Reliability Analysis of Smart Card Technology Implementation

Koushik Saha

Westcliff University

TEM640/263-PTZ-A - PST Professional - Spring 2026 - Session 3 - Professor Haddad

Professor Omar Haddad

January 16, 2026

Reliability Analysis of Smart Card Technology Implementation

During the initial introduction of smart cards in the 1990s, there were significant challenges for organizations to assess their long-term reliability without fully committing to large-scale use. This case study explores how a large island-state organization with around 300,000 employees tackled the decision to deploy smart card technology for employee identification and security access to hundreds of facilities. The organization had to find a structured way of confirming whether the smart cards could indeed live up to the claim of the supplier of a five-year operational lifespan without affecting workflow efficiency or security protocols.

Case Summary

The organization intended to use the smart cards as employee identity cards with two goals. First, the smart cards would contain vital employee details and credentials for access, which would be facilitated by the memory chips with 24 memory cells. Second, the installation of smart card readers at facilities and secured workstations would regulate, monitor, and record employee access activities centrally through the computer network. The success of this system depended on the absolute reliability exhibited independently by both the smart cards and their readers, since failure would hamper the day-to-day activities and security arrangements. The supplier of the smart cards asserted that their device could work well for at least five years with no need for replacement, but the organization was prudent in asking for third-party verification for this guarantee before proceeding. This was an urgent requirement, especially considering that with 300,000 cards in use, even the least failure rate could result in malfunctioning cards amounting to tens of thousands.

Problem Statement

The first challenge was to assess if the supplier's five-year lifespan was a reasonable expectation in a real-world setting. The technical difficulty was to make sense of the failure distribution pattern in the smart cards over the five-year period. Supposing the smart cards followed an exponential failure distribution with a mean time to failure of five years, the result was ominous mathematics. In this case, about 63.2% of the 300,000 smart cards would be likely to fail within the five-year period, causing chaos in the workflow and substantial support in terms of logistics to handle the failure associated with replacement and so on.

The organization had to set a measurable reliability target that would not make the technology adoption be perceived as problematic. This involved turning the general claim of the supplier into specific statistical reliability requirements. In addition, the team needed to develop a comprehensive testing plan that would convincingly show whether the smart cards could meet the predetermined reliability targets. A further complication was to relate the number of card transactions to calendar time and hence required reasonable assumptions concerning user behavior. The organization made the 80:20 assumption that 80% of the users would be light users averaging 10 daily transactions, whereas 20% of the users would be heavy users averaging 50 daily transactions. Based on a standard working year of 300 days, they would be able to turn transaction-based reliability metrics into meaningful timeframes for operational planning.

Solution

The organization’s engineering group devised a sophisticated approach for transforming the supplier’s qualitative statement about reliability into a set of quantitative demands. They began by deciding that a certain number of failures within a five-

year period was inevitable. They thus decided that card failure rates should be limited such that card complaint numbers should not be high. After a thorough process of consideration, it was decided that a card failure rate of up to a maximum of 2 per day should be acceptable. This corresponds to a failure rate of a maximum of 600 per annum and a total failure of 3,000 within a five-year span. Given a total of 300,000 cards in use, it meant that only a maximum of 1% should have failed.

Based on this 99% reliability, the target mean time to failure was calculated to be 497.5 years when considering that the card fails at a constant rate. The team then proceeded to assess the transaction target based on this reliability using 80:20 user distribution and 300 workdays a year. The result required the target to be close to 2,700,000 transactions for the card. The testing procedure the team employed was very rigorous and realistic. Every card was connected to a reader that had a random number generator to generate messages to fill all 24 cells. The reader then checked the data that had been written. Every full write and read operation was counted as one transaction. Different reader models processed transactions at distinct rates. Therefore, the team was very conservative in setting the maximum time for a transaction to two minutes.

For 100 subscribers doing continuous testing at 30 transactions per hour, the optimum test would demand 62,170 transactions, which would take around 87 days. However, the timeline to implement the solution brought a natural limitation to this task as well. Since the organizational requirement demanded the completion of the test report within two months, the maximum time available for the actual test would not exceed 52 days. Considering this limitation, the number of sample smart cards to be required was computed to be 166.

Critical Analysis

In this case, the solution proposed to ensure reliability is well-organized and mathematically precise. Its greatest strength is its systematic conversion of a statement of reliability from a qualitative to a quantified metric. By setting up thresholds of failure based not on technical detail but rather on practical considerations of administration, it is clear that this organization was not foolishly seeking perfection in reliability. Rather, it took into account practical considerations in setting up reliability, recognizing the futility of perfect reliability in practical terms. In setting up its testing protocol to test all 24 memory cells in a transaction, it was especially shrewd in recognizing that testing reliability in this way was testing it in the area of its greatest weakness.

However, I might consider a few other angles, if I were working on this problem: the solution assumes a failure rate that is uniformly distributed over five years, but smart cards might fail differently throughout their product lifecycle. Research in reliability engineering for many electronic components reveals a bathtub curve-a high likelihood of early life failures due to manufacturing defects and again during wear-out periods. Employing methods of accelerated life testing could have shortened the test duration while casting some light on degradation depending on age. This would be achieved by exposing cards to increased stress conditions such as high transaction frequencies, temperature cycling, or humidity exposure, simulating years of normal usage in short time frames.

Second, the testing protocol involved only memory read-write cycles and not the physical stresses that can cause card failure, which in real life could be the result of physical rather than electronic stresses. Cards kept in a purse or wallet are subjected to bending stresses, electromagnetic interference from other electronic equipment, and environmental stresses, which

may not be properly represented or simulated in a lab test situation. It would be useful to have a test strategy involving limited field testing in which selected personnel test a prototype card over several months, gathering data on failure modes not identified in purely electronic testing protocols.

Moreover, the methodology could also have used a more defined risk assessment methodology to prioritize failure modes based on their level of severity. Not all failure modes for a smart card are equal. A card that starts to fail by taking several reads to authenticate might be frustrating but is less serious than one that refuses to work at all when passing through a critical security checkpoint. By performing failure mode and effects analysis, it could have given more priority to failure modes that need to be addressed by the test itself to prevent and could have given more focus to the acceptable failure rate thresholds (Stamatis, 2003). However, the proposed solution methodology has struck the right balance between science and practicality to give the organization the necessary confidence to move ahead with the adoption of the technology while setting realistic expectations.

References

Ebeling, C. E. (2019). *An introduction to reliability and maintainability engineering* (3rd ed.). Waveland Press.

Stamatis, D. H. (2003). *Failure mode and effect analysis: FMEA from theory to execution* (2nd ed.). ASQ Quality Press.

Tang, L. C. (n.d.). Case 5: Reliability of smart cards. In *Operations management: Maintenance engineering and reliability analysis* (pp. 757-760). [Textbook chapter].