The People’s Republic of Fieldbus

What to know about Ethernet for Plant Automation

DEFCON 32, ICS Village
08/09/24 Friday, 3:00-3:25 PM PST

Jonathan Reiter
Engineer, Dragos
@bees@infosec.exchange

Why should I care?

- Interesting tech
- Peculiar regionalisms
- Geopolitically fraught
- Potential relevance to operators

The Speaker

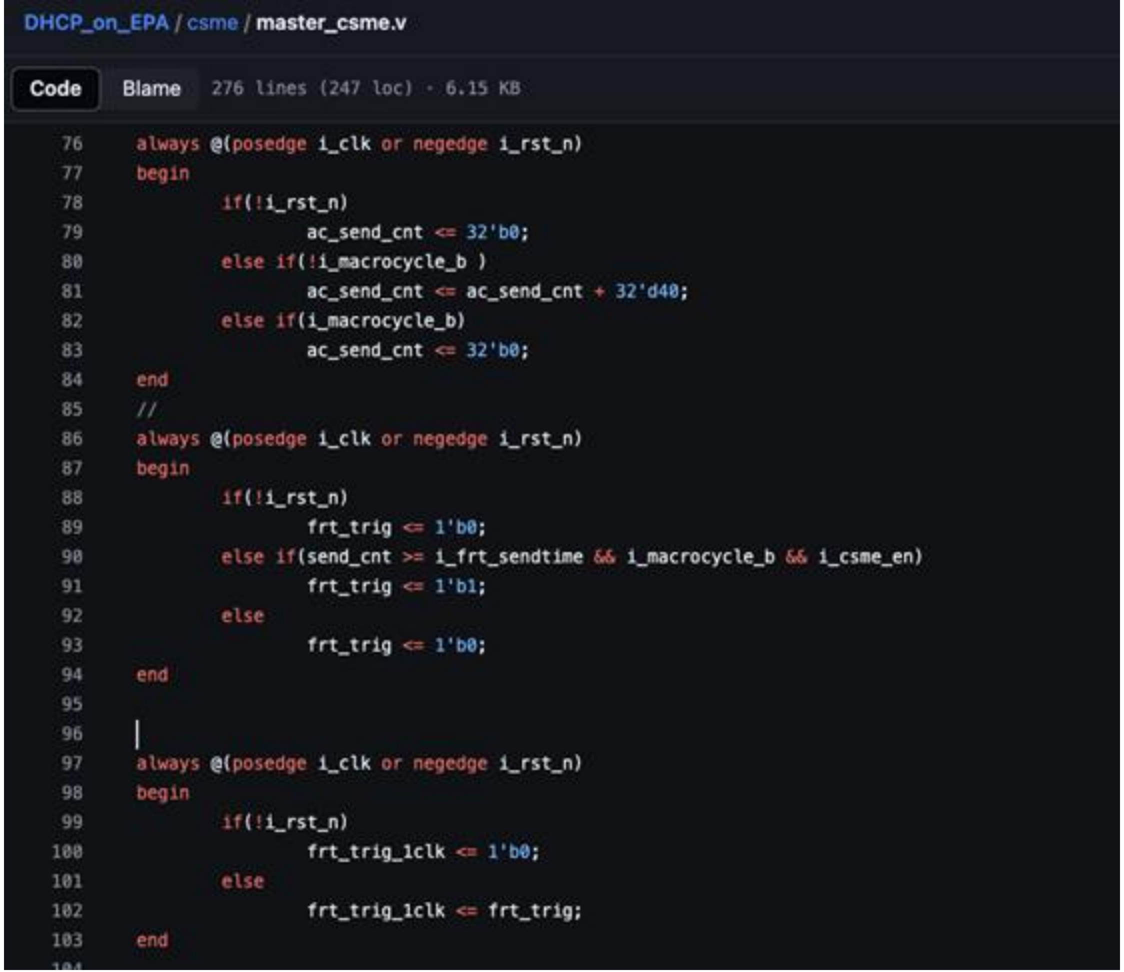
- Some sort of data freak
- Dragos by day
- CTI by night

The Protocol

1. Built on Ethernet
    1. Sometimes traditional (100BASE-TX)
    2. Sometimes beefy (Ethernet-APL, 10BASE-T1L)
2. Real time by encapsulation
    1. Slicing and slotting by MAC, by Ethertype
    2. Determinism via scheduling (EPA CSME)
    3. Comparable: **EPL, TCnet, PROFINET**
    4. Not comparable: **SERCOS, EtherCAT**
3. Designed for compatibility
    1. Two different real time conventions
    2. Streaming media support
    3. Traditional TCP/IP support
    4. Redundancy and safety standards

Layer	Fast Real Time	Real Time	Block Real Time	Not Real Time
Application		**EPA Applications**		IT Applications
Presentation		**EPA socket mappings**		
Session		UDP, TCP		
Transport		IP (ARP, ICMP, IGMP, etc.)		
Network	**EPA_CSME (FRT)**	**EPA Communication Scheduling Management Entity (RT)**		
Data Link	ISO/IEC 8802-3, IEEE 802.11, IEEE 802.15 link layer			
Physical	ISO/IEC 8802-3, IEEE 802.11, IEEE 802.15 physical layer			

