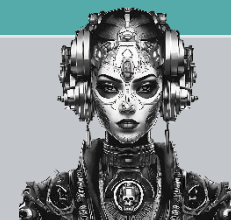




PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



My Computer



WordPad



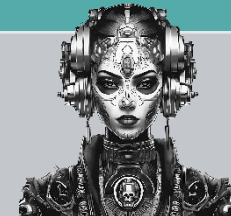
MS-DOS
Prompt



Recycle Bin



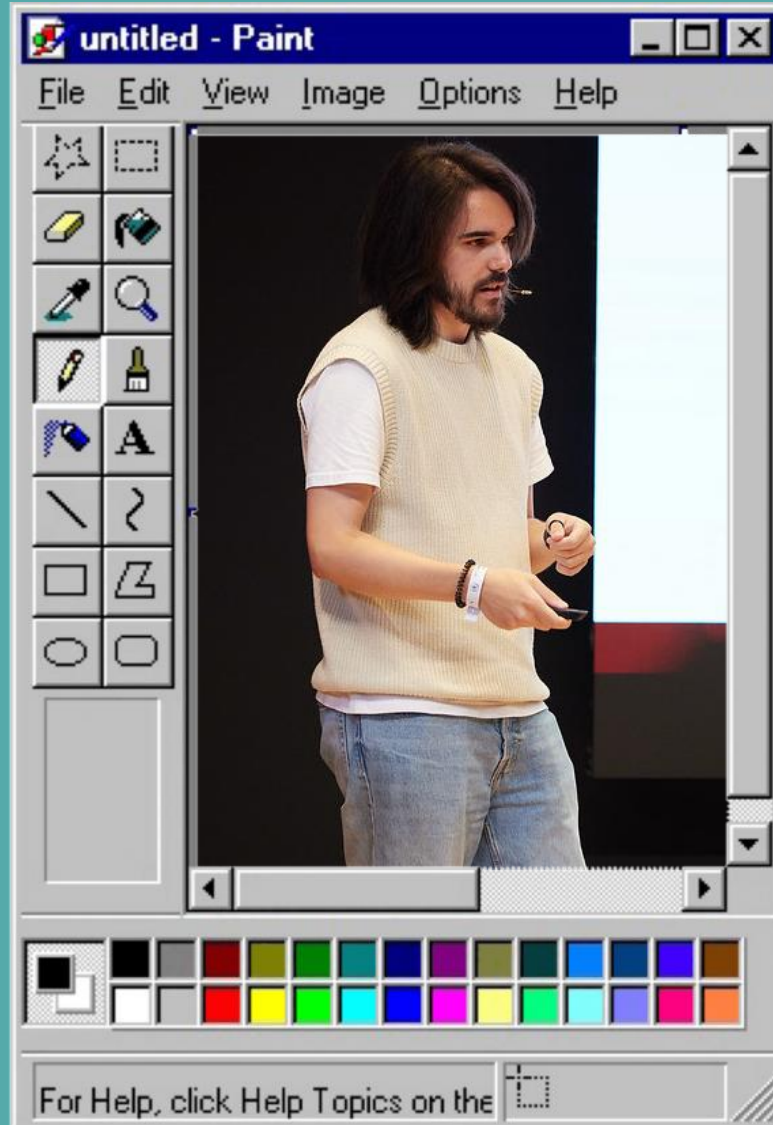
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



General - Notepad

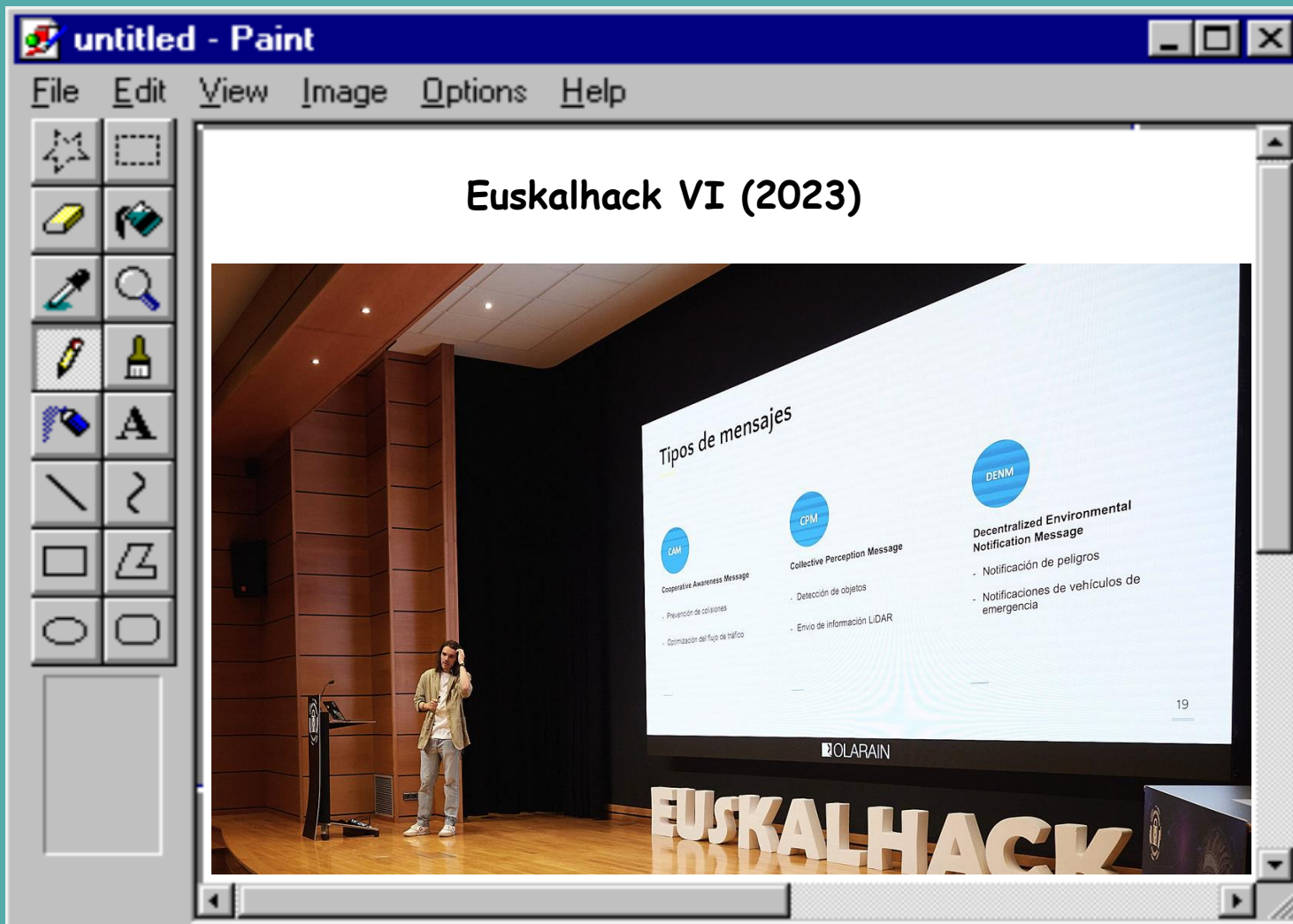
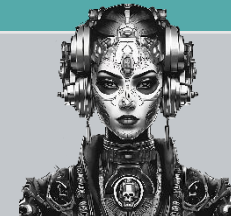
File Edit Search Help

- **Técnico de Investigación | Seguridad Digital - Vicomtech**
2022 - Presente
- **Grado Superior en Administración de Sistemas Informáticos en Red**
2019 - 2021
- **Curso de Especialización en Ciberseguridad en Entornos de las Tecnologías de la Información**
2021 - 2022
- **Grado en ciberseguridad**
2023 - Presente



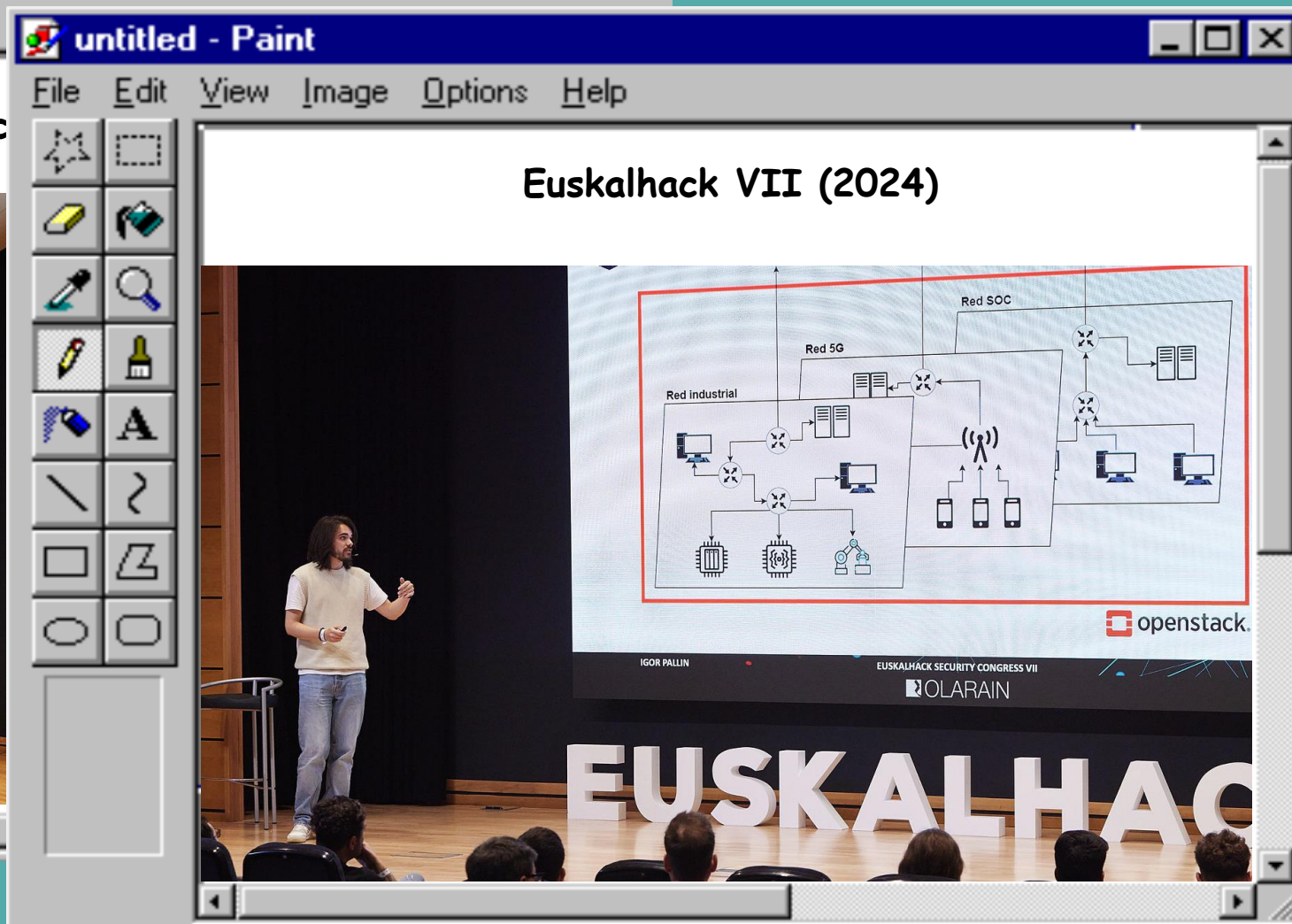
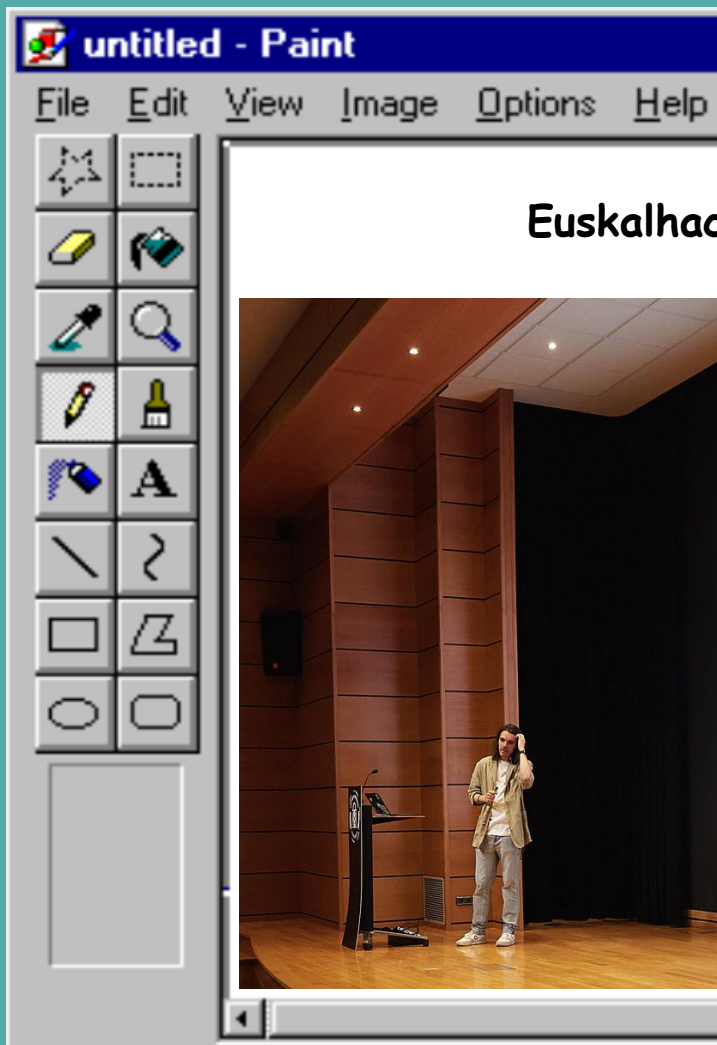
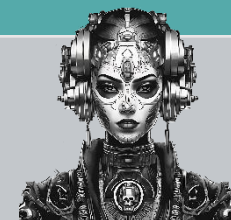


