Media advisory / Information Presse
28 janvier 2025

Embargo jusqu'au 28/01/2025

La cybersécurité embarquée française se structure.

Executive summary

Le GT Cybersécurité de Embedded France rassemble des **acteurs de haut niveau spécialisés dans les thématiques cyber des systèmes embarqués**. Notre action coordonnée vise à aider tous les acteurs de la chaîne de création de systèmes embarqués complexes à réduire significativement les impacts des cyberattaques. Nous nous appuierons sur notre écosystème, ainsi que sur les initiatives, normes et réglementations en place pour faire **progresser les compétences nationales et internationales en matière de protection cyber des systèmes embarqués**.
Les éléments constitutifs de notre feuille de route incluent, d'une part, la création d'un **parcours pédagogique**, et d'autre part, un **référentiel appelé "cyber scoring together"**. Ce référentiel permettra à chacun de mesurer de manière neutre le niveau réel de protection atteint et, collectivement, il aidera les différentes filières de l'industrie de l'embarqué à améliorer leur propre résilience.

Face à la multiplication des cyberattaques, le constat est alarmant, mais de réelles opportunités existent pour surmonter les risques

Les cyberattaques qui frappent les dispositifs embarqués prennent une ampleur inédite, à la fois par leur nombre et par l'extension de leurs domaines d'application.

- Nombre : Les statistiques de l'ANSSI/CERT (CVE de MITRE) montrent un accroissement permanent des menaces. Ces attaques entraînent pour les entreprises et collectivités touchées des pertes financières considérables.
- Domaines d'application : tous les secteurs peuvent être touchés. Ainsi une cyberattaque russe sur les liaisons satellites a-t-elle mis à l'arrêt 30 000 éoliennes ! On peut aussi citer les attaques ransomware Android, Jailbreaking Tesla, etc.

Aujourd'hui, il est crucial de se poser les questions clés :

- Quel est le point commun à toutes ces attaques ?
- Comment expliquer leur déploiement sur les *systèmes embarqués* qui s'accompagne d'impacts majeurs ?
- Qui s'attache à combattre véritablement ce fléau et comment ?

L'écosystème de l'embarqué – Embedded France

Les systèmes embarqués inclus dans tout type d'équipement ou de véhicule —quel que soit sa destination (terrestre, marin, aérien ou spatial)— englobent tous les dispositifs combinant électronique, logiciels de contrôle/commande et communications, opérant sous des contraintes strictes telles que le temps réel, la rapidité et la fiabilité. C'est un ***domaine d'excellence française****. Créée en 2013, Embedded France a réalisé en 10 ans un travail de fond pour structurer et dynamiser l'écosystème de l'Embarqué s'appuyant notamment sur des groupes de travail (GT) indépendants et volontaires pour accomplir sa mission*.

Du défi de la sureté de fonctionnement à celui de la cybersécurité…

Une des grandes réussites de l'embarqué français réside dans la maîtrise de la **sûreté de fonctionnement (safety)** : nos trains roulent, nos avions volent, nos centrales nucléaires produisent de l'électricité, et ce, sans incident. Quelles sont les raisons de ce succès ?

1. Une approche rigoureuse, logique et mathématique de la conceptualisation (analyse, interférence, probabilités, preuve formelle, etc.).
2. La mise en place de normes et certifications via des standards (IEC 61508, ISO 26262), permettant la composition (SEooC = Safety Element out of Context), avec des leviers au niveau des interfaces, comme le reporting vers l'hôte et les hypothèses sur l'environnement.
3. La structuration d'un écosystème et de ses acteurs dans une chaîne de confiance (spécifications, implémentation, vérification, certification).
4. Des échanges pertinents entre filières et acteurs de la chaîne de confiance.

Ainsi, de nombreux systèmes et systèmes de systèmes industriels (dont des opérateurs d'importance vitale et des infrastructures critiques opérant 24/7) fonctionnent de manière nominale et sans perturbation. **La sûreté de fonctionnement s'est révélée être une source de valeur durable, maintenue au plus haut niveau d'exigence pour les systèmes critiques d'aujourd'hui**.
C'est pourquoi, la thématique de la sûreté de fonctionnement est portée par plusieurs groupes de travail de l'association Embedded France.

