These security requirements are extracted from the workshop 1 solutions. Do they correspond to the “criteria of good requirements”? If not, please refine them so that they would correspond to the “criteria of good requirements”.
SecReq.1: Automation of the receipt generation or checking fuel capacity and sold amount of fuel as often as possible.

SecReq.2: Cash register computer must compare data about company car / employee ID to ERP and give warning if there is a mismatch.

SecReq.3: IT department must follow security advisories and patch the vulnerable systems, given that solutions are available.

SecReq.4: Implementing at least two workplaces for serving customers in filling station.

SecReq.5: Appropriate trainings shall be provided to all employees of PowerAB with regards to information security awareness.

SecReq.6: Database backup server accounts should be sufficiently protected against unauthorized access.

SecReq.7: IT managers should plan the placement of card readers near 24/7 cameras, which are monitored from a security officer.

SecReq.8: Have a backup server for redundancy and push uptime to near 100%.

SecReq.9: Using better security applications.

SecReq.10: The firewall should continuously monitor the communication channel and block suspicious software while transmitting message from account department to personnel department.
SecReq.1: Automation of the receipt generation or checking fuel capacity and sold amount of fuel as often as possible.

SecReq.2: Cash register computer must compare data about company car / employee ID to ERP and give warning if there is a mismatch.

SecReq.3: IT department must follow security advisories and patch the vulnerable systems, given that solutions are available.
SecReq.1: Automation of the receipt generation or checking fuel capacity and sold amount of fuel as often as possible.

SecReq.2: Cash register computer must compare data about company car/employee ID to ERP and give warning if there is a mismatch.

SecReq.3: IT department must follow security advisories and patch the vulnerable systems, given that solutions are available.

SecReq.1.1: Fuel system should check fuel capacity
SecReq.1.2: Receipt system should generate receipts

SecReq.2: Cash register computer should notify attendant about mismatch between car number and employee ID

SecReq.3: IT department should patch PowerAB software systems
SecReq.4: Implementing at least two workplaces for serving customers in filling station.

SecReq.5: Appropriate trainings shall be provided to all employees of PowerAB with regards to information security awareness.

SecReq.6: Database backup server accounts should be sufficiently protected against unauthorized access.
SecReq.4: Implementing at least two workplaces for serving customers in filling station.

SecReq.5: Appropriate trainings shall be provided to all employees of PowerAB with regards to information security awareness.

SecReq.6: Database backup server accounts should be sufficiently protected against unauthorized access.

SecReq.4: Management should create two workplaces for serving customers.

SecReq.5: Management should provide security awareness training for the PowerAB employees.

SecReq.6: Database backup server accounts should be protected against unauthorized access.
SecReq.7: IT managers should plan the placement of card readers near 24/7 cameras, which are monitored from a security officer.

SecReq.8: Have a backup server for redundancy and push uptime to near 100%.
SecReq.7: IT managers should plan the placement of card readers near 24/7 cameras, which are monitored from a security officer.

SecReq.8: Have a backup server for redundancy and push uptime to near 100%.

SecReq.7: Security officer should monitor the card readers.

SecReq.8: The backup server should ensure the uptime of 99.1%.
SecReq.9: Using better security applications.

SecReq.10: The firewall should continuously monitor the communication channel and block suspicious software while transmitting message from account department to personnel department.
SecReq.9: Using better security applications.

SecReq.9: “I do not know how to fix it !!!”

SecReq.10: The firewall should **continuously** monitor the communication channel and block suspicious software while transmitting message from account department to personnel department.

SecReq.10.1: The firewall should monitor the communication channel.

SecReq.10.2: The firewall should block the untrusted software.

*Explain “untrusted”!*