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



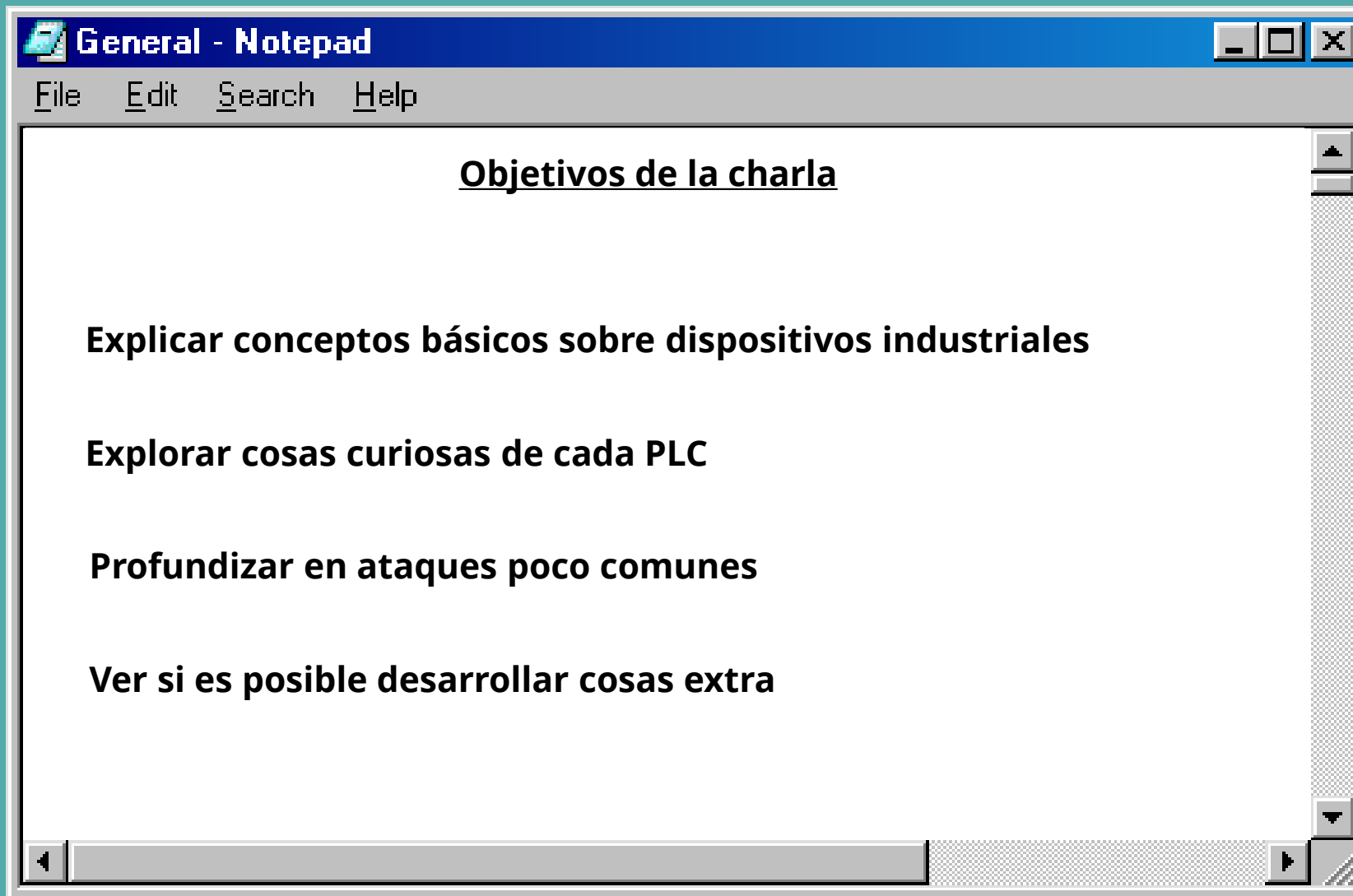
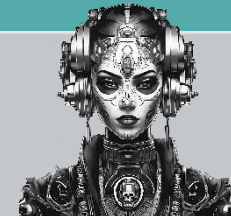


Pequeña aclaración



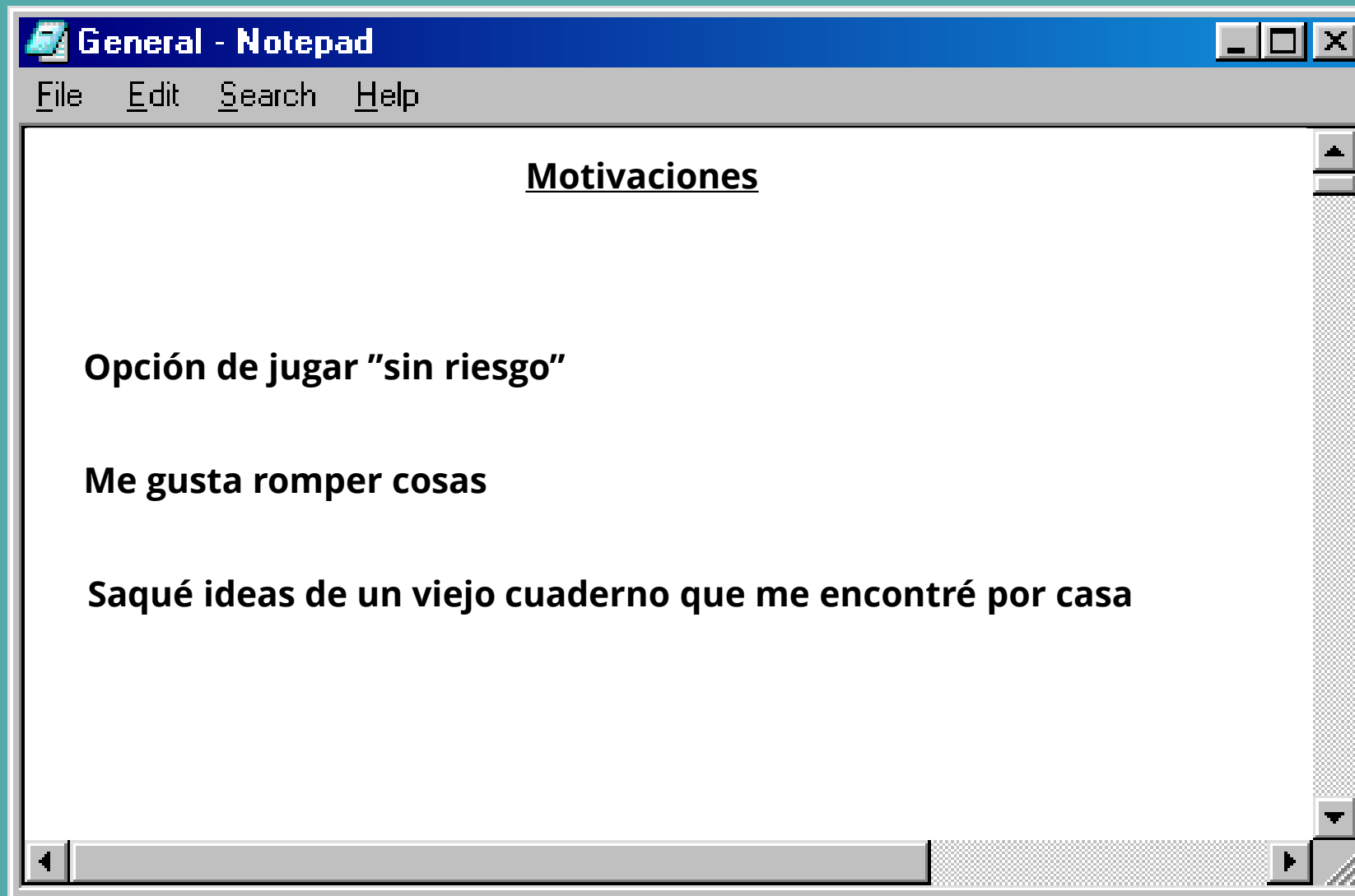
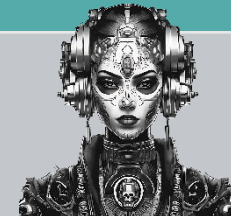


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



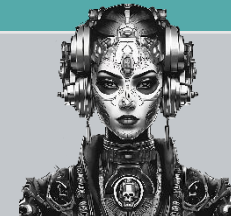


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Index

- Intro
- Qué son los PLCs/IPCs
- Detalles de cada PLC

SIEMENS

B&R

BECKHOFF

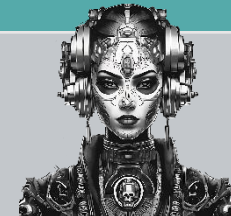
**PHOENIX
CONTACT**

OMRON





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

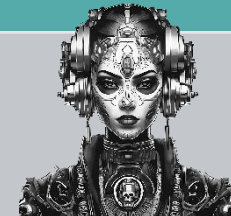
PLC

- **Ejecutan lógica de control en tiempo real**
- **Lenguajes de programación: Ladder, FBD, ST, etc.**
- **Muy robusto: resistente a calor, polvo, interferencias**
- **Modular: se expande con tarjetas I/O, comunicación, etc.**
- **Software de ingeniería propietario (TIA Portal, TwinCAT...)**





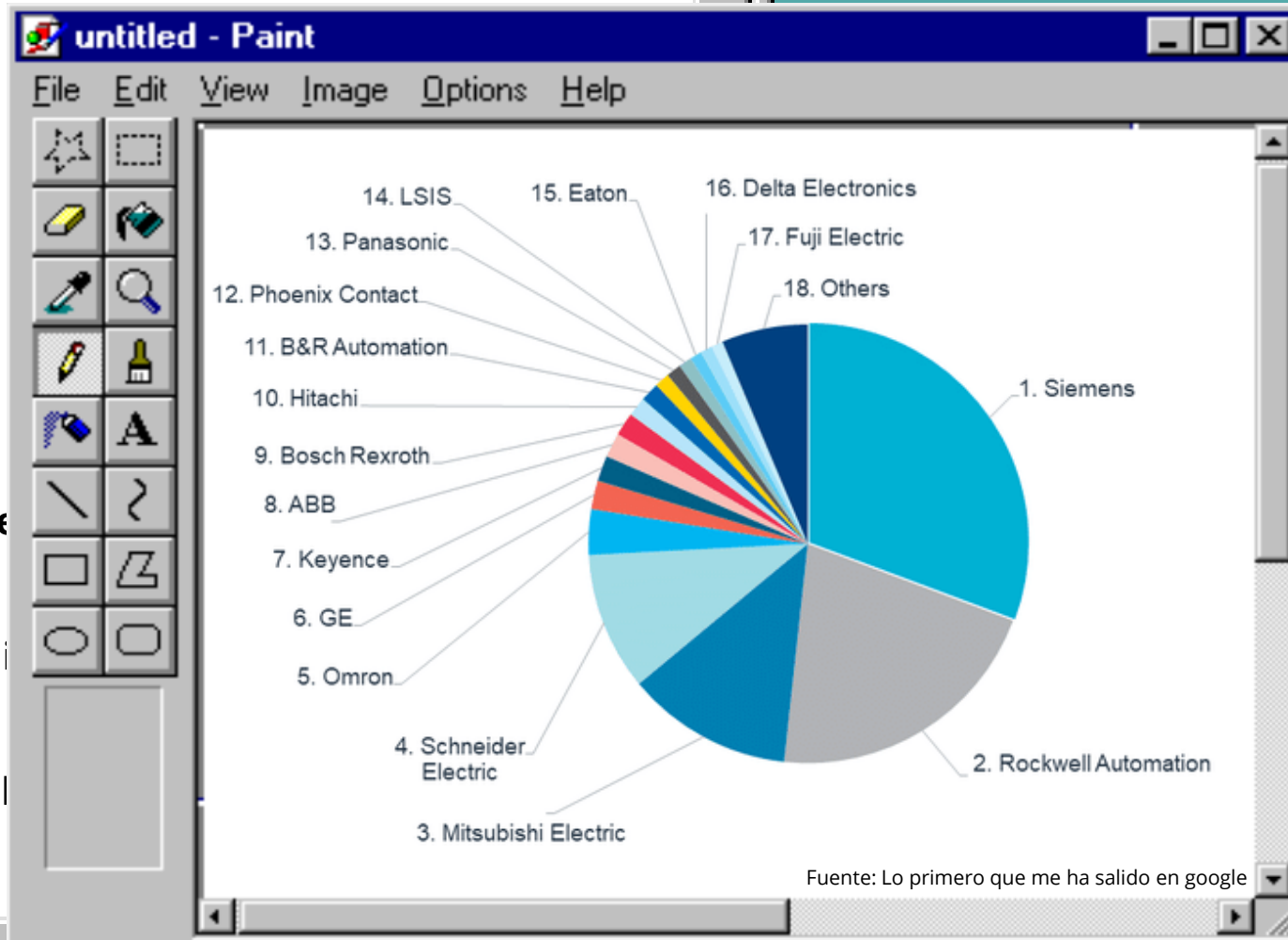
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

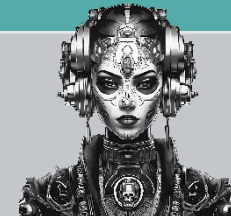
PLC

- Ejecutan lógica de control en tiempo real
- Lenguajes IEC 61131-3: Ladder, FBD, ST, etc.
- Muy robusto: resistente a calor, polvo, interferencia
- Modular: se expande con tarjetas I/O, comunicación
- Software de ingeniería propietario (TIA Portal)





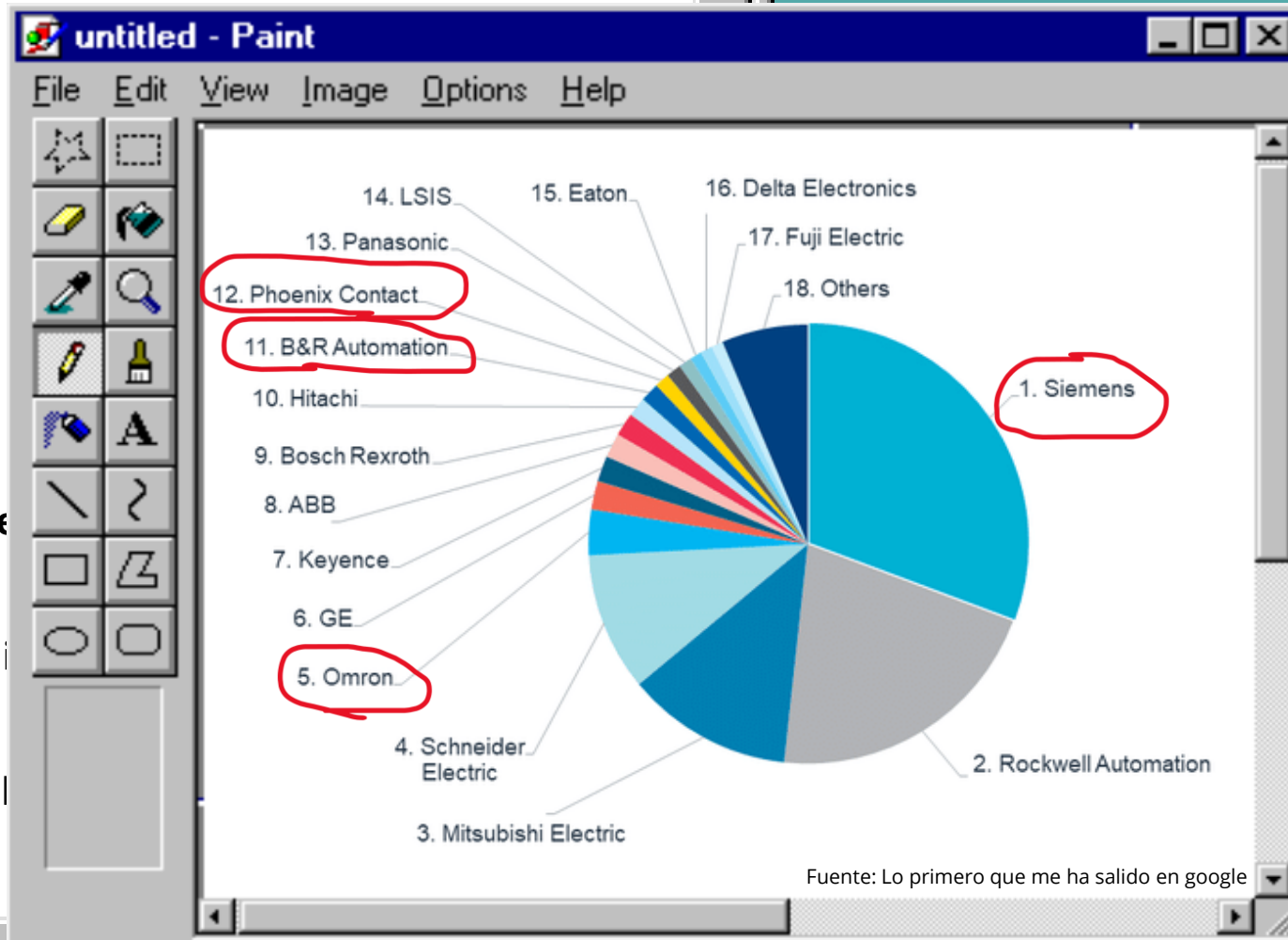
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

