La sécurité des ascenseurs avec des communications Ethernet-Based Real-Time

Ayoub Soury, Denis Genon-Catalot, Jean-Marc Thiriet

La sécurité des ascenseurs avec des communications Ethernet-Based Real-Time

Ayoub SOURY, Denis GENON-CATALOT et Jean-Marc THIRIET
Université Grenoble Alpes - Laboratoire de Conception et d'Intégration des Systèmes (LCIS) et GIPSA-LAB
{ayoub.soury, denis.genon-catalot}@lcis.grenoble-inp.fr
jean-marc.thiriet@gipsa-lab.grenoble-inp.fr

Résumé : l'évolution des systèmes de contrôle industriels tendent vers des infrastructures de plus en plus connectées, ce qui les rendent plus dépendantes de réseaux et de protocoles de communication utilisés. Plusieurs travaux existants se sont focalisés sur la fiabilité de ces systèmes et la robustesse de leurs modèles de contrôle en cas de pannes ou de dysfonctionnement. Ces travaux n'ont pas considéré l'aspect réseau qui est devenu un vecteur d'attaque important étant donné l'utilisation de protocoles de communication pour l'échange des informations entre les équipements. Les conséquences de ces attaques, parfois deviennent extrêmement dévastatrices. En effet, récemment ces réseaux sont devenus la cible de plusieurs attaques en exploitant des vulnérabilités présentes dans les couches logicielles ou protocolaires de leurs équipements. Dans le cadre de la nouvelle génération de commande de l'ascenseur, un cas de transition sera analysé à partir d'un composant électrique/électrotechnique au réseau de composants électroniques communiqués dans le cadre de la sécurité du système de déplacement d'un ascenseur. La proposition repose sur la sécurité des modules IP interconnectés entre eux, qui supportent un protocole temps réel industriel (Powerlink, EtherCat et Sercos). Cette proposition représente un des démonstrateurs du projet collaboratif avec un noyau déterministe sûr de fonctionnement par construction.

Mots clés : protocoles de communication, ascenseur, réseau de composants électroniques, sécurité des modules IP, Powerlink, EtherCat.

1. INTRODUCTION

Aujourd'hui, la chaine de sécurité d'un ascenseur repose sur des éléments électromécaniques reliés entre eux de façon filaire comme montre la Fig 1.

Celle-ci nécessite donc un grand nombre de câbles qui ont un impact direct sur le coût du produit ainsi que sur sa complexité d'installation et donc son coût d'installation.

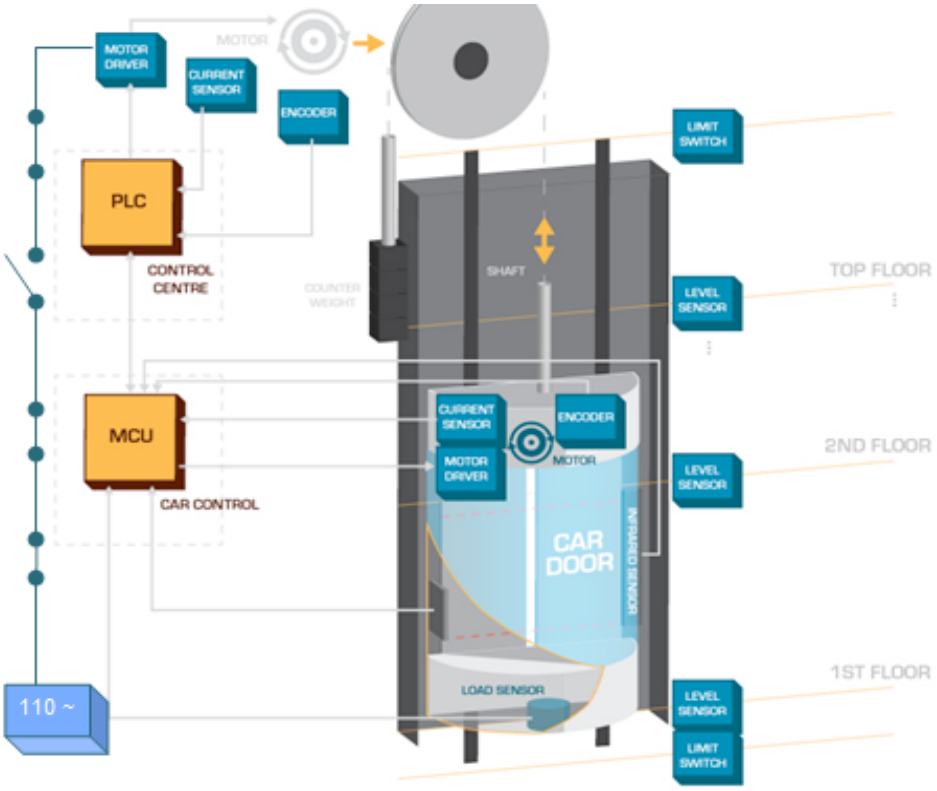

Figure 1 : Chaine de sécurité classique pour l'ascenseur.

