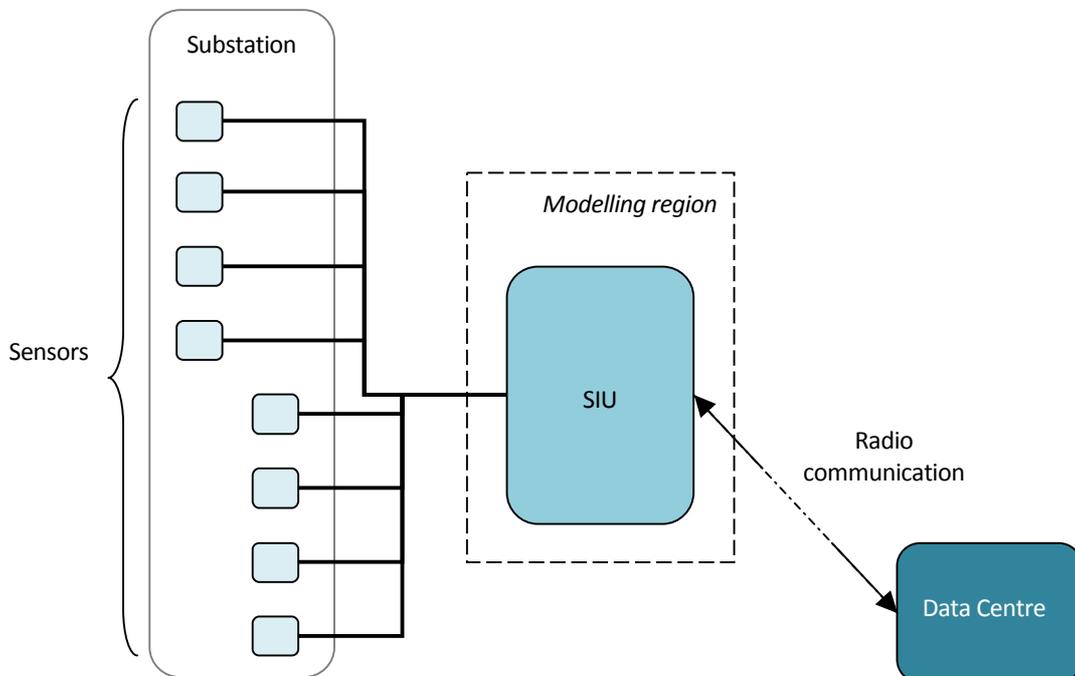


Figure 1 – a diagrammatic representation of the monitoring system

The system shall issue a warning when a limit is breached:

	Description
SGCS-LVM-NON-005	The limits should not be changed except by an outside control system.
Notes:	An example of an outside control system is the laptop used to set up the SIU during installation.

	Description
SGCS-LVM-NON-006	The warning shall be issued immediately after the readings which exceed the limit are received by the SIU – this shall still be true when multiple limits are exceeded at the same time.
Notes:	

	Description
SGCS-LVM-NON-007	The warning shall be retained (until input by an outside control system or operator is provided) if the system subsequently drops back below the limit. However in this interim period – if the type of warning is not detrimental to the health of the device - the system should not be prevented from functioning as normal
Notes:	

The system should provide continuous reliable monitoring:

	Description
SGCS-LVM-FUN-008	It shall be possible for the reporting interval and reporting mode to be changed at any time.
Notes:	The reporting mode means average, total, etc.

	Description
SGCS-LVM-NON-009	Changing the reporting mode or reporting interval should not cause any loss of records.
Notes:	The reporting mode means average, total, etc.

	Description
SGCS-LVM-NON-010	The reporting interval and reporting mode should only be changed by an outside control system and not internally.
Notes:	

	Description
SGCS-LVM-NON-011	There shall be limited memory in the system.
Notes:	

	Description
SGCS-LVM-NON-012	If the memory is full then the most historical record shall be deleted on arrival of a new record.
Notes:	

	Description
SGCS-LVM-FUN-013	Only if the memory is full or there is direct intervention by an outside control system should records be removed.
Notes:	An example of a direct intervention by an outside control system is when the data centre signals that it has received a set of records.

