

①

RTAC OUT OF BOX

1. HTTPS / WEB → SET USER ACCT & ETHERNET PORTS
THEN 2. AL SELEATOR RTAC FOR PROJECT SETUP → SETTINGS, PULLING IED DATA, PULLS RELAY TO SCADA ~~LOGIC~~, RUNNING USER LOGIC
- ALSO →
• DIAGNOSTICS
• NETWORK CONFIG
• ALARM / SDE LOGS
• RELAY OSCILLOGRAPHY

COMMON RTAC APPLICATIONS

- PORT SWITCH
- DEVICE SERVER, PORT SERVER, NETWORK GATEWAY
- PROTOCOL TRANSLATOR / GATEWAY → SEL PROTOCOL → DNP → SCADA
- PPL, PLL LOGIC PROCESSOR → GATHER DATA, COMPARE, SHARE
- SECURITY GATEWAY → DIVIDES SCADA FROM SUBSTATION NETWORK → AKA PMU'S PHASOR MEASUREMENT UNITS
- SYNCHROPHASOR PROCESSOR → TO COMPARE ANGLES OF MAGNITUDE B/W LOCATIONS @ SPECIFIC TIMES
- TIME SYNC

SECURE REMOTE ENG. ACCESS

VIA RADIUS OR LDAP → ~~ARE~~ CENTRAL AUTHENTICATION SCHEME SO USER AUTH SETTINGS CAN BE SET FROM CENTRAL / CORPORATE SERVER V.S CHANGING AUTH. SCHEMES ON EVERY RELAY.

HMI

3555 + 3560 CAN RENDER HMI LOCALLY

★ IP OF PC SHOULD MATCH SUBNET OF RTAC FOR TCP/IP COMM.

EXE-GUARD

TAKES SNAPSHOT / IMG OF RTAC W/ ROOT & SOFTWARE AND IF ANY CHANGES OCCUR → IT SETS ALARM BIT ^{THAT} MAPS TO SCADA /

OPTIONALLY CAN SHUT RTAC DOWN

[RTAC → RUNS EMBEDDED LINUX, CANT GET TO SHELL OR RUN APPS]

RTAC USB IP: 172.29.131.1

FROM WEB DASHBOARD:

POST SUMMARY - PHYS. CHECKS
CURRENT PROJECT
FIRMWARE VERSION

NETWORK SETTINGS

NIC → TURN PORT ON/OFF

ETHERCAT → ACTION TO

BOND → BOND TWO INTERFACES LIKE
BACKUP FAILURE REMOTE

BRIDGE → ACT LIKE UNMANAGED SWITCH

DHCP → AUTO IP ASSIGNMENT, NEEDS
DHCP SERVER

IP: x x x y/z ← SITE

REPORTS

CONNECTED IED
SHOWS INTERFACES

IF FORGOT PASSWORD:

- JMP 6 TO POSITION C
- USER: EDISON
- PASS: BLANK

SOLVING RTAC CONNECTIVITY - USB FRONT PORT

1. CONFIRM PRESENCE OF SEL USB ETHERNET / RNDIS GADGET
W/ WINDOWS DEVICE MGR.

2. USE IPCONFIG / PING TO VALIDATE CONFIG

↳ RTAC SHOULD PROVIDE NEW IP ADDRESS ON
THAT ONE PORT

- ETHERNET

- CONFIRM ABILITY TO PING, THEN:
- CONFIRM NO FIREWALL IS BLOCKING TRAFFIC:

1-CONT

- NOW ADD ACCESS POINT ROUTER
 - DELIVERY PROTOCOL B/W ACCESS POINTS
- CAN BE NAMED ANYTHING
- IDEALLY: SOURCE POINT: ENG_ACCESS_TAP
- WHEN SELECTING DESTINATION ACCESS POINTS
 - ... - AP: DIRECT TRANS.
 - ... - TAP: TRANSPARENT CONNECTION ← THEN, INSERT
- THEN, CONFIRM SOURCE + DESTINATION
- NOW, POU CONNECTION SETTINGS
 - PIN: AUTO-CONNECT → SET TO TRUE (DEFAULT VALUE NOT VISIBILITY)
- TEST W/ QUICKSET: WHEN POINTING TO RTAC, RELAY PROMPT SHOULD RETURN

2 NOW CREATE SERVER DEVICE

ADD > OTHER > SEL PROTOCOL

• SERVER, ETHERNET TUNNELED SERIAL

CONFIG:

COMM - SERIAL TUNNELING MODE: SSH /

SEL - COMM OFFLINE: 300,000

PRE-TERM TIMEOUT: 1

POST-TERM TIMEOUT: 0

TERM STRING: <CTRL-D>

CLIENT IP ADDRESS: [REDACTED]

CLIENT IP PORT: 5000 X

SERVER IP:
3253

TEAM SOFTWARE
CONNECTION

→ BACK TO QUICKSET

COMM PARAMETERS:

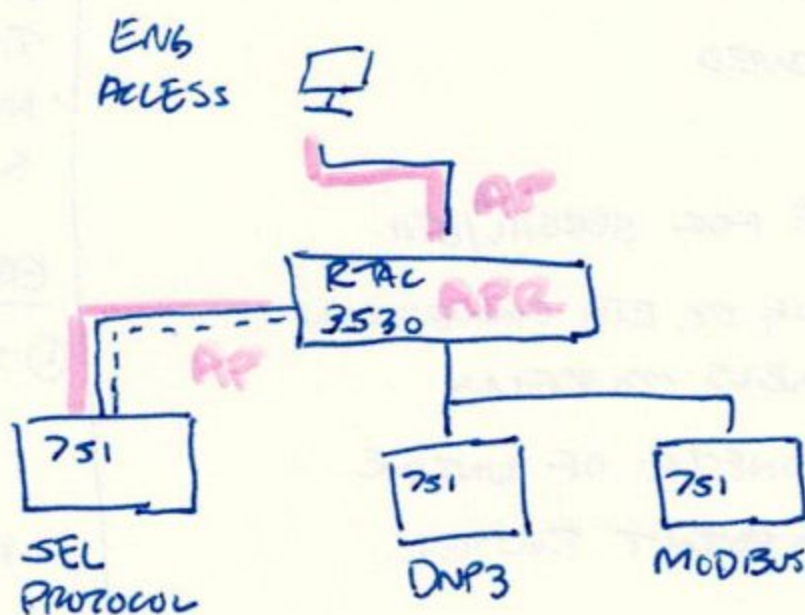
HOST IP: 192.168.2.XX

PORT #: 3253

FILE TRANS: SSH

USER ID] RTAC LOGIN
PASS] NOT RELAY

STATION SYS DIAGRAM



(2)

PROJECT CONFIG.