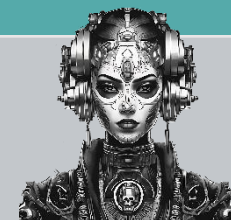
PLC

- Ejecutan lógica de control en tiempo real
- Lenguajes IEC 61131-3: Ladder, FBD, ST, etc.
- Muy robusto: resistente a calor, polvo, interferencia
- Modular: se expande con tarjetas I/O, comunicación
- Software de ingeniería propietario (TIA Portal)



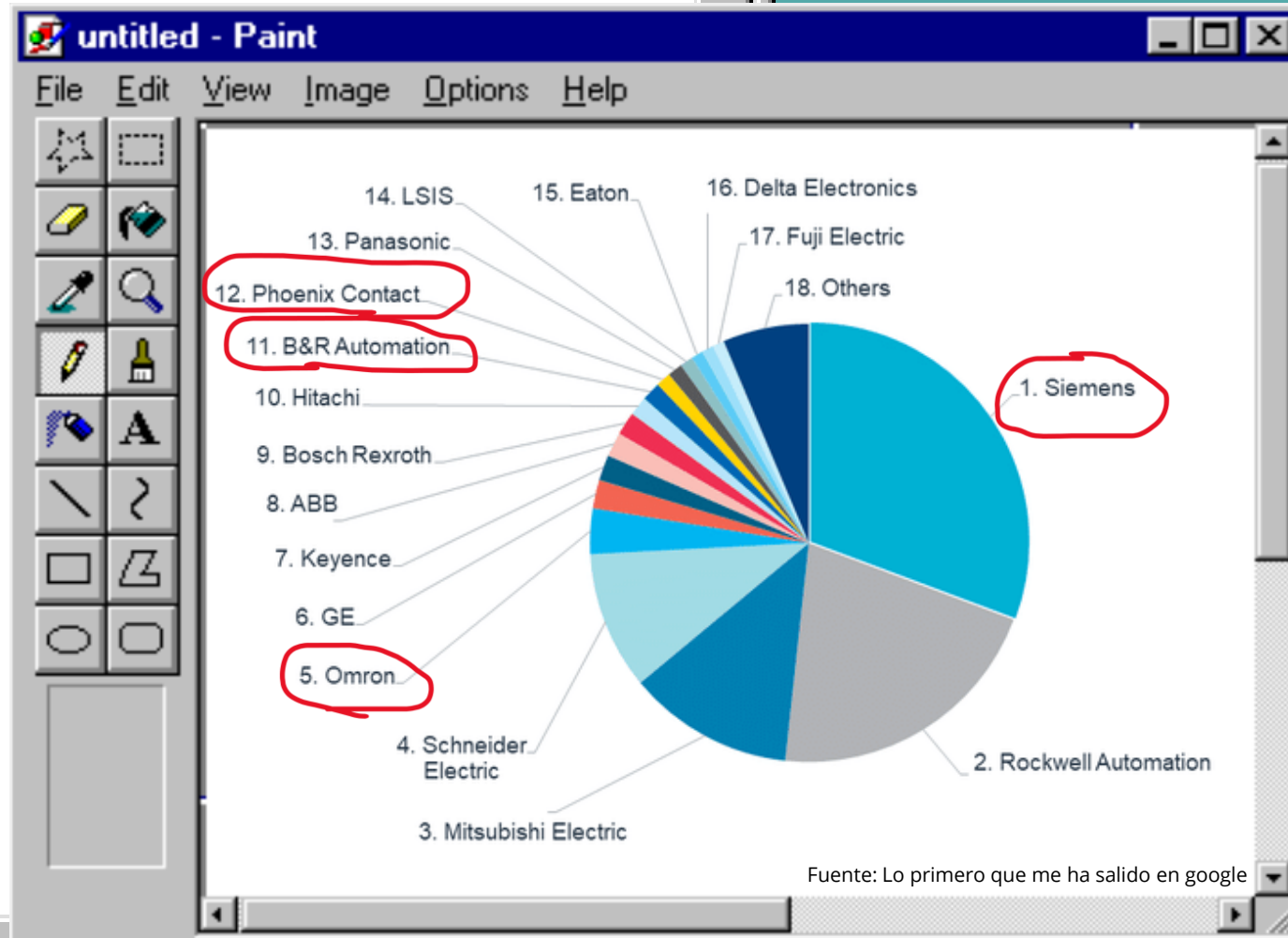


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

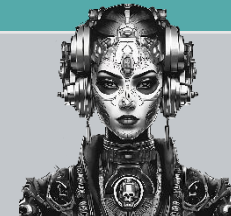
Por qué estas marcas?



Fuente: Lo primero que me ha salido en google



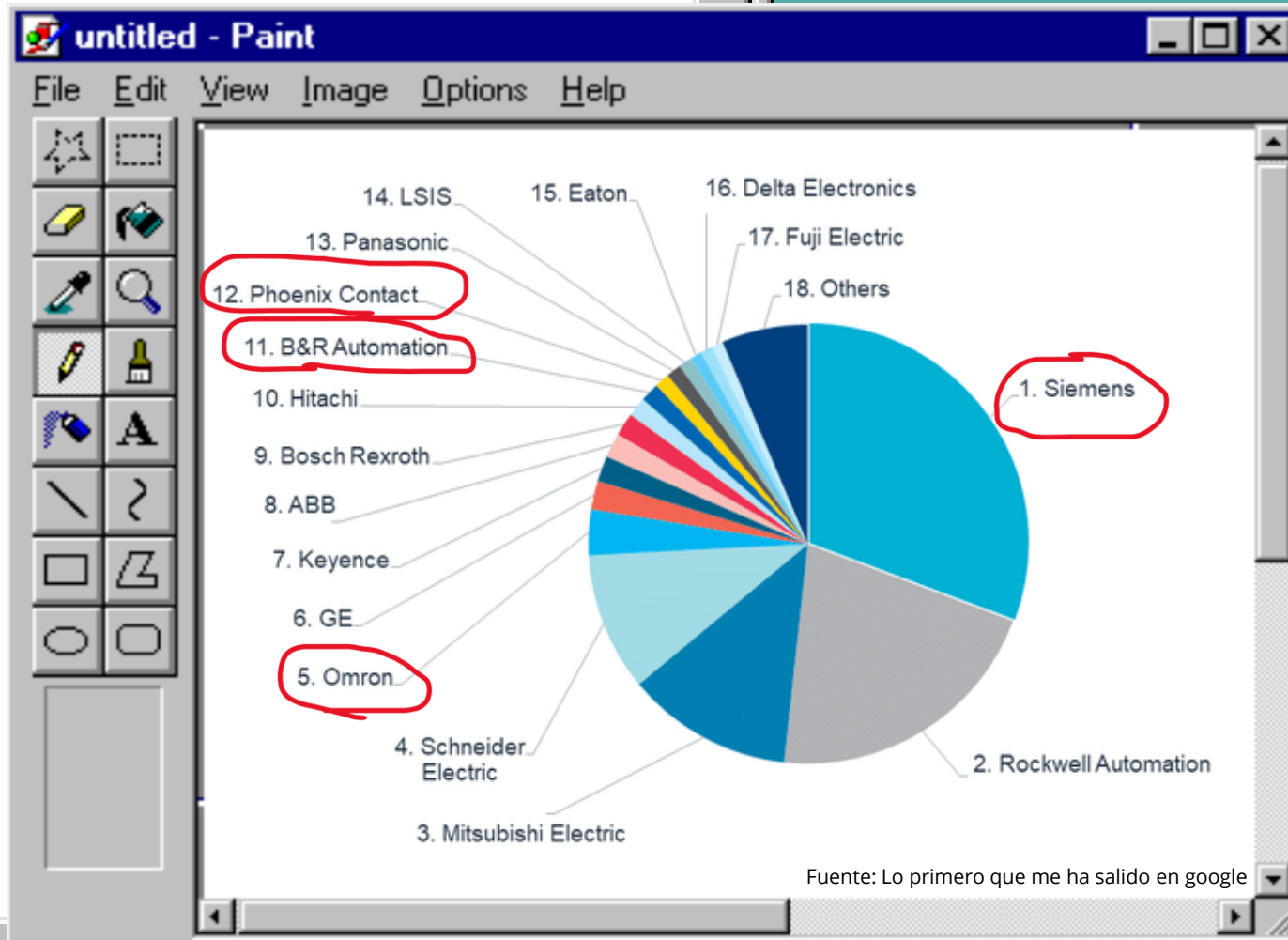
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

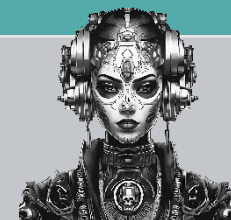
Por qué estas marcas?

- Son los que tenía a mano
- No voy a comprar un PLC, están muy caros





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help



My Computer



WordPad

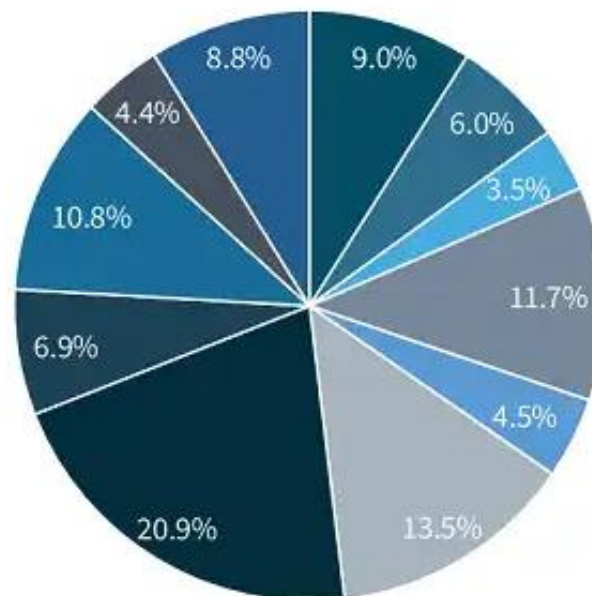


MS-DOS
Prompt



Recycle Bin

Global Programmable Logic Controller Market Share (%), By End-Use, 2024



■ Aerospace & Defence

■ Automotive

■ Chemical

■ Energy & Utilities

■ Food & Beverages

■ Healthcare

■ Manufacturing

■ Mining & Metal

■ Oil & Gas

■ Transportation

■ Others

Source: www.gminsights.com



Fun Fact:

trenes

Profinet con
redundancia
extra

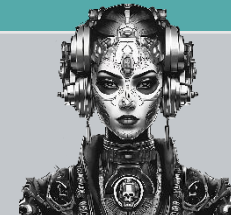


Sibas 32





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

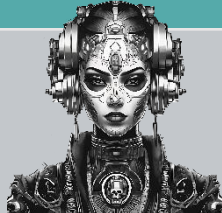
IPC

- **Arquitectura estándar (x86/x64)**
- **Ejecuta Windows, Linux, BSD...**
- **Puede correr HMI, SCADA, IA, bases de datos**
- **Hardware robusto, pero menos especializado**
- **Software más libre: C++, Python, sistemas abiertos**





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

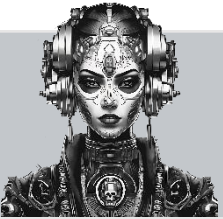
PLCs & IPCs

	PLC	IPC
OS	RTOS / firmware propietario	Windows / Linux / BSD
Tiempo real	Sí	Depende del OS
Programación	Ladder, FBD, S	SCADA, Python, C++, etc.
Flexibilidad	Baja (entorno cerrado)	Alta (entorno abierto)
Virtualizable	Difícil	Fácil





