REQUIREMENTS DEFINITION DOCUMENT FOR A SOFTWARE PRODUCT LINE OF CAR CRASH MANAGEMENT SYSTEMS

April 17, 2013

http://cserg0.site.uottawa.ca/cma2013models/

Authors:
Afredo Capozucca, Betty H.C. Cheng, Geri Georg, Nicolas Guelfi, Paul Istoan, Gunter Mussbacher

The authors would like to thank all participants of the 2011 AOM Bellairs Workshop for their contributions to this document: Omar Alam, Shaukat Ali, Robert France, Adam Jensen, Jean-Marc Jézéquel, Jörg Kienzle, Jacques Klein, Somayeh Malakuti, Sai Pradeep Mandalaparty, and Ana Moreira.

Table of Contents

1. Introduction

THE purpose of this document is to define the requirements of a Software Product Line (SPL) called bCMS-SPL[1] and aimed at managing car crash crises. Basic features along with desired variations are proposed such that it results in a small SPL definition. The primary focus of the proposed variations is to allow for static and dynamic variations (i.e., dynamic change between variants at runtime). The software product line is described in the following manner: the specification of a "reference variant" of the SPL referred to as bCMS is first provided; in a specific section, we then include all the information concerning possible variations that could be applied to bCMS. In this way, all the variation points and their possible implementations are introduced.

bCMS-SPL serves to illustrate the individual advantages and disadvantages of aspect-oriented modeling (AOM), feature-oriented (FOM), object-oriented modeling (OOM), service-oriented modeling (SOM), and other approaches at the Second International Workshop on Comparing Modeling Approaches (CMA) to be held at Models 2012. The CMA workshop will bring together practitioners of different modeling approaches including AOM, FOM, OOM, SOM, and other approaches to discuss and evaluate their various approaches in the context of the bCMS-SPL and provided comparison criteria. Practitioners can choose to either specify the bCMS-SPL or to focus on bCMS only. In either case, the modeling community is invited to demonstrate their approaches on the *entire* bCMS system or on the *entire* bCMS-SPL, thus providing a basis for discussion, comparison, and evaluation. For the bCMS-SPL, not all variations have to be modeled depending on their priority (see the beginning of Section 7 for more details on the priorities of variations).

While there are many AOM approaches, from requirements to low-level design, it is still difficult to compare them and know under which conditions different approaches are most applicable. This comparison, however, is crucially important to unify existing AOM and more traditional OOM as well as FOM, SOM, and other approaches and to generalize individual approaches into a comprehensive end-to-end method. Such a method that spans from early requirements to low-level design and that includes validation does not yet exist, and it is not readily evident how such a method would actually work in practice. As part of identifying potential comprehensive methodologies, we must be able to evaluate on a focused example different AOM approaches with each other and also against more traditional OOM as well as FOM, SOM, and other approaches, and apply the same criteria to each approach. The comparison criteria will be made available on the CMA workshop website well before the CMA workshop is held.

Experiences with the original case study crisis management system[2] indicate that a large scope for the case study leads to different researchers exploring different parts of the system. When different parts of a system are modeled using different approaches, it becomes difficult to compare these approaches. Hence, while the bCMS-SPL is based on the original, it is much more focused and comprises only one use case, a few non-functional requirements, and a few variations.

The approach chosen in this requirements document is rather "agnostic", thus we tried both in terms of terminology used and document structure followed to be as "clergy independent" as possible. The abstraction and completeness levels chosen are supposed to be sufficient to reach our main goal as described above.

[1]The 'b' of bCMS stands for Barbados, the country to which this case study is historically related, but also for the second version of the car crash crisis management system.

[2] Kienzle, J., Guelfi, N., Mustafiz, S. (2010) Crisis Management Systems: A Case Study for Aspect-Oriented Modeling. Katz, S., Mezini, M., Kienzle, J. (eds.) Transactions on Aspect-Oriented Software Development VII, LNCS 6210, pp 1-22, DOI: 10.1007/978-3-642-16086-8_1.

We suppose that the execution of the services of any product line variant may be concurrent. This will depend on the constraints on the execution order described for each service definition. Nevertheless, we do not use any modeling notation to this aim and the concerned constraints are hence spread over the textual descriptions[3].