ALLOCATION RTAL DEFAULTS:

- ADMIN - ENGINEER
- TAIL - OTTER ← ALL CAPS

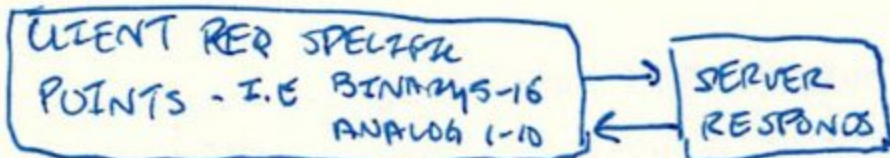
COMPARE PROJECTS

SELECT TWO & RIGHT CLICK

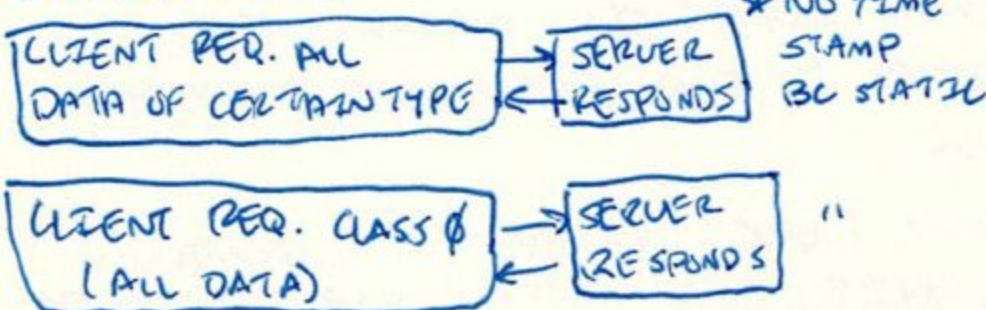
CONFIGURE RTAL TO SPEAK 1ST PROTOCOL
DNP3/IP RTAL CLIENT / SEL 751 SERVER

- IS MASTER / SLAVE OR CLIENT / SERVER
V.S. PEER TO PEER (P2P)
- EVENT BASED REPORTING
 - IED BUFFER FOR TEMP. EVENT STORAGE
 - ANALOG EXCURSION (1. OR QUANTITY)
- BINARY CHANGE OF STATE
 - MULTIPLE CHANGE DETECTION
 - SDE
- EVENT CLASSIFICATION
 - C1
 - C2
 - C3
- OBJECT-BASED FORMATTING
 - DOESN'T HAVE DIRECT MEMORY ACCESS LIKE MODBUS
 - OBJECT TYPES
 - VALUE
 - CHANGE
 - FROZEN

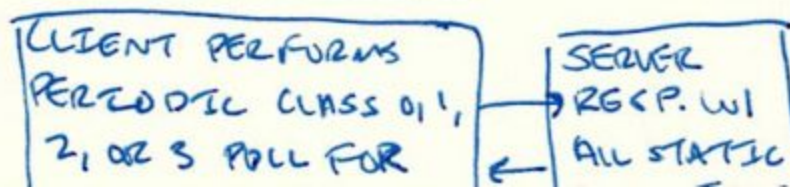
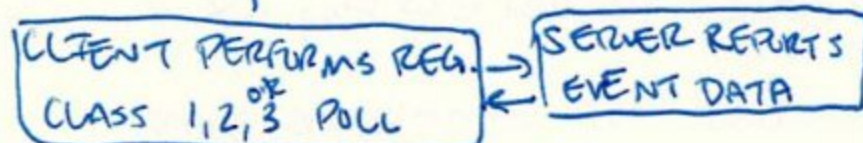
TRADITIONAL POLL REQUEST



STATIC POLLS



REPORT BY EXCEPTION & ONLY CHANGES



DNP3 - BINARY INPUT
MODBUS - DISCRETE INPUT
SEL PROTOCOL - RELAY WORD BIT
E+. LED1, 52A, PB9

CHECK TCP PORTS:

- CAN YOU SEE ME. ORG Port
- TELNET 172.29.131.1 443
- NMAP -p443,1217,... 172.29...
ALL PORTS IP
- POWERSHELL WIN-R
- TEST-NET CONNECTION

COMMAND:
!HOSTNAME

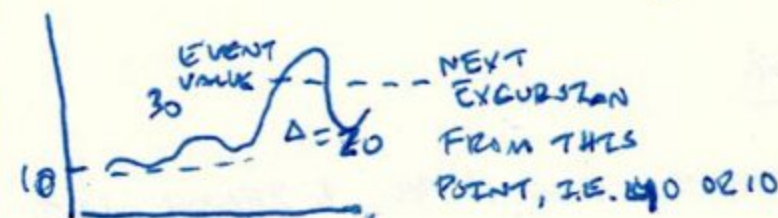
CONNAME 172... -PORT 443

CLASS DATA

TYPICAL:

- BINARY = 1
- ANALOG = 2
- COUNTER = 3

ANALOG DEADBAND EXCURSION



TAGS & VARIABLES

[TYPE: (SPS) QUALITY OF INFO.]

TAGS - DATA STRUCTURE

- SPS = SINGLE POINT VALUE
- MV = MEASURED VALUE
- DEVICES, CLIENT (IED) OR SERVER (SLADA)
- SYSTEM TAGS

VARIABLES - SIMPLE QUANTITY

- BOOLEAN = TRUE / FALSE
- INT = #
- CUSTOM IEC 61131 PROGRAMS
- GLOBAL VARIABLES (GVLs)

TAG NAME STRUCTURE:

DEVICE_NAME.TAG_NAME.SUBTAG.SUBTAG...

↳ UNDERSCORE IS ONLY SPECIAL CHAR. ALLOWED

SPS TAG TYPE	ATTRIBUTE	TYPE	DESC.
STATUS	Bool	Quantity - t	Actual 0 or 1 status
t	Timestamp	Timestamp	Quantity of point (ANALOG, GOOD)
		Timestamp	Timestamp of last state change

3

MU TAG TYPE

DNP3 - ANALOG INPUT | MODBUS - INPUT REGISTER | SEL PROTOCOL - METERING QUALITY (EX. FREQUENCY, WATTS, VARs)

ATTRIBUTE	TYPE	DESC.
INST MAG, MAG	REAL	CURRENT ANALOG VALUE, LAST DEADBAND VALUE
q	QUALITY_t	QUALITY OF POINT (INVALID, GOOD, ETC)
t	TIMESTAMP_t	TIME STAMP OF LAST STATE CHANGE (db EXCEEDED)
db, ZERO DB	REAL	DEADBAND, ZERO DEADBAND
RANGE, RANGE_L	RANGE_t, REAL	ANALOG "RANGE" (CHECK ALARM PARAMETERS)

STATIC VALUE RIGHT NOW → If db=10 & STATIC VALUE=100 THEN INST MAG=100 & IF NO CHANGE MAG=0
 IF STATIC GOES TO 115 THEN BOTH VALUES =115