Les systèmes sûrs partagent néanmoins la caractéristique d'être particulièrement stables quant à leurs fonctionnalités et isolés des interférences des autres sous-systèmes. Ils sont donc moins vulnérables et moins atteignables par des cyberattaques. En revanche, **la cybersécurité est plus problématique sur des systèmes numériques dynamiques interconnectés.** Dans ce contexte, la cybersécurité doit aussi opérer au niveau des systèmes de systèmes : on parle de mettre en œuvre la **cybersécurité en environnement « confiance zéro » ou en anglais « zéro trust »** c'est-à-dire dans des environnements où il n'est pas possible de faire confiance aux utilisateurs ; dans ces environnements on est donc contraint de donner aux utlisateurs des accès très restreints à des

ressources très clairement établies et limitées. Etant donné que l'approche traditionnelle centralisée de type bastion ne suffit plus, il faut **envisager des contrôles de légitimité des flux à tous les niveaux et de manière permanente**.

En parallèle, nous constatons que les systèmes deviennent bien plus complexes car ils sont intelligents même au niveau de l'Edge. Cela représente une avancée technologique majeure puisque ces systèmes sont **capables de traiter et d'analyser des données en temps réel, directement à la périphérie du réseau**, sans nécessiter de transfert vers un centre de données centralisé. Cette capacité permet des réponses plus rapides et une meilleure gestion des ressources, toutefois elle introduit également une complexité accrue. Les protéger est donc un enjeu crucial.

En 2024, Embedded France a décidé de prendre à bras le corps la question des cyberattaques visant des systèmes embarqués.

Les systèmes embarqués constituent les socles de systèmes et à ce titre, on ne peut pas envisager de sécurité des systèmes et des systèmes de systèmes si la sécurité de base n'est pas garantie. De plus, les cyberattaques qui atteignent les systèmes embarqués sont les plus dangereuses car dans certains cas, elles peuvent avoir des répercussions directes sur la vie réelle versus la vie digitale. En effet, un système embarqué compromis ne se comporte plus de manière sûre, ce qui pourrait mettre en péril la sécurité des utilisateurs (ex : le piratage d'un aiguillage peut entraîner le déraillement d'un train ou une attaque sur une tour de contrôle peut provoquer un accident aérien). Par ailleurs, les systèmes embarqués sont vulnérables vis-à-vis de menaces qui sont potentiellement implantées, dormantes, prêtes à s'activer au moment le plus favorable ; ces menaces dormantes sont les plus virulentes car elles sont difficiles à détecter et peuvent avoir un impact majeur.

Les pépites françaises de la cybersécurité embarquée regroupent leurs forces

A ce jour, le GT Cybersécurité embarquée rassemble 17 membres actifs : Ampere (Renault), Cap Gemini Engineering, CetraC.io, ESIEE, Grenoble INP-Esisar, Mathworks, MOABI, ProvenRun, Quantyss, Safran, Sciensys, Secure-IC, SYSGO, Thales, TrustInSoft, Viveris, et We Are Cyber. Ces membres se distinguent par leur excellence en cybersécurité, chacun dans leur domaine de spécialité deep-tech !
Le GT est coordonné par ***Sylvain Guilley (Secure-IC) et Gerulf Kinkelin (CetraC.io)*** *épaulés par les pilotes des Groupes de Travail de l'association, Éliane Fourgeau (Présidente de Quantyss) et Franck Serratrice (Expert en Assurance Qualité Logicielle Embarquée chez Renault/Ampere).*

Tout comme la sûreté de fonctionnement des systèmes embarqués critiques, la cybersécurité embarquée requiert des compétences extrêmement pointues. Les attaquants ne ciblent plus seulement les sous-systèmes ou leurs composants internes, mais aussi les interfaces entre sous-systèmes, voire entre systèmes et systèmes de systèmes lorsqu'ils communiquent. Il s'agit donc de **répondre à un problème systémique global complexe, nécessitant une coordination entre chaque niveau constitutif du système** et le partage d'expertise entre ces niveaux.

Notre solution : la coordination entre acteurs responsables

Nous pensons que pour résoudre le problème des cyberattaques, il faut tirer parti des savoir-faire des différents acteurs. Notre GT va favoriser la **mise en commun des compétences**.
En partageant leurs connaissances et leurs expériences, ces professionnels peuvent développer des solutions robustes et intégrées qui répondent aux défis uniques posés par ces systèmes avancés.

