

Requisiti del componente Smart Sensor in zona 1											
FR #	Requisito fondamentale (FR)	Descrizione FR	Requisito del componente (CR)	CR ID	Peso CR (1-3)	Requisito vincolante	Capacità non vincolante (nice to have)	Applicabile? (S/No)	Se non applicabile, si prega di spiegare perché	Requisito soddisfatto? (0%-100%)	Se il requisito non è completamente soddisfatto, cosa manca?
1	FR 1 - Controllo di identificazione e autenticazione	Identificare e autenticare tutti gli utenti (persone, processi software e dispositivi), prima di consentire loro l'accesso al sistema o alle risorse	CR 1.1 - Identificazione e autenticazione dell'utente umano	CR 1.1	2	I componenti devono fornire la capacità di identificare e autenticare tutti gli utenti umani su tutte le interfacce in grado di farlo secondo. Tali capacità devono applicare tale identificazione e autenticazione a tutte le interfacce che funzionano l'accesso di utenti umani al componente per supportare la separazione dei compiti e il privilegio minimo in conformità con la politica e le procedure di sicurezza applicabili. Questa funzionalità può essere fornita tramite il hardware del componente o mediante integrazione in un sistema di identificazione e autenticazione a livello di sistema. NOTA: Le politiche di sicurezza applicabili sono di competenza locale.  Identificazione e autenticazione uniche: - I componenti devono fornire la capacità di identificare e autenticare in modo univoco tutti gli utenti umani.  Autenticazione e i più fattori per tutte le interfacce - I componenti devono fornire la capacità di applicare l'autenticazione a tutti i fattori per l'accesso di tutti gli utenti umani al componente.  I componenti devono fornire la capacità di identificare e autenticare con qualsiasi altro componente (applicazione software, "virtualized device", dispositivi hardware e dispositivi di rete). Se il componente, come risultato di un'applicazione, è in esecuzione sul sistema di un utente umano, allora, l'identificazione e l'autenticazione dell'utente umano possono far parte del processo di identificazione e autenticazione del componente stesso e gli altri componenti.  Identificazione e autenticazione uniche: - I componenti devono fornire la capacità di identificare e autenticare in modo univoco su qualsiasi altro componente.					
1	FR 1 - Controllo di identificazione e autenticazione	Identificare e autenticare tutti gli utenti (persone, processi software e dispositivi), prima di consentire loro l'accesso al sistema o alle risorse	CR 1.2 - Identificazione a autenticazione del processo software	CR 1.2	1	Identificazione e autenticazione uniche: - I componenti devono fornire la capacità di identificare e autenticare in modo univoco su qualsiasi altro componente.					
1	FR 1 - Controllo di identificazione e autenticazione	Identificare e autenticare tutti gli utenti (persone, processi software e dispositivi), prima di consentire loro l'accesso al sistema o alle risorse	CR 1.3 - Gestione degli account	CR 1.3	1	I componenti devono fornire la capacità di supportare la gestione di tutti gli account direttamente o integrati in un sistema che gestisce gli account.					
1	FR 1 - Controllo di identificazione e autenticazione	Identificare e autenticare tutti gli utenti (persone, processi software e dispositivi), prima di consentire loro l'accesso al sistema o alle risorse	CR 1.4 - Gestione degli identificatori	CR 1.4	1	I componenti devono fornire la capacità di delegare in un sistema che supporta la gestione degli identificatori / o / o fornire la capacità di supportare direttamente la gestione degli identificatori. I componenti devono fornire la capacità di: a) supportare l'uso del contenuto locale di un'autenticazione; b) supportare l'importazione delle modifiche agli autenticatori (predicati) apportate al momento dell'installazione; c) l'esecuzione automatica per operazioni periodiche di modifica / aggiornamento dell'autenticazione; e d) integrare gli autenticatori da dispositivi e modifiche non autorizzate quando siano attivati, utilizzati o bruciati.					
