Security Issues and Their Relationship to PI

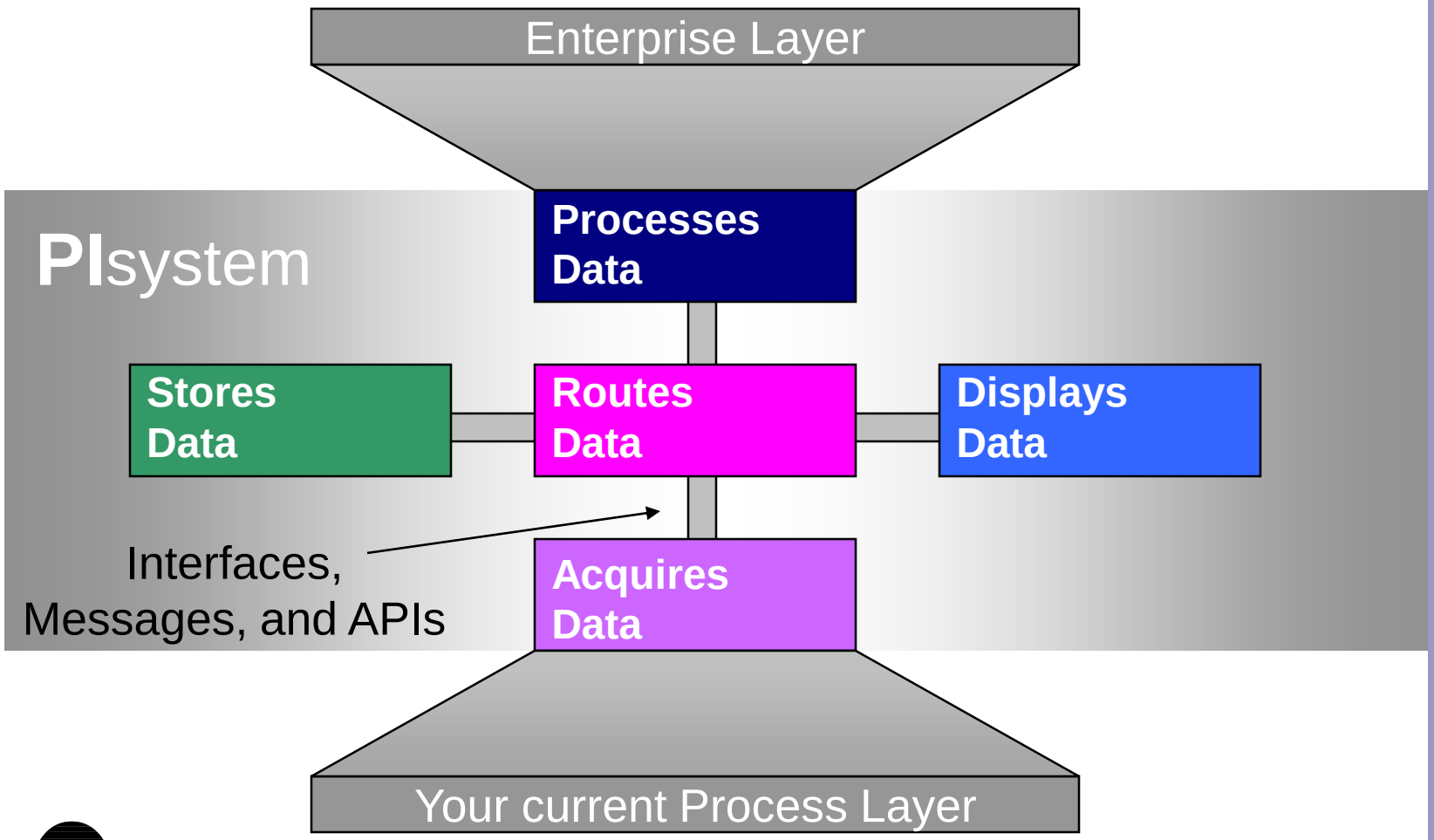
Ralph Mackiewicz – SISCO, Inc.

