Safety and security aware framework for the development of feedback control systems

J.P. Lobo*, P. Charchalakis*, E. Stipidis*

*Vetronics Research Centre, University of Brighton, UK – j.lobo@vetronics.org

Keywords: Control, Safety, Security, Framework, Modularity.

Abstract

The need to address safety and security related aspects at an early stage of development of feedback control systems (FCS) has been identified as vital for the optimisation of the development process of military land systems.
These systems often include network enabled capability (NEC) allowing the use of electronics architectures to integrate different sub-systems. However, this increased integration capability is associated with magnified safety risks and compromise from cyber attacks [4].
This paper discusses how the process of developing FCS for military land systems could benefit from the use of a framework that addresses safety and security issues at the system modelling level.
The core part of the suggested framework consists of a Simulink model to be used by design engineers as a blueprint for the development of a modular FCS that are expected to feature a modular architecture with dedicated sub-modules for the processing of data related to safety and security aspects.
Since the FCS developed through the use of framework features a modular architecture, the anticipated cost incurred in the design of the associated modular safety case is expected to be reduced, leading to an overall reduction of the cost of the re-certification process [1].

1 Introduction

Engineering systems from a variety of application domains have been increasingly exposed to the need for regular updates and upgrades. In systems where security and safety aspects are a major concern, technical modifications are typically followed by a re-certification process. The process of re-certifying a system is complex and costly, and from a safety and security perspective it has been advocated [6] that in order to increase the effectiveness of the certification process there is the need to ensure that the safety analysis is started at an earlier stage of a system development cycle, so that the assurance case can actually influence design decisions. This argument together with the principles that enabled the application of the modular safety case approach for systems based on Integrated Modular Avionics (IMA) [5] have played a vital role on the development of the framework.
This framework was developed as part of a research programme funded by the UK MOD/DSTL. Particular effort was placed in designing a framework that could address, at a system design level, issues related with safety and security aspects of feedback control systems.
Current military land systems increasingly rely on data networks to connect a vast array of vetronics (vehicle electronics) subsystems [2]. Therefore, it would be beneficial to consider the design of such feedback control systems while also taking into consideration safety and security aspects (e.g. end to end encryption).
Section 2 of this paper presents an overview of the developed framework and in section 3 the safety and security extensions of the framework are explained. In section 4 a set of four theoretical case studies are presented with the objective of evaluating whether or not the use of the framework could bring benefits related to the safety and security aspects of feedback control systems. Section 5 concludes the paper and contains considerations about future work.

2 Framework Overview

The framework brings together in one development package the benefits associated with concepts such as integrated architectures [7], model driven system engineering (MSDE) [8], and modular safety cases [3]. Hence, providing design engineers with a structured development process that could lead to control systems architectures that are more adaptable for future changes and more efficient in application reuse.
The suggested framework consists of a Simulink model to be used as a blueprint model for the development of FCS, and guidelines on how to start and navigate through the different modules of the model and understand the default data model of the Simulink model.
Figure 1 shows the top level architecture of the Simulink model and how data flows between the modules. Each of these modules except the Control Input Unit Modules CIUMs and the Control Input Output Modules COUMs is made of the sub-modules shown in Figure 2**.**
The interconnection between the modules of the Simulink model is achieved through the use of “bus based” links carrying dynamically configured bus data structures that are tagged into different categories.
To develop a feedback control system for a specific application the design engineer will have to decide how many Control Input Unit Modules (CIUMs) are going to be used

and customise them according to the requirements and specification of the application to be controlled. The same approach should be followed to customise the Control Output Unit Modules (COUMs). For the remaining modules the customisation should happen on the sub-modules of each module. Each module or sub-module should be customised with algorithms that implement the logic required by the application to be controlled and the outputs of the algorithms have to match the data bus format defined for the interfaces of each module. The framework also gives the possibility for design engineers to edit the default data model used in the Simulink model in order to have it adjusted to the requirements of the application to be controlled. This option adds extra complexity to the initial development of the FCS as it eventually requires the update of the algorithms of the internal sub-modules as well as the use of the bus editor facility to change the format of the data bus defined for the interfaces of each module and sub-module.