VALUE @ WHICH # WILL DROP TO 0 (USUALLY GREEN)
 ALARM LIMIT SETTINGS (HI, LO)

CMU TAG TYPE

SEL PROTOCOL - PHASOR-BASED (MAGNITUDE & ANGLE) METERING QUANTITY (EX. IA, IB, IC, VA, VB, VC)
 SAME TABLE AS MU TAG, BUT FIRST ROW:

INST VAL, VAL | REAL | CURRENT ANALOG VALUE, LAST DEADBAND VALUE

OPERSPC TAG TYPE

DNP3 - BINARY OUTPUT (DNPC) | MODBUS - COIL SET / CLEAR (MDBCL) | SEL PROTOCOL - BREAKER BIT, REMOTE BIT (SBRCL, SRBCL) (EX. CC, OC, RBO1)

ATTRIBUTE	TYPE	DESC.
Ctrl VAL	BOOL (T/F)	TRIGGER COMMAND (RISING EDGE)
q	"	
t	"	
PULSE CONFIG	PULSE CONFIG_t	PULSE / PERSISTENT CONTROL CONFIG.

TOGGLE ON/OFF

DNPC TAG TYPE

DNP3 - BINARY OUTPUT COMMAND (CONTROL RELAY OUTPUT BLOCK)

ATTRIBUTES	TYPE	DESC.
OPR PULSE	OPERSPC	PULSE COMMAND (CONTROL CODE 0x01)
OPR LATCH ON	OPERSPC	LATCH ON COMMAND (CC 0x03)
OPR LATCH OFF	OPERSPC	LATCH OFF COMMAND (CC 0x04)
OPR TRIP	OPERSPC	TRIP COMMAND (CC 0x05)

④

EX. DNP3/IP: RTAL CLIENT / SEL-751 SERVER

STEPS →

1. OPEN QUICKSET → FOR RELAY!

2. CHOOSE CORRECT COMM PORT

- DEFAULT FOR 751 FRONT PORT IS 9600 8N1

3. READ RELAY SETTINGS

4. PORT1 = ETHERNET PORT

- EPORT ENABLE PORT = Y

- IP: 192.168.1.26

- SUBNET MASK: [REDACTED]

IF
DNP / TCP/IP!
DEMO IS
SERIAL

5. SCROLL DOWN TO DNP

- SET ENDP TO 2

- DNPNUM = 20,000 (DEFAULT)

- DNPADR = 5 (DNP ADDRESS)

6. THEN, PORT1 > DNP PROTOCOL > DNP SESSION 1

- DNP MASTER = 192.168.1.25

THIS IS THE POLLING CLIENT - I.E THE RTAL

- TCP IS TRANSPORT PROTOCOL

- READR1 = 100

THIS IS "REPORT TO" ADDRESS

CLIENT POLLING HAS TO HAVE ADDRESS 100
OR RELAY WON'T REPLY

- DNPMAP1 = 1 (DEFAULT)

7. THEN, IN TREE, SCROLL TO DNP MAPS > DNP MAP 1

- SELECT ELEMENT & ADD/REMOVE TO MAP

- MUST MATCH B/W CLIENT/SERVER SO CLIENT
KNOW WHAT ITS GETTING

8. SEND SETTINGS TO 751

9. TO GET DNP MAP IN EXCEL →

① FILE → PRINT DEVICE SETTINGS → D1 →

② FILE → EXPORT → ALL → SAVE AS → ".XIS"

③ CREATE TAG NAMES VIA MERGE:

= IF (B2 <> "NA", A2 & "-" & B2, "")

10. EXPORT / IMPORT XML FOR A DEVICE

FOR TRANSFERRING SETTINGS / TEMPLATES

① CONFIG. 751 FOR DNP3/IP

② EDIT 751 DNP3 MAP

③ CONFIG RTAL TO POLL 751 VIA DNP3/IP

④ COMM MONITOR & WIRESHARK TO VIEW COMM.
TRAFFIC

NOW, ADDING RELAY IN ACCELERATOR:

① PROJECT TREE

- RIGHT CLICK, CHOOSE DEVICE

② CHOOSE CORRECT PROTOCOL!

③ THEN, CHOOSE CONNECTION TYPE

④ WHEN IP CONFIG, FOLLOWING
MUST MATCH:

- CLIENT IP PORT (DEFAULT) 20000

- SERVER IP ADDRESS (ADDRESS OF
RELAY)

- SERVER IP PORT 20000

+ IF ADDING 2ND: 20001 (AUTO)

⑤ DNP SETTINGS

- CLIENT DNP: 100

- SERVER DNP: 5

- INTEGRITY POLL: 5000 (5 SEC)

- C1,2,3 POLLING: 1000 (1 SEC)

- POLL TIMEOUT: 1500 (1.5 SEC)

- RETRIES: 3 (FOR REALITY)

FASTER FOR SERIAL

SLOWER FOR RADIO

GO LOWER FOR
CLOSED WOP
SYS

USUALLY SET
HIGHER IF
JUST SENDING
TO SLAVE

⑥ CREATE DNP3 TAGS

- BINARY INPUTS (WHAT WERE
EXPECTING)

⑦ PLUS SIGN ON
BOTTOM RIBBON

- START & QUANT: 36 (? ALWAYS)

⑧ COMM MONITOR

SHOWS DNP TRAFFIC

- CREATES .PCAP FILE FOR
WIRESHARK FOR DECODING

* IN HEXADECIMAL

⑤ - WEEK 2

GOALS:

- ① CONFIGURE SEL, MODBUS, & MICROBITS COMM. PROTOCOL APPLICATION SETTINGS
- ② CONFIGURE RTAG TO ALLOW ENH. ACCESS TO CONNECTED IEDS (NETWORK TIME PROTOCOL)
- ③ CONFIGURE RTAG TO ACCEPT & PROVIDE TIME SYNC VIA I-RTG, NTP, & MORE.