OSIsoft PI T&D Users Group Meeting

September 18, 2003

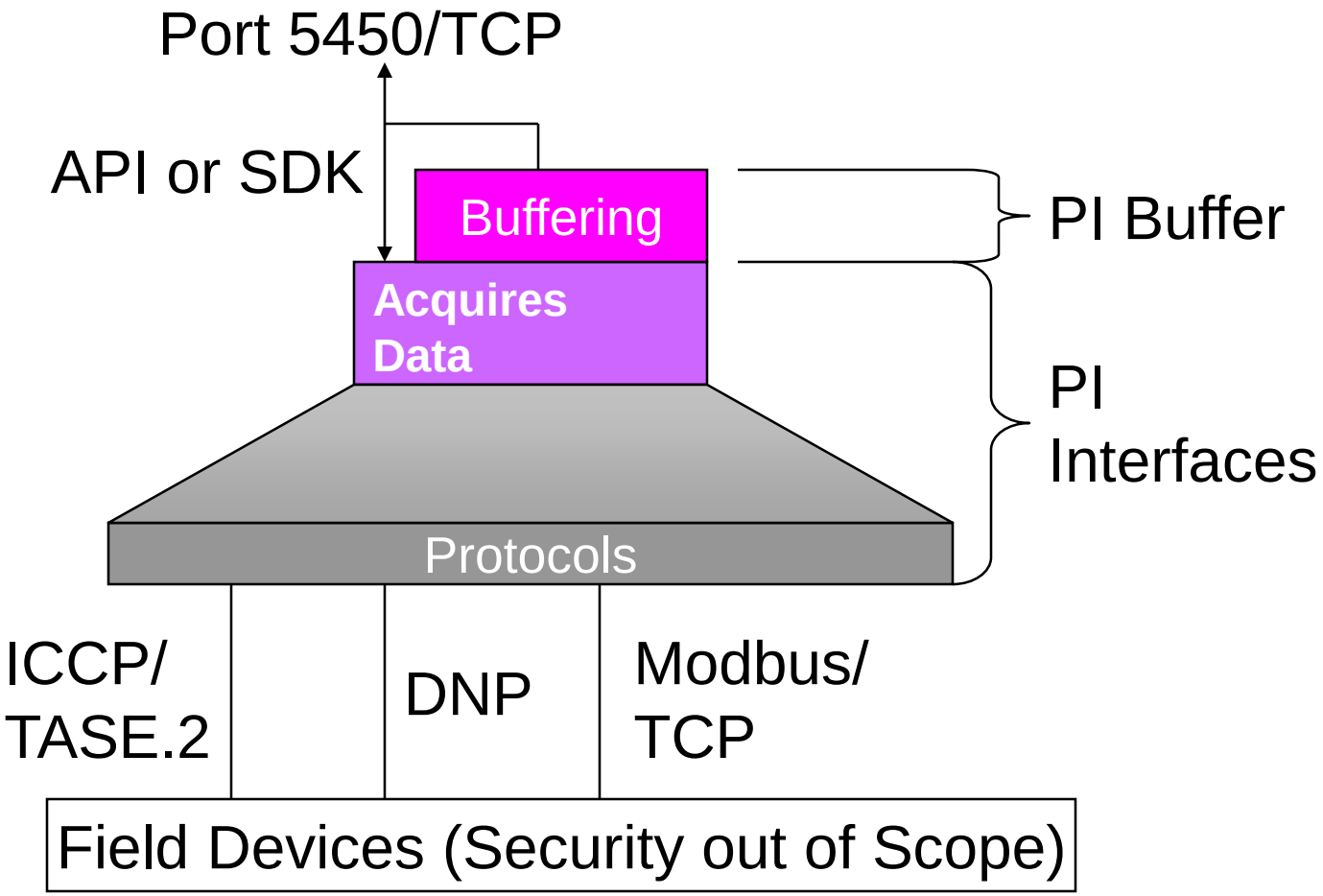
Sacramento, CA

What is PI



SISCO

Acquisition



Securing the Protocols

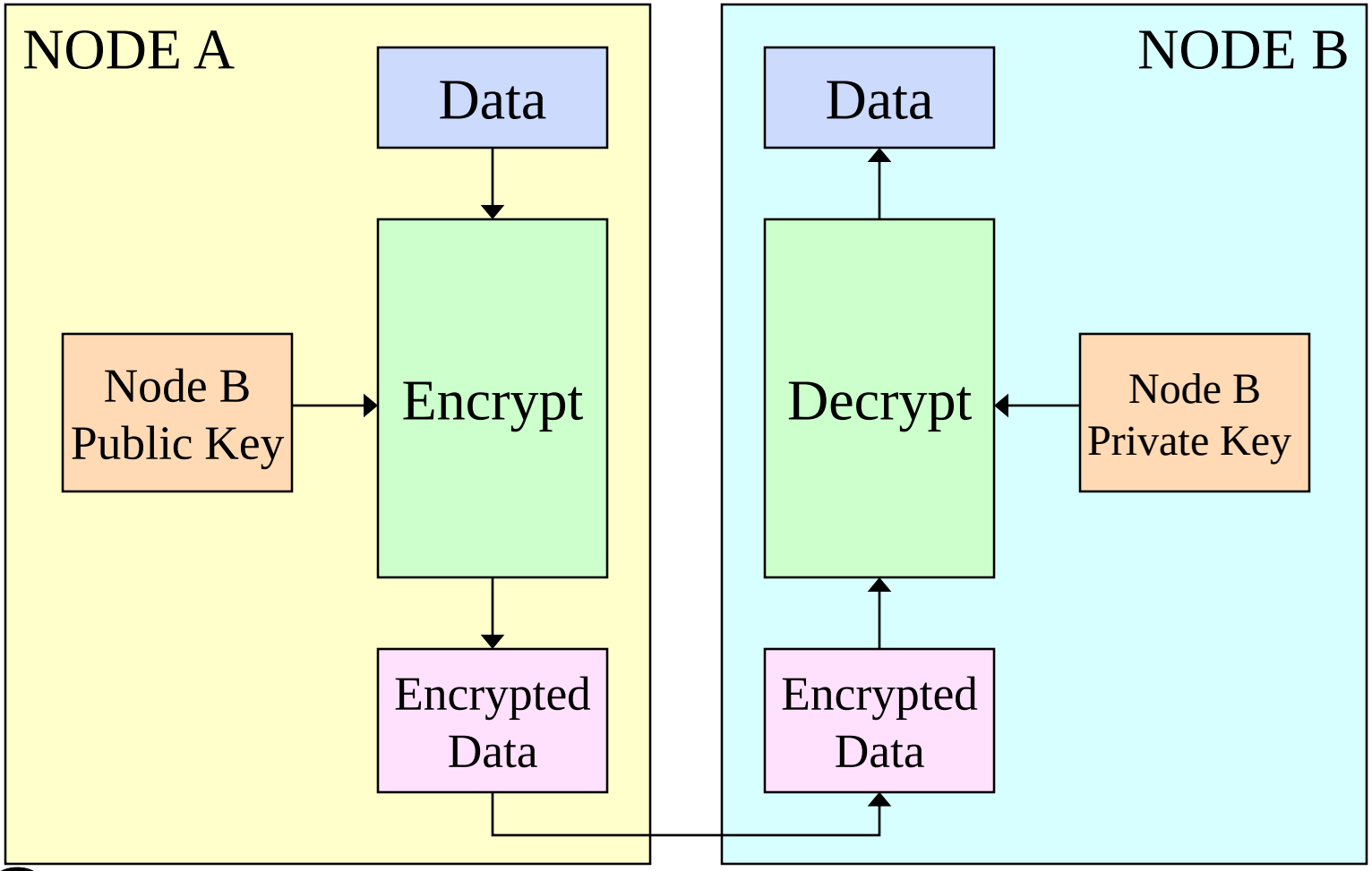
- Intranet usage needs to be evaluated in regards to:
  - Confidentiality (provided by encryption)
  - Integrity (provided by message authentication)
  - Authentication (e.g. username/password)

ICCP and DNP are being secured as part of IEC TC57 WG15 (neither requires VPN usage)

