

ÉCOLE NATIONALE POLYTECHNIQUE



Département d'Électronique

Mémoire de Projet de Fin d'Études

Présenté pour l'obtention du diplôme d'Ingénieur d'État en Électronique

**Conception et sécurisation d'un réseau de
calculateurs automobiles basé sur SoC FPGA**

ABDENNEBI Mohamed Ryad et KEIACHE Abdesselam

Présenté et soutenu publiquement le : 22 juin 2026

Membres du jury :

Président :	BOUMELA Nora	Dr.	ENP, Alger
Encadrant :	LANI Fatiha	Dr.	ENP, Alger
Co-encadrant :	DRAI Redouane	Dr.	CRTI, Alger
Examineur :	BOUSBIA-SALAH Hicham	Pr.	ENP, Alger

ENP 2026

ملخص

يتناول هذا العمل تصميم وتنفيذ بنية إلكترونية/كهربائية (E/E) آمنة وحتمية لمركبات الجيل الجديد، وفق نهج هجين يجمع بين النموذجين المناطقي والمجالّي.

يرتكز العمل المنجز على وحدات SoC FPGA بوصفها متحكمات مناطقيّة، مرتبطة بمتحكمات دقيقة تضطلع بوظائف الوحدات الإلكترونيّة التحكّمية في السيارة. تتربط هذه المتحكمات عبر شبكة عمود فقري TSN تكفل اتصالاً بين المناطق حتمياً وموثوقاً، مناسباً للتطبيقات الفورية. يدار النظام بأكمله ببيئة لينكس مدمجة مخصصة، طورت خصيصاً لهذا المشروع لتولي التنسيق الشامل للبنية وإدارة تبادل البيانات. وتضمن سلامة الاتصالات بدمج مسرع تشفير ماديّ منفذ في الجزء البرمجي (PL) من الدائرة.

الكلمات المفتاحية: بنية E/E مدمجة، شبكات TSN، الأمن السيبراني للسيارات.

Abstract

This thesis presents the design and implementation of a secure and deterministic E/E architecture for next-generation vehicles, based on a hybrid approach combining zonal and domain models.

The work relies on FPGA SoCs used as zone controllers, interfaced with microcontrollers performing the functions of automotive ECUs. The different controllers are interconnected through a TSN backbone ensuring deterministic, reliable inter-zone communication suited to real-time applications. The entire system is driven by a customized embedded Linux environment, developed specifically for this project, enabling the global orchestration of the architecture and the management of data exchanges.

Communication security is ensured through the integration of a hardware cryptographic accelerator implemented in the programmable logic (PL).

Keywords: Automotive E/E architecture, Time-Sensitive Networking (TSN), Automotive cybersecurity.

Résumé

Le mémoire s'inscrit dans la conception et la mise en œuvre d'une architecture E/E sécurisée et déterministe pour les véhicules de nouvelle génération, reposant sur une approche hybride combinant les modèles zonal et domaine.

Le travail réalisé s'appuie sur des SoC FPGA utilisés comme contrôleurs de zone, interfacés avec des microcontrôleurs assurant les fonctions de calculateurs automobiles. Les différents contrôleurs sont interconnectés au travers d'un backbone TSN assurant une communication interzone déterministe, fiable et adaptée aux applications temps réel. L'ensemble du système est piloté par un environnement Linux embarqué personnalisé, développé spécifiquement pour ce projet, permettant l'orchestration globale de l'architecture et la gestion des échanges, et pour la sécurité des communications, elle est assurée par l'intégration d'un accélérateur matériel de cryptographie implémenté dans la partie programmable (PL).

Mots-clés : Architecture E/E embarquée, Time-Sensitive Networking (TSN), Cybersécurité automobile.

