



# Tip of the Week :

- Setting/Using Access Locks

# [ TINE Security ]

- User Name
  - “easy to fake” but very practical for preventing inadvertent setting changes
  - Allowed Users List
    - File : users.csv
    - API: AppendRegisteredUserList()
    - Stock Property : “ADDUSER”
  - User taken from env (USERNAME) or java property (username)

# [ TINE Security ]

- Network Address
  - Very hard to “fake”
  - Allowed Networks List:
    - File: ipnets.csv (ipxnets.csv)
    - API: AppendRegisteredIPNetsList()
    - Stock Property : “ADDIPNET”
  - Network Address from incoming ethernet packet

# Checking the Access

- “READ” and “WRITE” access are de-coupled from input and output data!
- A “READ” call can send data to the server (as input parameters).
- A “WRITE” call can be a “trigger” which does not require data
  - e.g. “INIT”, “RESET”, “STOP”, etc.
- The equipment module dispatch handler always sees the requested “access”.
  - eqm(devName, devProperty, dout, din, access)
- “WRITE” command should check that the CA\_WRITE access bit is ON!
  - ```
if (access & CA_WRITE)
{
    ...
}
```

Question: Why are there so many properties called “rdSomething” and “wrSomething” ?

# [ ACCESS Locks ]

- Some control applications should be allowed to send command from only a single location (e.g. Interlock, transfer).
- But the application should be allowed to start and run in a read-only mode.
- Use an ACCESS LOCK
  - One and only one application client can issue WRITE command.

# [ ACCESS LOCKS ]

- Three levels of access lock
  - Un-locked (LOCK\_UNLOCKED)
  - Pre-emptive (LOCK\_PREEMPTIVE)
  - Persistent (LOCK\_PERSISTENT)
- STOCK Property “ACCESSLOCK”
  - “WRITE” takes 2 (short) parameters
    - Lock type and duration in seconds
  - “READ” returns 2 (NAME32) parameters
    - User and Network Address of the client with the lock

# [ ACCESS Locks ]

- Pre-emptive Locks can (and must) be re-assigned to the new caller.
- Persistent Locks cannot be pre-empted, but must be periodically renewed (maximum duration is 64 ksec -> 18 hrs).
- (Persistent Locks can be aborted with “LOCK\_ABORT”)
  - Back door to break an access lock (client disappeared?)
  - Better: maximum lock duration = 10 minutes and force the client to renew periodically.

# [ ACCESS Locks ]

- If a lock exists and a WRITE command is called (by the caller with the lock) the CA\_LOCKED access bit is added to the access!
- The Eqm dispatch handler can also request this bit !
  - if (access & CA\_LOCKED)  
    {  
        ...  
    }