*Comprehensive Requirements that Apply to all Use Cases*

| ID | Requirement |
| --- | --- |
| 0.1 | The architecture must use Hyperledger Fabric as the implementation. |
| 0.2 | The architecture must support multiple programming languages. |
| 0.3 | The architecture must support forward and backward compatibility. |
| 0.4 | The transaction schemas must use and require a schema version. |
| 0.5 | The federal government must provide: |
| 0.5.1 | One orderer node. |
| 0.5.2 | One peer node. |
| 0.5.3 | Public key infrastructure based on its needs. |
| 0.5.4 | An organization name to be used in configurations. |
| 0.5.5 | One or more membership service providers that may be used in configuration. |
| 0.6 | The state government must provide: |
| 0.6.1 | One orderer node. |
| 0.6.2 | One peer node. |
| 0.6.3 | Public key infrastructure based on its needs. |
| 0.6.4 | An organization name to be used in configurations. |
| 0.6.5 | One or more membership service providers that may be used in configuration. |
| 0.7 | Each manufacturer must provide: |
| 0.7.1 | One orderer node. |
| 0.7.2 | One peer node. |
| 0.7.3 | Public key infrastructure based on its needs. |
| 0.7.4 | An organization name to be used in configurations. |
| 0.7.5 | One or more membership service providers that may be used in configuration. |

*Comprehensive Requirements for the Firmware Update Use Case*

| ID | Requirement |
| --- | --- |
| 1.1 | The implementation must reside at the federal level per the geospatial design. |
| 1.2 | No personal information may be stored. |
| 1.3 | No sensitive data may be stored. |
| 1.4 | The minimum throughput must be 36 transactions per second. |
| 1.5 | Each transaction must have the following information: |
| 1.5.1 | A SHA-256 hash of the firmware artifact. |
| 1.5.2 | A unique identifier for the firmware. The identifier must be unique to the manufacturer. |
| 1.5.3 | The URL where the artifact is stored. |
| 1.5.4 | The version of the firmware artifact. |
| 1.5.5 | A key-value pair collection used to store metadata about the firmware. |
| 1.6 | No firmware artifact may be stored on the blockchain. |
| 1.7 | The firmware’s developer or the original equipment manufacturer must sign each transaction. |
| 1.9 | The chaincode must ensure the following: |
| 1.9.1 | Verify and validate that the request is valid and that the required information is provided. |
| 1.9.1.1 | If the request is invalid, reject the request. |
| 1.9.2 | Allow authorized participants to retrieve the firmware information. |
| 1.9.3 | Allow authorized participants to write firmware information. |

*Comprehensive Requirements for the FMVSS Certification Use Case*

| ID | Requirement |
| --- | --- |
| 2.1 | The implementation must reside at the federal level per the geospatial design. |
| 2.2 | No personal information may be stored. |
| 2.3 | No sensitive data may be stored. |
| 2.4 | The minimum throughput must be two transactions per second. |
| 2.5 | Each transaction must support the compliance requirements as documented in **Table 16**, **Table 17**, **Table 18**, **Table 19**, **Table 20**, **Table 21**, and **Table 22** |
| 2.6 | The chaincode must: |
| 2.6.1 | Verify and validate that the request is valid and that the required information is provided. |
| 2.6.1.1 | If the request is invalid, reject the request. |
| 2.6.2 | Allow authorized participants to retrieve FMVSS certifications. |
| 2.6.3 | Allow authorized participants to write FMVSS certifications. |