3 Safety and Security considerations

As it was mentioned in section 2, data flowing between the modules of the Simulink model is tagged into different categories. Data containing safety related information is tagged as safety data and data containing security related information is tagged as security data. Inside of each module of the Simulink model there are dedicated sub-modules to process safety data and security data as shown in Figure 2. These sub-modules can be customised with algorithms that implement the safety and security requirements of the application to be controlled.

The safety and security capabilities of the developed FCS can be changed by simply changing the algorithms on the safety and security sub-modules of each module of the Simulink model. This facility not only could allow a faster response to overcome eventual vulnerabilities, but it could also reduce the probability of a cyber attack by changing the data encryption mechanism more often.

One of the primary goals of the framework is to guide design engineers through a process to develop FCS, that addresses issues related with safety and security of FCS at the system design level. Hence, the presence of dedicated safety and security sub-modules in the framework's default Simulink model. This allows design engineers to be aware of the safety and security aspects of the FCS early on in the development life cycle.

Section 4 of this paper presents four theoretical case studies that were created to show how the use of the framework to develop FCS could bring long term benefits that vary from, increased safety and security capabilities, increased algorithm reusability, to an increased functional segmentation that can lead to the reduction of the cost incurred in the design of modular safety case associated with the feedback control system.

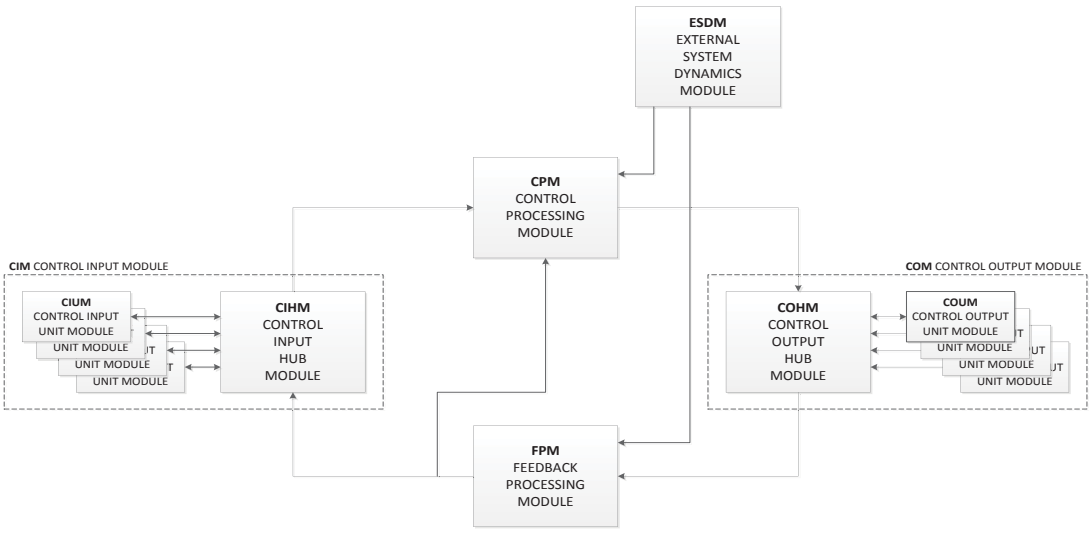

Figure 1 - Top level architecture of the Simulink model of the framework.

