Sécurité et sûreté dans la chaîne d'approvisionnement de l'industrie de l'automobile

Sebastian Fischmeister

Département de génie électrique et informatique
Université de Waterloo

esg.uwaterloo.ca

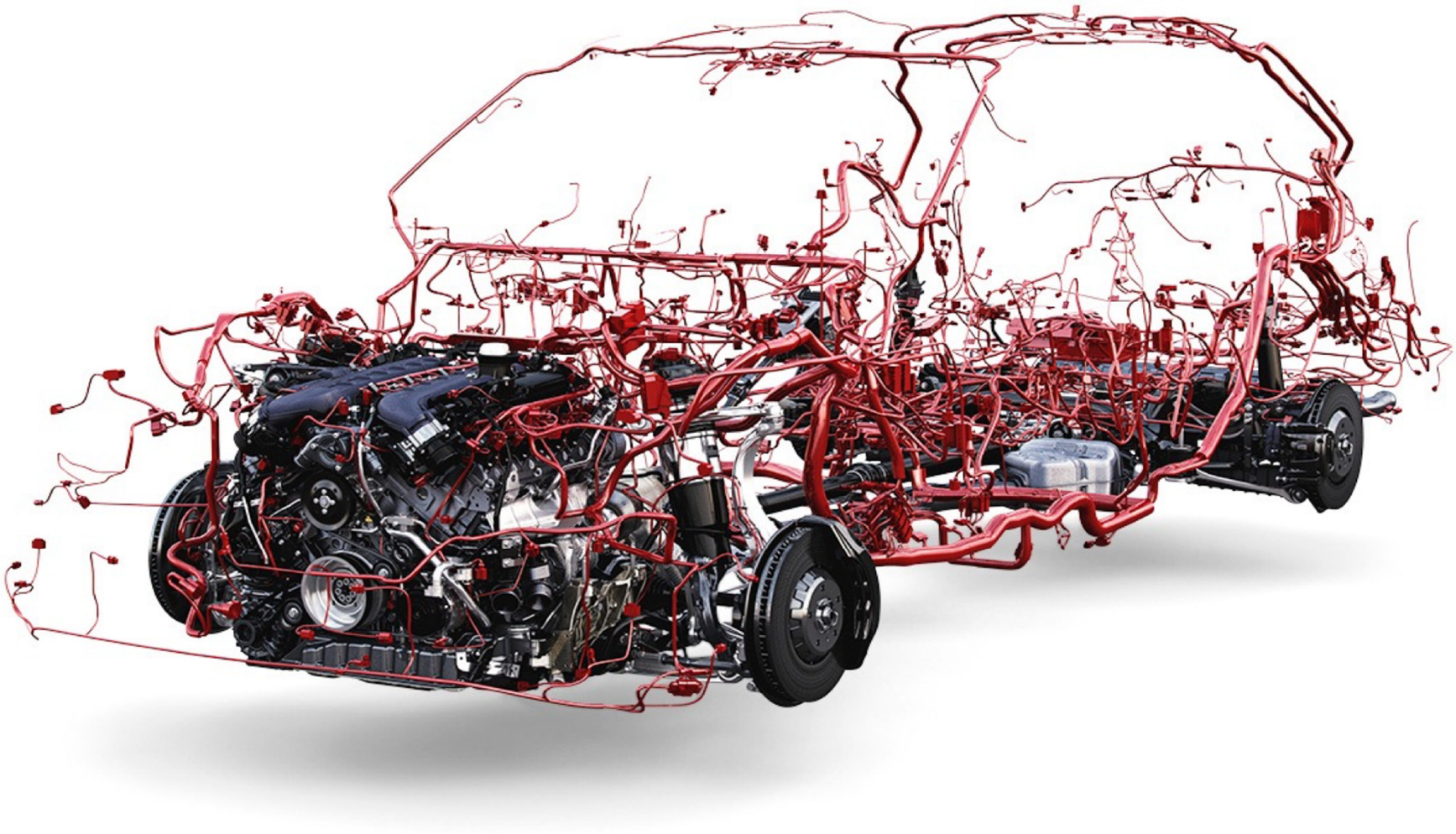
Objectifs

(Clause de non-responsabilité : exagéré pour l'effet dramatique)