1	FR 1 - Controllo di identificazione e autenticazione	Identificare e autenticare tutti gli utenti (persone, processi software e dispositivi), prima di consentire loro l'accesso al sistema o alle risorse	CR 1.5 - Gestione degli autenticatori	CR 1.5	1	Sicurezza hardware per autenticatori - Gli autenticatori su cui si basa il componente devono essere protetti contro i rischi di sicurezza: EDMRPC: memoria protetta da password, memoria OTP, controlli hardware di integrità dei dati e meccanismi di avvio sicuri dei dispositivi. I componenti che applicano l'autenticazione basata su password devono fornire o integrarsi in un sistema che fornisce la capacità di imporre una robustezza delle password configurabile secondo le linee guida riconosciute a livello internazionale.					
1	FR 1 - Controllo di identificazione e autenticazione	Identificare e autenticare tutti gli utenti (persone, processi software e dispositivi), prima di consentire loro l'accesso al sistema o alle risorse	CR 1.7 - Robustezza dell'autenticazione basata su password	CR 1.7	1	Gestione di password e limiti di durata per gli utenti umani: - I componenti devono fornire o integrarsi in un sistema che fornisce la capacità di proteggere diversi utenti umani dallo riutilizzo di una password per un numero configurabile di generazioni. Inoltre, il componente deve fornire la capacità di imporre restrizioni sulla durata minima e massima delle password per gli utenti umani. Tali capacità devono essere conformi alle pratiche comunemente accettate nel settore delle sicurezza. Il componente dovrebbe fornire la possibilità di ridimensionare il numero di modifiche le proprie password in un momento configurabile prima della scadenza.					
1	FR 1 - Controllo di identificazione e autenticazione	Identificare e autenticare tutti gli utenti (persone, processi software e dispositivi), prima di consentire loro l'accesso al sistema o alle risorse	CR 1.8 - Certificati di identificazione a chiave pubblica (PKI)	CR 1.8	1	Quando viene utilizzata l'infrastruttura a chiave pubblica (PKI), il componente deve fornire o integrarsi in un sistema che fornisce la capacità di gestire una PKI secondo le migliori pratiche comunemente accettate o standard definiti a chiave pubblica da una PKI esistente. Per i componenti che applicano l'autenticazione basata su chiave pubblica, tali componenti devono fornire direttamente o integrarsi in un sistema che fornisce la capacità, all'interno dello stesso sistema (NIST, 8): a) convertire i certificati verificando la validità della firma di un determinato certificato; b) controllare la catena di certificati e verificare se i certificati sono firmati (self-signed); c) distribuire i certificati firmati (burl certificati) a tutti gli host che comunicano con l'applicativo o un altro dispositivo certificato; d) controllare i certificati e controllare lo stato di revoca; e) stabilire il controllo di parte dell'utente (umano, processo software o dispositivo) della chiave privata corrispondente; f) eseguire l'autenticazione a un utente (umano, processo software o dispositivo); e g) assicurare che gli dispositivi e i host utilizzati per l'autenticazione con chiave pubblica siano conformi a CHA 3.					
1	FR 1 - Controllo di identificazione e autenticazione	Identificare e autenticare tutti gli utenti (persone, processi software e dispositivi), prima di consentire loro l'accesso al sistema o alle risorse	CR 1.9 - Robustezza dell'autenticazione basata su chiave pubblica	CR 1.9	1	Sicurezza hardware per l'autenticazione basata su chiave pubblica - I componenti devono fornire la capacità di proteggere chiavi private critiche e di lunga durata tramite meccanismi hardware. Quando il componente fornisce una capacità di autenticazione, il componente deve fornire la capacità di assicurare l'integrità delle informazioni dell'autenticazione durante il processo di autenticazione. Quando un componente fornisce una capacità di autenticazione, il componente deve fornire la possibilità di: a) imporre un limite di un numero configurabile di tentativi consecutivi di accesso non validato per di qualsiasi utente (umano, processo software o dispositivo) durante un periodo di tempo configurabile; e b) negare l'accesso per un determinato periodo di tempo (fino a quando non viene abilitato) per amministrare quando questo limite è stato raggiunto. Un amministratore può abilitare un account prima della scadenza del periodo di timeout.					