MODBUS TCP: RTAG CLIENT / $\left. \begin{matrix} 65122 - \text{NE} \\ 751 - \text{EX} \end{matrix} \right\}$ SERVER

MODBUS REGISTER

- REGISTER MAP USUALLY DEFINED BY MANF.
- USUALLY HARDCODED, IS CONFIGURABLE
- ALL BOOLEAN DATA TYPES ARE SINGLE-BIT REGISTERS
- HOLDING AND INPUT REGISTERS ARE 16-BIT

R/W = HOLDING

R/O = INPUT

REGISTER DATA TYPES & FUNCTION CODES

DESC	DATA TYPE	READ	WRITE
DISCRETE INPUT	1-BIT BOOL	02h	- - -
COIL	1-BIT BOOL	01h	05h 0Fh
INPUT REGISTER	16-BIT ANALOG	04h	- - -
HOLDING REGISTER	16-BIT ANALOG	03h	06h 10h

- SEL DOESN'T HAVE ANY REGISTERS OR OFFSETS FOR MODBUS AND IS ZERO-BASED / RAW

MODICON ADDRESSING

0X - OFFSET FOR COILS
RAW ADDRESS 0 =
MODICON ADDRESS 1

1X - OFFSET FOR DISCRETE INPUTS
RAW ADDRESS 100 =
MODICON ADDRESS 10101

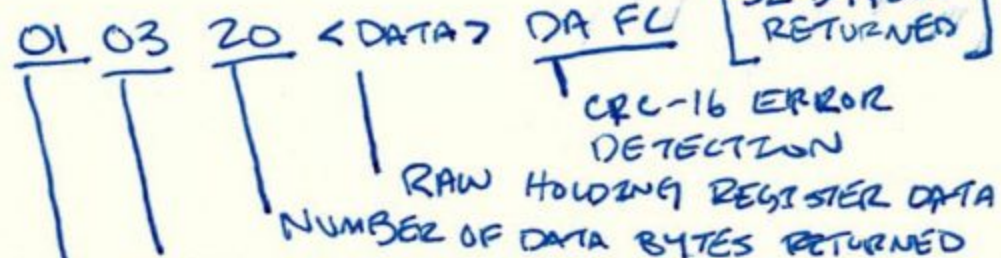
3X - OFFSET FOR INPUT
REGISTERS
RAW ADDRESS = 500
MODICON ADDRESS = 30501

4X - OFFSET FOR HOLDING REGISTERS
RAW ADDRESS = 1350
MODICON ADDRESS = 41351

SAMPLE POLL



EX. RESPONSE



1 BYTE = 2 BITS
★ 16 REGISTERS X 2 BYTES EA =

[32 BYTES RETURNED]

MODBUS TYPES

- ASCII - NOT SUPPORTED
- RTU - SERIAL
- TCP - ETHERNET
- RTU OVER TCP - ETHERNET TUNNELED SERIAL

NEW TAG TYPES - INS

DNP3 - ANALOG INPUT

MODBUS - INPUT OR HOLDING REGISTER

EX. FREQ, WATTS, VAR, COUNTER

ATTRIB.	TYPE	DESC.
SE VAL	DINT	INTEGER BASED
q	QUANTITY	ANALOG VALUE
t	TIMESTAMP	
RANGE, RANGE2	RANGE-t, REAL	ANALOG "RANGE" (HOLD ALARM & PARAMETERS)

TAG - OPERING

DNP3 - ANALOG OUTPUT (INL)

MODBUS - HOLDING REGISTER (INL)

EX. READ/WRITE, SETPOINT VALUE

CELVAL	DINT	INTEGER ANALOG
TRIGGER	BOOL (T/F)	QUANTITY TO WRITE
q	QUANTITY	TRIGGER SETPOINT WRITE (RISING EDGE)
t	TIMESTAMP	

⑥

EXERCISE - MODBUS TCP/RTAL CLIENT/RELAY SERVER

- CONFIG RELAY AS MODBUS TCP SERVER
- CONFIG RTAL AS MODBUS TCP CLIENT
 - CONFIG COMMS
 - ADD TAGS
 - ADD POLLS TO POPULATE TAGS
- USE RTAL WEB PAGE TO GENERATE COMM MONITOR OF MODBUS TRAFFIC

RELAY MODBUS TCP SERVER CONFIG

- IN QUICKSET
- SCROLL TO PORT / ENABLE MODBUS SESSION
 - ENSURE IP IS SET TO CLIENT/MASTER (RTAL?)

RELAY MODBUS USER MAP SETTINGS

- ARROWS MOVE AVAIL. DATA TO MAP

BACK TO RTAL

- ADD DEVICE, BUT W/ MODBUS PROTOCOL
- ADD TAGS → HOLDING REGISTER TAB → (EX. 6)
- THEN, READ HOLDING REGISTER POLLS
 - SET ONE POLL, QTY 6
- VERIFY WORK IN CONTROLLER TAB

CH. 6: SEL PROTOCOL: RTAL CLIENT/SEL-751 SERVER

- SUPPORTED BY ALL SEL ZEDS
- COMBO OF ASCII & BINARY
- SUPPORTS AUTO CONFIG OF TAG DATA

TARGET DATA

- BINARY RELAY WORD BITS
 - PROTECTION TARGETS
 - RELAY CONTACT INPUTS & OUTPUTS

METER DATA

- ANALOG VALUES
 - VOLTAGE, CURRENT, FREQ.
 - FLOATING-POINT FORMAT (PHASORS IF APPROPRIATE)

SEL FAST METER

- BINARY MSGS THAT SCAN & RELIEVE TARGET & METERING DATA
- FORMAT OF BINARY DEFINED BY PRE-CONFIG FOR RELAY WORD-BIT INDEX POSITIONS
- RECEIVED AT STANDARD POLL RATE (NO TIME STAMP)

SEL FAST MSG → UNSOLICITED POLL AUTO CONFIG PROCESS COMMANDS

CRS - COMPRESSED ASCII W/O SPACES AND CHECKSUM & END

SNS - RETURNS SER TAG MAP & INDEX POSITION

DNAX - RETURNS INDEX MAP OF RELAY WORD BITS

Q*ASCII - CONFIG BLOCK → POWER CALL QUANTITIES

FLEX PARSING

OCCASIONALLY, NOT ALL TAGS ARE SEL/SER I.E. WEATHER STATION

- FLEX PARSING IS SUPPORTED BY SEL CLIENTS TO SEND/PARSE ASCII MSG'S IN POLL-RESPONSE STYLE

RTAL FOR NERC PRC-005 COMPLIANCE

- AUTO RETRIEVE EVENTS FROM ALL ZEDS
- ARCHIVE 512 EVENTS IN DB
- PUSH TO ACCELERATOR TEAM
- + ALERT STADA WHEN SETTINGS ARE CHANGED. W/ CONFIG. MONITOR

EXERCISE 70

⑦

CH. 7: RTAC TUNNELED RELAY ENG. ACCESS

SEL PROTOCOLS, ALLOWS UNIQUE ENG. ACCESS
SLIPSTREAMING IN LINE W/ DATA STREAM
[NOT AVAIL. IN MODBUS OR DNP3]

CONNECTIONS

TRANSPARENT:

- RELAY COMM STAYS ONLINE
- POLLING & ENG ACCESS SLIPSTREAMED

DIRECT TRANSP:

- POLLING STOPS
- SHOWS OFFLINE ON RTAC POU PIN SETTINGS
- GOOD FOR TUNNELING TO HMI
- QUICKSET HMI POLLS RELAY FOR BINARY DATA

IF NOT THIS SETTING, YOU WOULD HAVE TWO POLLS RUN

NEW FIRMWARE AUTO SWITCHES THESE TWO

CONFIG METHODS

- ACCESS POINT(S) + AP ROUTERS
- SEL SERVER
 - CONFIG ON RTAC
 - CONNECT W/ TERMINAL PROGRAM

CONNECTION DIFFERENCES

NORMAL OPERATION: ████████ POLLS RELAY 1/SEC

TRANSPARENT

- RTAC POLLING ACTIVE WHILE SESSION IS ACTIVE
- NON-PRINTABLE ASCII CHARACTERS BLOCKED

QUICKSET
FILE TRANS.
REQUIRE
NON-PRINT CHAR.