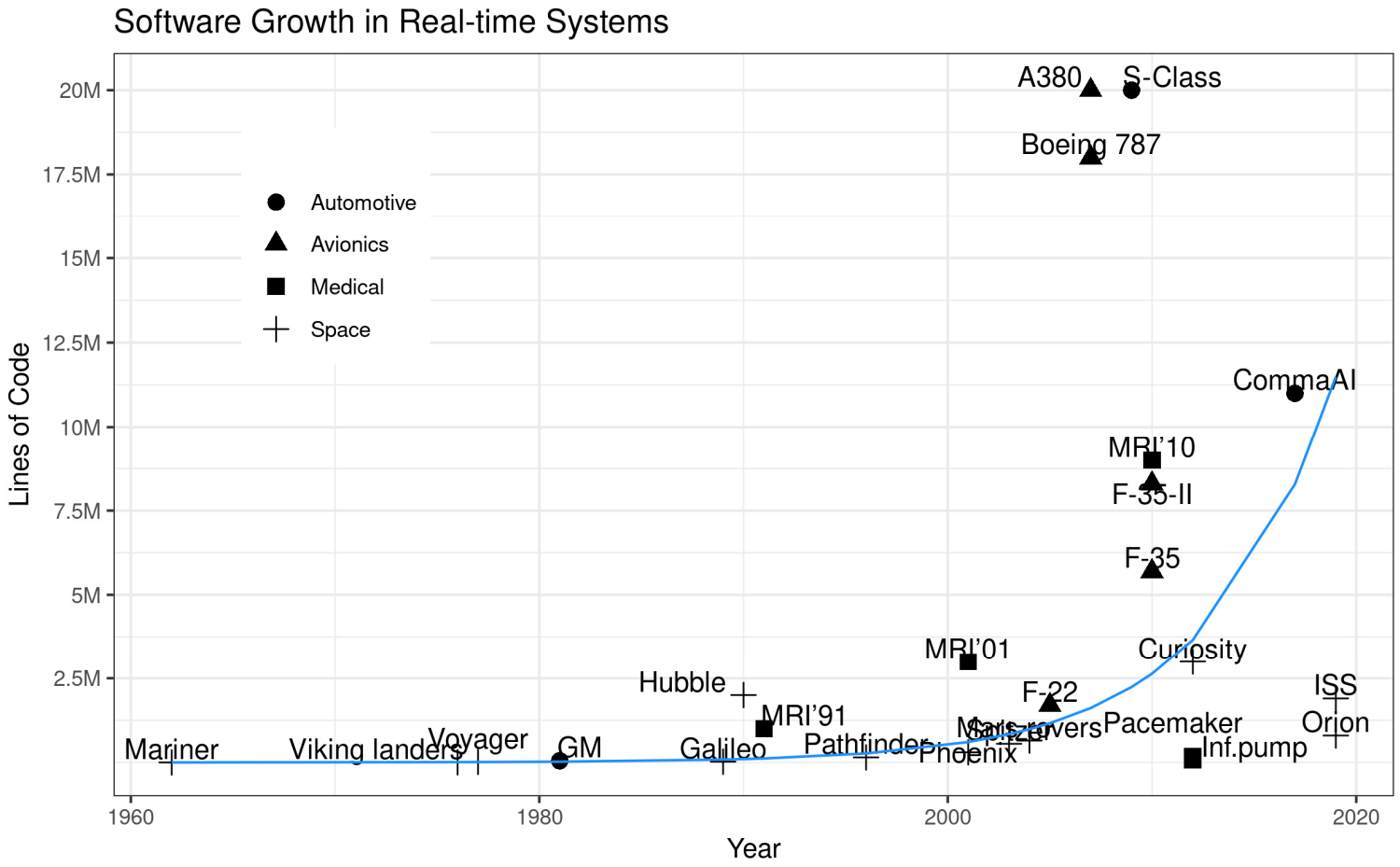
- Montrer que nous n'avons aucune idée de ce qui se passe dans les systèmes modernes.
- Montrer que les attaquants (=les hommes d'affaires) exploitent cette situation aujourd'hui.
- Montrer que les Canadiens sont en danger, à cause de cela.
- Montrer un côté positif et appeler à l'action.