This document introduces first the scope and stakeholders of the system in Sections 2 and 3, respectively. Then, functional and non-functional requirements are specified in Sections 4 and 5, respectively. While Section 6 discusses hardware and standards, Section 7 highlights variation points. The document concludes with a data dictionary in Section 8 and a glossary in Section 9.

2. Scope

THE bCMS system is a distributed crash management system that is responsible for coordinating the communication between a fire station coordinator (FSC) and a police station coordinator (PSC) to handle a crisis in a timely manner (see Figure 1). Internal communication among the police personnel (including the PSC) is outside the scope of the desired system. The same assumption applies to the fire personnel (including the FSC). Information regarding the crisis as it pertains to the tasks of the coordinators will be updated and maintained during and after the crisis.

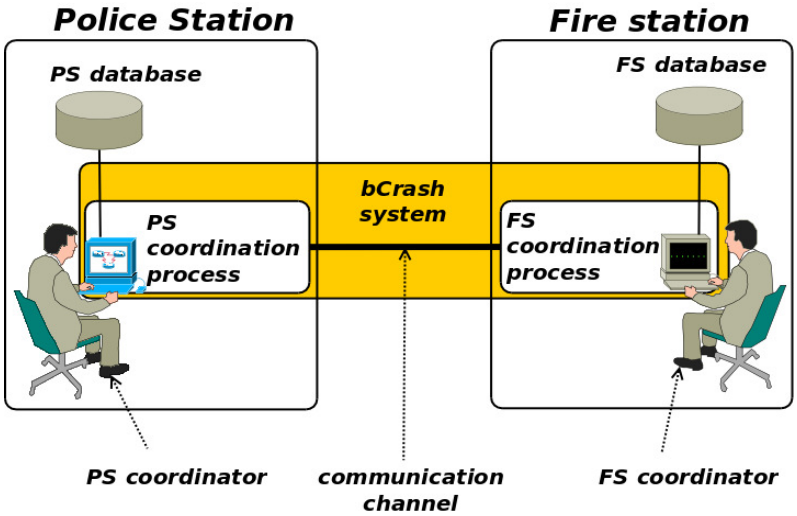

Figure 1: Overall view of the environment and the desired system.

There are two collaborative sub-systems. Thus, the global coordination is the result of the parallel composition of the (software) coordination processes controlled by the two (human) distributed coordinators (i.e., PSC and FSC). There is no central database; fire and police stations maintain separate databases and may only access information from the other database through the bCMS system. Each coordination process is hence in charge of adding and updating information in its respective database.

For simplicity, the context of the bCMS system is an accident involving an overturned oil tanker on a highway, where the tanker is on fire. The actual execution of the mission (e.g., rescue victims or remove obstacles) is outside the scope of the bCMS system except for specific information about the mission as required by the coordinators. This information includes the crisis details and the route plan as defined in the data dictionary in Section 8. Furthermore, the current version of the

[3]mainly in the use case scenario descriptions

bCMS system assumes that sufficient resources are available (e.g., fire trucks). Finally, there is only one fire station and only one police station and only one crisis at a time.

bCMS starts operating at the point when a given crisis has been detected and declared both at the fire station and the police station, independently. The coordinators (i.e., PSC and FSC) have already defined the parameters necessary to start handling the crisis. The initial emergency call of a witness and any subsequent notifications of the crisis from additional witnesses through either the police station and/or fire station call centers are outside the scope of the desired system.

A number of policies exist governing the timing for actions to be completed, the number of vehicles to be deployed for different types of crises, etc. The development and compliance checking of these policies are outside the scope of the desired system.

Any variation of the system detailed in Section 7 may be either selected at design time or activated at run time.

3. Stakeholders

ALL stakeholders of the system are detailed in this section. After a brief description of a stakeholder, the *objectives* of the stakeholder are first stated. Thereafter, the *responsibilities* of the stakeholder are detailed which help to achieve the stakeholder's objectives to a certain degree. While the objectives characterize the general problems addressed by the bCMS system, the responsibilities describe concrete actions that are expected from a stakeholder. Some of these responsibilities can be traced to the use case in Section 4, and hence must be supported by the bCMS system. Responsibilities that cannot be traced to the use case are outside the scope of the system. All stakeholders listed in this section have an interest in the system or are affected by the system in some way, but only a subset of the stakeholders are directly involved in the use case described in Section 4.