DIRECT TRANSPARENT

- RTAC POLLING STOPS
- ALL CHARACTERS ALLOWED

ACCESS POINTS

- FLEXIBLE CONFIG MODE FOR SERIAL/ETH
- AP ACCEPTS INCOMING PC ETH CONNECTION ON RTAC & AUTO TUNNELS TO RELAY
- EACH RELAY REQ. CONFIG OF UNIQUE ACCESS POINT & ACCESS POINT ROUTER

SEL SERVER

- CONFIG'S ENG ACCESS TO ALL SEL PROTOCOL DEVICES AUTOMATICALLY
- REQ. LEGALY PORT SWITCH COMMANDS (SEL-2030, 2030, 2032)

PORT SWITCH COMMANDS

- WHO - LISTS ALL DEVICES
- POR * - SELECT DEVICE FOR TRANS. CONNECT
- POR * D - " DIRECT TRANS. CONNECTION
- QUICKSET COMM:
- ALL → ENTER PASS → WHO → POR 254

TELNET PROTOCOL

- PROVIDES VIRTUAL TERMINAL ACCESS TO COMMAND LINE DEVICE OVER ETH. NETWORK USING DEFAULT TCP PORT 23
- TRADITIONALLY USED IN COMPUTING ENV. W/ MAINFRAME & DUMB TERMINAL
- SUPPORTED BY MOST SEL DEVICES
- TRANSFERS DATA IN PLAIN TEXT!!
- NOT SECURE FOR SENSITIVE DATA ON NON-SECURE NETWORK

SSH PROTOCOL

- DESIGNED AS SECURE REPLACEMENT FOR TELNET PROTOCOL
- DEFAULT TCP PORT 22
- MOST-USED REMOTE ACCESS PROTOCOL FOR LINUX & UNIX-BASED COMPUTING SYSTEMS
- REQ. USER AUTH.
- ENCRYPTS DATA BEFORE OVER-TIME WIRE TRANSMISSION
- NOT SUPPORTED BY RELAYS, BUT SUPPORTED BY RTAC & 3600 SERIES

EXERCISE - RTAC TUNNELED RELAY ACCESS

- ① INSERT ACCESS POINT (RTAC → RELAY)
 - CLIENT CONNECT ALREADY A POINT, & NOW NEED ONE GOING RELAY → RTAC
 - ADD ACCESS POINT, ETHERNET INCOMING (LISTEN FOR CONNECT)
 - CONNECTION TYPE: TELNET

8

CH. 8 - RTAC TIME SYNC AND SOE LOGGING

RTAC SUPPORTS:

IRIG-B:

NTP: TIME SYNC OF NON CRITICAL DEVICES

PTP: PRECISION TIME PROTOCOL (SAT. CLOCK TO NETWORK)

DNP3: 1-10 MS SYNC VIA ETH OR SERIAL

IEC 60870: EU STANDARD, SIMILAR TO DNP3
↳ MSG. LATENCY

NON-DETERMINISTIC + RELIANT ON NETWORK

RTAC
SYSTEM
TIME

IRIG-B

OUTPUT
GENERATOR

BNC OUT

DB9 PORTS
PINS 4 & 6

RTAC DEFAULT IS UTC

NTP + PTP NEED DELAYS IN NETWORK THAT SUPPORT THEIR PROTOCOL

IRIG-B IS MOST ACCURATE (NANO-SEC)

PTP - SUB MICRO SEC

SCADA (DNP + 60870-101/4) - 1 MS PRECISION

NTP + PTP - WORK OVER ETH, BOTH HAVE MASTER CLOCK (USUALLY SAT)

- BOTH HAVE DELAY COMPENSATION FOR NON-DETERMINISTIC NATURE OF ETH
+ SWITCH LATENCY

- NTP - NOT GOOD AT COMPENSATING FOR NETWORK

IF PTP TIME SYNCING AT HARDWARE LEVEL, IT WILL ↑ ACCURACY OF MSG RECEIPT

- IF SOFTWARE BASED, IS LESS PRECISE

RTAC HAS INTERNAL CLOCK FOR TIME B/W TIME SYNC.

THAT WAY IT CAN MEASURE DRIFT FROM MASTER CLOCK

IF TIME SOURCE IS LOST, DRIFT VALUE IS USED BY RTAC

TO AUTO-ADJ TIME

IRIG-B TIME SYNC

• OUTPUT FROM GPS HIGH-ACCURACY CLOCK

• TWO WIRE ± SIGNAL (COAXIAL DASHY CHAIN IS TYPICAL)

• 0 TO 5V VARIABLE PULSE LENGTH SQUARE WAVE
(< 0.8V OFF, > 3.2V ON)

• USUALLY UNMODULATED, ONE COMPLETE CYCLE OF 100 PULSES PER SECOND

- IRIG-B002: SEC, MIN, HR, DAY, ONLY BINARY SEC

- IRIG-B006: ALL B002 + ADDITIONAL CTRL FUNCTIONS & ↑ ACCURACY

• REQ. FOR MODERN SYNCHROPHASE-BASED TIMING SYSTEMS

- CAN READ W/ SCOPE

IRIG-B006 CONTROL FUNCTIONS

* IEEE1344 OR 37.118 EXT.

• LEAP SEC. PENDING

• LEAP SEC

• DAY LIGHT SAVING PENDING

• DAY LIGHT SAVING

• TIME ZONE OFFSET

• TIME QUALITY (0 = BEST)
(15 = WORST)



