Secure PLC Coding Tips and Tricks

Jacob Brodsky, PE; Jacobs Cyber Security Group

S4 Technical Branch Conference 2020

www.jacobs.com | worldwide

Why Discuss This?

- Security specialists do not know how process works
- Engineers are not taught good programming habits

- Good code leads to more rapid diagnostics
  - Can determine and isolate hacks more rapidly
  - Make working with protocol sensitive firewalls easier

Here there be dragons

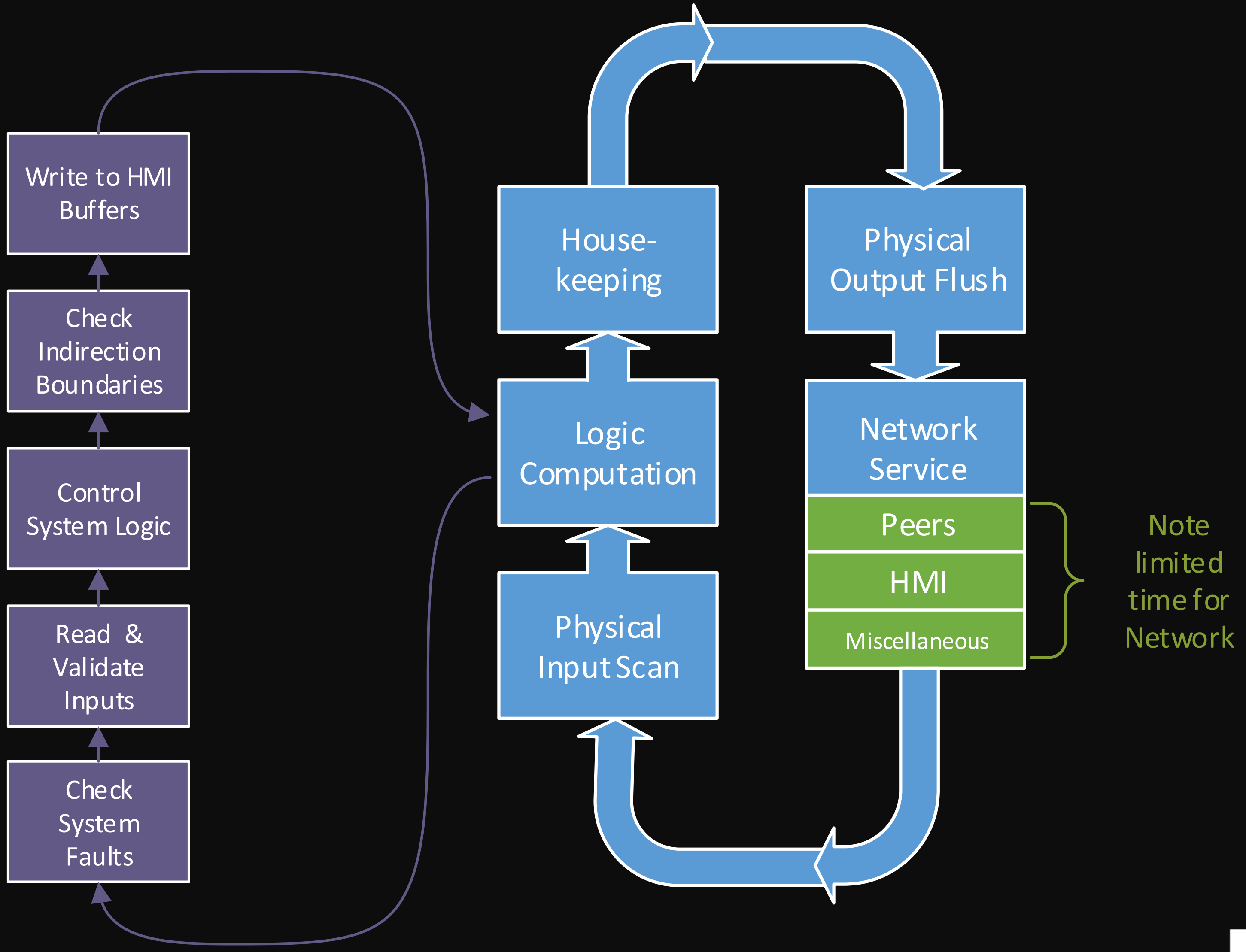
What Languages to use?