From Feng et al 2012


DHCP_on_EPA / csme / master_csme.v
Code
Blame
276 lines (247 loc) · 6.15 KB

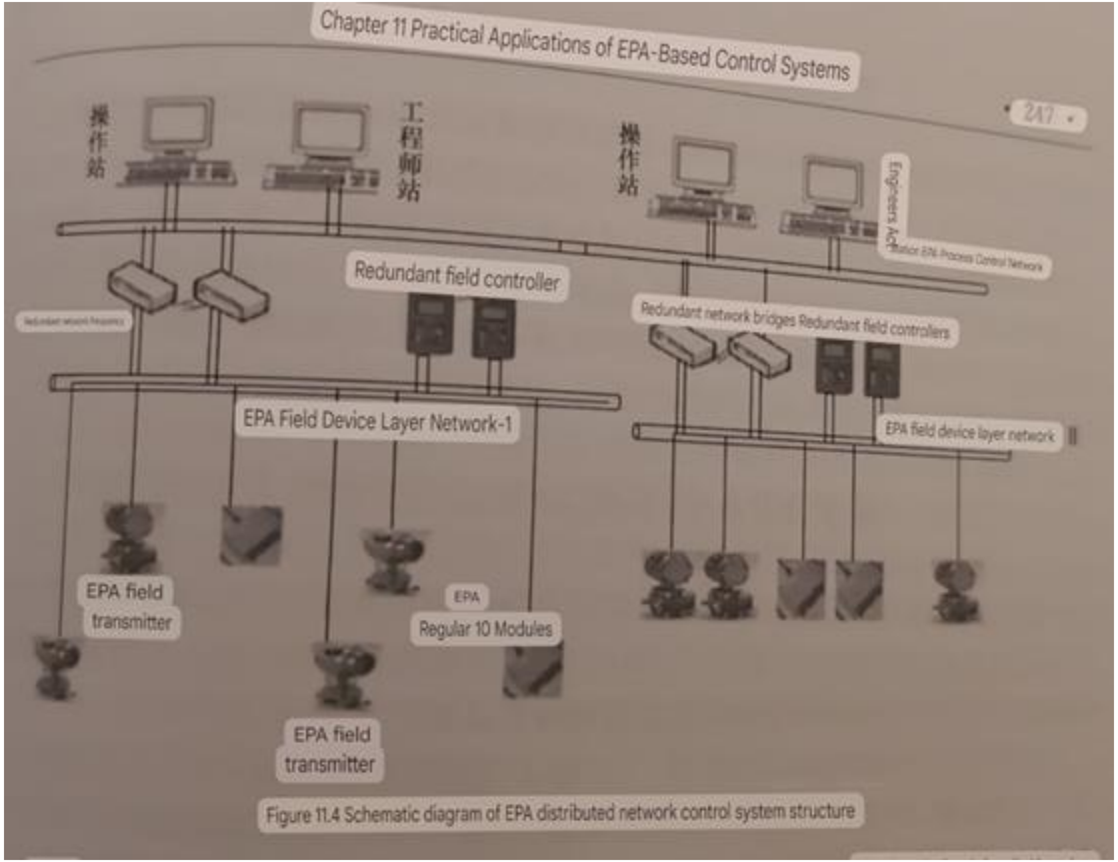
```
always @(posedge i_clk or negedge i_rst_n)
begin
        if(!i_rst_n)
                ac_send_cnt <= 32'b0;
        else if(!i_macrocycle_b )
                ac_send_cnt <= ac_send_cnt + 32'd40;
        else if(i_macrocycle_b)
                ac_send_cnt <= 32'b0;
end
//
always @(posedge i_clk or negedge i_rst_n)
begin
        if(!i_rst_n)
                frt_trig <= 1'b0;
        else if(send_cnt >= i_frt_sendtime && i_macrocycle_b && i_csme_en)
                frt_trig <= 1'b1;
        else
                frt_trig <= 1'b0;
end


always @(posedge i_clk or negedge i_rst_n)
begin
        if(!i_rst_n)
                frt_trig_1clk <= 1'b0;
        else
                frt_trig_1clk <= frt_trig;
end
```

Via caomei123456789

The Players

1. The World
2. The State
   1. 863 Program
   2. IEC triumphalism
3. Big Business
   1. SUPCON
   2. Kyland

Case 1: Greenfield deployment



Chapter 11 Practical Applications of EPA-Based Control Systems

247

操作站
工程师站
操作站
Engineers Act
Station EPA Process Control Network
Redundant field controller
Redundant network bridges Redundant field controllers
EPA Field Device Layer Network-1
EPA field device layer network II
EPA field transmitter
EPA
Regular 10 Modules
EPA field transmitter

Figure 11.4 Schematic diagram of EPA distributed network control system structure

From Feng et al 2012

Case 2: Obsolescence

The Future

1. OSINT
   a. Configurations
   b. Programs
   c. Research
   d. Source code
2. What is not public domain
   a. Implementations
   b. Hardware support
   c. Market share
3. The future
   a. Publish translations
   b. Teardowns and reversing
   c. Open source dissection
   d. More regional standards

Abridged Bibliography

Ditecting, Yu Yao

Tang, Zhang, and Zhang 2011

GB/T 20171

Feng et al 2012

Tan et al 2011

IEC PAS 62409:2005

Li, Zhang, and Peng 2012

Tan et al 2011

Winkel 2006

Lu et al 2013

Zhen 2012

Zhi and Pearson 2016

Felser 2009

Thank You!