NTP

• TRADITIONAL METHOD FOR TIME

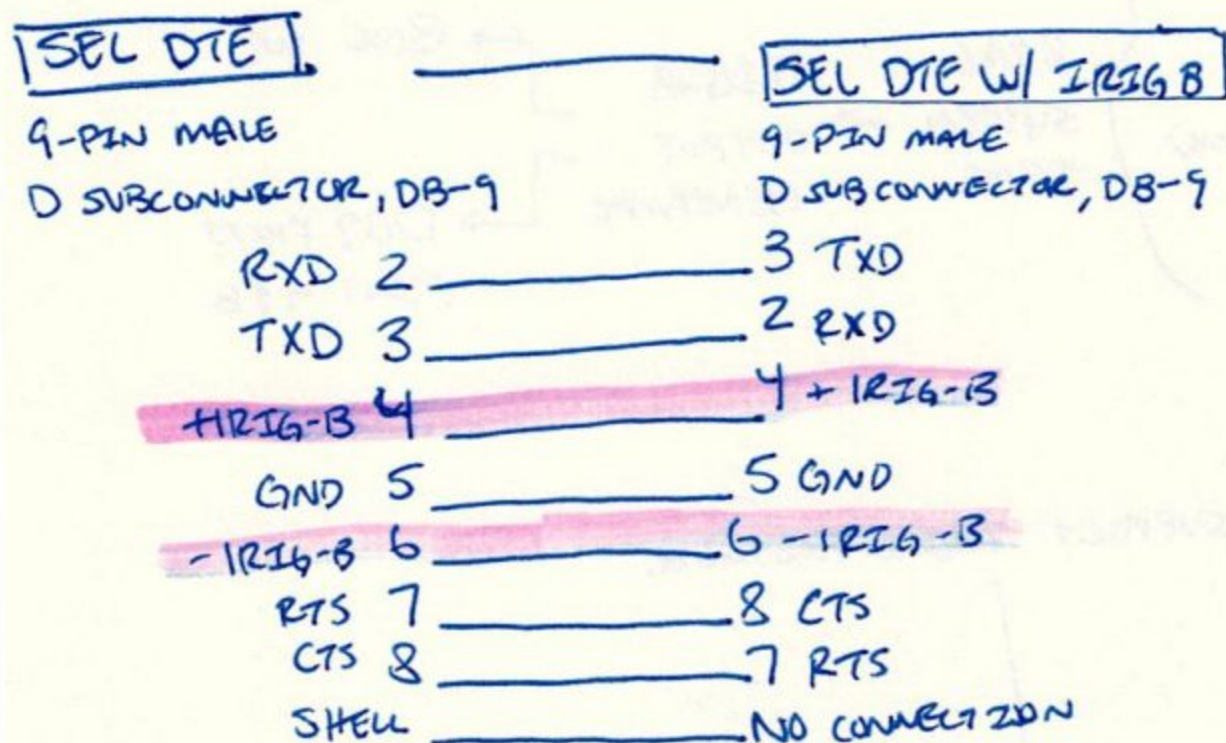
• SENDS UTC TIME VIA UDP/IP

• ACCURATE W/I ± 1 TO 10 MS

• GOOD ENOUGH FOR STD. SOE REQ BUT NOT SYNCHROPHASORS

W/ SEL-C273A CABLE

IRIG SIGNAL VIA SERIAL:



SYSLOG

- STANDARD FOR REMOTE MESSAGE LOGGING
- FOR SYS MGMT + SECURITY AUDITING → [SEQUENCE OF EVENTS]
- RTAL USES FOR ANY NEW ENTRIES IN SDE LOG

WEB INTERFACE → REPORTS / SDE → SEE SYS TAGS FOR LOGS

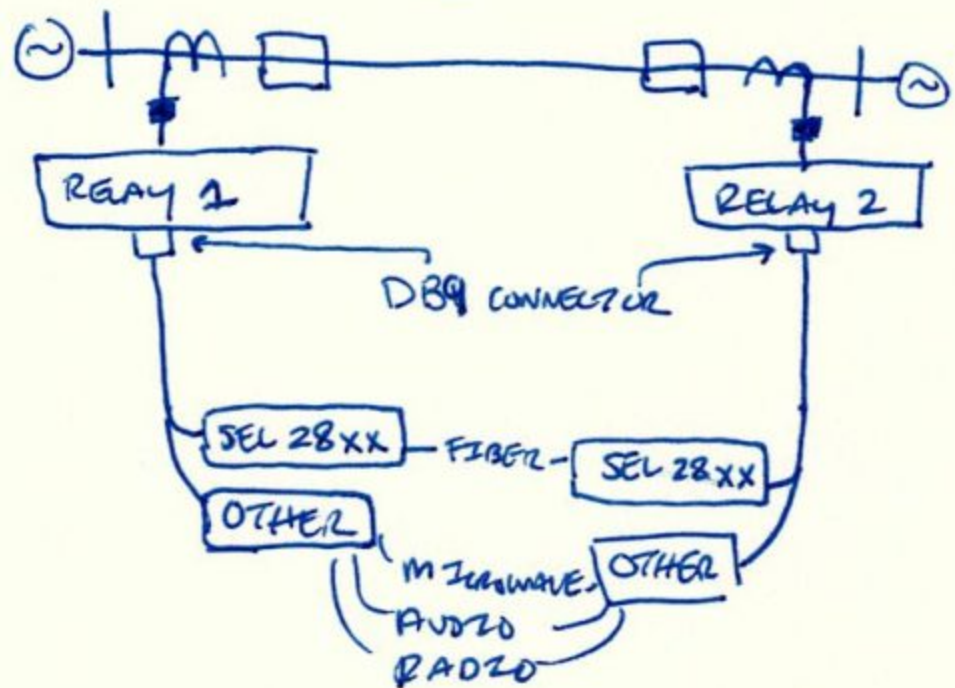
"SYSLOG WATCHER" IS SYSLOG SERVER USED TO VIEW
SYSLOG REPORTS

(9)

CH. 9 - MIRROR BIT COMMUNICATION & IEC 61131-3 INTRODUCTION

SEL PROPRIETARY PROTOCOL FOR PEER-TO-PEER COMM.

- SIMPLE, FAST - RELAY 1 SENDS 8-BITS TO RELAY 2
 ↳ RELAY 2 THEN SENDS 8-BITS BACK TO RELAY 1
 - HAPPENS IN MS
- NOT RLY A MIRROR BC BOTH INDIVIDUAL GROUPS OF 8-BITS



- EIA-232 ASYNC MSH (6-0-1)
- 8-BITS OF MULTI-DIRECTIONAL STATUS/CONTROL
- 10-20 MS TRANSFER TIME
- MB COMM RATE IS 2-8 MS, DEPENDING ON DEVICES

EXERCISE 9

- QUICKSET, PORT X (3 or 5)
- PRTO: MB OR MB8A ← EITHER SO LONG AS THEY MATCH
- CLICK ON MIRROR BIT IN TREE \$
 TXIO: 1
 RXIO: 2 (RTAC WILL SET TO FLIP)

