## Comments on the latest draft of the software updates paper

The following requirements needs to be included to ensure software update verification and validation:

* *Manufacturers should be required to provide evidence for validation of the update and verification procedures used to ensure that the software update is in compliance with adequate quality control requirements. The evidence includes:*
* *Standards adherence to ensure process rigor for safety and security of software updates*
* *Statistical/Empirical evidence (Field operational test data results and/or simulation test results) for gauging the safety/ security impact of software updates*
* *For every software update, validation scope should not be limited to the validation of the individual update. The extent of the impact of the software change has to be analyzed on the entire system. This impact needs to be documented and shall be presented to the approval authority, if demanded.*
* *Manufactures should also be able to demonstrate the level of validation coverage they have conducted on the software update. The level of validation coverage has to decided based on:*
  + *Complexity of software update design*
  + *Safety/security Risk associated with intended use and functions of the update.*

*Manufacturers shall be required to provide evidence regarding the rationale for the level of validation coverage they have adhered to. As complexity and associated risk of the software update increases, the level of validation coverage should also increase.*

* *Validation requirements and responsibilities should be clearly identified in case an update is initiated/ developed by a downstream supplier. The responsibility for software update verification and validations needs to dispersed within the chain of development. Appropriate responsibility allocation measures shall be implemented in case of multi vendor update development. Manufacturers shall maintain appropriate documentation/ evidence for the same and shall present it to the approval authority if needed.*
* *Manufacturers shall establish the software development life cycle model as appropriate for the update release process. (This can include traditional V-model, waterfall model or agile model for update development). Irrespective of the life cycle model, manufactures shall maintain appropriate evidence for update validation and demonstrate the same to the approval authority if needed for the following activities:*
  + - *Planning document/ evidence which identifies the update development model and necessary resources, management review requirements, procedures for anomaly reporting and review and approval of software development results.*
    - *Identification, analysis, and documentation of information about the update and its intended use. Description of the implementation of the functionality on a high level/ functional level.*
    - *Identification of operating conditions, user characteristics, potential hazards and safety requirements, consequences of software updates failures and corresponding mitigating measures .*
    - *Software requirements traceability analysis for updates to trace software requirements to (and from) system requirements and to risk analysis results. Traceability analysis shall also confirm that design implements all of the software update requirements. Traceability shall also be extended to the testing phase and it shall be demonstrated that the all implementations of the design are covered in the testing phase. The manufacturer shall maintain appropriate evidence/ documentation for traceability verification throughout the development lifecycle and shall demonstrate to the approval authority*
    - *Manufacturers shall ensure that the most rigorous level of error checking is employed in the software update development process. All errors and (or) warnings associated with the development process shall be documented and demonstrated to the approval authority, including evidence for root cause analysis for safety critical system errors. Evidence for countermeasures employed for successful mitigation of these errors and justification for the decision to leave issues unresolved(if any) shall be maintained and demonstrated.*
    - *Manufacturers shall demonstrate the compliance of update source code with the respective design specifications and design dilemmas(where a functional requirement has been not implemented to have adherence for safety/ security requirement and vice versa). Proof of source code evaluation process(static/ dynamic analyses) shall also be maintained as a part of update verification process.*
    - *Manufacturers shall maintain software update test plans that identifies the particular tasks to be conducted at each stage of development and include justification of the level of effort represented by their corresponding completion criteria. Test plans shall clearly indicate the definition of what is to be tested.*
    - *Evidence of Structural/ code based testing shall be demonstrated to determine what percentage of the update code(completeness) has been evaluated in the testing process.*
    - *Functional testing results shall be demonstrated for the verification of functionality of a program and its interfaces.*
    - *Statistical testing (using randomly generated test data)/ field operational test results shall also be demonstrated in additional to structural and functional testing results to the approval authority. The test scenarios(data) for the same shall be determined based on the operational profile of an update.*
    - *Results of repeatable tests(simulation, tests under boundary conditions, fault injection, durability tests, stress tests, highly accelerated life testing etc.), and analyses( FMEA, FTA, ETA, simulation etc.) shall also be demonstrated for ensuring the credibility of the update testing process.*
    - *Manufacturers shall also demonstrate documentation/ proof of testing of software changes that occurs during the update development lifecycle. This includes changes like updated requirements, modified designs or error corrections.*
    - *Regression analysis results shall be demonstrated to ensure that the new update doesn’t affect the existing functionality or type approvals. If existing type approvals are affected, it shall be the responsibility of the manufacturer to apply for new type approval/ extension for the same.*