Dans un souci d'économie (réduction des couts d'installation, de maintenance, de certification …) et de modernisation (gain en fiabilité, robustesse, évolutivité, capacité à détecter et identifier les défauts …), nous souhaitons réaliser les fonctions de sécurité non plus par des moyens électromécaniques mais via un système électronique programmable (**P**rogrammable **E**lectronic components and **S**ystems in **S**afety **R**elated **A**pplications for **L**ifts PESSRAL). L'objectif de ce démonstrateur est donc concevoir un PESSRAL en intégrant les éléments suivants :

- Usage d'un bus sécurité certifié SIL3.
- Application de la norme IEC61508.
- Montrer les gains en matière simplification de la phase de certification et réduction des efforts de test:
    - En s'appuyant sur l'approche déterministe et cadencée par le temps.
    - En s'appuyant sur les propriétés de ségrégation spatio-temporelle et déterminisme d'un noyau temps réel.

- Capacité à intégrer des fonctions tierces non critiques sans remettre en cause la certification des fonctions critiques.

- Héberger des fonctions critiques et non critiques sur le même microcontrôleur.

- Faire la preuve du système par construction et non pas par validation.

L'originalité de cette réalisation réside dans l'usage d'une solution logicielle innovante en l'occurrence Kron-OS de la société Krono-safe. Kron-OS se base sur un noyau déterministe. Ce noyau répond à l'IEC 880 (Safety System of Nuclear Power, RFS (Règles de sécurité françaises), DO-178B et la SAE [1]).

Notre modèle de communication doit répondre à son tour à l'IEC61508 d'ordre général, et la PESSRAL qui est la dérivée de l'IEC 61508 pour le domaine applicatif des ascenseurs en particulier. L'objectif est d'assurer la sécurité des personnes qui sont transportés. Le niveau de disponibilité du système est à mettre au second plan par rapport à la sécurité. Le démonstrateur ascenseur, est une partie de l'ADN4SE (**A**telier de **D**éveloppement et **N**oyau pour **S**ystèmes **E**mbarqués). Son objectif est de concevoir et développer les fonctions de sûreté d'un ascenseur par des systèmes électroniques. Ces derniers utilisent un noyau déterministe et ses outils associés en répondant aux normes de sécurité pour l'ascenseur afin d'arriver à la certification du produit. Les normes applicables pour la conception d'un système de sécurité pour ascenseur sont EN 81-1 (spécification des prescriptions de sécurité relatives à la conception et à l'installation des ascenseurs électriques) et PESSRAL (Programmable Electronic components and Systems in Safety Related Applications for Lifts) ISO22201 :2008 (norme relative aux systèmes électroniques programmables intégrés à la chaine de sécurité d'un ascenseur).

2. IEC 61508 ET PESSRAL :

Pour minimiser les échecs (failures) et maintenir la sureté de fonctionnement dans les systèmes électriques, électroniques et électroniques programmables à un niveau déterminé, l'IEC 61508 spécifie 4 niveaux d'intégrité de sécurité en matière de sureté de fonctionnement (SIL1, SIL2, SIL3, SIL4) [2] qui couvrent les fonctionnalités de sécurité du système et lui exige dès sa conception à répondre et satisfaire certains critères et conditions de sécurité. Pour notre domaine d'application (Lift), on va s'intéresser au

niveau SIL3 de l'IEC 61508. Ce niveau est exigé par le noyau qui supporte cette solution. Pour atteindre ce niveau d'intégrité de sécurité, notre système doit répondre à un certain nombre d'exigence spécifique à l'application des ascenseurs comme il est indiqué dans la Table 1 et la Table 2.