Les véhicules modernes sont au-delà de la compréhension profonde de l’esprit humain

Les voitures sont compliquées



La complexité du code est croissante

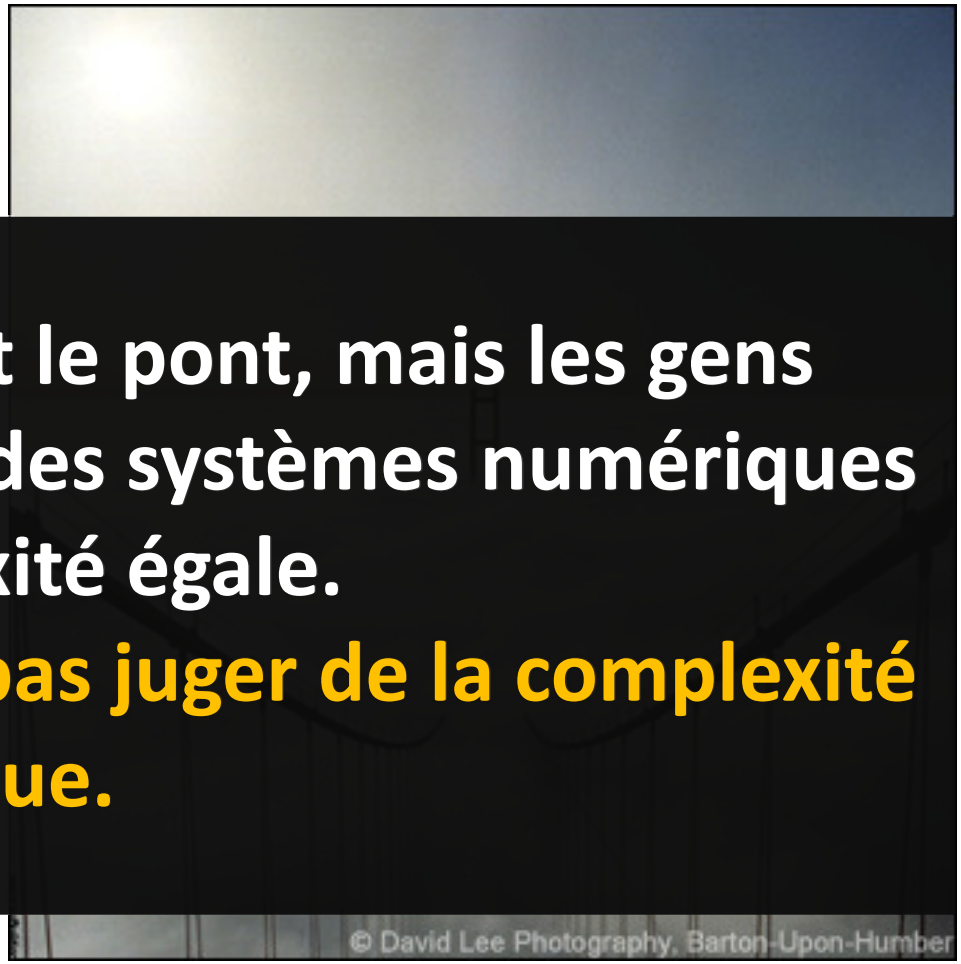


– Ford F150 : **150 M**

– Entre 30 et 100 ECU dans les voitures

(à travers 6 sources citables)