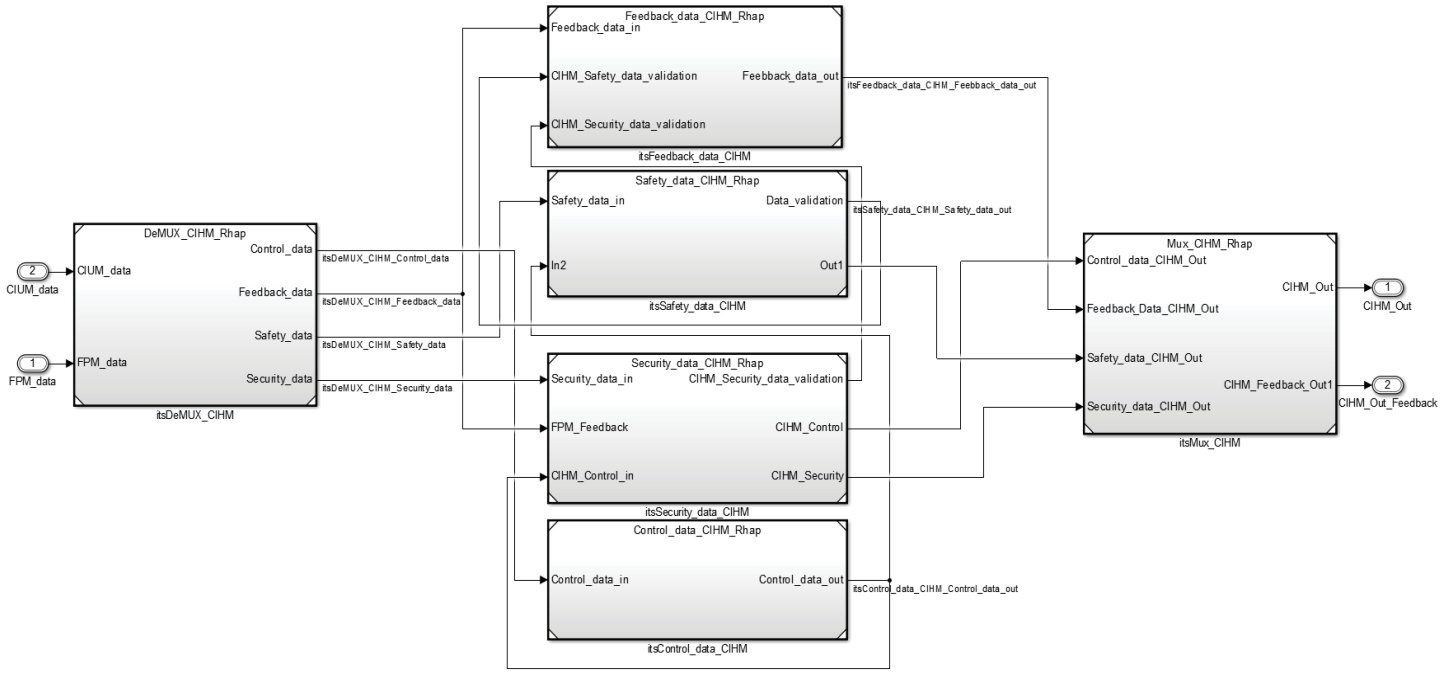

Figure 2 - Processing segmentation inside the main modules of the framework

4 Case Studies

The following theoretical case studies aim to highlight the safety and security benefits that could be achieved through the use of the framework for the development of modular feedback control systems. The case studies are considered as a sequence of engineering development steps spanning throughout the lifetime of a drive-by-wire system, covering initial development, capability upgrades, and urgent critical updates. Such an example can be considered as applicable to both military land vehicles and modern / future civilian vehicles, as system safety and security are both directly linked with human safety.

Case study 1. This case study shows the typical use of the framework for the initial development of a basic FCS for a drive-by-wire vehicle. The designer(s) will take the reference high-level model of the framework and by following the provided guidelines populate the relative sub-modules with the application specific algorithms and hardware / software interfaces. With full visibility of the model components, the developers will be able to customise and tailor any parts necessary to fit their application requirements, while at the same time having pre-prepared the generic elements that are common to typical FCS applications. The inherent presence of safety and security sub-components, already integrated into the model design, will provide a baseline to the developer(s) and enable smoother integration of the safety and security requirements with the development of the control algorithm's functional and system requirements. The provided separation of the control algorithm (control and feedback), safety, and security sub-components will also enable their parallel development by multiple developers working on their individual specific designs, with a pre-existing integration path.

