

Au-delà de la clé USB

Un contrôleur intelligent peut libérer le potentiel de la norme de stockage amovible leader du marché dans les applications embarquées

Damien Col, Technical Marketing Manager Hyperstone

Vu de l'extérieur, peu de choses paraissent plus simples qu'une clé USB, ou une carte mémoire au format SD. Tous deux contiennent de la mémoire Flash, une interface USB et un contrôleur de stockage, qui fournit un support générique pour le stockage non-volatile organisé en fichiers. Mais la plupart des dispositifs génériques n'offrent pas de fonctions permettant de gérer facilement les nombreuses utilisations que permet ce format type très compact aussi répandu : de très nombreux systèmes sont désormais capables de gérer des supports USB ou SD en standard, qui peuvent servir à bien plus qu'au simple stockage de données.

Ces facteurs font des périphériques de stockage au format USB ou SD d'excellentes plateformes sur lesquelles construire des applications à valeur ajoutée, avec des fonctionnalités, une fiabilité et une sécurité améliorées. Pour garantir une disponibilité élevée et un fonctionnement sûr, la fiabilité du stockage est vitale. Les contrôleurs USB et SD conventionnels assurent certaines opérations, comme le nivellement d'usure pour préserver la durée de vie et l'endurance d'écriture limitée de la mémoire Flash. Cependant, ces dispositifs sont conçus pour les applications grand-public dont les exigences sont différentes de celles des applications embarquées. Ils sont généralement optimisés pour le stockage de données en vrac, comme des fichiers multimédia ou des documents, alors que les systèmes embarqués ont des fonctionnalités très diverses avec des contraintes différentes de celles du stockage permanent.

Les systèmes embarqués ont besoin de solutions de stockage non-volatile fiables et optimisées pour des transactions beaucoup plus modestes, comme des mises à jour de capteurs ou d'autres données temps-réel. Le profil type des écritures sur le système de fichiers peut être très différent de celui correspondant à la mise à jour de gros fichiers. Une même variable représentant l'état du capteur peut être réécrite des millions de fois en

fonctionnement normal. Souvent, les emplacements de stockage sont extrêmement fragmentés, ce qui se traduit par des accès très déséquilibrés. Cela remet en question la fiabilité de n'importe quelle mémoire Flash et entraîne des défaillances si ce n'est pas géré correctement, même si le reste de l'espace de stockage est relativement peu utilisé.

Les concepteurs de systèmes embarqués doivent également s'assurer que les mises à jour s'effectuent correctement, et que le contenu de la mémoire non-volatile ne se trouve pas inutilisable suite à une erreur d'écriture, à une panne de courant ou à un plantage en cours d'utilisation. C'est là qu'un contrôleur de stockage optimisé pour environnements embarqués a un rôle à jouer ! Ce contrôleur doit disposer des fonctions nécessaires pour assurer un stockage non-volatile fiable à un certain nombre d'applications embarquées.

En outre, grâce au support d'algorithmes personnalisés, il est possible d'optimiser l'utilité du périphérique de stockage. Un contrôleur intelligent associé à un jeu complet de fonctions accessibles via une API (Application Programming Interface, ou interface de programmation d'application), peut devenir un composant clé du système embarqué, ou se comporter comme un coprocesseur intelligent capable de tirer pleinement parti de la mémoire Flash amovible.

La capacité d'embarquer des fonctions de chiffrement et d'autres technologies sécurisées dans un dispositif mémoire indépendant de la CPU hôte permet d'améliorer considérablement la résistance d'un système aux effractions et ouvre de nouveaux marchés au stockage amovible intelligent. Grâce aux fonctions de sécurité intégrées dans une clé USB ou une carte SD approuvée, le responsable système peut assurer le rejet des périphériques non-protégés. Une solution standard basée sur des contrôleurs de stockage USB grand-public ne peut pas fournir de tels niveaux de fonctionnalité, de fiabilité et de sécurité. Un contrôleur de stockage USB programmable intégrant les fonctions de base nécessaires à gérer un stockage Flash fiable peut offrir tellement plus.