Nous ne pouvons pas comprendre les systèmes numériques



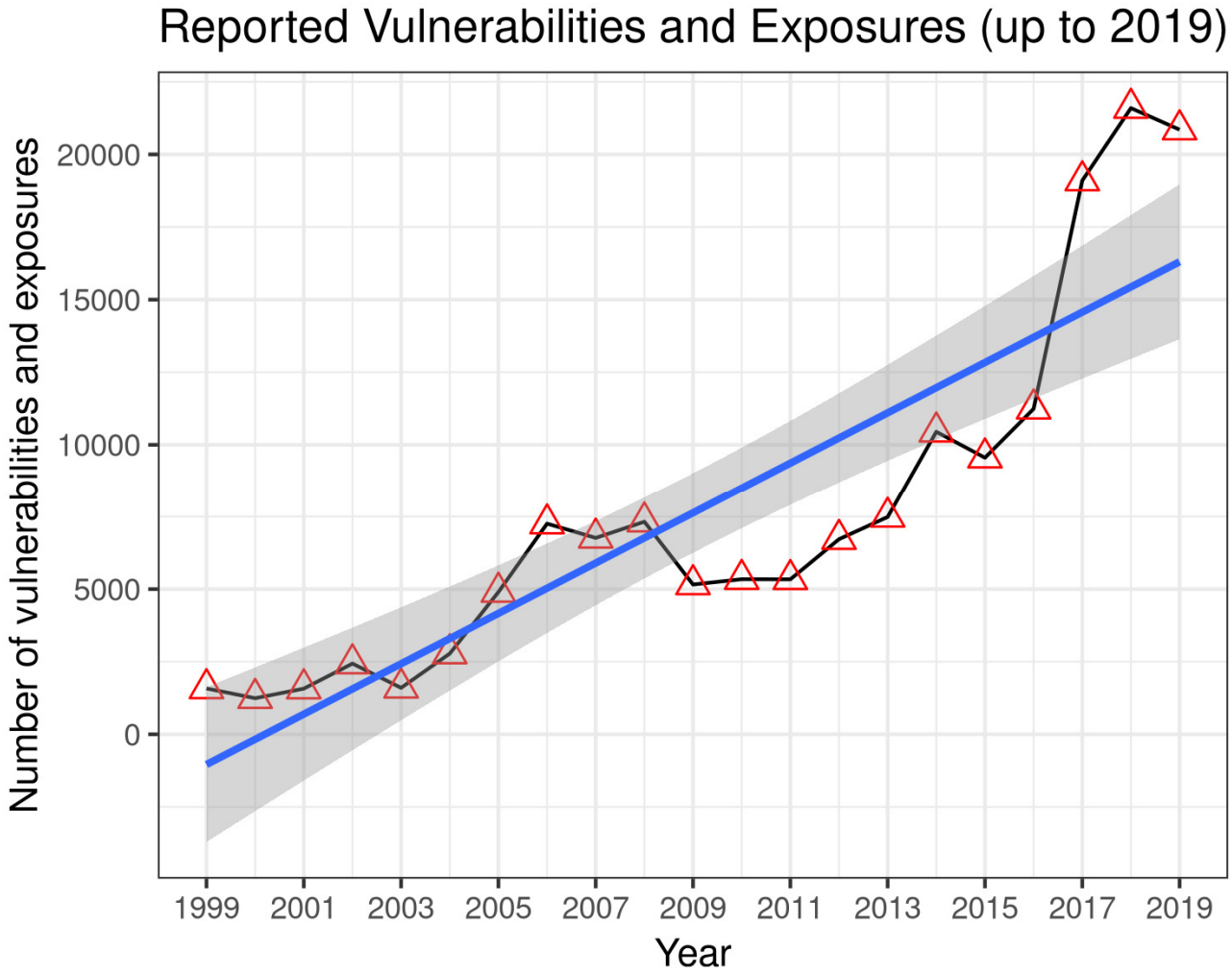
Personne ne construirait le pont, mais les gens essaieraient de construire des systèmes numériques de complexité égale.

=> Les humains ne savent pas juger de la complexité logique.

Les systèmes sont les éléments de sécurité les plus importants et sont reliés

Problème : Il rend les attaques évolutives!

