



Autoliv



CODESonar
CODESECURE

Comment Autoliv a transformé la qualité de son code embarqué grâce à CodeSonar ?

Sécurité,
conformité et
productivité
améliorées

Mickael PASTOR

Software Quality and
Process Responsible

Autoliv, leader dans les systèmes de sécurité automobile, développe des applications critiques pour volants, ceintures et airbags, basées sur une architecture logicielle complexe.

Avant l'adoption de CodeSonar, les équipes utilisaient des outils d'analyse statique de code qui présentaient plusieurs limites : difficulté à centraliser les warnings et les justifications, problèmes de merge lors de la remontée des rapports, et suivi manuel fastidieux de la conformité aux standards de sécurité et aux règles MISRA.

L'intégration de CodeSonar a permis à Autoliv de centraliser les résultats d'analyse, de gérer les priorités et justifications directement dans l'IDE Eclipse, et de détecter des vulnérabilités critiques, notamment liées à la mémoire et aux buffers. L'adoption de l'outil a été rapide et intuitive pour les 60 développeurs impliqués, avec plus de 12 000 analyses réalisées sur une vingtaine de projets, représentant environ 150 000 lignes de code par projet.

Grâce à CodeSonar, Autoliv a amélioré la qualité de son code, renforcé la sécurité de ses produits et simplifié le reporting, tout en ouvrant la voie à l'extension de l'outil à d'autres entités et types de projets.

*CodeSonar correspond parfaitement à nos besoins et s'intègre de manière transparente à notre environnement de développement, ce qui nous a permis de réaliser un **gain de temps** considérable. Plus encore, CodeSonar **détecte un nombre de warnings bien supérieur à ce que peuvent offrir les outils d'analyse statique classiques**. C'est un atout précieux pour garantir la qualité et la sécurité de nos logiciels critiques.*

Contexte et Challenge

Autoliv développe des systèmes embarqués critiques pour le secteur automobile, où la sécurité est une priorité absolue. La division électronique conçoit des applications logicielles pour des produits tels que les volants, ceintures et airbags. Ces applications reposent sur une architecture logicielle commune. Ce modèle génère une forte réutilisation du code, mais nécessite également une gestion rigoureuse des justifications et des warnings à travers tous les niveaux.

Avant l'adoption de CodeSonar, les équipes faisaient face à plusieurs défis :

- Difficulté à centraliser warnings et justifications entre projets et plateformes.
- Problèmes d'accès concurrent et de merge compliquant la remontée des rapports.
- Suivi manuel des règles MISRA et cybersécurité long, sujet à erreurs et coûteux.
- Réutilisation du code entre plateformes rendant difficile l'homogénéisation des justifications et analyses.

Ces challenges ont conduit Autoliv à rechercher une solution d'analyse statique plus moderne et performante, capable de détecter des vulnérabilités complexes tout en facilitant le workflow des équipes de développement.

Mise en œuvre

Autoliv

Pour répondre aux défis rencontrés par les équipes Autoliv, le choix s'est porté sur **CodeSonar**, après un benchmark détaillé comparant plusieurs outils. CodeSonar a été retenu pour sa capacité à détecter des vulnérabilités complexes, notamment celles liées à la mémoire et aux buffers overrun.

Intégration technique et adoption :

- Les analyses sont lancées en ligne de commande et les résultats sont importés directement dans l'IDE Eclipse.
- Les développeurs peuvent gérer les justifications et prioriser les corrections directement depuis l'IDE, simplifiant le workflow quotidien.
- L'automatisation des analyses a été mise en place facilement via des scripts intégrés dans l'environnement de compilation (tableaux de bord).
- L'outil est intuitif, nécessitant un support minimal pour son adoption, et a été rapidement intégré par **60 développeurs** actifs.

Bénéfices

CODESonar[®] CODESECURE

- **Centralisation et partage des warnings et annotations**, avec suivi uniforme à travers les projets.
- **Gain de temps pour le reporting**, grâce à l'export vers Power BI et aux scripts Python personnalisés.
- **Détection de vulnérabilités critiques**, notamment buffer overrun et mauvaise gestion mémoire, difficiles à identifier avec les outils précédents.
- **Adoption rapide et intégration naturelle** dans le workflow des équipes.
- **Couverture complète des standards MISRA et cybersécurité**, assurant la conformité sur les projets critiques.
- **Extensibilité** : possibilité d'étendre l'usage de CodeSonar à d'autres entités et types de projets, y compris des applications mobiles Java pour différents sites internationaux.

*En deux ans, les équipes ont réalisé plus de **12 000 analyses** sur une vingtaine de projets, représentant environ **150 000 lignes de code par projet**. Grâce à CodeSonar, Autoliv a ainsi amélioré la qualité du code, réduit les risques de vulnérabilités critiques, et optimisé la productivité des équipes, tout en simplifiant le processus de reporting et de justification.*