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



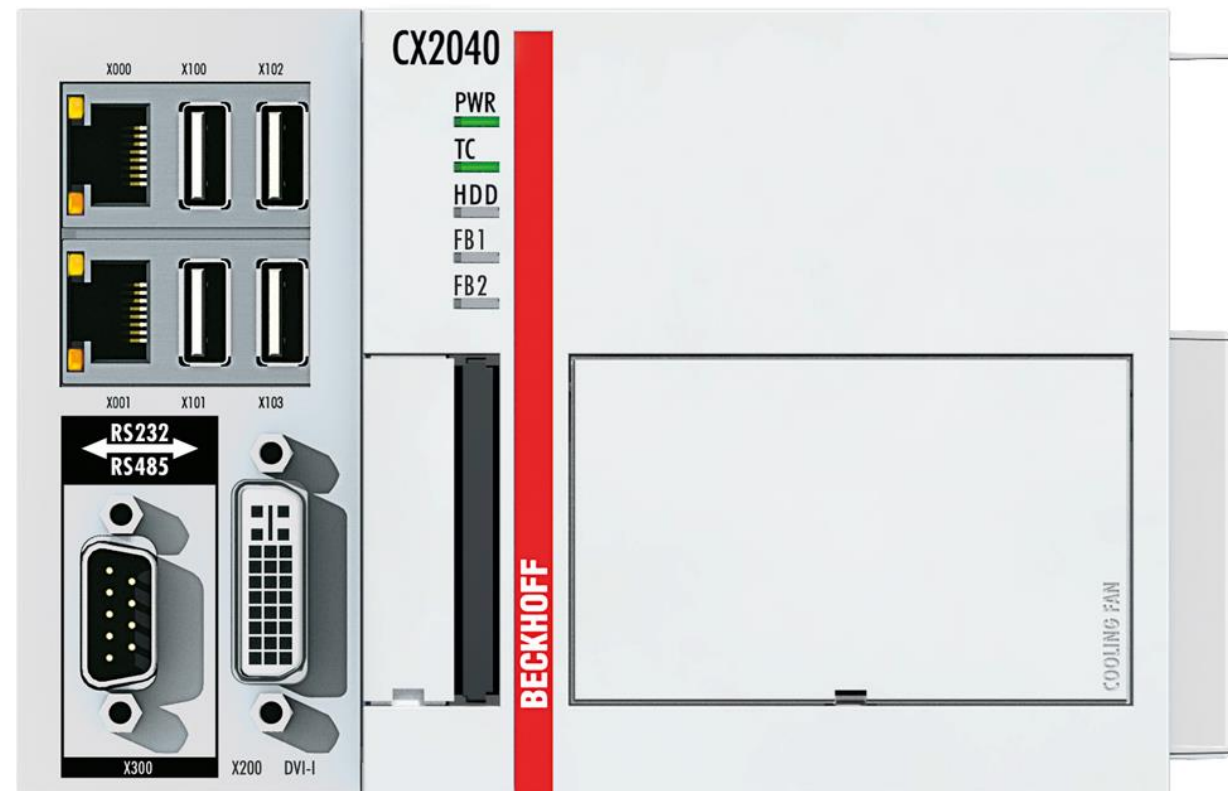
Examen Sorpresa



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Examen Sorpresa



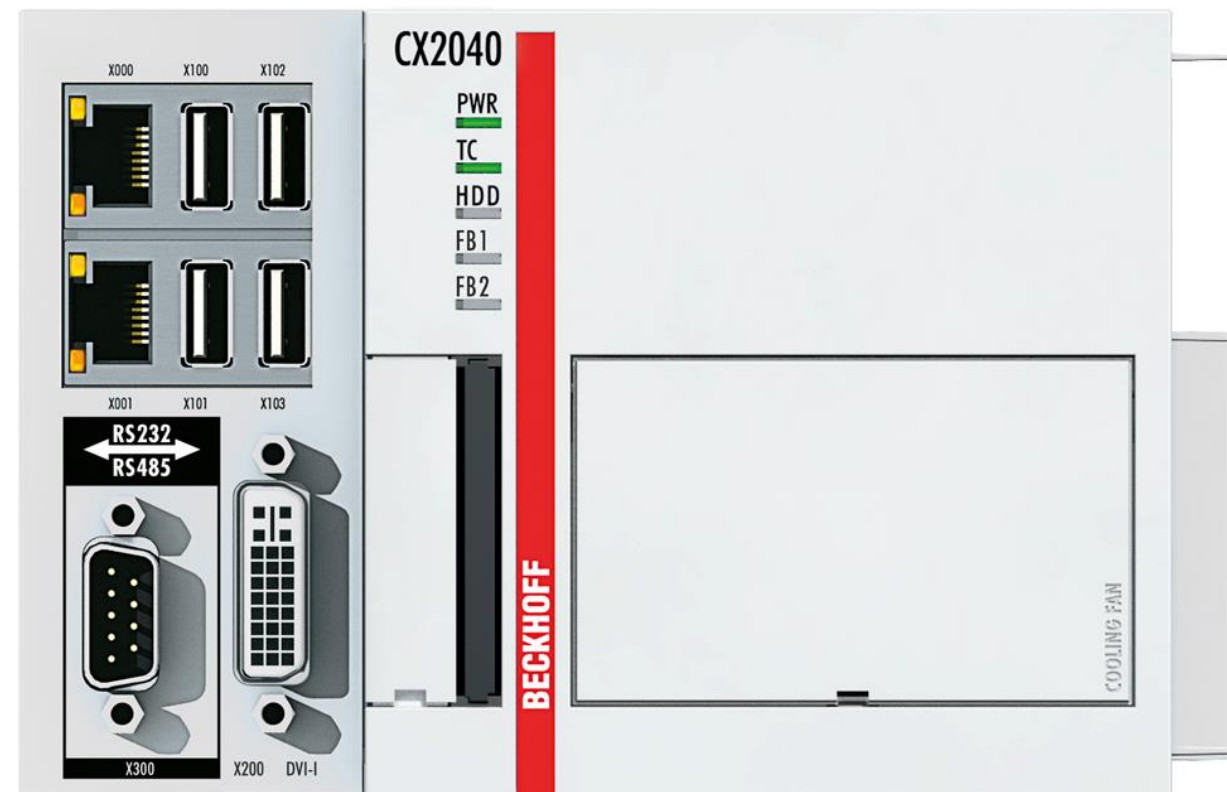


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Examen Sorpresa

Arquitectura x86





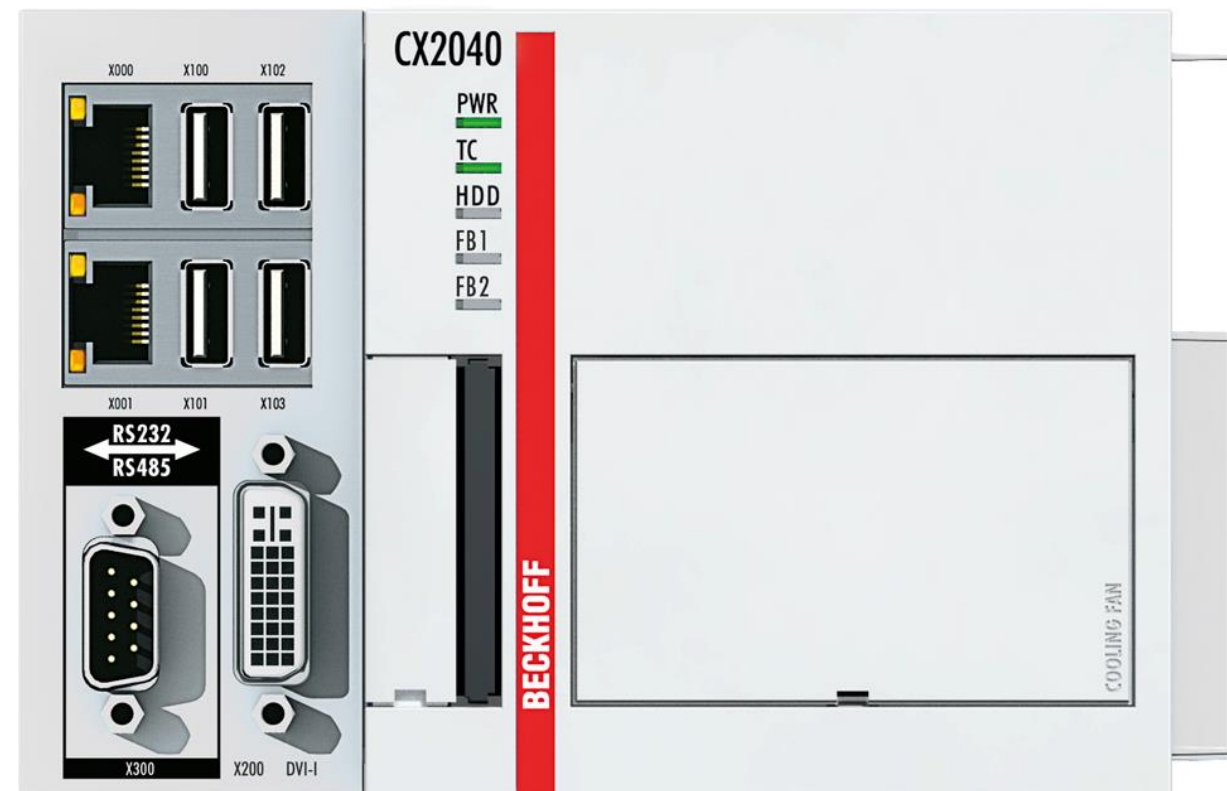
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Examen Sorpresa