At the end of the development cycle it is expected that the use of the framework to develop the FCS for the vehicle would result on a system design with a highly modular and generically structured core Simulink model. The design will feature minimal internal inter-dependencies between the algorithms running on the different blocks and sub-modules. By following these guidelines, it is thus made possible to keep future changes (or late-stage modifications due to last-minute requirements changes or design fault detection) to modify existing components or integrate new ones confined to well-defined parts of the feedback control model. An optimised and simplified re-development procedure would also reduce the cost of re-certifying the modified system design [1] and lead to overall through-life cost savings.

Case study 2. This case study considers the requirement for integration of a new input (e.g. steering wheel) or output (e.g. actuator) device to the drive-by-wire system of the vehicle described in case study 1, as a replacement to an existing device. Such an example represents a typical scenario where a device has to be replaced with a new model due to the discovery of internal device design faults found post-design, during mass-production, or post-production of the vehicle. Such a system change requirement could also be applicable to the adaptation of an existing drive-by-wire system to a new vehicle design.

As the FCS of the vehicle was developed based on the framework, the replacement of the new device will require most changes to be applied to the device applicable sub-components, rather than the core control & feedback algorithm components. Such changes would require simply

the replacement of a Control Input Unit Module (CIUM) or a Control Output Unit Module (COUM) with a new module, or by updating the internal algorithm of the existing modules if the functional differences are small. The modular and abstracted design of the model, combined with the standardised inter-communication of sub-modules, will make it possible for the remaining components of the control model not to have to be modified, unless the newly integrated device incorporates major changes to the functional operation of the whole system.
Assuming that a modular safety case associated with the FCS from case study 1 had been produced and is available, the re-certification process of the new FCS would only require changes in the relevant safety case module of the components that have been modified. In addition, considering that the security related aspects of the system remain the same despite the integration of a new device, the relative sub-blocks of the previous device's model could also be reused.
It is considered that scenarios such as the one presented in this case study would have much higher associated costs for development and certification, if conducted on a system design without design-time provisions for modular control, safety, and security. Additional benefits from a modular framework based approach would also be increased user / customer satisfaction gained from the quicker development cycle turn-around.

Case study 3. This case study considers the introduction of an urgent requirement to modify, either partially or fully, the security aspects of the drive-by-wire system of the vehicle described in case study 1. Such an example would be applicable to highly inter-connected vehicle platforms, encompassing both military and civilian vehicle platforms that have presented a security vulnerability, which is exploitable and can potentially interfere with the safe control of the vehicle. It also highlights how the provisions for separated modules to process data related with safety and security aspects, made by the framework and integrated from the initial design of the system, can be beneficial in the long term.
It is considered that the majority of the required changes would be focused on elements such as changes to signing / encryption certificates, encryption algorithm selection, and signing / encryption algorithm specific implementations. Modifications to the system's model would thus be focused and isolated to the security sub-blocks without affecting the control and safety related elements. Any changes to the inter-communication between the internal modules would also be easier to implement due to the structured bus-based and data model approach of the framework. Re-certification of the modified system design would be similar to the 2nd case study, through the use of a modular safety case approach.
The overall benefits to the system designer would be similar to the 2nd case study, and possibly greater as the changes to the core control and safety elements could be minimal to none.

Case study 4. This case study considers the typical scenario of an existing entity adopting the use of the framework while having an established FCS, using a gradual transition to keep associated costs spread throughout a longer period compared to a complete overhaul or redesign of the legacy system.
The abstracted and modular design of the framework's model allows the user to re-use legacy control algorithms by implementing a "black-box" approach where the existing control models are treated as independent entities and integrated within the framework's modules. The framework's model is thus effectively functioning as a wrapper creating a virtually modular FCS. The initial integration could implement all or parts (the most important and costly to redesign algorithms) of the legacy system. With the adoption of the framework's model, the developer will also be able to use the security elements of the framework, effectively adding security related features to the legacy system.
Following this initial integration, the developer will be able to upgrade the system (as described in case studies 2 & 3) gradually phasing out the legacy elements and ending up with a fully modular FCS. Such staggered development capability is considered a key enabler for the adoption of new concepts in areas where adoption of new technologies is inhibited due to the industry's preference of using pre-existing and trusted technologies.