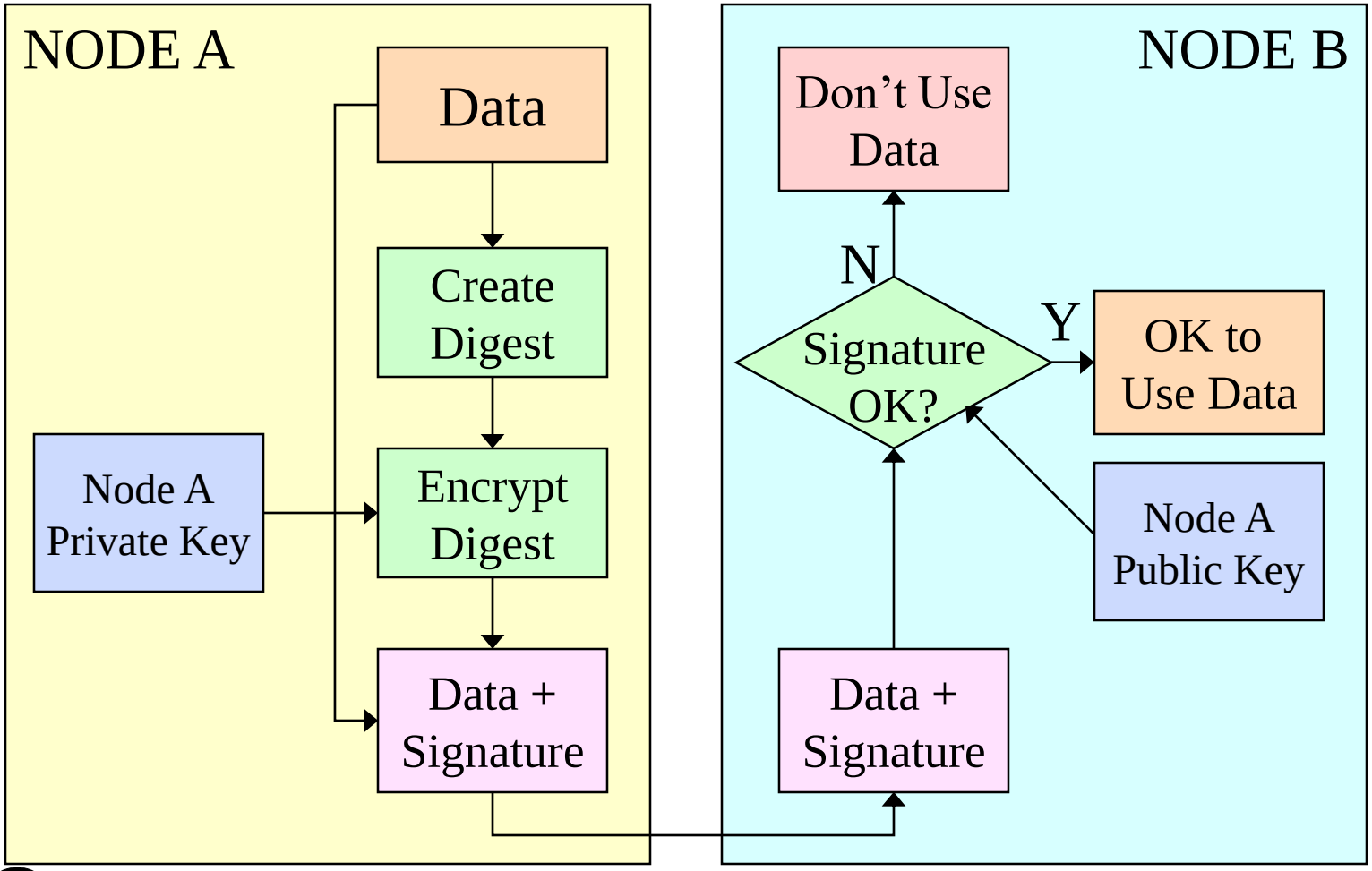
Modbus has no standards body, suggest VPN usage.