Arquitectura x86

Modularidad





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

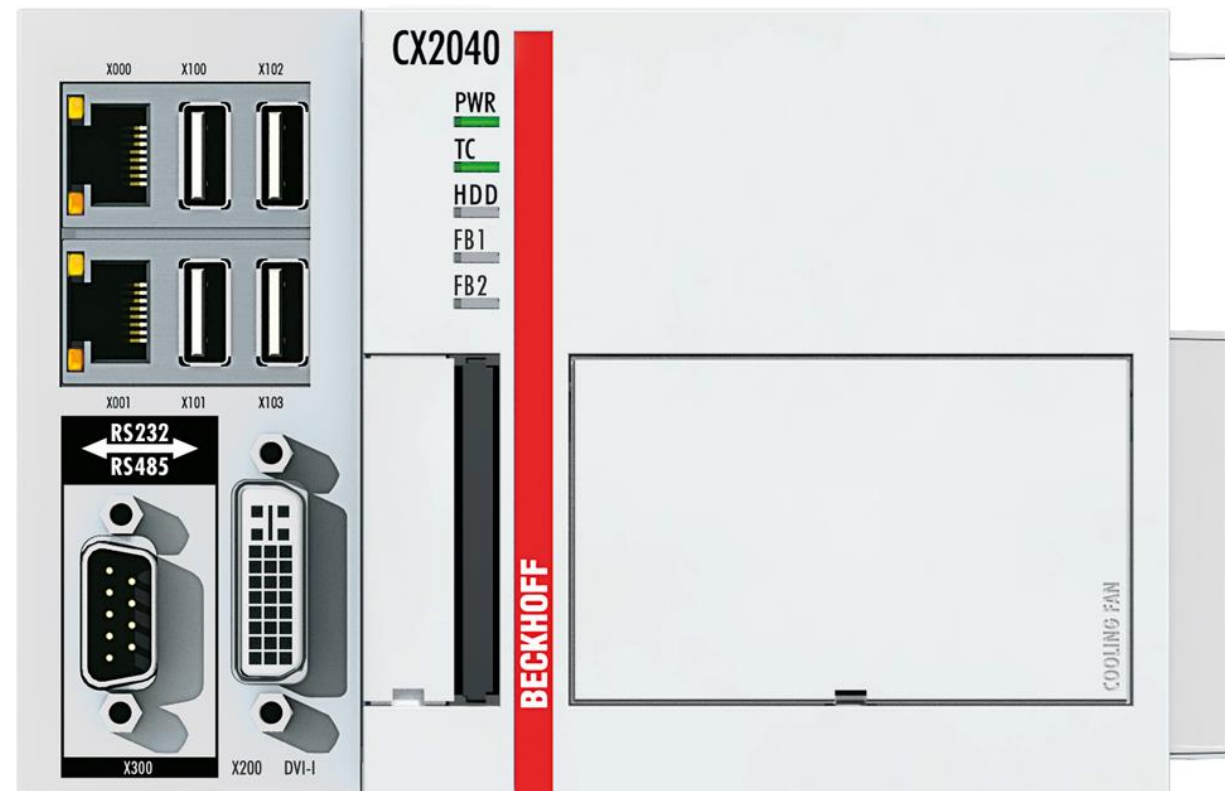


Examen Sorpresa

Arquitectura x86

Modularidad

Windows





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



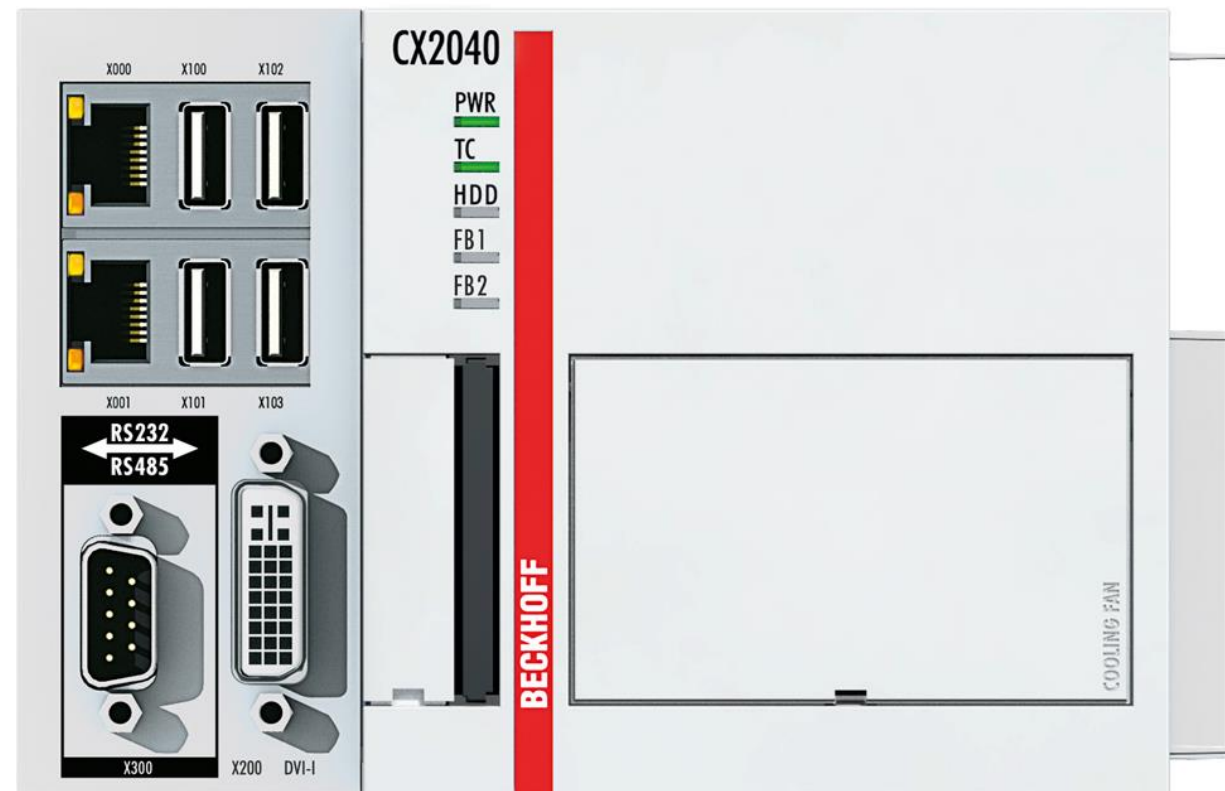
Examen Sorpresa

Arquitectura x86

Modularidad

Windows

Ejecución determinista en tiempo real





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Examen Sorpresa

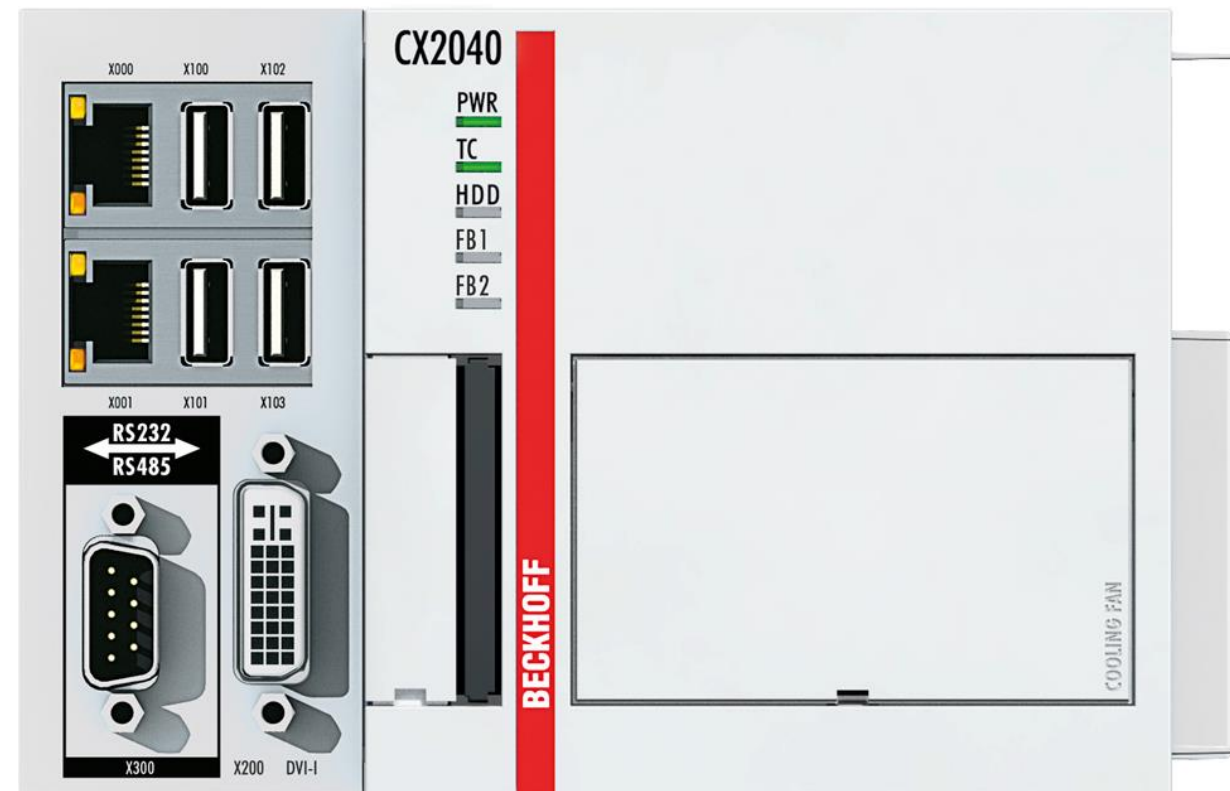
Arquitectura x86

Modularidad

Windows

Ejecución determinista en tiempo real

Entorno de Desarrollo propietario





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Examen Sorpresa

Arquitectura x86

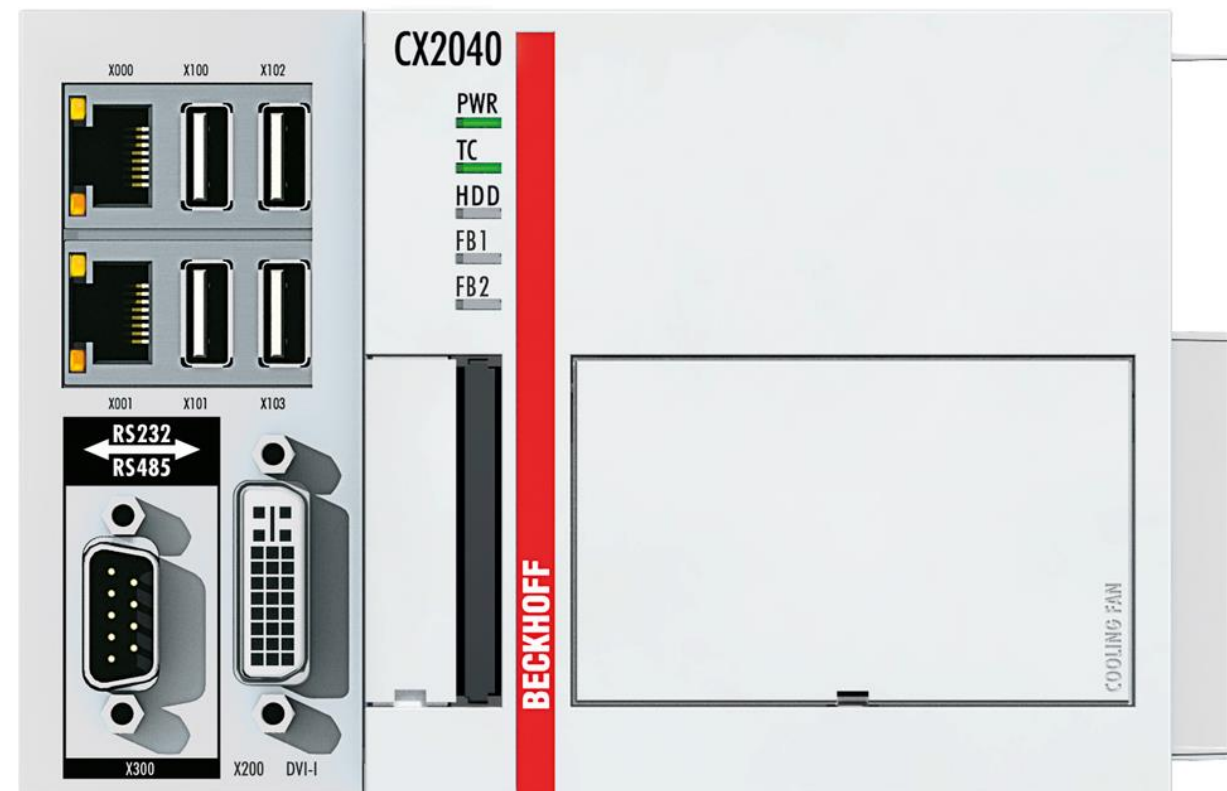
Modularidad

Windows

Ejecución determinista en tiempo real

Entorno de Desarrollo propietario

PLC o IPC?





CX2040 | Basic CPU module (service phase)



The CX2040 has a 2.1 GHz Intel® Core™ i7 quad-core CPU. Due to its high power the CPU is equipped with a fan with ball bearings and speed monitoring. In addition to the CPU and chipset the CX2040 also contains the main memory with 4 GB RAM as standard. The controller boots from the CFast flash memory card.

The basic configuration of the CX2040 includes a CFast memory card, two independent Gbit [Ethernet](#) interfaces, four USB 2.0 interfaces and a DVI-I interface.

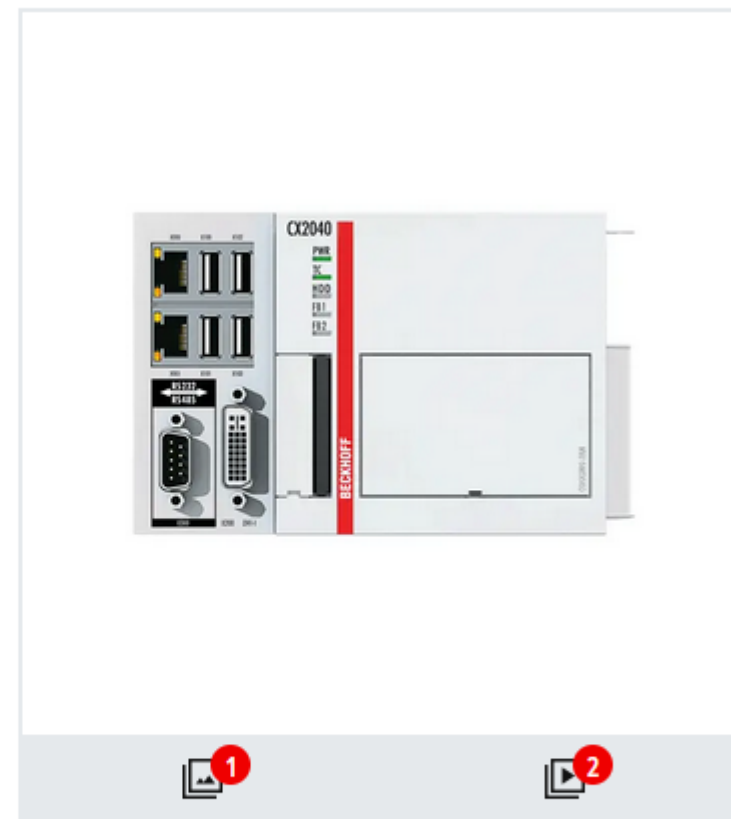
The CPU has a 128 kB NOVRAM persistent data memory for situations where no UPS is used.

The unit can optionally be ordered with a fieldbus or serial interface. Other components from the CX2000 family can be connected via the multi-pin terminals on either side. The operating system is Microsoft Windows Embedded Compact 7 or Windows 10 IoT Enterprise 2016 LTSB. [TwinCAT](#) automation software transforms a CX2040 system into a powerful [PLC](#) and motion control system that can be operated with or without visualization. Due to its high-performance the CX2040 can be used for interpolating 3-D path movements with TwinCAT NC I.

Up to four modules can be connected to the basic CPU module. The connection order is irrelevant. Internally the modules are connected via PCI Express® and can be connected subsequently to the CPU in the field.

The power supply for the CPU module comes from a CX2100-0014 or CX2100-0914 power supply module, which is connected on the right-hand side of the CPU. Two further CFast memory card modules (CX2550-0010) can be connected between the power supply unit and the CPU, so that a total of up to three CFast cards can be used. RAID can be used in situations where more than one CFast card is used.

The extended operating temperature range between -25 and +60°C enables application in climatically demanding situations.



Product status: service phase | recommended alternative: [CX2043](#)



Product finder IPC



Show/hide columns

Show pictures

Copy

Export

Print

Full screen mode

Comparison	Producto	Product category	Number of cores i	CPU type i	TwinCAT 3 platform level	TwinCAT 2 support i	Operating system i
		↔ ×	↔ ×	↔ ×	↔ ×	↔ ×	↔ ×
☐	CX2043 Embedded PC with AMD Ryzen™ V1807B	Embedded PC	4	AMD Ryzen™	P60	yes	Win 10 IoT Enterprise 2019 LTSC (32 bit), Win 10 IoT Enterprise 2019 LTSC (64 bit), Win 10 IoT Enterprise 2021 LTSC (64 bit), Win 11 IoT Enterprise 2024 LTSC (64 Bit), TwinCAT/BSD
☐	CX2042 Embedded PC with Intel® Xeon® D-1527	Embedded PC	4	Intel® Xeon®	P70	no	Win 10 IoT Enterprise 2016 LTSB (64 bit), Win 10 IoT Enterprise 2019 LTSC (64 bit), Win 10 IoT Enterprise 2021 LTSC (64 bit), TwinCAT/BSD



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Antes de empezar





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Antes de empezar



**Percepción
general de un PLC**

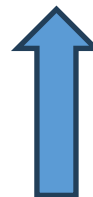


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Antes de empezar

(UPSTREAM)



**Protocolos para configuración
+
TCP y derivados**

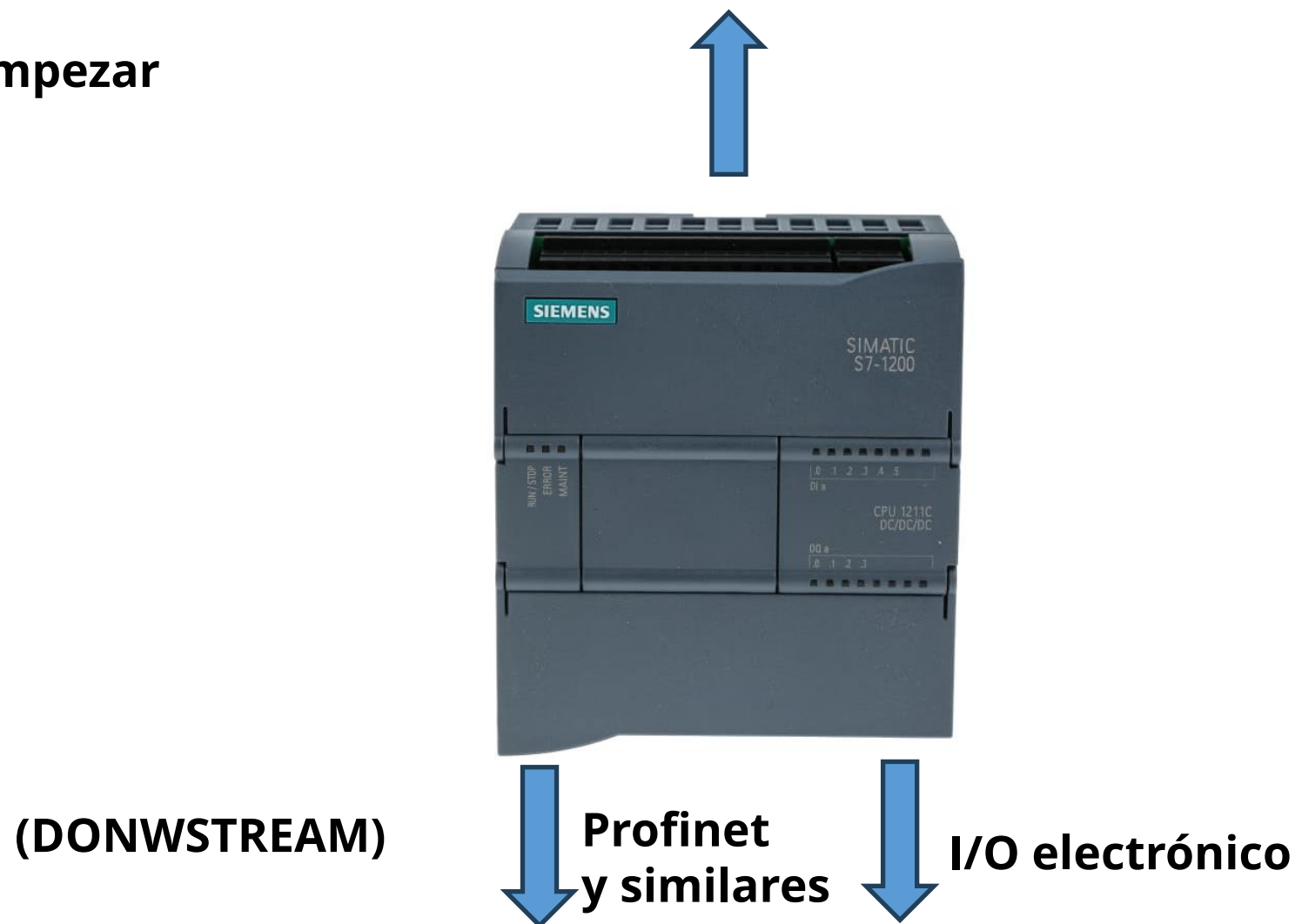




PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Antes de empezar





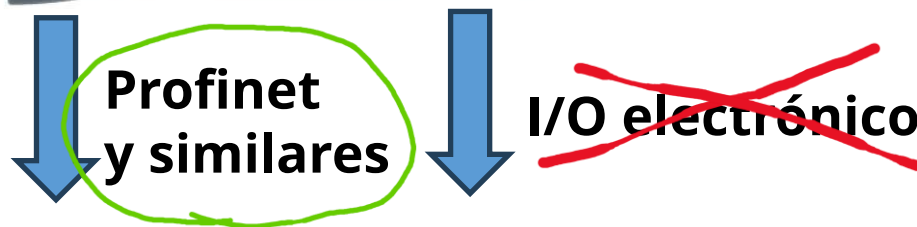
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Antes de empezar