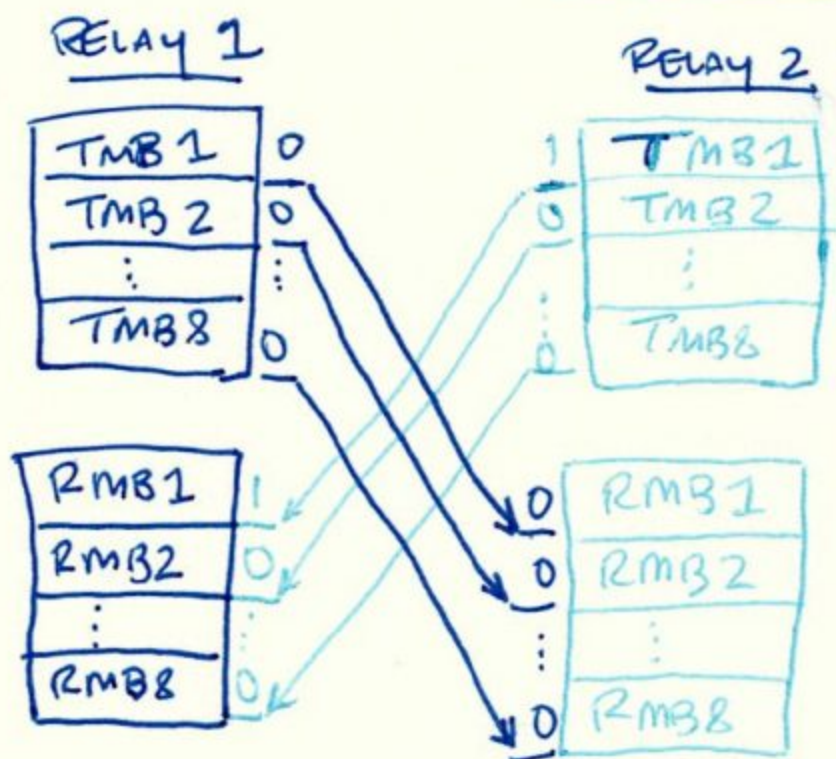
→ NOW, RTAC ACCELERATOR

- ADD OTHER, SELECT RELAY, THEN MIRROR BITS (SERIAL IS ONLY OPTION)
- SETTINGS - PORT: SELECT CORRECT COMM PORT
 DATA: 6
 PARITY: ODD } I.E (6,0,2)
 STOP: 2

NOW, TEST W/ INSERT IEC 61131-3 PROGRAM
 IN POP-UP, SELECT CFC (CONTINUOUS FUNCTION CHART)
 - TOP PART IS WHERE YOU PUT LOCAL VAR'S
 CLICK TOOLBOX TO POPULATE MAP
 + PIN

Turns LED ON/OFF IF MB ACTIVE & ONLINE

TRANSMIT IS MIRRORRED TO RECEIVE

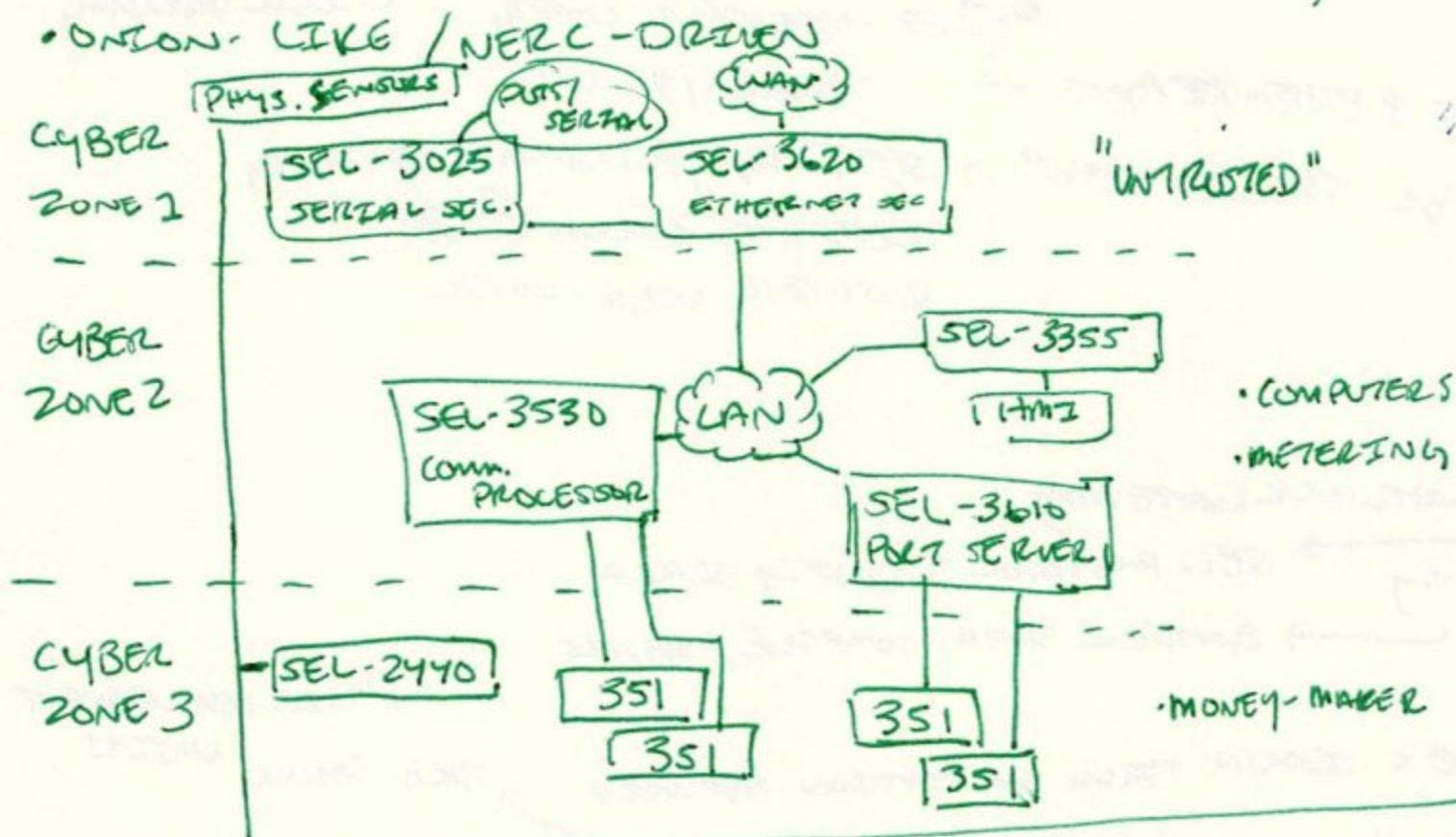


COMM MEDIA REQ.

