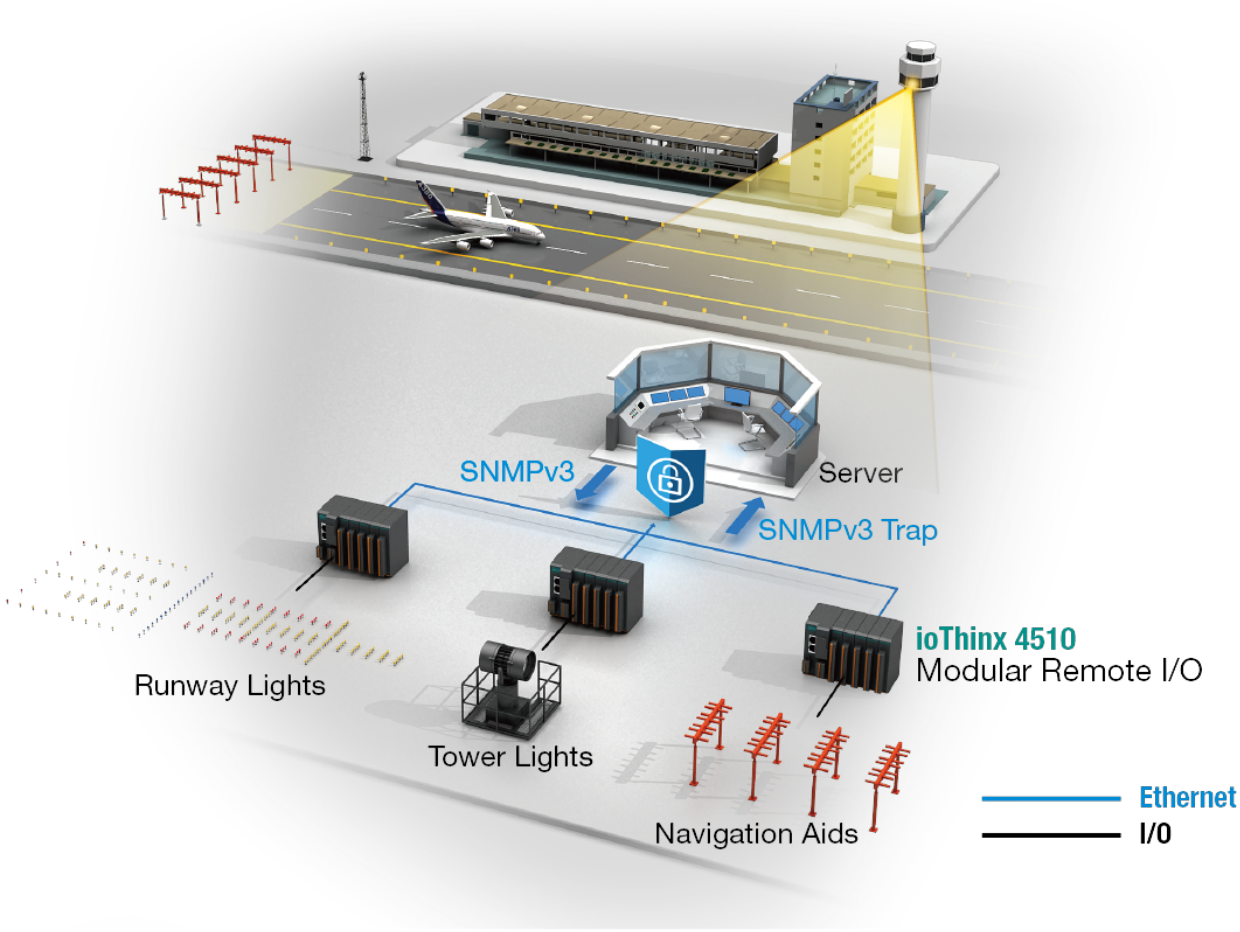
Secure Data Transmission Increases Air Traffic Managment Safety

Security has long been a top priority in the aeronautical industry, and air
Traffic Managment (ATM), whcih refers to the entirety of systems and actions required to manage
the movement of aircraft both on the ground and in the air , plays a major role
in maintaining secure aeronatical transportation. in different pases of operations a wide range of diverse
facilities and devices need to communicate with each other. An mportant aspect of ATM is that it must
be able to operate in all kind of conditions, including outdoors, in hars weather and at remote sites
and all relevant data need to be collected and moitored correctly and securely to maintain
safe and stable operations



Based on this brief introdruction, we can conclude that the devices and components comprising an ATM system must satisfy the following requirements:

1. An industrial-grade rugged design suitable for harsh environments, including outdoors, at remote sites and over long distances, to ensure that ATM operation is both reliable and stable
2. Top-notch network security to protect data from ahckers, Since OT protocols such as Modbus are generally not designed with transmission security in mind, some governments require high-profile areas such as airports to use IT protocols for Internet-facing data transmissions. The most popular IT protocols in use today emphasize a highly secure design. Essential aspects of such protocols inclue data encryption,which presents a solid first line of defense against eavesdropping and hacking. SNMP, for example is widely used in the IT field, Combined with SNMP Trap and Inform, SNMP can be used with both polling-based and alarm-based commmunication, making it one of the most popular protocols for airrport monitoring