> *Les compétences, les métiers, et l'offre sont en place.*
> *Le groupe de travail cybersécurité d'Embedded France va orchestrer la coordination de tous les acteurs.*

Cette coordination est nécessaire car la menace est évolutive. En effet, l'ennemi est rusé : il exploite chaque faille pour atteindre ses objectifs. Il s'agit d'un combat asymétrique. Une bonne protection nécessite une connaissance approfondie des biens à protéger, une anticipation des attaques et une mise en œuvre sans faille, exigeant rigueur et précision.

Nous rappelons que la **différence entre sûreté et cybersécurité est qu'un système sûr l'est de manière permanente, tandis qu'un système n'est sécurisé qu'à un instant donné**. Le cyberattaquant sait composer des chemins d'attaque polymorphiques (ingénierie sociale, faiblesse contextuelle, exploitation de bugs, etc.). Il s'améliore, s'organise et s'adapte en permanence : de nombreuses attaques utilisent aujourd'hui l'intelligence artificielle pour identifier des failles et les exploiter !

Ces défis ont déjà été relevés par certaines industries, comme le secteur bancaire, la distribution de contenus multimédia et la défense. Cependant, ces systèmes sont souvent fermés, propriétaires et non-interopérables. Or, ces domaines se décloisonnent…
Pour ne rien arranger, le besoin de cybersécurité s'est étendu à de nombreux autres systèmes (institutions, véhicules, usines, industries de l'"utility", etc.). Tous ces systèmes sont complexes : rapides (temps réel), parallèles (mesures/actions dynamiques), ouverts (connectés à l'Edge) et adaptatifs (AIoT). D'où une deuxième différence avec les systèmes sûrs : la **cybersécurité doit s'intégrer dans la complexité du système sans entraver son bon fonctionnement**.

Ainsi le besoin de *coordination* entre les différents métiers, et les différentes solutions techniques est réel.

Le Groupe de Travail entretient une relation étroite avec le Pôle d'excellence cyber (PEC) dans le cadre d'une potentielle collaboration, avec la volonté affirmée de s'insérer parmi les acteurs clés de la cybersécurité embarquée. Cela confirme sa volonté de travailler dans un esprit fédérateur.

Créé en 2014 sous l'égide du ministère des Armées et de la Région Bretagne, **le Pôle d'excellence cyber regroupe aujourd'hui 132 membres et 15 partenaire**s. Son objectif est de contribuer au développement de la cyberdéfense régalienne à dimension Européenne en s'appuyant sur à la fois sur les forces de la région, notamment en matière de formation et de recherche et celles du ministère des Armées. Il bénéficie en particulier de la concentration, en Bretagne, d'une part significative des ressources Cyber du ministère des Armées, renforcées par l'implication de l'ANSSI et de certains services de l'Etat.

Nous allons relever le défi !

> Le Groupe de Travail (GT) Cybersécurité Embarquée d'Embedded France est solidement uni autour de sa mission : aider les entreprises de l'embarqué à développer des systèmes plus sécurisés et **moins vulnérables aux attaques, soit proactivement par une bonne conception, soit en réagissant efficacement lors de leur déploiement**.

Nous sommes fiers de nos trois principaux atouts :

1. **Notre expertise** : En tant que forces vives de la cybersécurité embarquée et de la cyber résilience, nous avons la volonté de réussir notre mission ! Nous sommes parmi les meilleurs au niveau international, grâce à plusieurs années de R&D et aux défis posés par les autorités françaises. Nos solutions sont technologiquement abouties et ont obtenu des certifications de sécurité de niveau supérieur. Par ailleurs, elles jouissent d'une reconnaissance en France et à l'étranger, comme le démontre l'adoption mondiale de nos technologies et produits. De plus, nous couvrons tous les aspects nécessaires :