1	FR 1 - Controllo di identificazione e autenticazione	Identificare e autenticare tutti gli utenti (persone, processi software e dispositivi), prima di consentire loro l'accesso al sistema o alle risorse	CR 1.10 - Feedback dell'autenticazione	CR 1.10	1	Quando un componente fornisce un'interfaccia utente accessibile / Web, deve fornire la capacità di trasmettere un messaggio di controllo su un sistema prima dell'autenticazione. Il messaggio di controllo sull'uso del sistema deve essere configurabile da personale autorizzato. Per i componenti che utilizzano chiavi simmetriche, il componente deve consentire di: a) stabilire la chiave simmetrica mediante chiavi convenite; b) conservare in modo sicuro il segreto condiviso (l'autenticazione è valida finché che il segreto condiviso rimane segreto); c) tentare l'autenticazione in regime simmetrico; e d) assicurare che gli dispositivi e i host utilizzati per l'autenticazione con chiavi simmetriche siano conformi a CHA 3.					
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.1 - Applicazione dell'autorizzazione	CR 2.1	1	Assunzione di controllo del superutente - I componenti devono supportare una assunzione di controllo minimale da parte del superutente per un tempo e una sequenza di eventi configurabili. NOTA 2 Implementazione di una assunzione di controllo controllata, basata su manuale di meccanismi autorizzati in caso di emergenza e dell'eventuale permesso a un superutente di consentire a un operatore di debug rudimentale a condurre misure senza chiudere le sessioni corrente e ridare la risorse sessione come un utente umano con privilegi superuser.					
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.2 - Controllo dell'uso vincolante	CR 2.2	2	Se un componente fornisce un'interfaccia utente accessibile, deve fornire la capacità di integrarsi nel sistema che supporta l'autenticazione, il monitoraggio e la restrizione di utilizzo in base alle politiche di sicurezza comunemente accettate. Nel caso in cui un dispositivo host utilizzi tecnologie di codice mobile, tale dispositivo host deve consentire di applicare una politica di sicurezza sull'utilizzo delle tecnologie di codice mobile. La politica di sicurezza deve prevedere almeno le seguenti azioni per ciascuna tecnologia di codice mobile utilizzata sul dispositivo host: a) controllare l'installazione del codice mobile; b) controllare quali utenti (umani, processo software o dispositivi) sono autorizzati a cambiare il codice mobile sul dispositivo host; e c) controllare l'installazione del codice in base a verifiche di integrità sul codice mobile e prima dell'esecuzione del codice.					
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.3 - Blocco della sessione	CR 2.3	2	Controllo dell'autenticazione del codice mobile: il dispositivo host deve fornire la capacità di applicare una politica di sicurezza che consenta al dispositivo di controllare l'installazione del codice mobile sulla base dei risultati di una verifica di autenticazione prima dell'installazione del codice. Se un componente fornisce un'interfaccia utente accessibile, sia a livello locale che attraverso una rete, il componente deve fornire la capacità: a) per proteggere da ulteriori accessi avvenendo a blocco della sessione dopo un periodo di inattività configurabile e mediante un avviso manuale da parte dell'utente (umano, processo software o dispositivo); e b) che bloccare la sessione, venga in vigore fino a quando l'utente preme la procedura della sessione, o un altro utente autorizzato, rilibera l'accesso utilizzando le procedure di identificazione e autenticazione appropriate. Se un componente supporta sessioni remote, l'implementazione deve consentire di terminare una sessione remota automaticamente dopo un periodo di inattività configurabile, manualmente da un'entità locale o in modo remoto dall'utente (umano, processo software o dispositivo) che ha avviato la sessione.					