Plus de vulnérabilités chaque année



160 274 (Déc. 19)

Au cours des 10 dernières années :

- **236 par semaine**
- **1,4 par heure (!)**

La durabilité des véhicules remet en question les hypothèses commerciales en compromettant la sûreté et la sécurité

Démodé dans 1 an

En activité depuis les années 1950

Votre nouvelle voiture deviendra une vieille voiture hautement automatisée

MITRE enregistre 236 nouvelles vulnérabilités par semaine.

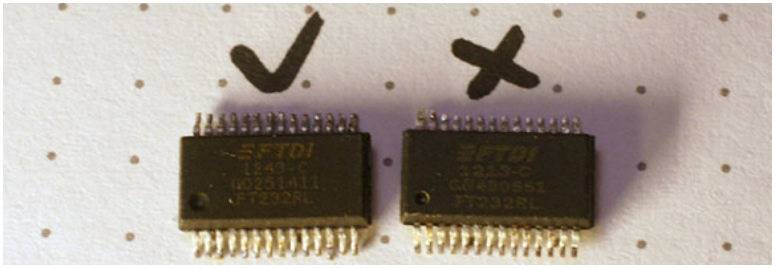
+ Services en nuage
+ Contact sans fil
+ Android/Apple dans la voiture
+ Ancienne V2V

Une frontière supplémentaire

CYBERSÉCURITÉ DE LA CHAÎNE D’APPROVISIONNEMENT

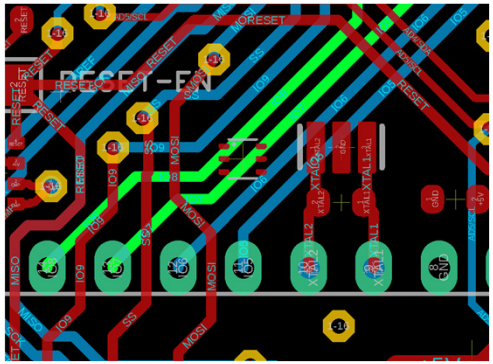
Problème : Faire confiance au matériel

- Intégrité du matériel sous-jacent?
- La livraison correspond-elle à ma commande?



