non-functional requirements

1. The system verification time should not exceed 2 seconds after swiping the card and entering the password.
2. After the user's identity is verified, the response time of entering the system should be within 2 seconds when the user chooses to enter the corresponding operating system or switches the corresponding operating system, and the latest response time should not exceed 4 seconds when the login system is at its peak.
3. The response time of refreshing the column should be within 1 second, and the user should not take more than 3 seconds to execute the command after performing the operation.
4. The time required for the sensor to receive the trigger signal and the alarm to emit an alarm must not exceed 300 milliseconds.
5. The time from receiving a call to the police or fire department to dialing must not exceed 2 seconds.
6. The delay between the automatic alarm of the system and the response of the alarm receiver of the fire department or police department must not exceed 10 seconds.
7. Different users have different identities and permissions, so it is necessary to provide trusted authorization management services on the premise that the user's identity is authentic and trusted, to protect the data from illegal/unauthorized access and tampering, and to ensure the confidentiality and integrity of the data.
8. It provides running log management and security audit functions to track the historical usage of the system.
9. The system can withstand common malicious attacks from the Internet. Such as virus (including Trojan horse) attack, password guessing attack, hacker intrusion and so on.

10. There are hints for input and checks for data to prevent data anomalies.