3.1. Fire Station Coordinator (FSC)

A FSC maintains control over a crisis situation by communicating with the police station coordinator (PSC) as well as firemen.

The objectives of a FSC are:

- to handle a crisis efficiently and effectively (e.g., minimize loss or injury to people and property),
- to get resources to the crisis location in the shortest amount of time,
- to have accurate estimation of resource needs and time of arrivals for resources,
- to have effective negotiation skills (e.g., with other coordinators),
- to have dependable communication with involved stakeholders,
- to maintain a feeling of control over the crisis (e.g., minimize stress level by providing and receiving crisis information to and from other coordinators in a timely fashion), and
- to provide clear, executable instructions to appropriate staff.

In order to achieve these objectives, the responsibilities of a FSC are:

- to determine where, when, and how many fire trucks to send,
- to communicate with the PSC to introduce herself,
- to keep PSC up to date regarding the nature of the crisis and the deployed resources,
- to propose a strategy for handling the crisis,
- to reach an agreement with the PSC on how to proceed,

- to receive updates regarding the crisis from individual firemen, and
- to collate and distribute updated information and instructions back to the firemen.

3.2. Fireman

A fireman acts on orders received from the FSC and reports crisis-related information back to the FSC. Furthermore, a fireman communicates with other firemen, victims, and witnesses at the crisis location.

The objectives of a fireman are:

- to stay alive,
- to minimize injury,
- to save and support the victim,
- to minimize damage to property,
- to work well in a team,
- to have confidence in the coordinator and follow instructions well, and
- to keep up to date regarding the crisis situation.

In order to achieve these objectives, the responsibilities of a fireman are:

- to receive requests to go to/return from the crisis location,
- to report location status to FSC,
- to report conditions of the crisis to FSC and all firemen, and
- to communicate with the victim and the witness at the crisis location.

3.3. Police Station Coordinator (PSC)

A PSC maintains control over a crisis situation by communicating with the fire station coordinator (FSC) as well as policemen.

The objectives of a PSC are the same as the objectives of a FSC.

In order to achieve these objectives, a PSC performs the same activities as a FSC. The description in Section 3.1 hence applies except that fire trucks are replaced with police cars, PSC with FSC, and firemen with policemen.

3.4. Police Officer

A police officer acts on orders received from the PSC and reports crisis-related information back to the PSC. Furthermore, a police officer communicates with other policemen, victims, and witnesses at the crisis location.

The objectives of a police officer are the same as the objectives of a fireman. In addition, a police officer wants to re-establish order disturbed by a crisis (e.g., manage traffic and people).

In order to achieve these objectives, a police officer performs the same activities as a fireman in terms of communicating with his coordinator. Hence, the description in Section 3.2 applies except that FSC is replaced with PSC.

3.5. Victim

A victim has been adversely affected by the crisis and may communicate with policemen and

firemen.

The objectives of a victim are:

- to be rescued in the shortest amount of time,
- to recover from injuries and/or loss in the shortest amount of time,
- to minimize stress caused by the crisis,
- to be informed of crisis status as it impacts the victim, and
- to know what to do at different stages of the crisis.

In order to achieve these objectives, the responsibilities of a victim are:

- to provide crisis-related information (including information about their location, identity, and medical history) to firemen and policemen, and
- to follow instructions from firemen and policemen.

3.6. Witness (at the crisis location)

A witness has observed the crisis and communicates with policemen and firemen.

The objectives of a witness are:

- to provide accurate information about the crisis to the police and fire personnel, and
- to know what to do.

In order to achieve these objectives, the responsibilities of a witness are:

- to provide information to firemen and policemen, and
- to follow instructions from firemen and policemen.

3.7. Government Agencies

Government agencies provide funding for the system and expect improvements of the communities' living standard from the deployment of the system.

The objectives of a government agency are:

- to keep the community safe, and
- to ensure effective response times with minimal costs.

In order to achieve these objectives, the responsibilities of a government agency are:

- to provide funding for fire and police departments, and
- to establish policies for both groups (e.g., security, response time expectations).