- Four Primary Languages
  - **I**nstruction **L**ist (**IL**)
  - **L**adder **D**iagrams (**LD**)
  - **F**unction **B**lock **D**iagram (**FBD**)
  - **S**tructured **T**ext (**ST**)
- **S**equential **F**unction **C**harts (**SFC**) for handling state changes
- **IL** good for speed and portability
- **ST** good for high level math
- **LD** and **FBD** good for permissives, interlocks, timed operations

Avoid Programming All Logic in One Controller

- Keep Program segments small
  - Use more complex blocks to simplify ladder
  - Break LD or ST segments in to smaller parts
- Use peer to peer networking among other controllers
  - Code for failure of Peer Communications
  - Consider what each small controller should do if isolated
- Keep Controller close to I/O

Typical PLC Scan Cycle

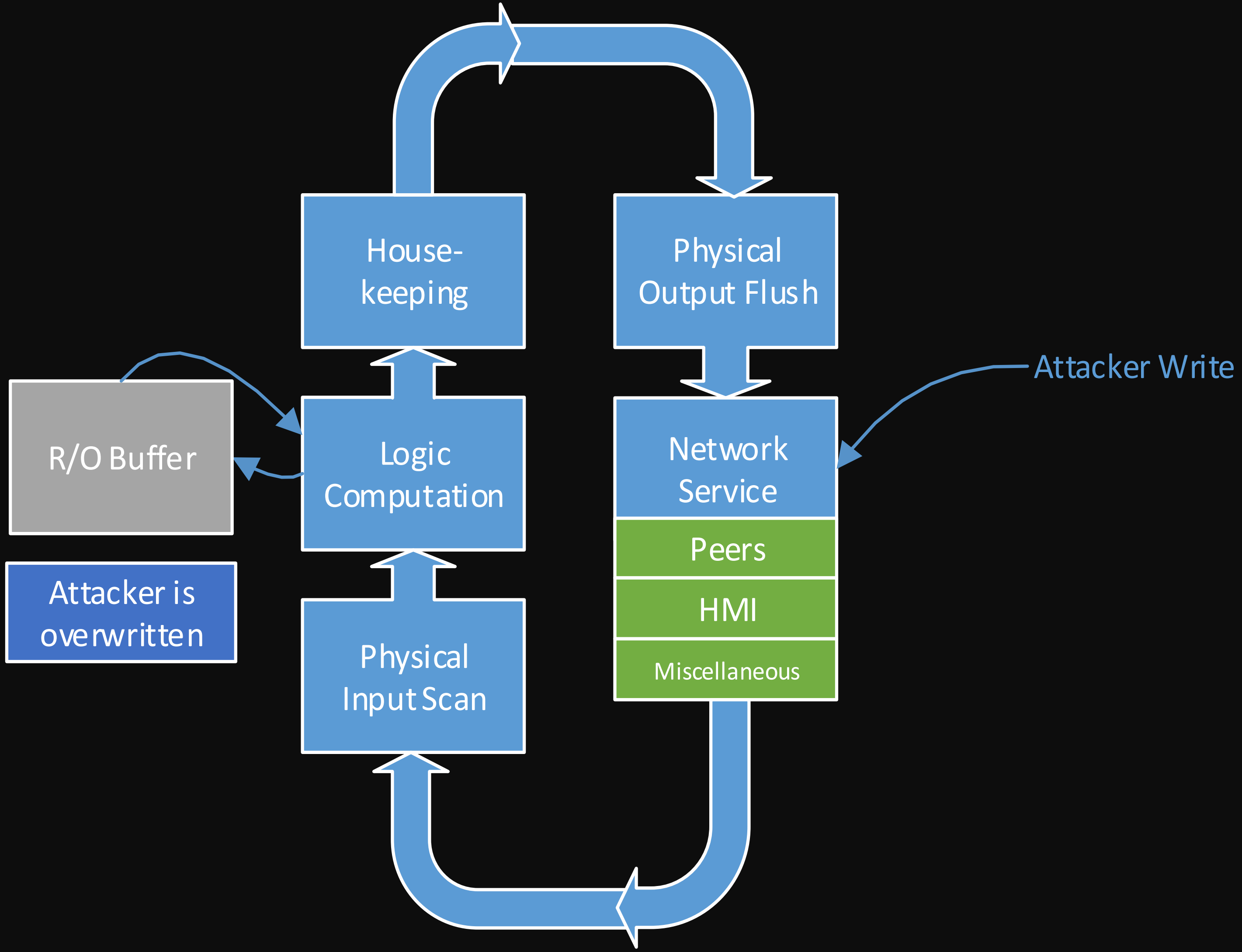


HMI Reads/Writes ONLY from Designated Array/Structure

- All Display Values in R/O Buffer
- All Values written by HMI are Validated
- Context Sensitive Firewall rules easier to handle