    1. Education et sensibilisation (ESIEE, Grenoble INP-Esisar), consulting (Quantyss)
    2. Briques technologiques de base – racines de confiance (CetraC.io, Secure-IC)
    3. Technologies de protection en profondeur (ProvenRun, Safran, Secure-IC, SYSGO, TrustInSoft)
    4. Technologies de recherche de vulnérabilités via des outils réactifs et de pen-testing (Moabi, We Are Cyber)
    5. Sécurité dans l'intégration : "secure by design" (Cap Gemini Engineering, Mathworks, Sciensys, Viveris)
    6. Sécurité des opérations sur un système final, avec supervision (Ampere, Thalès)

2. **Notre coordination** : Il est désormais essentiel d'aligner nos forces et nos expertises. Nous avons donc décidé de nous coordonner via le GT, où nous partageons nos retours d'expérience et nos bonnes pratiques. **À l'instar du groupe de travail sur la sûreté de fonctionnement au sein d'EF, notre connaissance des règlements et notre adoption des normes et des schémas de certification en vigueur sont des composantes structurantes**. Nous appliquons proactivement les régulations en matière de cybersécurité, notamment au niveau français (recommandations et procédures ANSSI, DGA) et européen (EU CRA, EUCC, EUCS, NIS2, RED).
   Nous nous appuyons sur des schémas de certification, comme des schémas horizontaux de type Critères Communs & ses dérivés (SESIP, EMVCo, etc.), ou des schémas sectoriels comme l'IEC 62443 pour l'industrie, l'ISO/SAE 21434 pour l'automobile, etc.

3. **Notre initiative** : Nous allons **donner les moyens aux entreprises / institutions de se protéger efficacement, en leur proposant un parcours cyber de référence adapté à leurs besoins.** Nous alignerons nos savoir-faire pour répondre à leurs enjeux. Nous développerons deux outils complémentaires :

    1. Un parcours cyber : Ce parcours, conçu dans un langage accessible aux entreprises souhaitant renforcer leurs compétences en cybersécurité, détaille les étapes clés pour mettre en place des processus de protection contre les cyberattaques. Il couvre la gouvernance, la formation et l'amélioration continue, les certifications, le déploiement des solutions technologiques adéquates (matériels et logiciels), ainsi que leur gestion efficace (configuration, supervision, analyse et réaction).

2. Une boussole sur le niveau de cyber-protection atteint :
Nous travaillons actuellement à la définition d'une métrique appelée **"cyber scoring together",** qui permettra d'évaluer le niveau de sécurité atteint en termes de KPI cyber. Ce référentiel sera bien entendu étalonné sur les normes transversales et sectorielles afin de fournir un niveau global quantitatif, permettant ainsi à tous de progresser. Cet outil de mesure de la maturité cyber a vocation à être utilisé au-delà de nos frontières et permettra à notre tissu économique de conserver **une souveraineté en cybersécurité embarquée**. En effet, la présence d'une métrique indépendante endiguera le risque de se voir imposer un référentiel privé (étranger) qui s'imposerait alors à nous.

Contact Groupe de Travail Cybersécurité

Sylvain Guilley : sylvain.guilley@secure-ic.com
Gerulf Kinkelin : gerulf@cetrac.io

Groupe de Travail Cybersécurité

Contact presse:

Cendrine Barruyer
DG d'Embedded France
06 61 84 53 70
cbarruyer@embedded-france.org

A propos

L'association Embedded France (EF) a été créée en 2013 suite à deux rapports commandés par deux ministres successifs de l'Économie pour dynamiser cette filière innovante et stratégique. Embedded France est l'association des représentants français des logiciels et systèmes embarqués. Association loi de 1901, ***Embedded France est ouverte à tous les acteurs industriels (grands groupes, PME, start-ups…), académiques (Universités, Instituts de recherche, Ecoles d'ingénieurs …) et aux associations professionnelles représentatives de domaines intégrant des systèmes embarqués.*** *Embedded France a pour objectif de développer l'emploi et les synergies dans le secteur de l'Embarqué.*
L'association est à l'initiative —aux côtés d'organisations professionnelles structurantes (FIEEC, ACSIEL, SNESE, SPDEI)— de la création du conseil stratégique de la filière électronique, une filière qui compte 1100 entreprises hautement spécialisées et qualifiées, et représente 200 000 emplois directs et 150 000 emplois indirects. Depuis sa création en 2013, Embedded France est reconnue par les pouvoirs publics comme un des acteurs qui contribuent à la compétitivité de l'Industrie du Futur.