3.8. Communication Compromiser ☹

A communication compromiser wants to achieve personal gain, whether it is monetary or otherwise, by accessing confidential information and disrupting the handling of the crisis situation.

The objectives of a communication compromiser are:

- to disrupt the response to the crisis for some personal gain.

In order to achieve these objectives, the actions of a communication compromiser are:

- to gain access to confidential information,
- to change confidential information, and

- to disrupt communications.

4. Functional Requirements

THIS section details the use case of the bCMS system. Underlined items are further defined in the data dictionary in Section 8.

Use Case: Communicate with Other Coordinator

Actors: PSC, FSC
Goal: To resolve a crisis situation as quickly and cost-effectively as possible in cooperation with other coordinator. Coordination is required as police may enable fire personnel to reach the crisis location faster (e.g., by escorting the fire trucks or by creating roadblocks).
Precondition: PSC and FSC are aware of crisis, but have not established contact with each other.

Main Scenarios:

1. PSC and FSC establish communication and identification of coordinators.
2. PSC and FSC exchange crisis details.
3. PSC and FSC develop a coordinated route plan in a timely fashion for number of vehicles to be deployed to specific locations with respective ETAs.
    3.1. PSC and FSC state their respective number of fire trucks and police vehicles to deploy.
    3.2. PSC proposes one route for fire trucks and one route for police vehicles to reach crisis site.
    3.3. FSC agrees to route.
4. PSC and FSC communicate to each other that their respective vehicles have been dispatched according to plan (per vehicle).
5. PSC and FSC communicate to each other arrival (per vehicle) at targeted locations.
6. PSC and FSC communicate to each other completion (per vehicle) of their respective objectives.
7. PSC and FSC agree to close the crisis.

Alternative and Exceptional Scenarios:

At step 3 when the duration of the negotiation exceeds a predefined limit:

3.a1. A timeout is recorded in the system.
3.a2. PSC and FSC are alerted that a timeout has occurred for completing the negotiation.
3.a3. PSC and FSC are allowed to continue with the sub-step of step 3 where the timeout occurred.
3.a4. In parallel to 3.a3, PSC and FSC report the reason for timeout.

At step 3.3 when the FSC disagrees with the proposed route:

3.3.a1. The PSC removes the proposed route from the possible routes.
3.3.a2. Continue with step 3.2.

At step 3.3.a2 when there is no more route left to be proposed:

3.3.a2.a1. The PSC informs the FSC that the route will not be coordinated and that updates of vehicle locations and crisis details are still to be exchanged.
3.3.a2.a2. Continue with step 4.

At step 5 when a police vehicle/fire truck does not reach its destination within the ETA because of vehicle break down:

5.a1. The PSC/FSC informs the other coordinator of the new ETA and, if necessary, that a replacement vehicle is on its way.

5.a2. Continue with step 5.

At step 5 when a police vehicle/fire truck does not reach its destination within the ETA because of traffic or blocked routes:

5.b1. Continue with step 3.

At step 5 when the crisis is more severe than expected:

5.c1. Continue with step 3.

At step 5 when the crisis is less severe than expected:

5.d1. The PSC/FSC informs the other coordinator of recall of one or more police vehicles/fire trucks, respectively.

5.d2. Continue with step 5.

At any step M when communication is not available:

M.a1. PSC and FSC continue to address the crisis individually, and both will coordinate through their personnel once their personnel have reached the crisis site (this resolution is out of scope for bCMS).

At any step N when communication has been restored after a period of unavailable communication:

N.a1. If the crisis has been resolved (i.e., the objectives of all vehicles have been reached), then continue with step 7.

N.a2. If communication between PSC and FSC has not yet been established (step 1 has not yet been reached), then continue with step 1.

N.a3. If the route agreement has been reached (the use case is between step 4 and 6, inclusive), then exchange information on routes established for police and fire, location of vehicles, and status of crisis and for each vehicle continue with step 4, 5, or 6 depending on the location of a vehicle.

N.a4. If the route agreement has not been reached and the time limit for the route negotiation has not yet expired (the use case is between step 2 and 3.2, inclusive), then continue with step N.