How This Keeps Attackers At Bay

1. Attacker Writes to Buffer
2. Logic Recomputes
3. Overwrites Attack Data
4. Network Service Reports no change

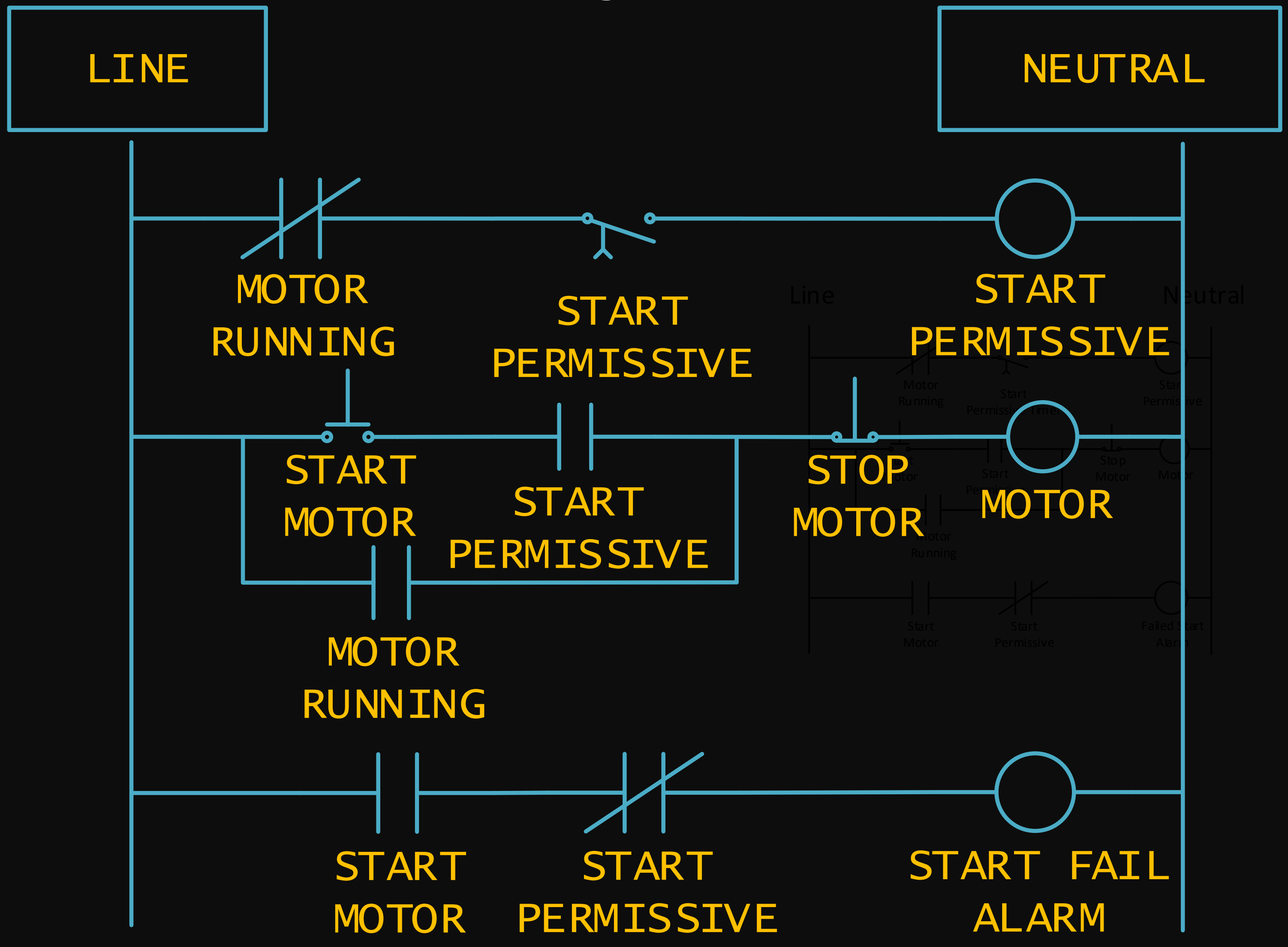


JACOBS®

Validate Inputs and Outputs

- Validate Counter/Timer inputs
  - Do you WANT a value of 655.35 seconds for a 1.35 second timer?
- Debounce/Filter Inputs
- Forward & Reverse, Open & Close, Start & Stop asserted together?
- Have PLC Application Alarm points for HMI
- Limit what you can send/receive to Variable Frequency Drives
  - Consider using 4-20 mA control lines instead of network
- Are motors/actuators being restarted or moved too frequently?