- FULL-DUPLEX COMMS ✓
- EIA-232 SERIAL PORT INTERFACE (UP TO 38,400 bps)
- IMMUNITY TO POWER SYS FAULT GEN TRANSIENTS
- ACCEPTABLE SPEED FOR APPLICATION

① APP 3620

CYBER SECURITY - ETHERNET SECURITY GATEWAY



SEL-3620 IS ACCESS LAYER

- FIREWALL
- IPSEC VPN'S
- PORT SWITCH
- PROXY SERVICES
- PASSWORD MGMT
- TIME HUB
- CENTRALIZED AUTH
- AUDIT LOGS

SUBSTATION FIREWALL

- DENY BY DEFAULT
- STATEFUL FIREWALL

→ ENCRYPTION BASED ON PRIME #'S BC THERE'S NO FORMULA FOR THEM, THERE HAS TO BE A LOOKUP TABLE →

- OSI REFERENCE MODEL (7-LAYER)
- TELNET - PORT 23
- KUROSE/ROSS COMPUTER NETWORKING
- LISLO - CCNA

ES TOOL DEVELOPMENT

RS6 - RELAY SETTINGS GENERATOR TOOL (RS6GT) → [TOOL: SEL-5231 SEL CONFIG. API]

- TOOL FOR BULK CREATION / MOD OF RELAY SETTINGS FROM RDB FILES
- FOR USE W/ COMMAND LINE OR GUI FOR ACTIONS / EXCEL FOR RDB UPDATES

BROKEN INTO 3 CATEGORIES:

1. SPREAD SHEET GENERATION

- A. WORDBIT & SETTINGS FILE SUMMARY
- B. INPUT STARTING POINTS
 - i. TEMPLATE (FEW TO MANY)
 - ii. SETTINGS UPDATE (MANY TO MANY)

2. RDB GENERATION

3. RDB COMPARISON

- A. ON SETTINGS GENERATION
- B. FILE TO FILE W/ COMMON SETTINGS NAMES
- C. SETTINGS VALUE MATCHING

③ ES - TOOL DEV

STR - SUBNET TO RTAC

- TO CONVERT SUBNET CONFIGS TO RTAC SETTINGS

IEC 61850 - SEL V | RICK BRYSAN

OUTCOMES

- NAME LOGICAL ADDRESSES
- IDENTIFY CONTENTS OF DATASETS
- IDENTIFY SCL FILE TYPES USED IN ACCELERATOR ARCHITECT

61850 IS NOT A PROTOCOL - ITS A STANDARD
+ FOR SUBSTATION AUTOMATION SYSTEMS (SAS)

SECTION 2: COMMUNICATION SERVICES

SCADA

MMS

- PULL / RESPONSE / CONTROLS
- REPORTS / LOGS
- (SLOW - 1 SEC)

TIME-CRIT

- GOOSE
- SV W/ 4 KHZ / 4.8 KHZ
- TIME-SYNCD DATA
- SAMPLES
- (UNSOLICITED)

TIMESYNC

- IEEE 1588
- IEEE C37.238
- PTP (< 1μs)

GOOSE

- PUBLISH / SUBSCRIBE BEHAVIOR
- MULTICAST MESSAGES
- NO DATA CHANGE: PERIODIC DATA PUBLICATION
- HIGH SPEED & DETERMINISTIC
- NO REPLIES OR ACKNOWLEDGMENTS

OSI MODEL

① PHYSICAL

- ELECTRICAL, OPTICAL, WIRELESS COMMS
- ETHERNET, SERIAL CABLES, RADIO COM

② DATA LINK

- DEVICE IDENTIFICATION + ERROR DETECTION MECHANISMS
- EX: MAC ADDRESSES FOR PHYS. ADDRESSING

③ NETWORK LAYER

- ROUTING PATHS FOR DATA PACKETS
- EX: RELAY DATA TRAVELS MULTIPLE NETWORK DEVICES OR SUBNETS. ENCL. WILL CONFIG IP ADDRESSES AND ROUTING PROTOCOLS TO ENSURE MSGS REACH DESTINATION

④ TRANSPORT LAYER

- SEL DEVICES USE TRANSPORT LAYER FUNCTIONS TO ENSURE ERROR DETECTION & RECOVERY DURING DATA TRANSMISSION

⑤ APPLICATION LAYER

- SOFTWARE / HMI
- MISMATCHED CONFIGS
- WRONG PROTOCOL SETUP

OSI LAYER	ERROR TYPE	TEST METHOD	EX. COMMAND / TEST	RESOLUTION ACTION
PHYS	CABLE / PORT	VISUAL OR PING	PING FAILS, NO RESPONSE	CHECK + REPLACE CABLES
DATA	FRAME OR MAC-LEVEL	COM PN	MIRRORED BITS ERROR	CONFIG MAC'S, RESOLVE FRAME ISSUES
NETWORK	IP ROUTING OR UNREACHABLE HOSTS	PING	PING SHOWS PACKET LOSS	RECONFIG IP / SUBNET
TRANSPORT	RETRANSMISSION ISSUES	ARQ (IN SETTINGS)	SLOW DNPS REPLY	ENABLE RETRANSMISSION, ADJUST FLOW
				RECONFIG PROTOCOLS

② ES- TOOL DEVELOPMENT

COMMISSIONING ASSISTANT TOOL - CAT

- FOR COLLECTING SETTINGS & INFORMATION FROM MANY RELAYS SIMULTANEOUSLY AND STORING IN EXCEL AS .XLS FILES

MBT - 16 PORT MIRRORED-BITS TESTER

- RTAC 3530 PROGRAM - GIVES FEEDBACK WHEN BITS RECEIVED
- GO ONLINE IN RTAC ACCELERATOR
- HMI ACCESED, LOOK FOR 'MIRRORED-BITS-CONTROLLER' UNDER GUI
 - DEFAULT BAUD RATE IS: 19,200
 - RXID: 2 ← DEFAULTS
 - TXID: 1 ←

ALO - AUTO CONSTRUCT

- POINT-TO-POINT TESTING FOR DC & AC CAD DRAWINGS

MPL - MAP CREATOR

- AUTOMATES DOCUMENTATION, RTAC, & ZENON HMI SETTINGS FOR DATA COLLECTION PROJECTS
- EXCEL SHEET
- CREATES POINT MAPS TO CUSTOMER FOR INTEGRATION INTO SCADA/DMS
- XML CODE CAN BE GENERATED FOR RTAC IMPORT

CDT - COMPLIANCE AND DATA ANALYSIS TOOL

- UPLOAD CLR FILE
 - DEFINE STUDY AREA
 - SEARCH FOR BUSES
 - DRAG INTO BES OR NON-BES
 - THEN, "SET AREA FOR STUDY"
 - GENERATE REPORTS
 - DISCREPANCY
 - IMPEDENCE
 - TIE LINE
 - ★ SHOULD MATCH ASPEN OUTPUT
1. IMPORT SETTINGS FILE → ONLY FOR TIE-LINE
2. SELECT RELAY
- DISCREPANCY REPORT IS MAINLY FOR IMPEDENCE Δ B/W PRIMARY & SECONDARY RELAYS
 - IMPEDENCE REPORT GENERATES IMPEDENCE IN PER UNIT, INCL. MUTUAL COUPLING INFO THAT CAN BE COMPARED TO TRANSMISSION PLANNING REPORT PROVIDED BY CX
 - TIE LINE IS GOOD FOR SETTINGS DEV. FOR RELAYS