Exigence	Mesure
EXI_PESSRALA1_01	Use of watchdog
EXI_PESSRALA1_02	Use of components only within their specifications
EXI_PESSRALA1_03	Defined safe state in the event of a power failure or reset
EXI_PESSRALA1_04	Defined safe shut-off state in case of over-voltage or under voltage00000000000
EXI_PESSRALA1_05	Use of only solid-state memories
EXI_PESSRALA1_06	Read/write test of variable data memory during boot procedure
EXI_PESSRALA1_07	Remote access only to informative data (e.g. statistics)
EXI_PESSRALA1_08	No possibility to change the program code, either automatically by the system or remote intervention
EXI_PESSRALA1_09	Test of program-code memory and fixed-data memory during boot procedure with a method at least equivalent to sum check

Table 1 : Exigences matérielles [3].

Programmable Electronic components and Systems in Safety Related Applications for Lifts, norme dérivée de l'IEC 61508, et propre à notre domaine d'application détaille ces exigences et les identifie en exigences métiers et exigences matérielles. Ces exigences sont décrites dans les deux tables ; Table 1 et Table 2.

Exigence	Mesure	IEC 61508
EXI_PESSARELA2_01	Program structure (i.e. modularity, data handling, interface definition) according to the state of the art (see IEC 61508-3)	X
EXI_PESSARELA2_02	During boot procedures a safe state of the lift shall be maintained	—
EXI_PESSARELA2_03	Limited use of interrupts; use of nested interrupts only if all possible sequences of interrupts are predictable	X
EXI_PESSARELA2_04	No triggering of watchdog by interrupt procedure except in combination with other program sequence conditions	X
EXI_PESSARELA2_05	No power-down procedures, such as saving of data, for safety related functions	—
EXI_PESSARELA2_06	Stack manager in the hardware and/or software with appropriate reaction procedure	X
EXI_PESSARELA2_07	Iteration loops shorter than system reaction time, e.g. by limiting the number of loops or checking execution time	—
EXI_PESSARELA2_08	Array pointer offset checks, if not included in the programming language used	X
EXI_PESSARELA2_09	Defined handling of exceptions (e.g. divisions by zero, overflow, variable range checking, etc.) that forces the system into a defined safe state	—
EXI_PESSARELA2_10	No recursive programming, except in well tried standard libraries, in approved operating systems, or in high-level language compilers. For these exceptions, separate stacks for separate tasks shall be provided and controlled by a memory management unit	X
EXI_PESSARELA2_11	Documentation of programming library interfaces and operating systems at least as complete as the user program itself	—
EXI_PESSARELA2_12	Plausibility checks on data relevant to safety functions, e.g. input patterns, input ranges, internal data	X
EXI_PESSARELA2_13	If any operational mode can be invoked for testing or validation purposes, normal operation of the lift shall not be possible until this mode has been terminated	X

EXI_PESSARELA2_14	Reach a safe state with due consideration to the system reaction time in a bus communication system with safety functions in case of loss of communication or a fault in a bus participant	X
EXI_PESSARELA2_15	No reconfiguration of the CPU-bus system, except during the boot procedure NOTE Periodical refresh of the CPU-bus system is not considered as being a reconfiguration.	X
EXI_PESSARELA2_16	No reconfiguration of I/O lines, except during the boot procedures NOTE Periodical refresh of the I/O configuration registers is not considered as a reconfiguration.	X

Table 2 : Exigences Software-Système [3].

3. LES APPROCHES REAL-TIME ETHERNET: RTE

Des nouveaux concepts de communication industriels commencent à évoluer après deux ans de la guerre de réseaux de terrain. L'IEC TC65 a lancé un nouveau projet de standardisation pour la communication industriel. Définir le real-time Ethernet dans l'industrie parait une conséquence logique de l'introduction d'Ethernet dans 'industrial automation'. les chercheurs ne cessent de proposer des solutions pour les spécifications d'Ethernet, afin de répondre aux critères « temps-réel ». il y a ceux qui proposent des solutions pour la qualité de service, pour la synchronisation entre les dispositifs ou la modification du traitement de paquet [4]. On peut classer ces solutions à base d'Ethernet en 3 classes, en considérant le temps de réponse de chaque solution [4] comme montre la Fig 2.