5 Conclusion

This paper presented the safety and security aspects of a modular framework developed to optimise the development process of feedback control systems for complex and critical systems, such as drive-by-wire implementations for military land systems and civilian vehicles. The structure of the framework was presented to show how safety and security aspects are integrated within the design and how the inherent abstraction and modular concepts of the framework aid the development process. A set of case studies were discussed to demonstrate the applicability of the framework and the possible benefits that can be gained at various points of the lifetime of a feedback control system. The continuous presence of safety and security aspects throughout all cases shows how such aspects can be considered simultaneously and at the same importance level as the core "feedback control" requirement of such a model. In addition, it is considered that this presence of the dedicated safety and security related sub-modules in the framework's default Simulink model could have a very positive impact on a design engineers' mind set. Such benefits could vary from an increased awareness for safety and security aspects from an early stage of the development of FCS, to being able to increase the security level of legacy systems.
The results presented in this paper also indicate that the modular architecture and functional segmentation with integrated safety and security provisions, featured by feedback control systems developed with the framework, could enable the practicability of designing modular safety cases associated to the developed feedback control system. The advent of this practicability will reduce the cost of re-certification of changed systems and lead to an overall through-life cost saving [1]. The benefits associated with the

use of the framework as a development package could be particularly valuable to the military land systems industry, where the increased need to improve crew survivability has led to an increased frequency of required upgrades. Such upgrades have in some occasions been affected by very lengthy development and delivery times due to the complexity of the re-certification process. Similar to the military domain, modern and future civilian vehicles are becoming increasingly inter-connected, highlighting the need for heightened security requirements within the platform's safety-critical sub-systems, along with the typical safety requirements.

6 References

[1] Agusta Westland Limited, BAE SYSTEMS, GE Aviation, General Dynamics United Kingdom Limited, SELEX Galileo Ltd, "Modular Safety Cases Facilitating Incremental Upgrade to Military Capability by Managing the Complexity of Safety Assurance ", 2012.

[2] Abdulmasih, D., Oikonomidis, P.I., Annis, R., Stipidis, E., and Charchalakis, P., "Operational integrity monitoring for military vehicle's integrated vetronics architecture," in *System Safety, 2011 6th IET International Conference on*, 2011, pp. 1-6.

[3] Bate, I. and Kelly, T., "Architectural considerations in the certification of modular systems", *Reliability Engineering & System Safety,* vol. 81, pp. 303-324, 2003.

[4] Deshpande, A., Obi, O., Stipidis, E., and Charchalakis, P., "Integrated vetronics survivability: Requirements for vetronics survivability strategies," in *System Safety, 2011 6th IET International Conference on*, 2011, pp. 1-6.

[5] Kelly, T., "Using software architecture techniques to support the modular certification of safety-critical systems", presented at the Proceedings of the eleventh Australian workshop on Safety critical systems and software - Volume 69, Melbourne, Australia, 2006.

[6] Leveson, N., "The Use of Safety Cases in Certification and Regulation", *Journal of System Safety,* vol. Vol. 47, November-December 2011 2011.

[7] Prisaznuk, P.J., "Integrated modular avionics," in *Aerospace and Electronics Conference, 1992. NAECON 1992., Proceedings of the IEEE 1992 National*, 1992, pp. 39-45 vol.1.

[8] Seng, C., Chi-Biu, W., Haibo, J., Hongtao, P., Moore, P., Kalawsky, R., and O'brien, J., "Model Driven System Engineering for vehicle system utilizing Model Driven Architecture approach and hardware-in-the-loop simulation," in *Mechatronics and Automation (ICMA), 2011 International Conference on*, 2011, pp. 1451-1456.