(DONWSTREAM)





Antes de empezar

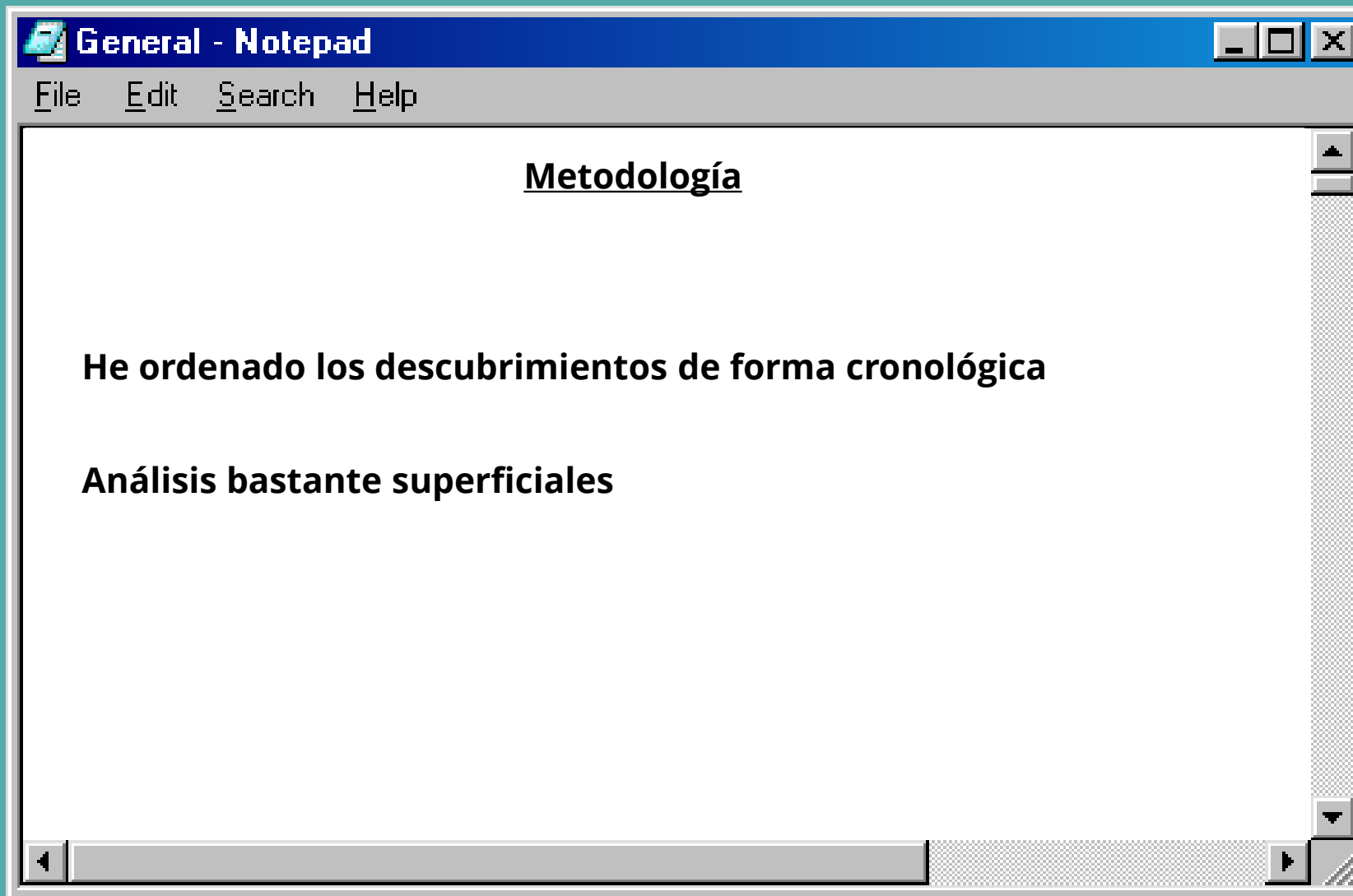
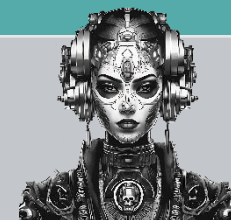
(LATERAL)



**Comunicación con
módulos extra**

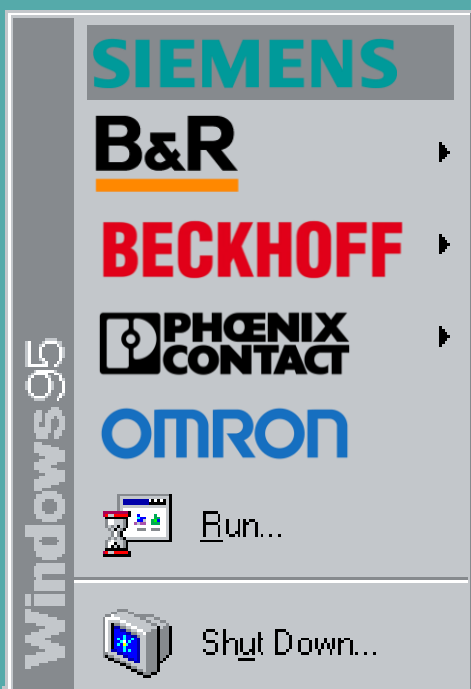
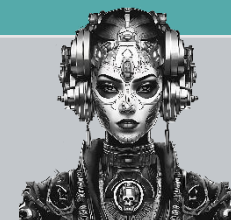


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



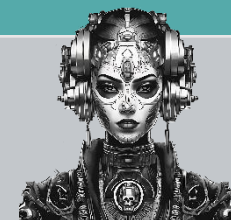


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

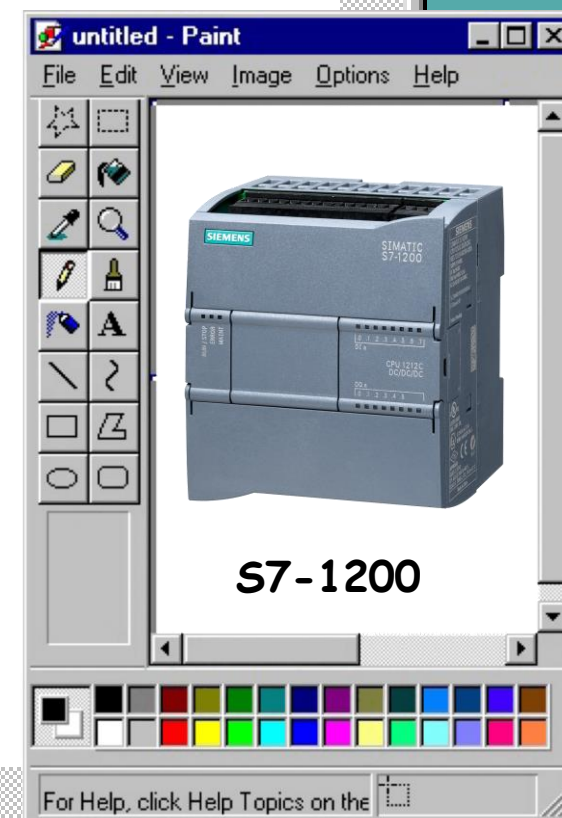


File Edit Search Help

Breakthrough

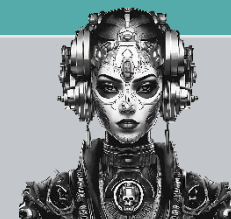
SIEMENS

- Vulnerabilidades ya conocidas
- Extracción del firmware
- Sistema de seguridad de tarjetas
- Puertos de expansión



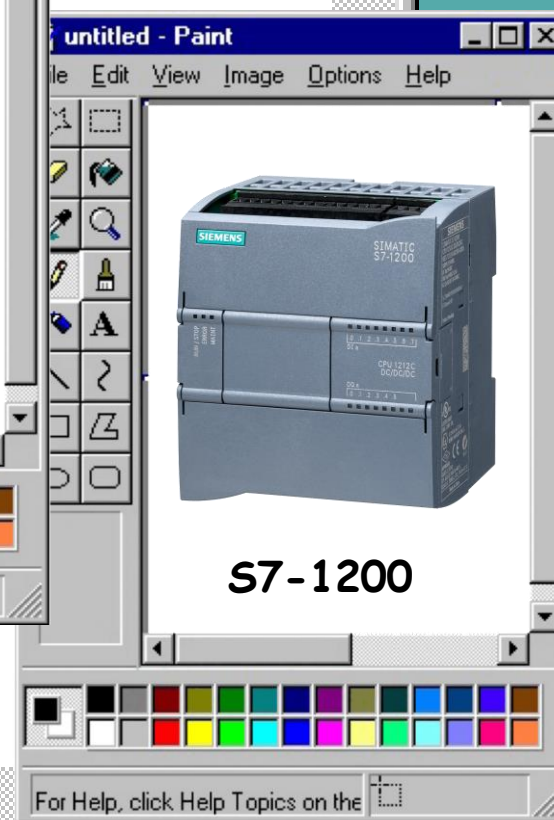
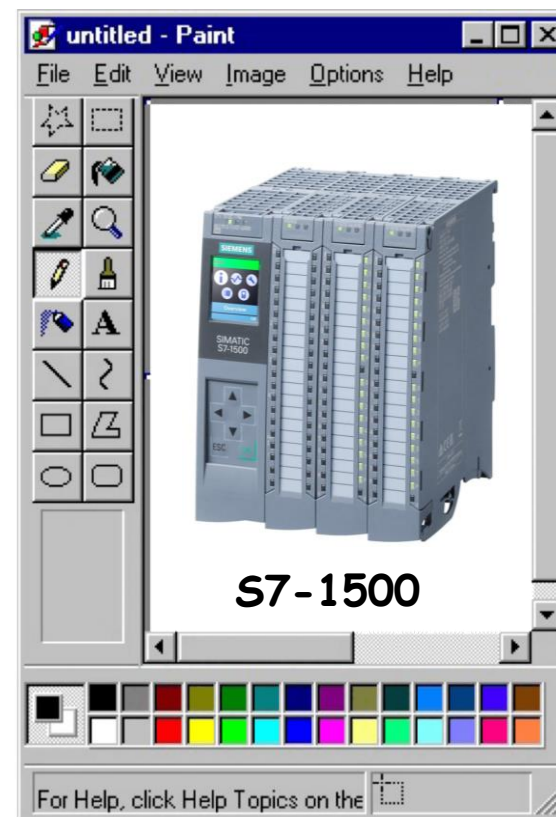
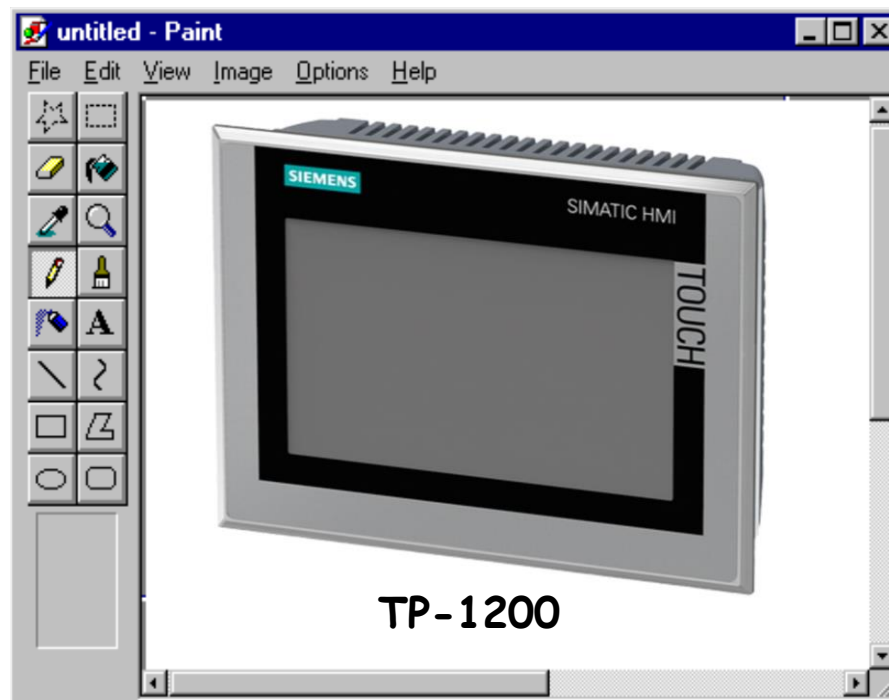


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



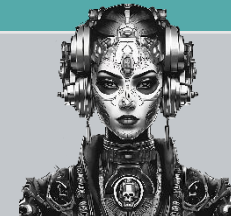
File Edit Search Help

Breakthrough





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Ficha técnica (S7-1200)

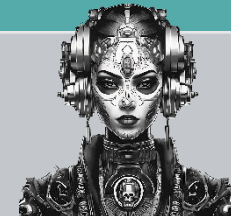
SIEMENS

- **Arquitectura:** ARM Cortex-M
- **OS base:** RTOS propietario de Siemens
- **Entorno de programación:** TIA portal
- **Interfaces:** Ethernet, USB, SD
- **Comunicaciones:** S7Comm, Profinet, MODBUS TCP, OPC UA





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Hasta ahora

SIEMENS

The Race to Native Code Execution in Siemens PLCs

CVE-2020-15782

2021: kernel-level native code execution, remotely



Hardware Hacking

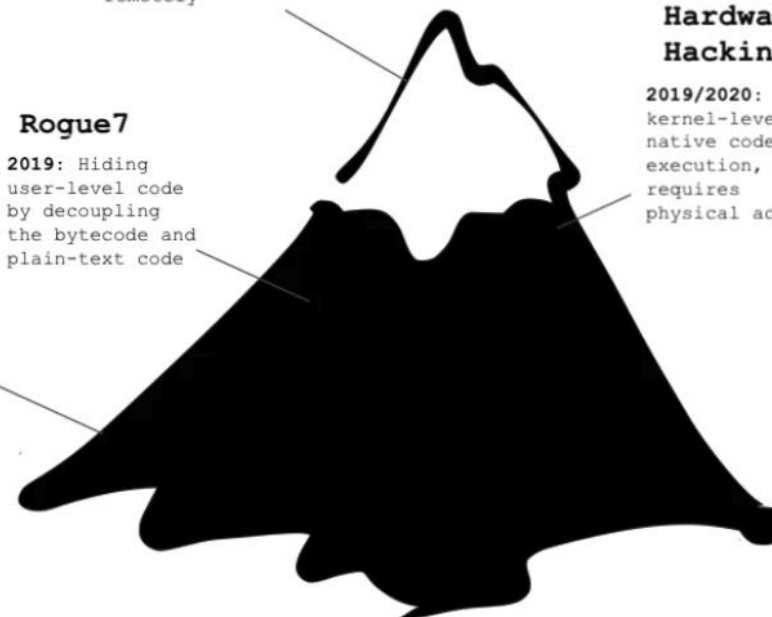
2019/2020: kernel-level native code execution, but requires physical access

Rogue7

2019: Hiding user-level code by decoupling the bytecode and plain-text code

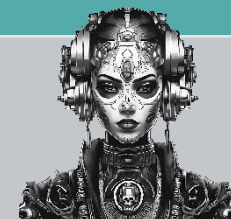
Stuxnet

2010: Hiding user-level code by intercepting codeblocks on the EWS





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Back



Forward



Stop



Refresh



Home



Search



Favorites



History

Address

https://sec-consult.com/

Links



an Eviden business

CAREER ABOUT US CONTACT EN Q

Compliance & Regulations Security Testing Processes & Organisation Incident Response Vulnerability Lab Blog

Home / Blog / Reverse Engineering Architecture And Pinout of Custom Asics

Reverse Engineering Architecture And Pinout of Custom Asics

28.02.2019 hardware vulnerability

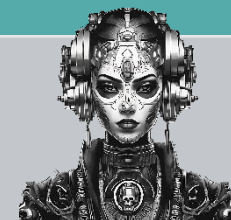
Learn about the process of initial reverse engineering the pinout of unknown ASICs by using moderate methods. The two described ICs are good examples out of many industry-solutions and have been chosen to demonstrate how design decisions from vendors are made. The exploited potential leak of the supply-chain can be leveraged by a hardware reverse engineer to extract internal information about such systems.



