How would you test an ATM? What functions of the ATM would you check, and from what perspectives?

II. Functional Testing:

1. Verify the card reader is working correctly (a screen to insert pin is shown when inserting a valid card) Verify the correct pin is accepted (the ATM will display the account information when Pin is correct)
2. Verify the Navigation buttons are working correctly on all screens (each button takes you to the corresponding screen - Touch screen buttons should be included - if available)
3. Verify each number from the keypad is working as expected
4. Verify the Cancel button is working as expected
5. Verify the OK button is working as expected
6. Verify messages for each scenario:
    a. incorrect pin,
    b. no available cash in the ATM,
    c. insufficient Cash,
    d. Card not recognized,
    e. wrongly inserted Card,
    f. unaccepted amount (in case it is too small, or incorrect)
7. Cash withdrawal:
    a. Verify the withdraw function (the correct amount of money is dispensed by the ATM when the Amount is between the set limits)
    b. Verify if a user can perform only one cash withdrawal per pin insert
    c. Verify the confirmation message is displayed
8. Verify the "Deposit" functionality with valid bills/Checks (if available)
9. Verify the "Pay the bill" functionality if available
10. Verify the print receipt for available balance, cash withdraw
11. Verify the "Refill" action can be done successfully by a bank operator
12. Verify the Service mode is working as expected.
13. Verify the accessibility functions for disabled persons (deaf, blind, etc.)
14. Verify the ATM times-out after a period of inactivity.
15. Verify using different cards (emitted by different banks)
16. Verify out of service screen is shown when there is an issue with the ATM

Negative testing:

1. Verify that inserting less than 4 digits will not let you submit the pin
2. Verify that inserting a wrong 4-digit pin does not allow to access account information
3. Verify the card is blocked after inserting 3 times wrong pin
4. Verify that inserting an unaccepted amount to withdraw will show an error message and will ask for a correct amount
5. Verify that the customer can not withdraw less than the minimum amount
6. Verify that the customer can not withdraw more than the maximum amount allowed (by ATM or by bank standards) in one transaction
7. Verify that the customer cannot do more cash transactions than the maximum transaction number allowed for his account (if applicable)

8. Verify that the customer cannot withdraw more than the maximum amount (per day, week, month) allowed in multiple transaction (if applicable for account)
9. Verify the customer cannot withdraw an amount greater than the account balance
10. Verify the customer cannot access account information with an expired card
11. Verify the deposit by inserting unaccepted bills/invalid checks
12. Verify withdrawal functionality by inserting invalid amounts (for ex: ",4")

II. Non-functional testing
1. Verify if the text on the screen button is visible clearly.
2. Verify the font of the text on the screen buttons.
3. Verify each number button on the Keypad.
4. Verify the text color of the keypad buttons. The numbers should be visible clearly .
5. Verify the text color and font of the data on the screen. The user should be able to read it clearly.
6. Verify the translations on all languages are done correctly
7. Do a performance testing on all actions to make sure the response time is acceptable.

Checks will be performed from the following perspectives: the Customer, the bank operator, the technical engineer, and the banking system.

2. How would you test inputs containing:

II. Strings:
1. Test all accepted characters (included accented characters or special alphabets if accepted)
2. Test with unaccepted characters
3. Test minimum/maximum number of characters (if applicable)
4. Test against XSS using scripts that injects malicious code in the website using characters that may trigger code execution such as " < >
5. Send SQL injection scripts to test if they will be executed

III. b. Paths/Files
1. verify it accepts valid path valid path format for example: "C:\Users\User1\Desktop"
2. verify it accepts absolute/relative paths if applicable
3. verify the invalid path is not accepted
4. Verify the valid characters are accepted (included accented or special characters)
5. Verify the invalid characters (such as / * ? < >)
6. Test against XSS using scripts that injects malicious code in the website using characters that may trigger code execution such as " < >
7. Send SQL injection scripts to test if they will be executed

IV. Time and Date

1. Verify the date field accept dates in the specified format (ex: dd/mm/yy or mm/dd/yy or yyyy).
2. Verify the day field accepts values between 1 and 30/31 according to the month.
3. Verify the day field does not accept any values less than 1 or greater than 31. For example: day field should not accept 0 and 32 or more.
4. Verify that the day field does not accept 30/31 for the second month (February).
5. Verify the day field does not accept 29 for the second month (February) unless it is a leap year.
6. Verify the day field accepts the format 1 and 01.
7. Verify the month field accepts the format 1 and 01 as well as month name (ex: "June") – if applicable.
8. Verify the month field accepts value between 1 and 12.
9. Verify the month field does not accept 0 and 13 or more.
10. Verify the year field does not accept 0000
11. Verify the year field does not accept 'yy' (12) if the required format is 'yyyy' (2012).
12. Verify the day, month and year are separated by – or /.
13. Verify the date field cannot be left blank if the field is set as mandatory.