En utilisant des fonctions personnalisées, le développeur système peut mettre en œuvre un large éventail de fonctions à valeur ajoutée. Par exemple, il peut s'assurer que le système ne puisse lire ou écrire des données sur un appareil sans fournir un certificat de sécurité valide. Cela peut servir à empêcher le vol d'IP (Intellectual Property, ou propriété intellectuelle) ou à éviter l'introduction de logiciels malveillants par le biais d'interfaces qui sont

extrêmement difficiles à sécuriser, mais qui autorisent néanmoins l'utilisation de stockage amovible dans l'équipement final. De cette façon, par exemple, un fabricant peut préserver la possibilité pour les techniciens de maintenance d'installer des mises à jour logicielles ou d'accéder aux données d'exécution, mais avec le bénéfice supplémentaire d'une authentification.

Pour assurer un accès sécurisé à la mémoire Flash, le contrôleur de stockage doit savoir gérer des primitives de chiffrement efficaces, qu'une application utilisateur pourra assembler au sein d'une solution. Pouvoir accéder à du matériel spécifique est une autre exigence.

Pour plus de protection, le dispositif peut lui-même inclure des données biométriques ou des capteurs, pour s'assurer qu'il ne puisse être utilisé qu'à un endroit précis. Un capteur GPS intégré au dispositif USB ou à la carte SD elle-même, par exemple, permet de vérifier qu'il ou elle est utilisé dans un emplacement approuvé, et de déclencher une alerte en cas d'utilisation en dehors de la zone autorisée. Ces capteurs et ces fonctions supplémentaires permettent aux fabricants de fournir des clés à durée de vie limitée ou à localisation contrainte, qui ne fonctionnent que si le dispositif de stockage est présent. Un tel système permet d'envisager un large éventail de modèles économiques orientés services et ce type de fonctionnalité n'est pas disponible avec les contrôleurs de stockage Flash à vocation bureautique.

Pour la conception de ses contrôleurs intelligents de stockage Flash, Hyperstone a pris en compte ces exigences et bien d'autres. Le contrôleur exécute lui-même en standard un certain nombre de fonctions importantes pour les systèmes embarqués. Par exemple, les algorithmes de nivellement d'usure tiennent compte des petites écritures et des données fragmentées, en consolidant automatiquement ces éléments pour assurer un fonctionnement plus efficace et plus fiable. Grâce à l'intégration d'une API (Application Programming Interface, ou interface de programmation d'application), on peut aussi étendre les capacités du contrôleur de stockage intelligent, grâce à des fonctions définies par l'utilisateur.

L'API fournit les nombreux services nécessaires pour gérer des applications de stockage USB ou SD à valeur ajoutée. Les développeurs peuvent construire des applications à valeur ajoutée plus complexes en s'appuyant sur les services de base qui permettent d'accéder à du matériel spécifique sur la clé USB ou la carte SD. Pour ce faire, le contrôleur dispose de 16 lignes E/S polyvalentes qui peuvent être configurées en interfaces SDIO, SPI ou I2C. Grâce à ces interfaces,

il est possible de connecter un capteur numérique, des émetteurs-récepteurs RF ou des éléments supplémentaires. Par exemple, l'utilisateur peut configurer les lignes E/S pour gérer le protocole ISO7816, ce qui permet l'intégration de périphériques spécialisés comme un module SIM (Subscriber Identification Module, ou module d'identification d'abonné) pour effectuer l'authentification au nom du contrôleur de stockage. Le statut de sécurité de chaque lecture ou écriture peut être vérifié, et les données peuvent être cryptées et décryptées au vol en entrée en en sortie de la mémoire Flash. Cela évite que les données ne soient en risque si le support de stockage amovible était perdu ou volé.