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.6 - Terminazione della sessione remota	CR 2.6	2	I componenti devono fornire la capacità di limitare il numero di sessioni simultanee per interfaccia per ciascun utente (umano, processo software o dispositivo).					
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.7 - Controllo delle sessioni concorrenti	CR 2.7	2	I componenti devono consentire di generare registri di audit pertinenti a tutti i dati della sicurezza per le seguenti categorie: a) controllo d'accesso; b) eventi di sicurezza; c) eventi del consumo di controllo; d) eventi di backup e ripristino; e) modifiche dei privilegi; f) eventi del registro di controllo (audit log); g) registrazione individuali dei controlli (compendio); h) dati e dati; i) tutti i dispositivi di origine, processo software o account utente umani; j) integrità; k) rete; l) ID evento; e m) risultati dell'evento. NOTA: Le categorie di eventi di sicurezza sono applicabili solo se la funzionalità stessa è fornita dal componente. I componenti devono: a) fornire la capacità di allineare la capacità di archiviazione dei log di audit secondo le raccomandazioni comunemente accettate per la gestione dei registri; e b) fornire meccanismi di protezione contro il furto del componente quando esso raggiunga la capacità di archiviazione di audit.					
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.8 - Eventi sottoposti a audit	CR 2.8	1	Avviso quando viene raggiunta la soglia della capacità di archiviazione dei record di audit - I componenti devono fornire la possibilità di mettere in avviso quando la quota di archiviazione dei record di audit superata raggiunga una soglia configurabile. I componenti devono: a) fornire la capacità di proteggere dalla perdita di servizio funzioni essenziali in caso di fallimento dell'archiviazione dei dati; b) fornire la capacità di ottenere le azioni appropriate in risposta a un fallimento dell'archiviazione dei dati secondo le pratiche e le raccomandazioni del settore comunemente accettate. I componenti devono fornire la capacità di creare timestamp (comprendenti dati e ora) per l'evento/registro di audit.					
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.9 - Capacità di archiviazione dei log di audit	CR 2.9	1	Strutturazione temporale - I componenti devono fornire la possibilità di creare timestamp associati con una sequenza temporale a livello di sistema. Se un componente fornisce un'interfaccia utente umana, il componente deve fornire la capacità di determinare se un certo evento avviene durante una determinata azione. Gli elementi di controllo che non sono in grado di supportare tale capacità devono essere elencati nelle dichiarazioni dei componenti. I dispositivi host devono proteggere dall'uso non autorizzato dell'interfaccia a interfaccia fisiche di dispositivi e a test di failure (ad es. debug JTAG).					
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.10 - Risposta a fallimento nell'elaborazione degli audit	CR 2.10	1	Monitoraggio attivo - I dispositivi host devono fornire un monitoraggio attivo della interfaccia di dispositivi e host dei dispositivi e generare una serie di log di audit quando vengono rilevati tentativi di accesso e tali risposte.					