N.a5. If the route agreement has not been reached and the time limit for the route has expired (the use case is between step 3.1 and 3.2, inclusive), then exchange information on routes established for police and fire, location of vehicles, and status of crisis and for each vehicle continue with step 4, 5, or 6 depending on the location of a vehicle.

5. Non-Functional Requirements

THIS section briefly discusses three non-functional requirements. Underlined items are further defined in the data dictionary in Section 8.

5.1. Integrity

The system shall ensure that the integrity of the communication between coordinators regarding

crisis location, vehicle number, and vehicle location is preserved 99.99%[4] of the time.
The systems shall ensure that the integrity of all other data transmitted between the coordinators is preserved 95% of the time.

5.2. Availability

The crisis details and route plan of the fire station and the police station, as well as the information related to the identification of the coordinators shall be available with the exception of a total of 5 minutes during the time period when at least one crisis is active.
The crisis details and route plan of the fire station and the police station shall be available with the exception of a total of 30 minutes for every 48 hours when no crisis is active.

5.3. Performance

The system shall respond to user requests within 5 seconds 95% of the time.
The system shall respond to user requests within 30 seconds 99.99% of the time.

6. Hardware and Standards

THE FSC and PSC shall use their computer with a wired connection to a T1 link to communicate with each other. Communication between the FSC and PSC shall use the https Internet protocol.

7. Variations

THE purpose of this section is to define the requirements for the bCMS-SPL. The approach chosen for describing the SPL is to define and detail the possible variations points that could be applied to the "reference variant" bCMS, which is described in the previous sections.

Desired variations are proposed that result in a small SPL definition. The primary focus is to allow for static and dynamic variations (i.e., dynamic change between variants at runtime). Nonetheless, it is important to understand that a set of variants is not a variant of the SPL. For example, a software having several configuration modes, which might be changed dynamically, may be either a variant of a SPL or an implementation of a SPL framework with a variant derivation capability implemented using configuration means.

The variations proposed cover functional requirements variations in Section 7.1 to Section 7.4 and non-functional requirements variations in Section 7.5 to Section 7.7. Furthermore, for each variation two priorities are defined – one for requirements models and one for design models. A priority may either be "must have" (i.e., the variation must be part of the model) or "may have". In the latter case, an ordering of variations is specified (i.e., if a "may have" variation with number N is part of the model, then all other "may have" variations with a number smaller than N must also be part of the model).

Table 1: Priorities of Variations

Variation	Requirements Priority	Design Priority
Police and Fire Stations Multiplicity	must have	must have
Vehicles Management	must have	may have (#1)
Vehicles Management Communication Protocol	must have	may have (#2)

[4]The numbers provided in the section on non-functional requirements do not aim, of course, at being realistic and are not based on empirical studies. They are here to request the coverage of this type of requirement.

Variation	Requirements Priority	Design Priority
Crisis Multiplicity	must have	must have
Confidentiality of Data Communication	must have	must have
Authentication of System's Users	must have	may have (#3)
Communication Layer	must have	may have (#4)

7.1. Police and Fire Stations Multiplicity

Variation point: Multiplicity of Police Stations (PS) and Fire Stations (FS)
Variations:

1. one PS and one FS
2. many PS and many FS

Constraints: exclusive variants
Comment(s): In this requirement document, the situation with a single PSC and FSC was described. Based on performance and/or budget constraints as well as changes to policies, fire station and police station management may be restructured, leading to more than one PSC/FSC. In this case, a lead coordinator is required; he may change over the duration of the crisis.

7.2. Vehicles Management

Introduction of a dispatching service to provide the ability to send and receive messages to/from police vehicles, fire trucks, and citizen vehicles. Citizen vehicles report, for example, accidents.

Variation point: Vehicles Management
Variations:

1. PSC and FSC cannot send to and receive messages from police vehicles, fire trucks, and citizen vehicles.
2. Only the PSC can send to and receive messages from police vehicles and citizen vehicles.
3. Only the FSC can send to and receive messages from fire station trucks.
4. Both PSC and FSC can send routing information to their respective vehicles.
5. PSC can receive notification of accidents from citizen vehicles.