Internet zone



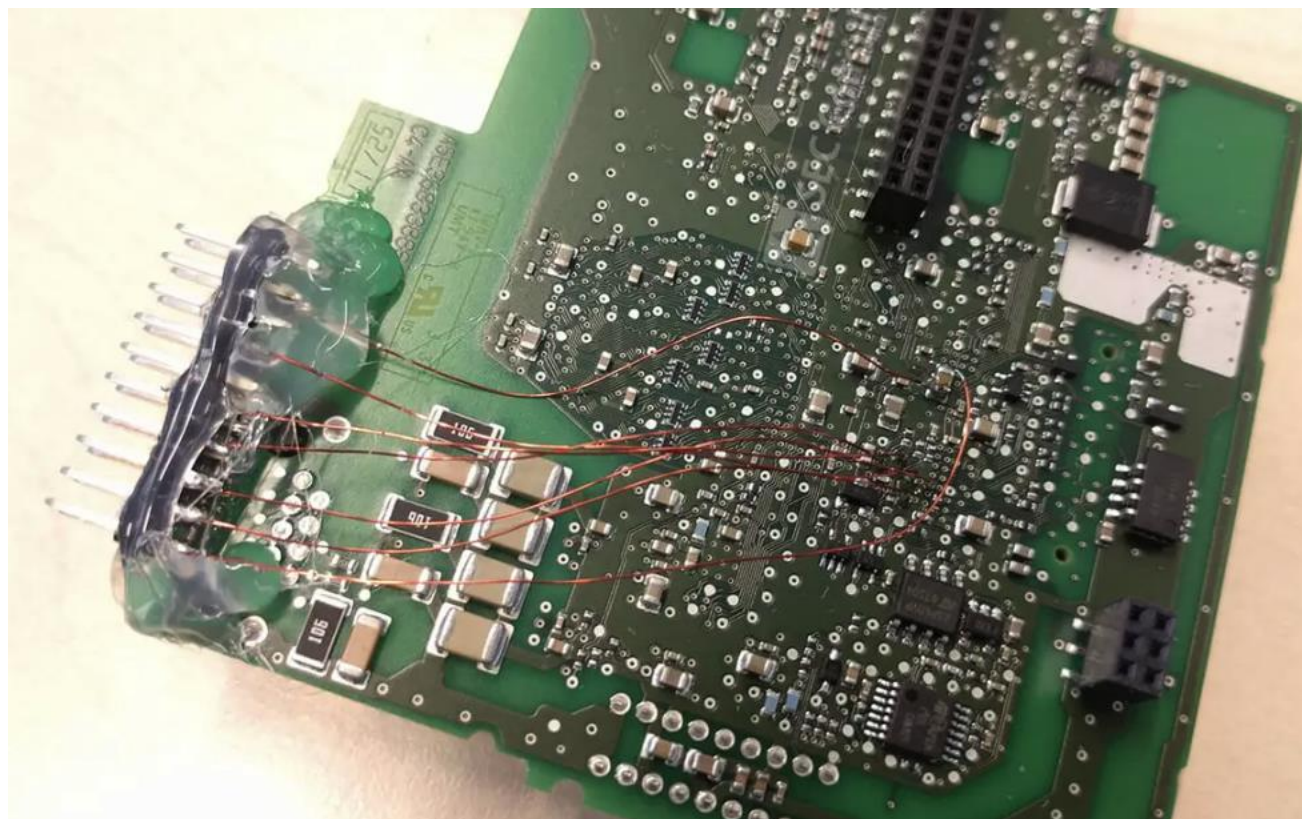
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

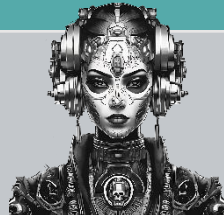
Extracción de firmware (Sec-Consult)

SIEMENS





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



BackForwardStopRefreshHomeSearchFavoritesHistory

Address

https://support.industry.siemens.com/

Links

SiePortal

Región e idioma

Contacto

Ayudar

Solicitud de soporte

Buscar en SiePortal

Inicio

Apoyo

Base de conocimientos

Products & Services

Apoyo

mySiePortal

Carrito

Tipo de artículo: **Notificación del producto** ID de artículo **109814248**, Fecha del artículo: **03/12/2022**

★★★★☆ (3)

Evaluar

Ya disponible el firmware V4.6 para el S7-1200

Artículo

Relacionado con producto(s)

Ya se encuentra disponible el firmware V4.6 para las CPUs del S7-1200 .

El firmware V4.6 es capaz de proporcionar más memoria para todas las CPUs debido a las personalizaciones del código. Los módulos de CPU de la generación HW V4 (número de referencia: 6ES721x-1xx40-0XB0) ya en uso pueden utilizar esta ampliación a través de la actualización del firmware. Además, el servicio SNMP está desactivado por defecto.

El firmware V4.6 es compatible con todo el hardware S7-1200 con la versión de firmware V4.0 o superior.

[CPUs afectadas y enlaces de descarga](#)

Producto	Número de referencia	Nuevo tamaño de memoria de trabajo	Enlace a la descarga de la versión de firmware
CPUs estándares			

Comparte esta página:

- mySupport Cockpit
- Igor Pallin
- >

Añadir a los favoritos mySupport
- >

Añadir a la documentación mySupport
- >

Favoritos
- >

Mis solicitudes
- >

Descargas CAX
- >

Mis Productos / Portapapeles
- +

Últimos artículos vistos

- Enlaces relacionados
- >

Herramienta de compatibilidad
- >

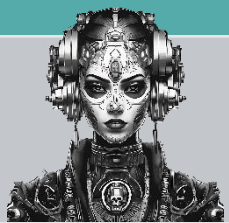
Registre su variador de SINAMICS
- >

Visit our Converting Community





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



My Computer

File Edit View Go Favorites Help

Back Forward Up Cut Copy Paste Undo Delete

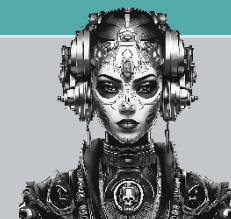
Address My Computer

Name	Date Modified	Size	Kind
FWUPDATE.S7S	15 Jun 2025 at 11:38	--	Folder
6ES7 510-1DJ01-0AB0 V02.09.08.upd	15 Apr 2025 at 12:26	25,8 MB	Document
6ES7 510-1DK03-0AB0 V04.00.00.upd	25 Nov 2024 at 17:33	43,3 MB	Document
6ES7 510-1SJ01-0AB0 V02.09.08.upd	15 Apr 2025 at 12:26	25,8 MB	Document
6ES7 510-1SK03-0AB0 V04.00.00.upd	25 Nov 2024 at 17:33	43,3 MB	Document
6ES7 511-1AK01-0AB0 V02.09.08.upd	15 Apr 2025 at 12:25	26 MB	Document
6ES7 511-1AK02-0AB0 V02.09.08.upd	15 Apr 2025 at 12:25	26 MB	Document
6ES7 511-1AL03-0AB0 V04.00.00.upd	25 Nov 2024 at 17:33	47,2 MB	Document
6ES7 511-1CK00-0AB0 V02.09.08.upd	15 Apr 2025 at 12:26	27,4 MB	Document
6ES7 511-1CK01-0AB0 V02.09.08.upd	15 Apr 2025 at 12:26	27,4 MB	Document
6ES7 511-1CL03-0AB0 V04.00.00.upd	25 Nov 2024 at 17:33	47,2 MB	Document
6ES7 511-1FK01-0AB0 V02.09.08.upd	15 Apr 2025 at 12:25	26 MB	Document
6ES7 511-1FK02-0AB0 V02.09.08.upd	15 Apr 2025 at 12:25	26 MB	Document
6ES7 511-1FL03-0AB0 V04.00.00.upd	25 Nov 2024 at 17:33	47,2 MB	Document
6ES7 511-1TK01-0AB0 V02.09.08.upd	15 Apr 2025 at 12:25	26 MB	Document
6ES7 511-1TL03-0AB0 V04.00.00.upd	25 Nov 2024 at 17:33	47,2 MB	Document

My Computer



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



My Computer

File Edit View Go Favorites Help

Back Forward Up Cut Copy Paste Undo Delete

Address My Computer

Name	Date Modified	Size	Kind
FWUPDA			Folder
6ES7 5		25,8 MB	Document
6ES7 5		43,3 MB	Document
6ES7 5		25,8 MB	Document
6ES7 5		43,3 MB	Document
6ES7 5		26 MB	Document
6ES7 5		26 MB	Document
6ES7 511-1AL03-0AB0 V04.00.00.upd	25 Nov 2024 at 17:33	47,2 MB	Document
6ES7 511-1CK00-0AB0 V02.09.08.upd	15 Apr 2025 at 12:26	27,4 MB	Document
6ES7 511-1CK01-0AB0 V02.09.08.upd	15 Apr 2025 at 12:26	27,4 MB	Document
6ES7 511-1CL03-0AB0 V04.00.00.upd	25 Nov 2024 at 17:33	47,2 MB	Document
6ES7 511-1FK01-0AB0 V02.09.08.upd	15 Apr 2025 at 12:25	26 MB	Document
6ES7 511-1FK02-0AB0 V02.09.08.upd	15 Apr 2025 at 12:25	26 MB	Document
6ES7 511-1FL03-0AB0 V04.00.00.upd	25 Nov 2024 at 17:33	47,2 MB	Document
6ES7 511-1TK01-0AB0 V02.09.08.upd	15 Apr 2025 at 12:25	26 MB	Document
6ES7 511-1TL03-0AB0 V04.00.00.upd	25 Nov 2024 at 17:33	47,2 MB	Document

Windows Networking

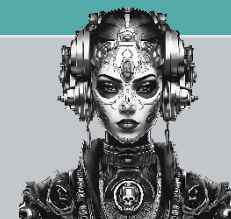
Bloqueo

OK

My Computer



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



Back



Forward



Stop



Refresh



Home



Search



Favorites



History

Address

https://es.rs-online.com/

Links

Tarjeta Micro SD Siemens, para usar con SIMATIC S7

SIEMENS

Código RS: 203-3542 | N° ref. fabric.: 6ES7953-8LM32-0AA0 | Fabricante: [Siemens](#)



Ver esta categoría

Precio Unidad*

533,45 €
(exc. IVA)

645,47 €
(inc. IVA)

Unidad(es)

Selecciona o escribe la cantidad

1

[Consultar fechas de entrega](#)

[Añadir](#)

Entrega GRATUITA para pedidos superiores a 80,00 €

Disponible

- Disponible(s) 3 unidad(es) para enviar desde otro centro de distribución

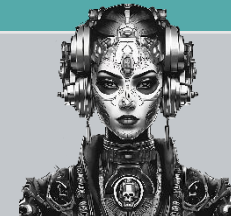
¿Necesitas comprar más? Introduce la nueva cantidad y clicla en "Consultar fechas de entrega"



Internet zone



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Proceso

SIEMENS

- Volcado de una tarjeta original (dd)
- Identificación de secciones
- Clonado de bloques



My Computer



WordPad



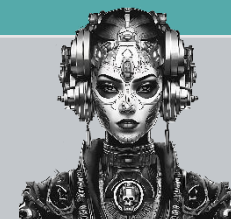
MS-DOS
Prompt



Recycle Bin



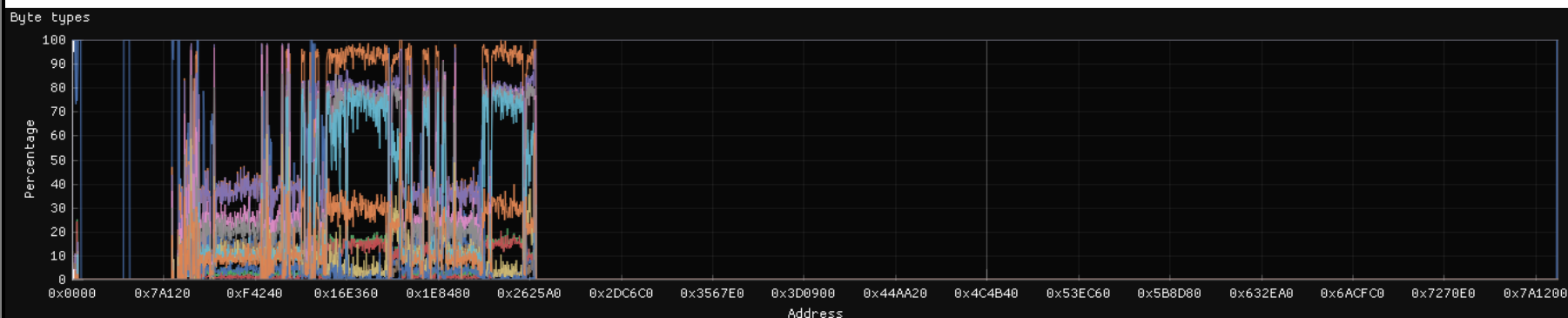
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