Table des matières

Liste des tableaux

Liste des figures

Liste des abréviations

Introduction générale **11**

Chapitre 1 : État de l'Art : Architectures E/E dans le Véhicule Moderne **13**

1.1	Évolution de l'électronique embarquée dans le véhicule	14
1.2	Protocoles et technologies de communication automobile	17
1.2.1	Présentation des principaux protocoles automobiles	17
1.2.2	Analyse comparative des protocoles	19
1.3	Architecture E/E distribuée classique	21
1.3.1	Organisation et fonctionnement	21
1.3.2	Limites et défis	22
1.4	Architectures E/E de nouvelle génération	23
1.4.1	Architecture centralisée	23
1.4.2	Architecture par domaine	24
1.4.3	Architecture zonale	25
1.4.4	Architectures hybrides	26
1.4.5	Déploiement industriel des architectures de nouvelle génération	27
1.5	Sécurité des Communications E/E	28
1.5.1	Surface d'attaque du réseau embarqué	28
1.5.2	Analyse des menaces selon l'approche TARA	30
1.5.3	Solutions existantes pour la sécurité des communications embarquées	30
1.6	Cadre Normatif et Standards du Domaine Automobile	31
1.7	Synthèse Critique de l'État de l'Art	33
1.8	Conclusion	35

Chapitre 2 : Analyse des Besoins et Conception du Système Proposé **36**

2.1	Analyse de la problématique	37
2.1.1	Limites quantifiées des architectures distribuées	37
2.1.2	Exigences des véhicules nouvelle génération	37
2.1.3	Contraintes d'homologation	37
2.2	Cahier des charges	38
2.2.1	Objectif général du système	39
2.2.2	Exigences fonctionnelles	39
2.2.3	Exigences non-fonctionnelles	41
2.2.4	Contraintes de conception	42
2.2.5	Critères et métriques de validation	42
2.3	Solution proposée	43
2.3.1	Vision globale de la solution	43

2.3.2	Architecture fonctionnelle globale	44
2.3.3	Sous-système de communication	45
2.3.4	Sous-système de synchronisation temporelle	46
2.3.5	Sous-système de cybersécurité	46
2.3.6	Analyse de conformité au cahier des charges	50
2.4	Architecture système retenue	51
2.4.1	Choix des plateformes de développement	51
2.4.2	Répartition fonctionnelle des nœuds du système	51
2.4.3	Répartition matérielle et logicielle au sein du MPSoC	52
2.5	Conclusion	52
Chapitre 3 : Fondements Théoriques et Technologies Utilisées		53
3.1	Time-Sensitive Networking (TSN)	54
3.2	Traitement Asymétrique Multiprocesseur (AMP)	61
3.3	Cybersécurité embarquée	67
3.4	Système d'Exploitation Linux Embarqué	74
3.5	Conclusion	79
Chapitre 4 : Implémentation Matérielle		80
4.1	Environnement de Développement	81
4.2	Conception du Design FPGA	81
4.2.1	Conception du Block Design	81
4.2.2	Blocs IP du Block Design	83
4.2.3	Intégration de l'accélérateur AES-GCM	83
4.3	Conclusion	90
Chapitre 5 : Implémentation Logicielle		91
5.1	Répartition des tâches entre les composants	92
5.2	Construction de l'OS embarqué dédié	95
5.3	Pipeline CAN sécurisé	101
5.4	Pipeline vidéo chiffré	104
5.5	Couche de sécurité	105
5.6	Conclusion	107
Chapitre 6 : Validation du Système et résultats		108
6.1	Environnement expérimental	109
6.2	Phase 1 : Validation fonctionnelle sans TSN	110
6.2.1	Benchmark et périmètre de mesure	110
6.2.2	Récapitulatif bout-en-bout	113
6.3	Phase 2 : Validation TSN et synchronisation	114
6.3.1	Synchronisation temporelle	114
6.3.2	Configuration TSN et dimensionnement des fenêtres	115
6.3.3	Surcoût du TSN et impact sur la latence	116
6.4	Phase 3 : Validation de la sécurité	116
6.5	Bilan et utilisation des ressources	117
6.6	Limites du prototype	119
Conclusion générale		120
Bibliographie		123
Annexes		127

Confidentiel