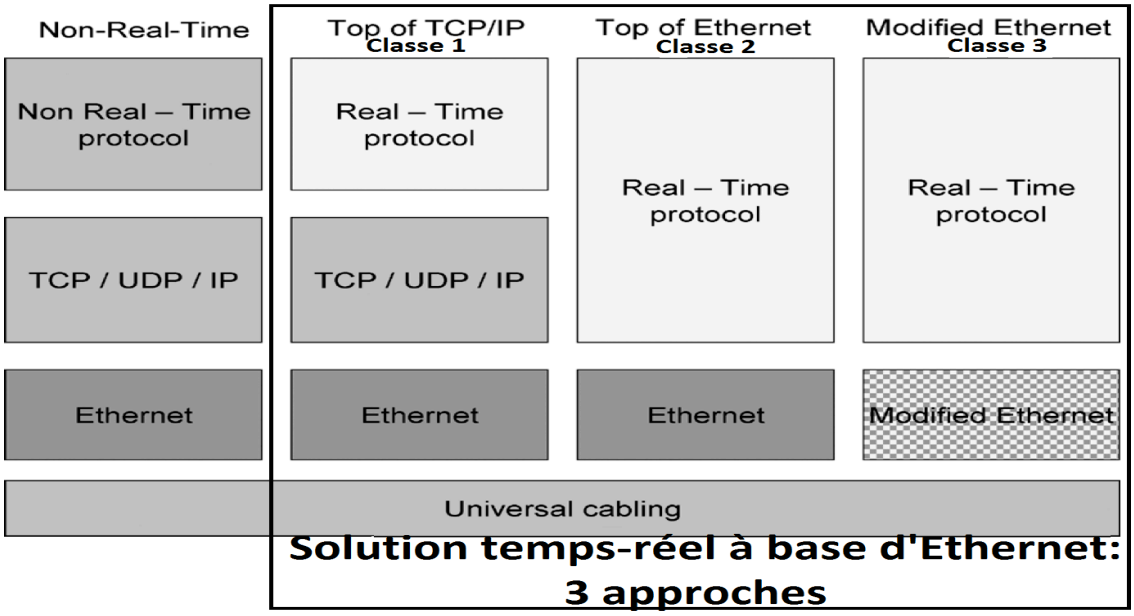

Figure 2 : Classification des Solutions RTE.

Ces solutions seront implémentées au-dessus d'un noyau déterministe sûr de fonctionnement par construction, qui exige certains critères pour accélérer et garantir la communication dans le système industriel. Le modèle de communication exigé par ce noyau, répond aux spécifications de celui-ci. Outre que le temps de réponse, le modèle doit garantir le niveau d'intégrité de sécurité SIL3 pendant la phase de communication pour garantir la portabilité du modèle sur un système d'exploitation déterministe dans des environnements embarqués. Dans ce travail, nous nous appuyons sur l'architecture actuelle de la chaine de sécurité dans les systèmes de contrôle d'ascenseur. On a introduit des nœuds de contrôle interconnectés entre eux à travers un réseau afin d'améliorer le comportement de la chaîne actuelle. La Figure 3, décrit la nouvelle architecture du système avec nos modifications dans la chaîne de sécurité.

