



CENTRE GOUVERNEMENTAL
DE CYBERDÉFENSE

SA-17(03)

Correspondance formelle

Juill. 2026



Acquisition sécurisée des systèmes/services

System and Services

SA-17(03) – Correspondance formelle (PcEE)

Énoncés :

Exiger que la développeuse ou le développeur du système, du composant du système ou du service qui s'y rapporte s'assure de :

- a. produire, en parfaite intégration avec le processus de développement, des spécifications formelles de haut niveau qui décrivent les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité sur le plan des exceptions, des messages d'erreur et des effets
- b. montrer – par des preuves accessibles et, s'il y a lieu, par des démonstrations informelles – que les spécifications de haut niveau sont conformes au modèle formel de stratégie
- c. montrer, par des démonstrations informelles, que les spécifications formelles de haut niveau prennent en compte toutes les interfaces du matériel, des logiciels et des micrologiciels servant à la sécurité
- d. montrer que les spécifications formelles de haut niveau décrivent précisément le matériel, les logiciels et les micrologiciels utilisés à des fins de sécurité
- e. décrire les mécanismes liés au matériel, aux logiciels et aux micrologiciels servant à la sécurité qui ne sont pas explicitement pris en compte dans les spécifications formelles de haut niveau, mais qui sont inhérents à ce matériel, à ces logiciels et à ces micrologiciels servant à la sécurité

Responsable : Aucun

Discussion :

La correspondance est un élément important de l'assurance gagnée en cours de modélisation. Elle démontre que la mise en œuvre constitue une transformation précise du modèle, et que tout code ou détail de mise en œuvre additionnel n'aura aucune incidence sur les comportements ou sur les stratégies en cours de modélisation. Les méthodes formelles peuvent être utilisées pour montrer que la description formelle d'un système est conforme aux propriétés de sécurité de haut niveau, et que la description formelle de système est adéquatement mise en œuvre, et ce, par la description d'un niveau inférieur, notamment la description des composants matériels. La cohérence entre les spécifications formelles de haut niveau et les modèles formels de stratégies est généralement impossible à prouver hors de tout doute. Par conséquent, une combinaison de méthodes formelles et informelles pourrait être requise pour démontrer la cohérence. La cohérence entre les spécifications de haut niveau et la mise en œuvre pourraient nécessiter l'utilisation de démonstrations informelles en raison des contraintes liées à l'applicabilité des méthodes formelles dans le but de prouver que les spécifications sont intégralement conformes à la mise en œuvre. Les mécanismes liés au matériel, aux logiciels et aux micrologiciels, qui sont strictement inhérents aux composants servant à la sécurité, comprennent les registres de mappage, ainsi que les entrées et sorties directes liées à la mémoire.