Motor Restart Delay



Motor NOT Running must Time Out before permitting Start Motor Command.

If Attempt to start Motor during this time, raise Start Fail Alarm

This is very over-simplified, please do not use for design purposes

Motor Restart Delay Notes

- Goal: Inhibit restarting a motor until enough energy bleeds off to safely restart

- Note that this is NOT in the PLC
  - Placing hardware inside motor bucket prevents stupid human tricks
  - PLC code can be subverted, this timer prevents damage

- If “Start Fail” alarm triggered, INVESTIGATE

Rapid Diagnostics

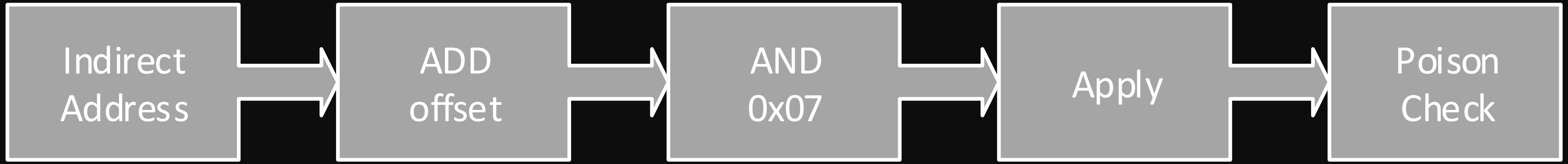
- Do not reuse registers/variables/coils
- General Rule: If PLC Cycle Time longer than AC cycle, WHY?
  - 16.67 mSec in North America
  - 20 mSec in Europe
- Allow for logic disable so inputs and outputs can be validated
- Monitor the control voltage in a motor bucket
- Monitor 4-20 mA loop current from power supply
- Latch transient events in PLC in case remote polling is not frequent enough to catch them

Validate Indirect Addresses

- Avoid indirect addressing if you can
  - Reasons for using them:
    - Lookup Tables for Non-linear functions
    - Sequencing & Staging many of the same assets
  - Set Hard Boundaries for Indirect addresses
- Consider using array w/ binary sizes: 8, 16, 32, etc.
- Check addresses before reading/writing them
  - ADD offset, AND with mask to prevent anything past boundaries
  - Catch fence-post errors by poisoning ends of array
  - Alarm on poisoned values

Safety with Indirect Addressing

Array Member 0	Array Member 1	Array Member 2	Array Member 3	Array Member 4	Array Member 5	Array Member 6	Array Member 7
Value= 65535	Value= 45	Value= 34	Value= 23	Value= 12	Value= 8	Value= 65535	Value= 65535


Indirect Address

ADD offset

AND 0x07

Apply

Poison Check

Peer To Peer Automation

- For critical PLC to PLC traffic
  - Use separate port
  - Consider using a Crossover Cable
  - YOU STILL NEED TO VALIDATE YOUR INPUTS!
- Do Not use OPC DA through an HMI
  - This used to be popular
  - HMI would become a critical asset
  - HMI attack surface is large
- Monitor Peer to Peer with a heartbeat function
  - Validates that both PLCs are live and operating somewhat nominally

Using Internal Status Registers

- Trap and report flags
  - Integer overflow
  - Divide by zero
  - Scan Overrun
- Track communications statistics (errors, total packets received, etc.)
  - Synchronous reporting of packets sent and received
  - Compare to Master station –should match!
- Report code version with hash
- Report changes in communications port states

Avoid Sets and Resets

- Hazards similar to Goto Command
  - Sometimes there is no substitute
  - Discourage its use
- There shall be only one Set/Reset instance per point
- Group S&R together so that you can find them both
- Do not assert a Set or Reset continuously
- Do not assert Set and Reset together
- Set up and latch alerts to let you know if this happens

- Why? It makes diagnostics easier!

Secure PLC Programming

March 16, 2020

JACOBS®

www.jacobs.com | worldwide