

Software requirements for direct recording electronic (DRE) voting machines

according to "Verordnung über den Einsatz von Wahlgeräten bei Wahlen zum Deutschen Bundestag und der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland" (Bundeswahlgeräteverordnung).

1. Identification

Each part of the system shall be identifiable. For each voting machine shall be detectable, that it corresponds to a type approved model.

- The source code files shall have a name and version number.
- The executable programs shall have a name and version number which cannot be changed during election.
- The manufacturer shall comply that the source code presented for type approval corresponds to the executable program of the voting machine presented for type approval.
- Each voting machine shall be assigned to a certain constituency (i.e. a certain candidate or party list) and a certain community. The assignment shall be observable.
- For each voting machine shall be detectable, that it corresponds to a type approved model. For each instance of each executable program shall be detectable, that it corresponds to the type approved executable program.

2. Functionality

The voting machine and its software must guarantee a free, equal and secret election process corresponding to the election law and other statutory regulations. First of all the information collected by the voting machine must be kept secure and unchangeable.

- The votes must be recorded correctly.
 - Each button of the voting machine must correspond to a certain function (e.g. a certain list entry), which is observable and which cannot be changed during election.
 - The voting machine shall not come to an undefined state through normal use or through failures in the operation.
 - The voting machine must accept and record the votes of each voter. The vote recording process shall not be aborted by any malfunction or defect. It shall be aborted only when the data integrity of current or old votes may be violated.
 - The voting process shall include two steps. The voter shall be able to check and correct his choices after first step. If he corrects choices, the data of the first choice should not be stored permanently.

- The voting machine must give an audible or visible signal, when the votes are recorded successfully.
- Each vote must be assigned to the correct election, the correct constituency, and the correct community.
- The buttons of the voting machine must be numbered. The counting results must be numbered the same way.
- An invalid vote (abstention) shall be recorded only if the voter presses the corresponding button. Defect votes shall not be treated as invalid (abstention) votes.
- The counter for the number of voters must be set to zero before the first voter begins. This must be observable.
- After evaluating the election results the voting machine must be locked for further voting.
- Each individual vote of a voter must be accepted and recorded independent of other votes.
- Each entry in a candidate or party list must be selectable independent of other entries in the same list or in other lists.
- The votes must be counted correctly.
 - The voting machine shall work in a way, that each voter is able to select entries only in those elections (lists) which were released for him. The voter shall operate the voting machine only, if the election staff released at least one election for him. The voting machine must be locked for further voting when the voter finished his voting process.
 - No voter shall be able to release elections (candidate or party lists).
 - The release of elections and the locking for further voting must be observable for the election staff.
 - Each vote shall be recorded only once (except copies for security reasons, which are not counted). Each program variable carrying vote information shall be resetted immediately after recording the vote successfully.
- The counter for the number of voters must be increased by one immediately after recording all votes of a voter successfully.
- The number of voters and the number of votes must be permanently observable.
- The votes must be recorded with redundancy. They must be readable even in case of single memory defects.

- The votes shall be counted without numerical problems (e.g. over/underflow).
- The counting results must be assigned to the right list entries (candidates or parties).
- The election result must be observable immediately after finishing the election process for all voters. The election result must be stored in a permanent manner (e.g. printed out) without falsifications.
- The voting machine must perform a check before and after each vote recording process. Inconsistencies (e.g. wrong counting results, unreadable or defect votes) must be indicated immediately. Severe problems must lock the voting machine.
- The method of recording and the method of counting must be the same for each list entry and for the invalid (abstention) votes.
- The voting machine must keep the votes secret.
 - The choices of a voter should not be visible outside the polling booth.
 - The choices of a voter should not produce an identifiable keystroke sound.
 - The recording process shall work in a manner that the recorded votes cannot be assigned to a certain voter.
 - The choices of a voter shall be visible only for the voter himself and only as long as his voting process lasts.
- The election staff must be able to undo a release of elections.
- The software for a certain election must work without interdependencies to software for other elections or to other software programs.

3. Reliability

Because of the risky application area the requirements concerning reliability are very high. Errors in election results must be avoided at nearly any cost.

- The software must correspond to the current general state of technology and to the recognised rules of technology in Software Engineering.
 - The program development must be in accordance with a software development (life cycle) model. The software development model must be documented, and, if required, be presented during an assessment procedure of the development processes.
 - The programming language must follow a language (coding) standard.
 - The program shall not contain problematic constructs (e.g. jumps, side effects). It shall not produce compiler warnings or static analyser warnings.

- The programming style must follow the principles of structured programming and data hiding or comparable principles.
- The recording of votes must work in a reliable manner.
 - The recording process shall not be interruptible.
 - No one should be able to undo the recording of votes.
 - The documentation for the election staff must describe each hardware and software failure which may occur (e.g. failures of displays or buttons, power loss, checksum problems). For each sort of failure the documentation must describe, whether and how the current voter may finish his voting process. The documentation must describe, whether the current votes will be recorded or not.
 - The recorded votes must be protected against deletion, falsifications, or visualisation, even in case of switching on and off the voting machine.
- Misuse and false operation of the voting machine shall not result in deletion, falsification, or visualisation of recorded votes.
- A system failure shall not result in deletion, falsification or visualisation of recorded votes.
- The election result must be obtainable even in case of system failure.
- Each hardware and software failure during election preparation, election day, and election evaluation must be registered for later analysis.
- The software shall perform a self-check and (as far as possible) a check of the hardware at each start-up.

4. Documentation

The documentation must contain carefully prepared manuals for the election staff and for the voters.

- The manufacturer shall deliver a detailed, consistent and understandable program documentation. This documentation must contain a test documentation.
- The manufacturer shall deliver a correct and understandable manual for the election staff.
 - The manual must describe how the software identification is checked, how the voting machine's identification and the identification of additional parts is checked, how the programming of constituency and community is checked, and how the correspondence to the type approval model is checked.

- The manual must describe how the functions of the voting machine are checked and how the voting machine is prepared for work.
- The manual must describe what should be done in the case of power loss, hardware and software failures (e.g. failures of displays, buttons, and printer, checksum problems), or system failure.
- The manual must contain a list of all possible error, warning, and informational messages which may occur. The list must contain hints how to continue work. If the election must be continued by other means (other device, ballot box) the manual must describe how the defect voting machine and its additional parts must be handled.
- The manual must describe how the counter for the number of voters or the number of votes must be checked during election process.
- The manufacturer must deliver a correct and readable introduction for voters. The introduction must contain a picture of the device and a picture of the machine's ballot paper. The introduction must contain the declaration, that the voter is allowed to select an invalid vote (abstention).
- The printout of the election result must contain at least: the name of the election, election date, constituency and community, identification of voting machine, software, and additional parts, and for each election: number of votes, number of invalid votes (abstentions), number of votes per list entry (candidate or party).