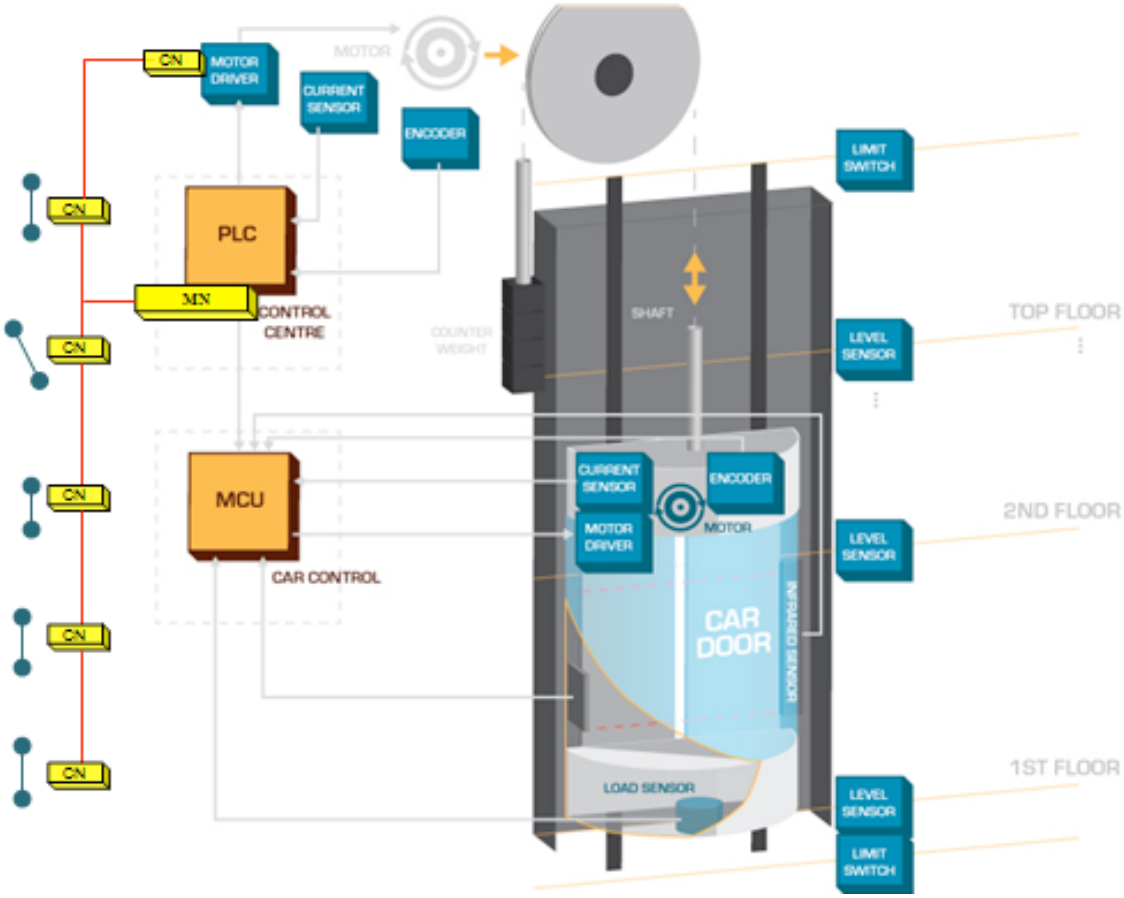

Figure 3 : Modification de la chaîne de sécurité dans le système de contrôle d'ascenseur.

4. CONCLUSION

Dans le cadre de ce projet, nous allons démontrer grâce au support de protocole IP adapté, que nous pouvons obtenir les critères de sureté de fonctionnement nécessaires pour les applications dans l'ascenseur. Les

critères de fonctionnement des machines de la norme IEC 61508 appliquées aux métiers de l'ascenseur ont fait évoluer vers les spécifications PESSRAL. L'aspect innovant de ce projet collaboratif, outre le fait de démontrer, la portabilité du noyau Kron-OS dans des environnements embarqués contraints (STM32F2xx), est de pouvoir remplacer les éléments de la chaine de sécurité (encore à contact électrique) par un réseau de terrain adapté pour l'ascenseur. L'article rappelle les critères nécessaires à atteindre lors du choix des protocoles pour garantir l'intégrité de la norme PESSRAL. La méthodologie mixée permet d'intégrer l'architecture de communication dans le développement afin d'en garantir les performances temporelles (sureté de fonctionnement par construction).Notre contribution au projet va permettre d'effectuer une analyse de la chaine de sécurité qu'il est impossible de diagnostiquer à ce jour (contact see). Cette stratégie autorisera la commande de déplacement de la cabine d'un ascenseur dans des conditions de sécurité bien identifiées ce qui simplifie grandement la manœuvre qu'aujourd'hui nécessite une intervention humaine localement. L'ensemble de ces travaux bénéficie du support financier du ministère de l'industrie sur des investissements d'avenir.

5. REFERENCES

[1] Chabrol, D., David, V., Aussaguès, C., Louise, S., & Daumas, F. (2005, November). Deterministic Distributed Safety-Critical Real-Time Systems within the Oasis Approach. In IASTED PDCS (pp. 260-268).

[2] IEC 61508-2:2000, "Functional safety of electrical/electronic/programmable electronic safety related systems" – Part 2:Requirements for electrical/electronic/programmable electronicsafety-related systems.

[3] PESSRAl: 2008, "lifts-design and development of programmable electronic systems in safety related application for lifts (PESSRAL)".

[4] Felser, M., & Sauter, T. (2004, September). Standardization of industrial ethernet-the next battlefield?. In Factory Communication Systems, 2004. Proceedings. 2004 IEEE International Workshop on (pp. 413-420).