SISCO

Public Key Encryption



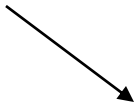
Digital Signatures



SISCO

PI Interfaces (DNP Example)

No User-Password Means No Authentication



The following is an example file:

```
REM                                                    PIDNP3.bat
REM ------------------------------------------------------------------
REM
REM Sample startup file for the FLS ECS Interface to the PI System
REM
REM ------------------------------------------------------------------
REM
REM Required command-line parameters
REM         /ps=x                    Point Source
REM         /xml=path   Path to device config File
REM         /id=x                    Identifier and instance number
REM
REM Optional command-line parameters

REM         /f=SS                                  Defines the period between
scans in
REM                                                seconds
REM         /dnpdbg=level            Specifies the level of debug messaging
REM         /event=class             Defines the scan class as event type data
REM         /host=host:port          PI server node
REM
REM Sample command line
REM PIDNP3 /ps=P /id=1 /f=5 /f=10 /f=12:00:00 /event=3:1 /ec=20
/dnpdbg=0x013F /xml=C:\PIPC\Interfaces\PIDNP3\PIDNP3.xml
REM ------------------------------------------------------------------
REM Revision History
REM Date      Author Comment
REM 20-Mar-02 JAC     Written
REM ------------------------------------------------------------
```

SISCO

Need for Additional Security

- If API nodes are outside the PI server(s) fire-walled network.
  - Need Authentication
  - Possibly Need Encryption
  - Want it to be transparent
- Can use:
  - Stunnel (a SSL generic wrapper) (http://www.stunnel.org)
  - IPV4-V6 Bridge on Windows XP.

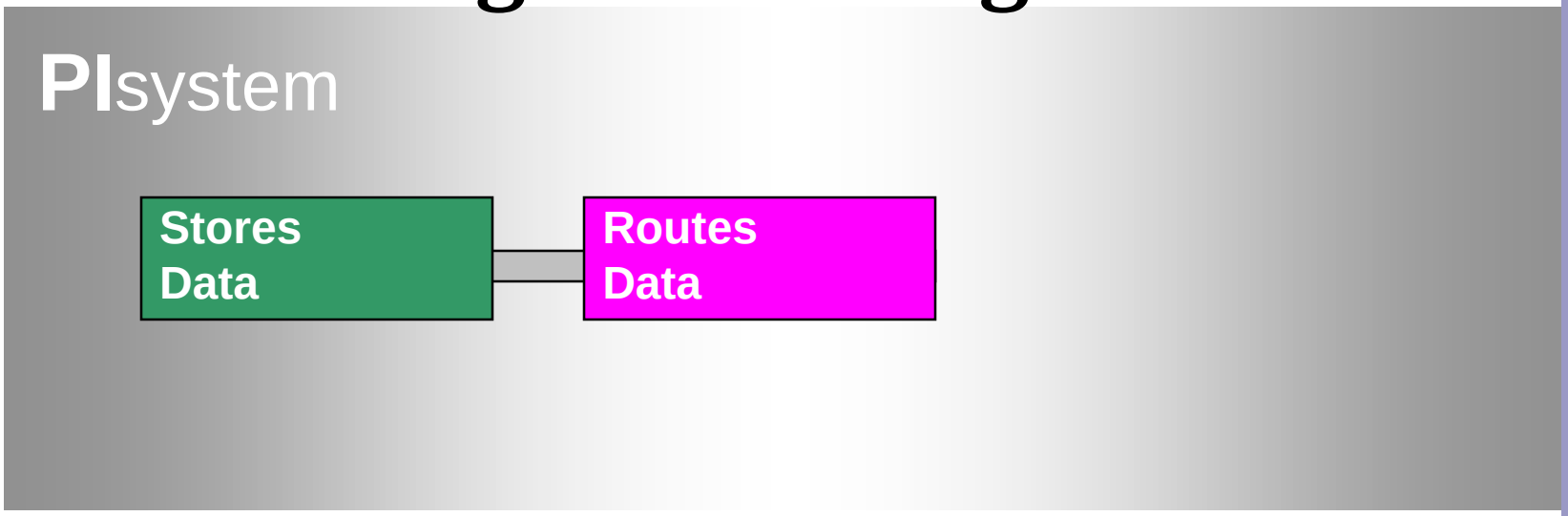
SISCO

What is Stunnel?