Constraints:

i. Variant 1 is exclusive with the other variants.
ii. Variant 4 implies variant 2 and 3.
iii. Variant 5 includes variant 2.

Comment(s): This variation point will impact the steps 4, 5, and 6 of the use case described in Section 4.

7.3. Vehicles Management Communication Protocol

In case the system offers the functionality of communication between PSC/FSC and their respective vehicles, the infrastructure of this communication should fulfill the following requirements:

Variation point: Vehicle Communication Protocol
Variations:

1. The messaging infrastructure uses SOAP over the Internet.
2. The messaging infrastructure uses a simple SSL security mechanism.

Constraints: AND variants

i. This variation point requires variants 2, 3, 4, or 5 of variation point 7.2.

Comment(s): This variation point impacts the same steps of the use case from Section 4 as variation point 7.2.

7.4. Crisis Multiplicity

In this document, we assume that the bCMS system can handle only one crisis at a time. Complex crisis management systems may handle several crises at a time, from possibly different domains. This is expressed by this variation point.

Variation point: Crisis Multiplicity
Variations:

1. single crisis
2. multiple crises

Constraints: exclusive variants
Comment(s): A multi crises system needs to integrate (when needed) crisis identification. It must be also possible to route vehicles from one crisis location to another crisis location. As there are multiple crises, each crisis needs to be uniquely identified and has its own particular set of data (GPS location, type, status, etc.). The system needs to manage and keep track of all this information. The scenario described in Section 4 applies to each individual crisis. Thus, the system will have to manage the execution of several scenarios (one for each crisis) in parallel.

7.5. Confidentiality of Data Communication

Variation point: Confidentiality of Data Communication
Variations:

1. encrypted communications
2. non-encrypted communications

Constraints: exclusive variants
Comment(s): This type of variation impacts the functioning of the system in multiple places, as it applies every time there is a data communication between actors of the system. For example, in the use case described in Section 4, this variation points impacts steps 1-7.

7.6. Authentication of System's Users

Variation point: Authentication of System's Users
Variations:

1. password based
2. certificate based
3. biometrics based
4. one time password (i.e., RSA secured ID)
5. challenge response (i.e., symmetric cryptographic based/mutual authorization/Kerberos)

Constraints: each variant might include zero or any combination of the listed variations concerning the authentication of users.
Comment(s): In the scenario described in Section 4, the authentication of the PSC and FSC takes place at step 1. However, user authentication may be required at different places within the system's scenario.

7.7. Communication Layer

Variation point: Communication Protocol used for Communication Between Actors and System.
Variations:

1. Proprietary communication protocol (used over a private network)
2. HTTP
3. SOAP

Constraints:

i. Variant 1 is exclusive with the other variants.

ii. Variants 2 and 3 can co-exist in a same variant, either applied to different actors or even for the same actor.

Comment(s): The scenario described in Section 4 corresponds to variation 1. However, the chosen communication layer should not have an impact on the analysis phase of the bCMS system. Conversely, it may have a deep impact on the design of the desired system.

8. Data Dictionary

Crisis Details:

- Identifier
- Location (GPS)
- Time
- Status (Active, Closed)
- Description

Route Plan:

- Crisis ID
- Number of police vehicles
- ID, ETA, and location (station, enrouteToLocation, atLocation, enrouteReturn) of each police vehicle
- Number of fire trucks
- ID, ETA, and location (same as above) of each fire truck
- Route (path to reach the location) for each police vehicle and each fire truck

Timeout Log:

- Crisis ID
- Time
- Date
- Reason PSC
- Reason FSC

9. Glossary

Term	**Definition**
AOM	Aspect-oriented Modeling
bCMS	The name of a bCMS-SPL "reference variant". It represents a single instance of a coordinated distributed crash management system.
bCMS-SPL	The name of the software product line described in this document.
CMA	Comparing Modeling Approaches
Dependability	reliability, safety, confidentiality, integrity, availability, maintainability
ETA	estimated time of arrival
FOM	Feature-oriented Modeling
FS	Fire Station
FSC	Fire Station Coordinator
OOM	Object-oriented Modeling
PS	Police Station
PSC	Police Station Coordinator
Security	confidentiality, integrity, availability
SOM	Service-oriented Modeling
SPL	Software Product Line