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.11 - Marche temporali (timestamp)	CR 2.11	1						
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.12 - Non riconoscibilità (non repudiation)	CR 2.12	1						
2	FR 2 - Controllo d'uso	Applicare i privilegi assegnati a un utente autorizzato (umano, processo software o dispositivo) per eseguire l'azione richiesta sul componente e monitorare l'utilizzo di tali privilegi.	CR 2.13 - Uso di interfaccia frusche diagnostiche e di test	CR 2.13	2						

3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	CR 3.3 - Verifica delle funzioni di sicurezza	CR 3.3	1	<p>I componenti devono fornire la capacità di supportare la verifica del funzionamento previsto delle funzioni di sicurezza e offrire quando vengono disposte secondo durante l'AT, SAT e manutenzione programmata. Queste funzioni di sicurezza includono tutte quelle necessarie per supportare i requisiti di sicurezza specificati nella presente lista guide:</p> <p>FAT = Flight Acceptance Test SAT = System Acceptance Test</p> <p>I componenti devono consentire di eseguire o supportare controlli di integrità su software, configurazione e altre informazioni, nonché la registrazione e la consultazione dei risultati di tali controlli essere integrati in un sistema in grado di eseguire o supportare controlli di integrità.</p> <p>Autenticità del software e delle informazioni - I componenti devono consentire di eseguire o supportare controlli di autenticità su software, configurazione e altre informazioni, nonché la registrazione e la consultazione dei risultati di tali controlli e essere integrati in un sistema in grado di eseguire o supportare i controlli di autenticità.</p> <p>Notifica automatica di violazioni dell'integrità - Se il componente sta eseguendo il controllo di integrità, deve essere in grado di fornire automaticamente una notifica a un'entità configurabile al fine di avviare o un tentativo di ripristinare una modifica non autorizzata.</p>
3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	CR 3.4 - Integrità del software e delle informazioni	CR 3.4	1	<p>I componenti devono consentire di eseguire o supportare controlli di autenticità su software, configurazione e altre informazioni, nonché la registrazione e la consultazione dei risultati di tali controlli e essere integrati in un sistema in grado di eseguire o supportare i controlli di autenticità.</p> <p>Notifica automatica di violazioni dell'integrità - Se il componente sta eseguendo il controllo di integrità, deve essere in grado di fornire automaticamente una notifica a un'entità configurabile al fine di avviare o un tentativo di ripristinare una modifica non autorizzata.</p>
3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	CR 3.5 - Validazione degli ingressi	CR 3.5	1	<p>I componenti devono consentire di eseguire o supportare controlli di autenticità su software, configurazione e altre informazioni, nonché la registrazione e la consultazione dei risultati di tali controlli e essere integrati in un sistema in grado di eseguire o supportare i controlli di autenticità.</p>
3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	CR 3.7 - Gestione degli errori	CR 3.7	1	<p>I componenti devono identificare e gestire le condizioni di errore in un modo che non fornisca informazioni che potrebbero essere sfruttate dagli avversari per attaccare l'FAC.</p> <p>I componenti devono fornire meccanismi per proteggere l'integrità delle versioni di comunicazione, tra cui:</p> <ul style="list-style-type: none"> <li>a) la capacità di invalidare gli identificatori di versione all'agente o altro chiusura della versione (compreso le versioni del browser)</li> <li>b) la capacità di generare un identificatore di versione univoco per ciascuna versione e riconoscere i valori di identificatori di versione generati dal cliente e</li> <li>c) la capacità di generare identificatori di versione unici convergenti di consultazione comunemente accettati.</li> </ul>
3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	CR 3.8 - Integrità della sessione	CR 3.8	2	<p>I componenti devono proteggere le informazioni di audit, log di audit e gli strumenti di audit (se presenti) da accessi non autorizzati, modifiche ed alterazioni.</p> <p>I dispositivi/host devono supportare la possibilità di essere aggiornati (spettro e spettro)</p>