- GNU Product
  - Certificate based configuration for authentication and encryption.
- Free for both commercial and non-commercial use.
- Source code available.
- Binary available for Windows based environments.

SISCO

Routing and Storage of Data



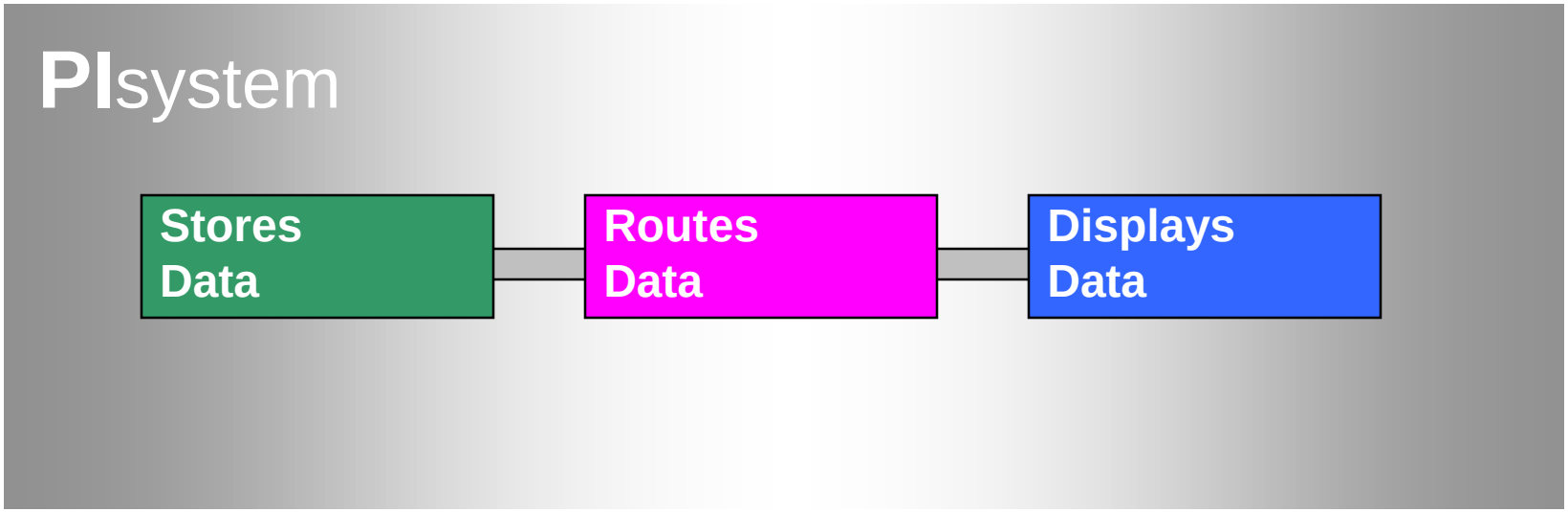
Typically in a controlled, fire-walled environment.

Typically on the same machine.

NT User Authentication and security (properly implemented) provides enough functionality.

SISCO

Processing Data



Four different Displays:

- Custom (e.g. VB)
- ProcessBook
- ActiveView
- PI ICE (Http/Web services)

SISCO

Custom, PB, and ActiveView Displays

- Both allow applications to use NT Security for login administration.
  - Applications must be constructed to make use of this ability (and not just an open PI Admin account).
- If encryption is needed, then Stunnel could be used (or equivalent).

SISCO

PI ICE

- Secure environment provided if properly configured.
- Make use of HTTPS for encryption.

SISCO

Summary

- PI products can be made extremely secure:
  - Proper administration of OS is required
  - Determination of where strong authentication is required.
  - Determination of where encryption is required based upon deployment topology.

SISCO

Thank You

Ralph Mackiewicz
SISCO, Inc.
6605 19½ Mile Road
Sterling Heights, MI 48314 USA
Tel: +586-254-0020
Fax: +586-254-0053
E-Mail: ralph@sisconet.com