Problème 2 : Puces de contrefaçon

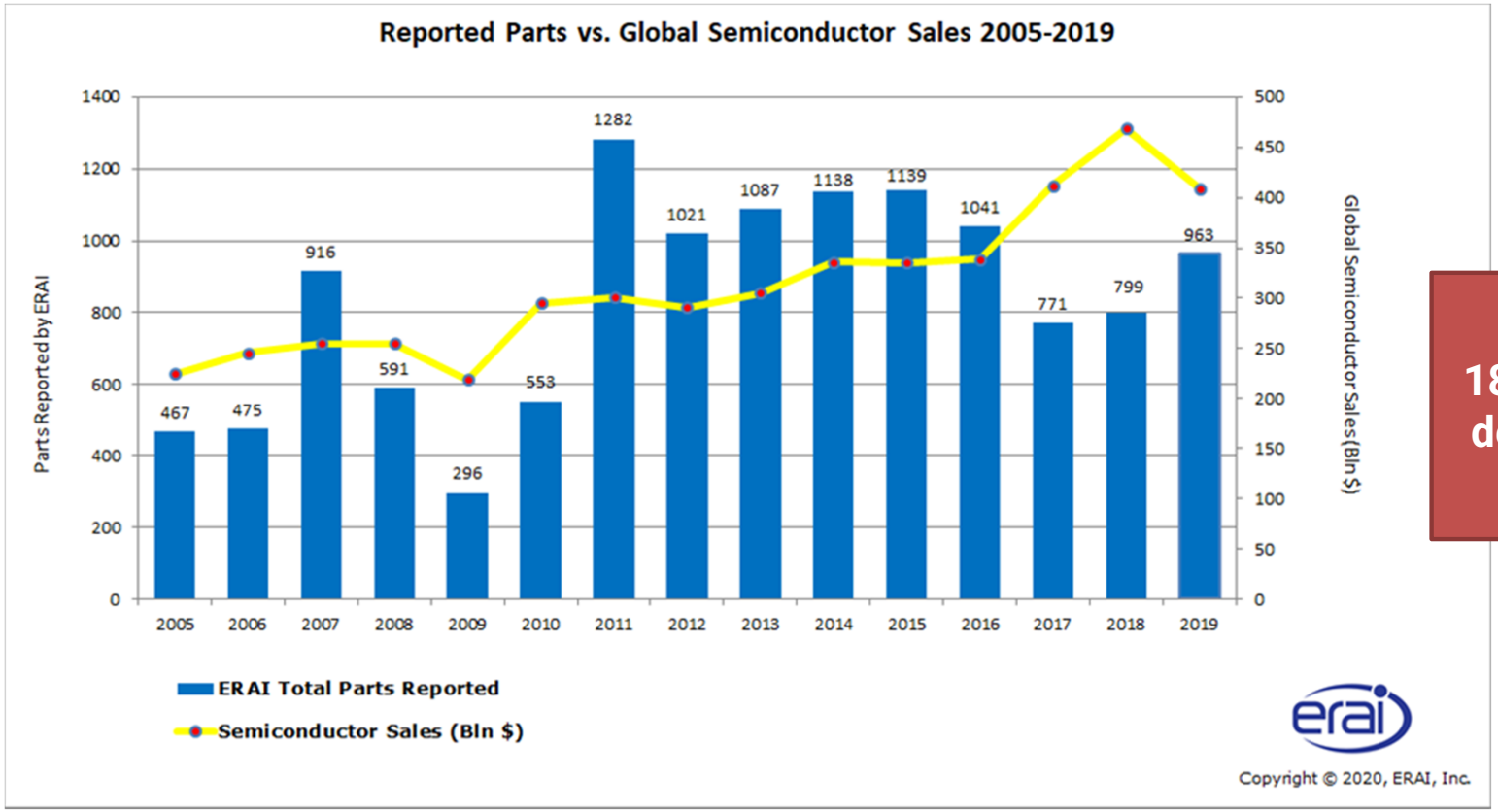
Problème 1 : Déchets électroniques recyclés vendus comme des pièces neuves



Problème 3 : Implants matériels

Cette décennie sera celle des attaques à travers la chaîne d'approvisionnement.

À quel point le problème est-il sérieux?

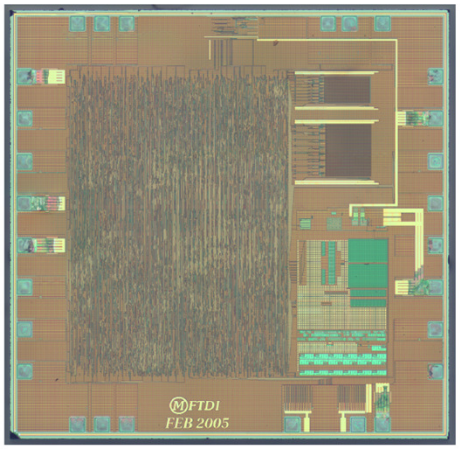


L'ERAI enregistre 18 nouvelles entrées de contrefaçons par semaine.

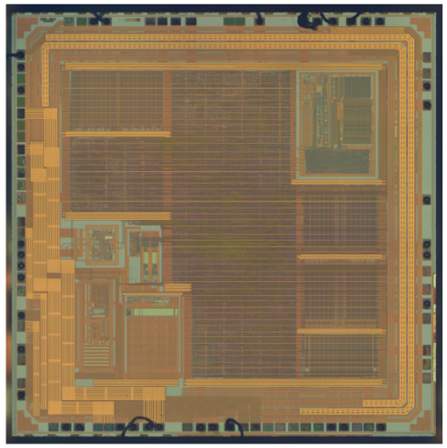
Tiré de : https://www.erai.com/erai_blog/3167/_2019_erai_reported_parts_statistics