3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	CR 3.9 - Protezione delle informazioni di audit	CR 3.9	1	<p>Autenticità e integrità dell'aggiornamento - I dispositivi host devono consentire l'autenticità e l'integrità di qualsiasi aggiornamento del software prima dell'installazione.</p> <p>I dispositivi host devono fornire la capacità di supportare la resistenza alla manomissione e meccanismi di rilevamento per proteggere dall'accesso fisico non autorizzato al dispositivo.</p>
3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	HOR 3.10 - Supporto agli aggiornamenti	HOR 3.10	1	<p>Notifica di un tentativo di manomissione - I dispositivi host devono essere in grado di fornire automaticamente la notifica a un sistema configurabile di dispositivi dopo essere scoperti un tentativo di effettuare un accesso fisico non autorizzato. Tutte le notifiche di manomissione dovranno essere registrate come parte delle funzioni generali di registrazione degli audit.</p> <p>I dispositivi host devono fornire la capacità di fornire e proteggere la riservatezza, l'integrità e l'autenticità delle chiavi e dei dati del firmware del prodotto da utilizzare come e più tardi di fiducia (trust) di trust, e il momento della fabbricazione del dispositivo.</p>
3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	HOR 3.11 - Resistenza e rilevamento della manomissione fisica	HOR 3.11	2	<p>I dispositivi host devono:</p> <ul style="list-style-type: none"> <li>Almeno la capacità di fornire e proteggere la riservatezza, l'integrità e l'autenticità delle chiavi e dei dati del proprietario del firmware (trust assets) da utilizzare come note of trust, e</li> <li>la capacità di fornire e proteggere tali chiavi e dati senza fare affidamento su componenti che potrebbero essere al di fuori della zona di sicurezza dei dispositivi.</li> </ul> <p>I dispositivi host devono verificare l'integrità del firmware, del software e dei dati di configurazione necessari per il processo di avvio dei componenti prima di essere utilizzati nel processo di avvio.</p>
3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	HOR 3.12 - Fornitura delle root of trust del prodotto	HOR 3.12	3	<p>Autenticità del processo di avvio - I dispositivi host devono utilizzare le root of trust del firmware dei componenti per verificare l'autenticità del firmware, del software e dei dati di configurazione necessari per il processo di avvio dei componenti prima di essere utilizzati nel processo di avvio.</p>
3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	HOR 3.13 - Fornitura delle root of trust dell'asset owner	HOR 3.13	3	<p>I componenti devono:</p> <ul style="list-style-type: none"> <li>Almeno la capacità di proteggere la riservatezza delle informazioni (non crittografate) per le quali sia supportata l'autenticazione esplicita e letture, e</li> <li>il supporto la protezione delle informazioni delle informazioni in transito per le quali è supportata un'autenticazione di lettura esplicita.</li> </ul> <p>I componenti devono fornire la capacità di cancellare tutte le informazioni, per le quali è supportata l'autenticazione esplicita in lettura, dai componenti che devono essere eliminati dal servizio attivo o in disutilizzo.</p>
3	FR 3 – Integrità del sistema	Garantire l'integrità del componente per proteggerlo da manipolazioni o modifiche non autorizzate.	HOR 3.14 - Integrità del processo di avvio	HOR 3.14	1	<p>Cancellazione delle risorse di memoria condivisa - I componenti devono fornire la capacità di proteggere da inaccessibilità di informazioni non autorizzate e non intenzionali tramite risorse di memoria condivisa volatile. Le risorse di memoria volatile sono quelle che generalmente non conservano le informazioni dopo essere state discolate dalla gestione della memoria. Tuttavia, si sono attivati contro le memorie ad accesso casuale (RAM) che potrebbero essere memorizzate sulle chiavi e sui dati del firmware prima che vengono effettivamente cancellati. Pertanto, quando le memorie condivise volatili viene rilasciate al sistema di controllo per essere utilizzate da un utente diverso, tutti i dati e le informazioni sulla chiavi devono essere eliminati dalla memoria in modo che non siano visibili o accessibili al nuovo utente.</p> <p>Verifica della cancellazione - I componenti devono fornire la capacità di verificare che la cancellazione delle informazioni sia avvenuta.</p> <p>I componenti devono consentire agli eventi esterni o agli strumenti autorizzati di accedere al log di audit in sola lettura.</p>