Although the first set of requirements only concern adding and removing elements that are local and hardwired to the SIU, modelling this will require a similar approach to the process of adding and removing smart meters from a network; thus providing an ideal initial testing ground for the authorisation and security issues in section 2, which can be built upon in later stages of the case study.

5. Suitability for influencing tool development

The case study must be able to provide suitable feedback to and validate the tool development in WP 3, WP 4 and WP 5. The following points address how the case study will satisfy this requisite:

- **Decomposition:** as mentioned in section 3, decomposition is a natural way to progress the modelling of a smart grid system, so there will be the opportunity to utilise the decomposition and composition tools extensively in the modelling process. This will include working with the propagation of changes to the model or requirements up and down the decomposition chain, and will also provide the opportunity to assess how a team can work on separate decomposed parts simultaneously.
- **Multi-simulation framework:** this will be necessary as although the modelling of the data interchange within the network will probably be discrete, the external inputs from the environment (such as the output of a thermostat) may be modelled as continuous functions. It might also prove more suitable to simulate the data flow from the network and the behaviour of the device as a response to this input separately.
- **Linking safety analysis with formal modelling:** as mentioned in section 2 it depends on the location and application as to whether the software developed could be considered safety-critical. Thus there is the opportunity to assess how to best integrate this safety-related analysis into the requirements for the model.
- **Linking requirements and traceability:** modelling a set of real-world systems which are already in development presents a more robust opportunity to trace authentic customer requirements, as this traceability will have to be presented at the end of the product development to the customer.
- **Code generation:** one of the aims of the case study (see section 6) is to produce a model which can be used during the actual development process of the industrial partner. It is most likely that for this to become a reality at some point the automatic generation of code will have to be demonstrated.
- **Automated proof and model-checking:** there are several scenarios when it will be apt to use automated proof and model checking; for example when there are multiple routes for a packet to travel through the network and all possibilities need to be covered or, using an example from section 2, it is required that no matter the progression of states of the system the power to the meter in a hospital must not be cut off.
- **Language extension / creating re-usable patterns:** the modelling techniques which are developed concerning the protocols, behaviour and configuration of the network should be reusable in other applications with similar communication structures, networks and standards.
- **Scalability:** The proposed timeline of work, as specified in section 4, fits well to the task of proving the Rodin platform can support systems of larger scale as the study will start with a single device – of which from previous work it is known the platform can successfully model – moving through larger systems and up to entire networks, thus providing a gradual increase in scale to fit with the gradual maintenance of the platform.

6. Expected Outcomes and Success Criteria

The ultimate goal of the case study is to produce a set of comprehensive modelling processes which can be used during the development of the real-world products supplied for the case study (and other similar systems in the future). However it is equally, if not more, important that during this time the following targets are achieved:

- The study can demonstrate that formal methods are beneficial when applied to smart grid solutions; i.e. the concept of a smart grid can be modelled and its properties verified.
- The study demonstrates that the complexity of the system can be mastered using refinement.
- The process demonstrates a reduced time-to-market by providing better levels of assurance than traditional engineering methods.
- The study provides understanding on how the ADVANCE tools can be applied in commercial environments and in doing so provide a more efficient approach than traditional engineering methods.
- The study uses real-world smart grid data to assist the modelling process.
- The case study demonstrates that the cost of development can be reduced by generating metrics.

There are also more tool-specific goals which need to be met:

- The study provides understanding on how safety analysis plays a role in and can be linked to formal methods.
- It is demonstrated that properties of the system can be verified through automated model checking and simulation.
- The end product demonstrates that code generation is possible and robust.
- The study provides examples of successfully utilising diagrammatic techniques to aid the generation of Event-B models, such as the state machines and UML-B tools.
- It is shown by the case study that the multi-simulation framework is successful in integrating discrete models of systems with continuous models of elements such as voltage variations.