Détection de chevaux de Troie matériels, d'implants et de contrefaçons

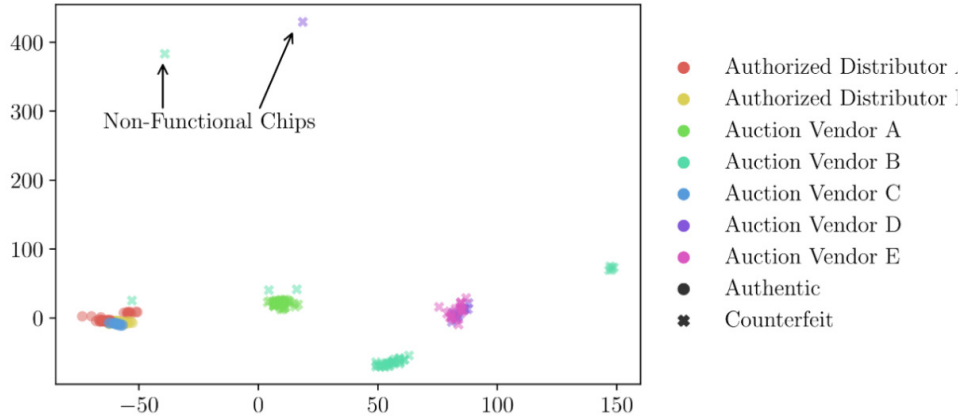
Nous avons acheté 220 puces à microcontrôleur FTDI sur le marché libre auprès de 7 différents vendeurs
= 120 (54 %) puces contrefaites trouvées au total



(a) Authentic Die [5]



(b) Counterfeit Die [5]



Bruce Power

Natural Resources Canada

National Defence

University of Waterloo | WatCAR driving innovation

Une lueur d’espoir : Évaluation de l’intégrité matérielle

- ✓ Non destructif
- ✓ Boîte noire
- ✓ Agnostique des fournisseurs
- ✓ In situ

Conçu à UWaterloo, commercialisé par : Palitronica

DÉTECTE LES ATTAQUES SUR LA CHAÎNE D’APPROVISIONNEMENT
Détecte les implants, les altérations et les faiblesses malicieusement insérés dans le microprogramme.

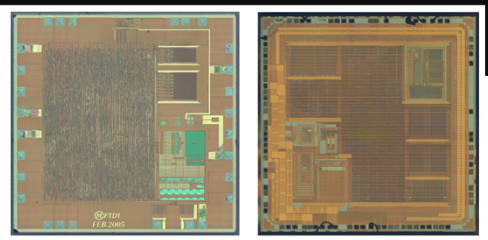
RÉVÈLE LES PIÈCES CONTREFAITES
Détermine l’intégrité du système et détecte les pièces de contrefaçon sans exiger d’inspection interne.

PROTÈGE CONTRE LES PORTES DÉROBÉES
Identifie les fonctionnalités non divulguées par un micrologiciel malveillant et une altération du matériel.

Veuillez à ce que vous recevez soit bien ce que vous avez commandé!

UNIVERSITY OF WATERLOO | WatCAR driving innovation

Conclusion



(a) Authentic Die [5] (b) Counterfeit Die [5]

54 % de contrefaçon!

- Les véhicules sont au-delà de la compréhension profonde d'un individu.
- La cybersécurité de la chaîne d'approvisionnement est importante de nos jours.
- Presque toutes les entreprises ont une confiance aveugle en leurs fournisseurs.
- Les Canadiens acceptent un risque de sécurité inconnu tout au long de la chaîne d'approvisionnement.
- Il existe de nos jours une technologie permettant d'assurer la cybersécurité globale de la chaîne d'approvisionnement.

Appel à l'action

- Il est urgent et important d'encourager l'investissement dans la cybersécurité de la chaîne d'approvisionnement.
- Aidez les CEP à comprendre vos besoins.

Contact :
Sebastian Fischmeister
sfischme@uwaterloo.ca

Département de génie électrique et informatique
Université de Waterloo
200, University Eve West
Waterloo, ON N2L 3G1

La réalisation de ce travail a été soutenue en partie par des partenaires industriels et le contribuable canadien, donc merci beaucoup à tous ceux qui paient des impôts.