System Requirements

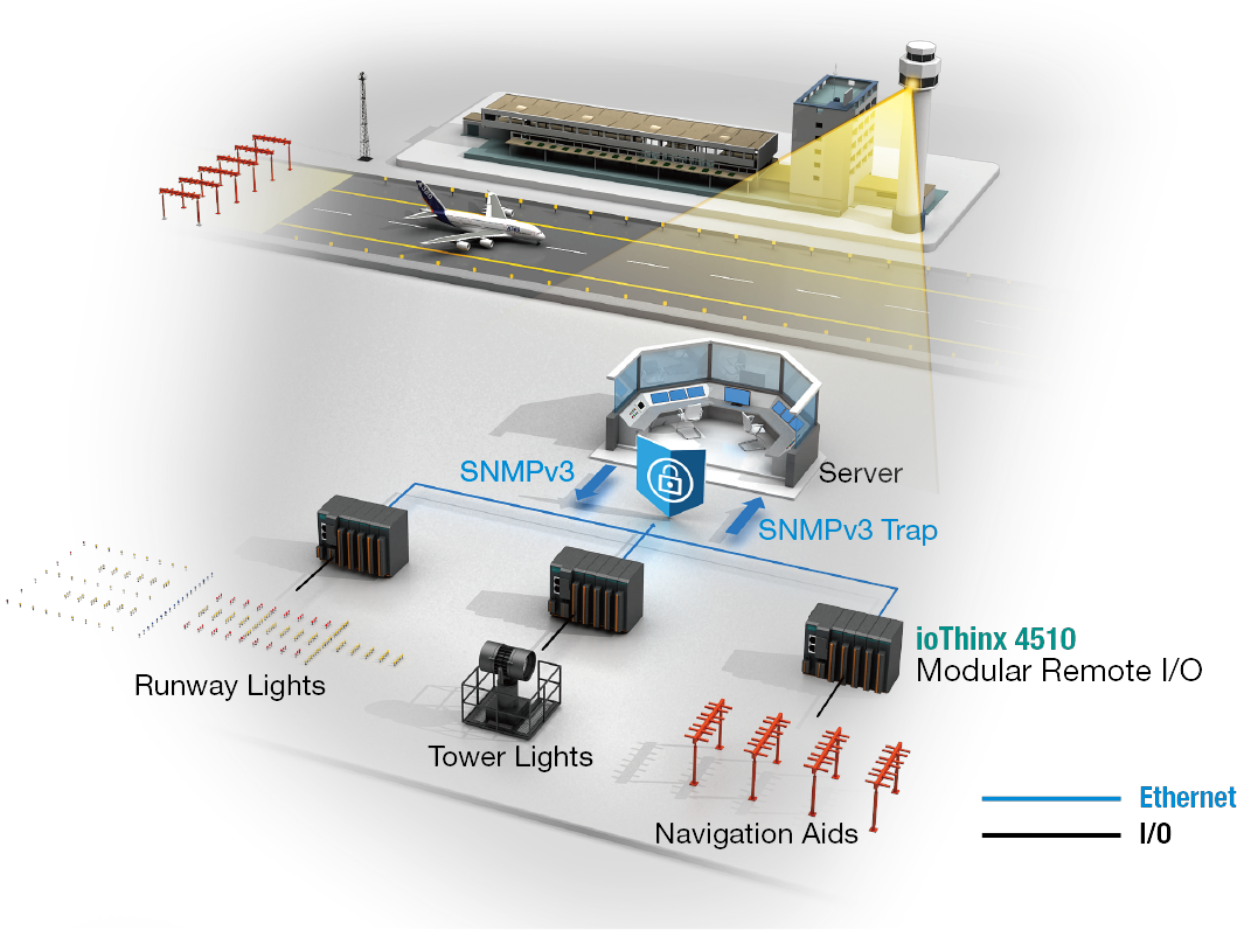
1. The ability to collect and monitor data from many different airport facilities, including runway lights, tower lights and navigation aids, as well as the ability to actively send data to the ATM aerver to minimize the response time for critical conditions.
2. Devices must be able to operate reliably in both extremely harsh hot and cold environments so that the devices can be deployed in airports around the world
3. SNMPv3 and SNMPv3 Trap are required for authenication and active alarms and data encryption is needed to prevent sensitive information from being stolen during transmission

Moxa´s Solution

Aremote I/O system deployed at an airport can be sued to acquire serial, digital and analog data from runway lights, tower lights and navigation aids and then tranmitted in real time to the control center. In additon products that feature advanced remote FI/O features and wide temperature operation are rugged enought to work 24/7 in all kinds of weather and harsh conditions to provide the nonstop operation demanded by airpord operation codes.

SNMPv3 and SNMPv3 Trap are required. Since SNMP is a polling-based protocol, the control center can poll remote I/Os.

With respect to security, SNMPv3 and SNMPv3 Trap support authentication and data encryption, making version 3 the most secure of all SNMP versions. The most popular encryption algorithm used by SNMP is MD5. However since MD5´s security weaknesses can be exploited by hackers, cybersecurity expers suggest using a more secure algorithm, like SHA2 to protect sensitve information. Moxa´s modular remote I/O products support the SHA224 and SHA256 encryption algorithms, both of which belong to the SHA2 family.



Why Moxa

1. Advanced modular remote I/O products that supports SNMPv3and SNMPv3 Trap for device-level security amd active data transmissions
2. SNMPv33 that supports SHA224 and SHA256 encryption algorithms to minimize the risk of data leakage.
3. Modular remote I/O products that support a variety of interfaces and protocols making it easy for users to expand their systems
4. Wide-temperature models that provide reliable operation at temperatures ranging from -40 to 75°C