Le module USB peut servir de connecteur sécurisé pour permettre l'accès au système en mode mise au point ou en mode test, uniquement lorsqu'un module authentifié est présent dans le port d'entrée/sortie. Un connecteur externe accessible à l'extérieur du module fournit les ports nécessaires. Certaines applications, cependant, n'ont pas besoin d'un tel niveau de sécurité. Un fournisseur peut choisir d'utiliser le port USB pour fournir des mises à jour ou des améliorations à ses clients. Par exemple, un microphone MEMS intégré au module et géré directement par le contrôleur de stockage permet d'ajouter une capacité d'enregistrement audio.

Dans l'architecture Hyperstone, l'extension firmware (micrologiciel) du client ne dépend pas de la technologie Flash sous-jacente. Les différences entre les différentes formes de mémoire Flash sont gérées par des fonctions intégrées au contrôleur lui-même. Les données binaires utilisateur peuvent être modifiées à l'aide d'écritures conventionnelles, et des verrous peuvent être mis en place sur les plages d'adresses utilisées par le firmware du contrôleur de stockage pour empêcher les écritures accidentelles ou malveillantes. Une fois le firmware chargé dans le dispositif, la possibilité de mise à jour peut être révoquée. La prise en charge d'un firmware redondant ainsi que la détection et la correction d'erreurs évite qu'une corruption éventuelle ou l'échec d'une mise à jour de firmware ne compromette le bon fonctionnement du dispositif.

Le développement du contrôleur de stockage Hyperstone fait appel à des outils logiciels standard connus de nombreux ingénieurs. Le support comprend une chaîne d'outils de compilation GNU. Pour la mise au point, on utilise l'IDE Eclipse et le débogueur GNU (GDB).

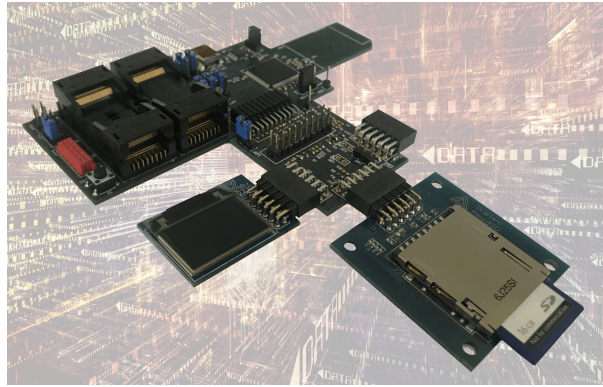


Figure 1. Hyperstone API extensions

Grâce à l'implémentation de "crochets" matériels et logiciels pour applications à valeur ajoutée, les contrôleurs de mémoire Flash Hyperstone permettent de créer de nouvelles classes de périphériques de stockage. Ces dispositifs non seulement améliorent la fiabilité et la sécurité des éléments de stockage eux-mêmes, mais ils servent d'épine dorsale résiliente vis-à-vis d'attaques contre les systèmes IoT (Internet of Things, ou internet des objets) et IIoT (Internet of Things, ou internet des objets industriel) Avec l'accès aux périphériques matériels via des E/S programmables, les modules de stockage eux-mêmes peuvent devenir des dispositifs intelligents, grâce à des récepteurs GPS, des encodeurs ou des capteurs MEMS, comme des accéléromètres, pour aller bien au-delà du simple rôle de dépôts de données. Le résultat est une technologie qui ouvre la porte à de toutes nouvelles classes de dispositifs de stockage amovible.

Biographical Statement Damien Col

Damien Col is responsible for technical papers, application notes and detailed technical information for customers and to support sales force (competitive analysis, performance benchmarking, communication of unique selling points and customer benefits). He also participates in new product specifications as well as defining and implementing Go-to-Market strategies, and representing Hyperstone in standardization committees. A seasoned professional with 20 year experience with technical positions across the globe (France, Germany, USA, UK, Israel), he previously held positions with various companies (ES2, Atmel, Synopsys, Sondrel). He holds a MScEE from ESIEE (Paris), and a MBA from EDHEC Business School (Nice, France).