6	FR 6 – Risposta tempestiva agli eventi	Rispondere alle violazioni della sicurezza avvisando la autorità competenti, riportando le prove necessarie della violazione e intraprendendo azioni correttive tempestive quando vengono rilevati incidenti.	CR 6.1 - Accessibilità dei log di audit	CR 6.1	1	<p>Accesso programmatico ai registri di audit - I componenti devono fornire l'accesso programmatico ai registri di controllo utilizzando un'interfaccia di programmazione dell'applicazione (API) in modo da rendere i registri di controllo a un sistema centralizzato.</p>
6	FR 6 – Risposta tempestiva agli eventi	Rispondere alle violazioni della sicurezza avvisando la autorità competenti, riportando le prove necessarie della violazione e intraprendendo azioni correttive tempestive quando vengono rilevati incidenti.	CR 6.2 - Monitoraggio continuo	CR 6.2	1	<p>I componenti devono fornire la capacità di essere continuamente monitorati utilizzando le tecniche e le raccomandazioni del settore della sicurezza comunemente accettate per rilevare, identificare e segnalare le violazioni delle sicurezza in modo tempestivo.</p> <p>I componenti devono fornire la capacità di mantenere le funzioni essenziali quando operano in modalità degradata o a seguito di un evento DoS.</p>
7	FR 7 – Disponibilità delle risorse	Garantire la disponibilità dei componenti contro il degrado o la negazione (DoS) di servizi essenziali.	CR 7.1 - Protezione dal Denial of Service	CR 7.1	3	<p>Grado di fusione di comunicazione dei componenti - I componenti devono fornire la capacità di ricevere gli effetti di eventi DoS del tipo informazioni e / o message flooding.</p> <p>I componenti forniscono la capacità di fornire l'accesso delle risorse da parte delle funzioni di sicurezza per proteggere dall'accesso delle risorse.</p>
7	FR 7 – Disponibilità delle risorse	Garantire la disponibilità dei componenti contro il degrado o la negazione (DoS) di servizi essenziali.	CR 7.2 - Gestione delle risorse	CR 7.2	3	<p>I componenti devono fornire la capacità di partecipare alle operazioni di backup a livello di sistema o altre che coinvolgono le risorse dei componenti (informazioni e livello di gestione e di sistemi). Il processo di backup non deve influire sulle normali operazioni dei componenti.</p>
7	FR 7 – Disponibilità delle risorse	Garantire la disponibilità dei componenti contro il degrado o la negazione (DoS) di servizi essenziali.	CR 7.3 - Backup del sistema di controllo	CR 7.3	1	<p>Verifica dell'integrità dei backup - I componenti devono fornire la capacità di validare l'integrità delle informazioni di backup prima dell'avvio di un ripristino di tali informazioni.</p>
7	FR 7 – Disponibilità delle risorse	Garantire la disponibilità dei componenti contro il degrado o la negazione (DoS) di servizi essenziali.	CR 7.4 - Ripristino e ricostruzione del sistema di controllo	CR 7.4	1	<p>I componenti devono fornire la capacità di essere ripristinati e ricostruiti in uno stato sicuro noto dopo un'informazione o un guasto.</p>
7	FR 7 – Disponibilità delle risorse	Garantire la disponibilità dei componenti contro il degrado o la negazione (DoS) di servizi essenziali.	CR 7.6 - Impostazione delle configurazioni di rete e di sicurezza	CR 7.6	1	<p>I componenti devono fornire la capacità di essere configurati in base alle configurazioni di rete e di sicurezza raccomandate descritte nelle guide di rete e di sicurezza dei fornitori del sistema di controllo. Il componente deve fornire un'interfaccia alle impostazioni di configurazione della rete e della sicurezza attualmente attive.</p>
7	FR 7 – Disponibilità delle risorse	Garantire la disponibilità dei componenti contro il degrado o la negazione (DoS) di servizi essenziali.	CR 7.7 - Minima funzionalità	CR 7.7	1	<p>Report loggati meccanicamente delle attuali impostazioni di sicurezza - I componenti devono consentire il genere di report loggati che elenchi le impostazioni di sicurezza attualmente implementate in un formato leggibile da sistemi automatici.</p>
7	FR 7 – Disponibilità delle risorse	Garantire la disponibilità dei componenti contro il degrado o la negazione (DoS) di servizi essenziali.	CR 7.8 - Intimità dei componenti del sistema di controllo	CR 7.8	1	<p>I componenti devono fornire la capacità di fornire specificamente l'uso di funzioni, porte, protocolli e / o servizi non necessari.</p> <p>I componenti devono fornire la capacità di supportare un inventario dei componenti del sistema di controllo che supporti l'elenco corrente dei componenti installati in un proprio loro sicurezza.</p>