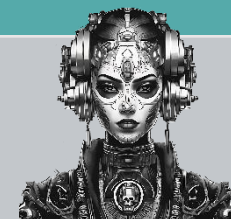
Entropía

SIEMENS





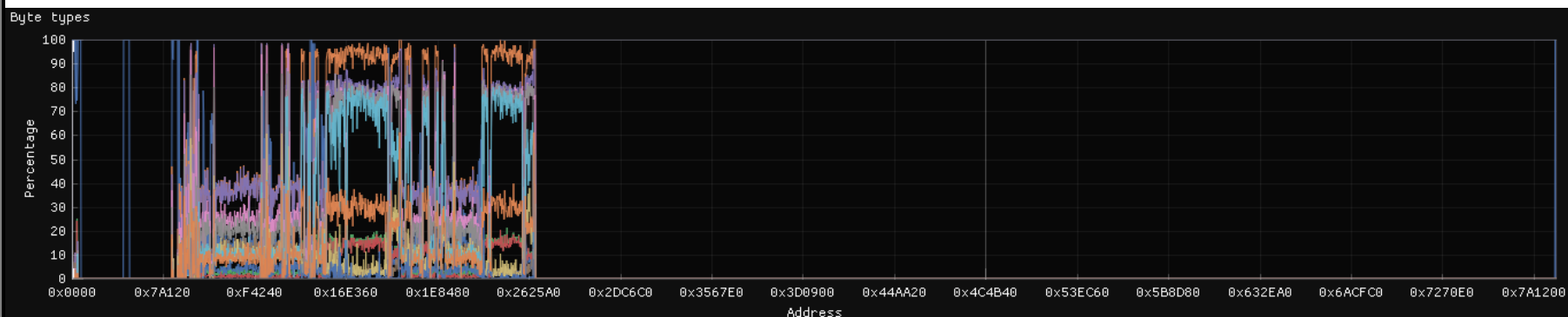
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Entropía

SIEMENS





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Medidas de seguridad

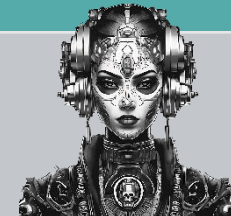
SIEMENS

- Se sobrescribe el BIOS Parameter Block
- Herramientas como binwalk no lo detectan bien

Address	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII
00000000:	4F	72	69	67	69	6E	61	6C	20	53	69	65	6D	65	6E	73	Original Siemens
00000010:	20	45	71	75	69	70	6D	65	6E	74	2E	20	55	73	65	20	Equipment. Use
00000020:	6F	6E	6C	79	20	77	69	74	68	20	53	69	65	6D	65	6E	only with Siemen
00000030:	73	20	53	49	4D	41	54	49	43	2E	20	44	6F	20	6E	6F	s SIMATIC. Do no
00000040:	74	20	66	6F	72	6D	61	74	20	6F	72	20	70	61	72	74	t format or part
00000050:	69	74	69	6F	6E	2E	00	00	00	00	00	00	00	00	00	00	ition,.....



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Método de diff

SIEMENS

S7-1500 // TP-1200

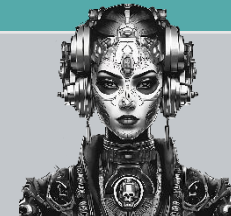
```
C:\Users\ipallin\Downloads\s7-1500_sd.img UTF8 Dos
1 Original Siemens Equipment. Use only with Siemens SIMATIC. Do not format or partition.
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

C:\Users\ipallin\Downloads\siemens-sd.img UTF8 Dos
1 Original Siemens Equipment. Use only with Siemens SIMATIC. Do not format or partition.
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
```





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

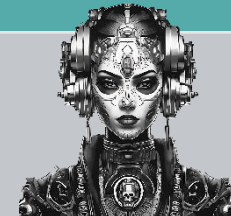
Puertos de expansión

SIEMENS





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Puerto izquierdo

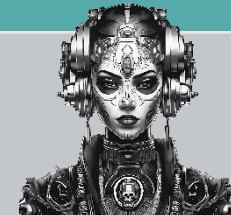
SIEMENS

- Módulos de comunicación y proceso
- Las señales se procesan en el módulo
- Mandan señales directamente a la CPU





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Puerto izquierdo

SIEMENS

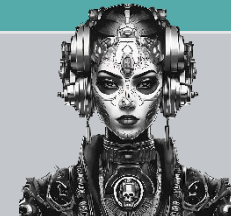
- Módulos de comunicación y proceso
- Las señales se procesan en el módulo
- Mandan señales directamente a la CPU
- Tiene toda la pinta de ser PROFIBUS

**PROFI
BUS**





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



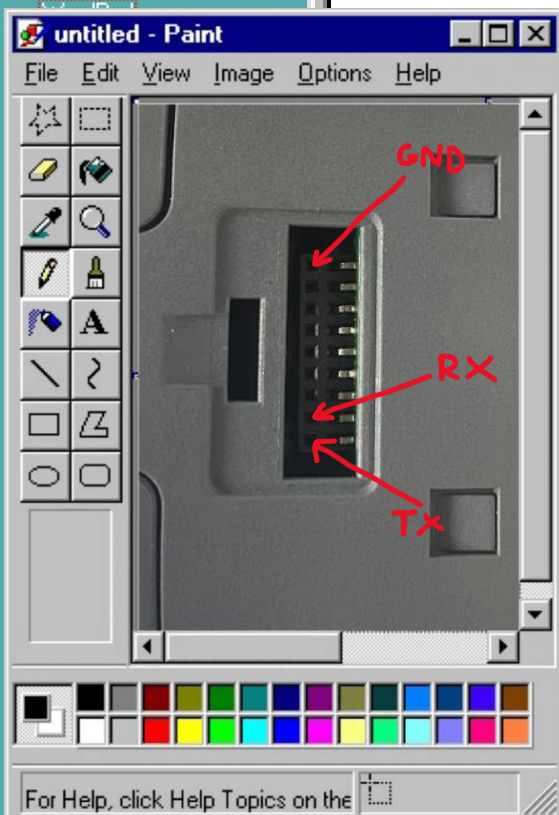
File Edit Search Help

Puerto izquierdo

SIEMENS

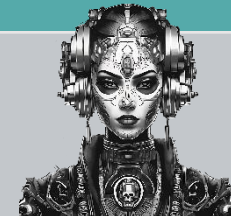
- Módulos de comunicación y proceso
- Las señales se procesan en el módulo
- Mandan señales directamente a la CPU
- Tiene toda la pinta de ser PROFIBUS
- UART integrado (según docs)

PROFI
BUS





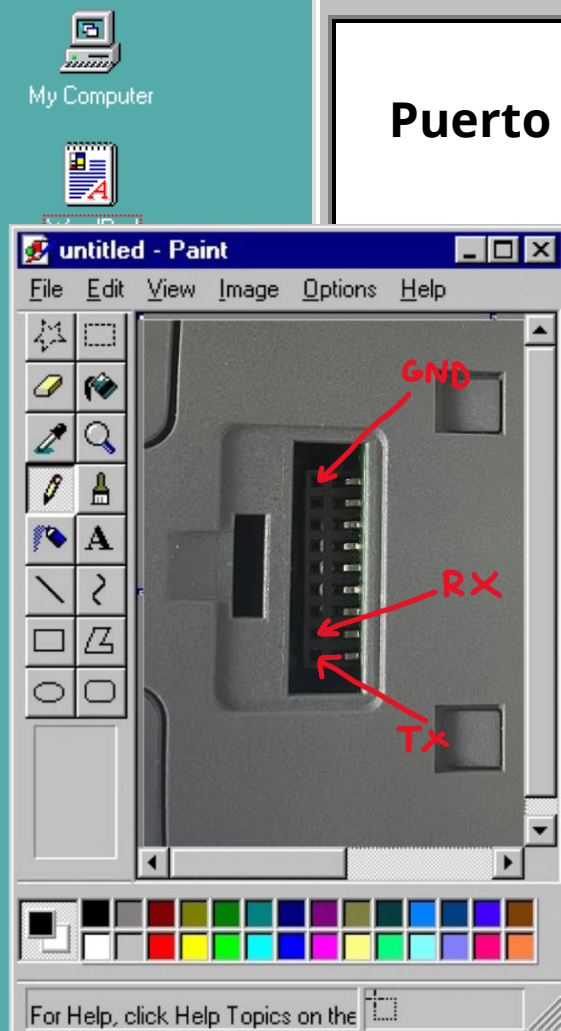
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



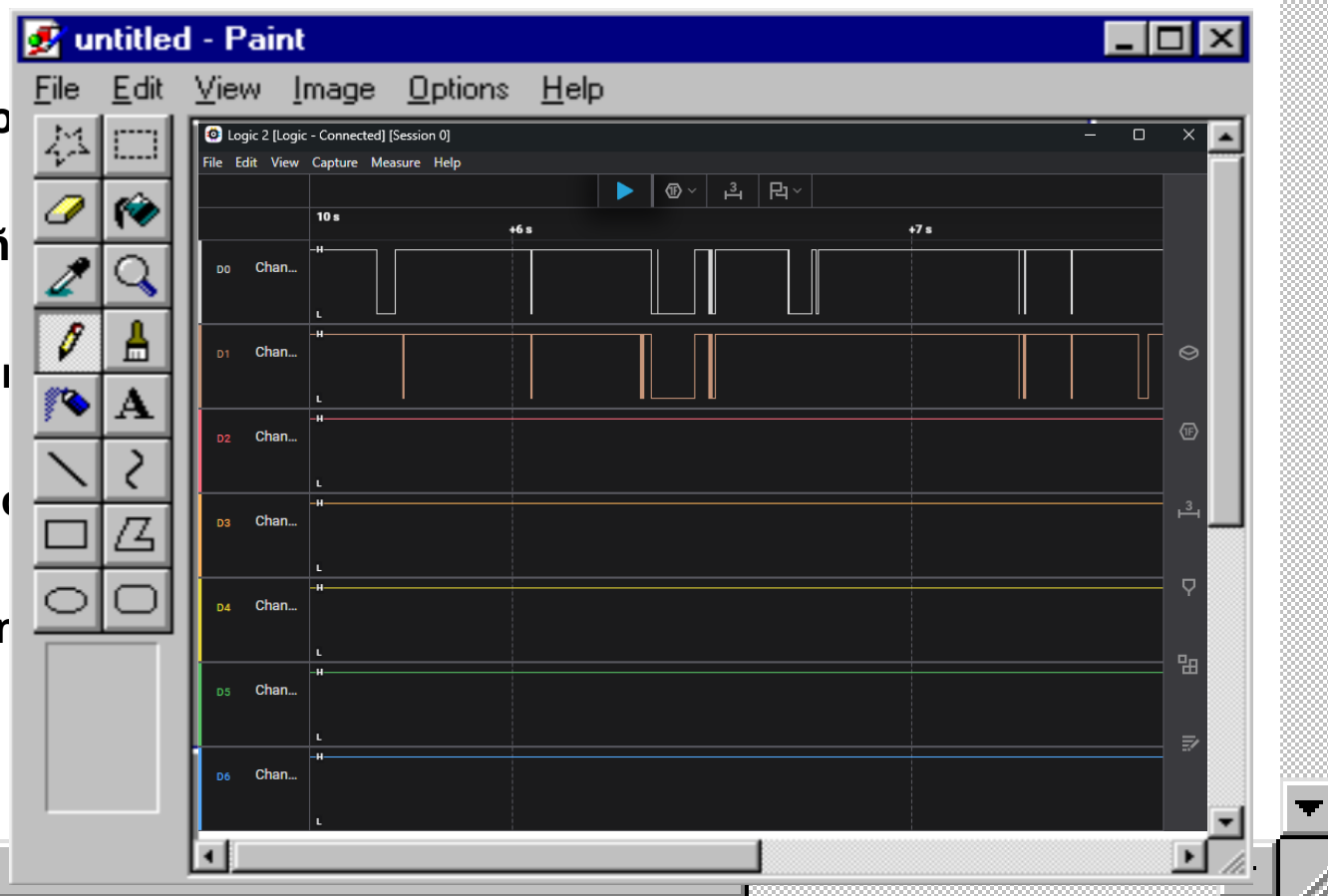
File Edit Search Help

Puerto izquierdo

SIEMENS

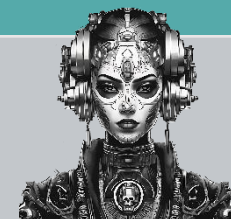


- Módulo
- Las señ
- Mandar
- Tiene t
- UART in





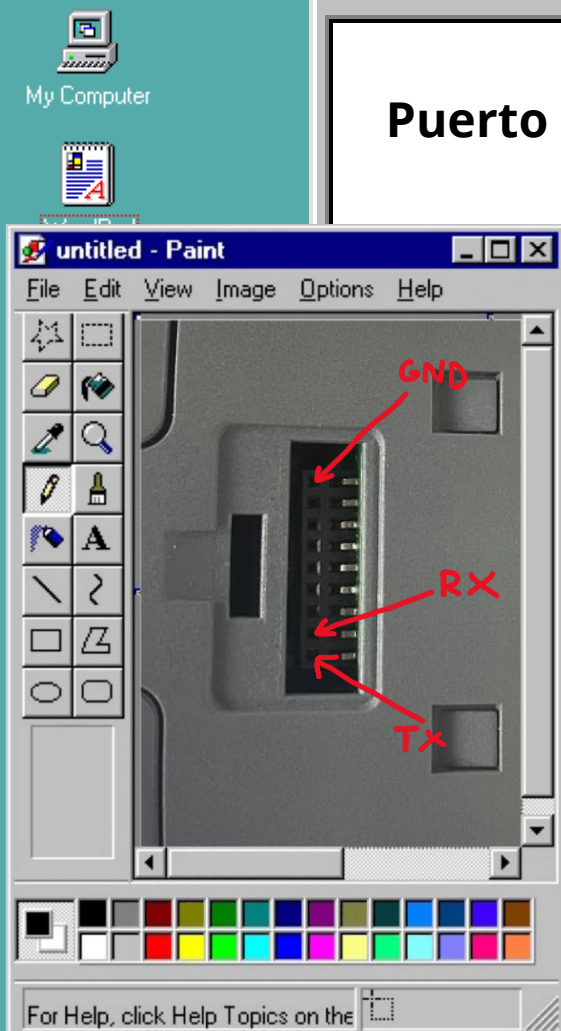
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



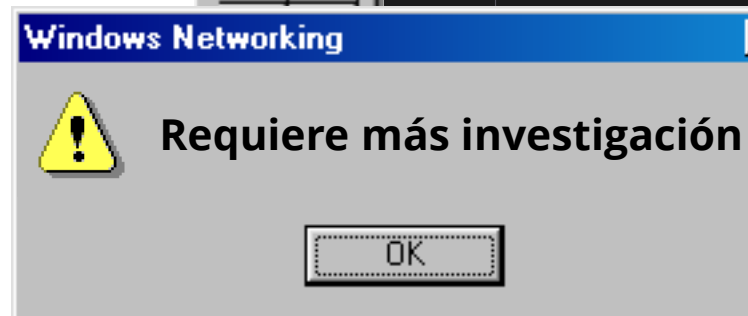
File Edit Search Help

Puerto izquierdo

SIEMENS

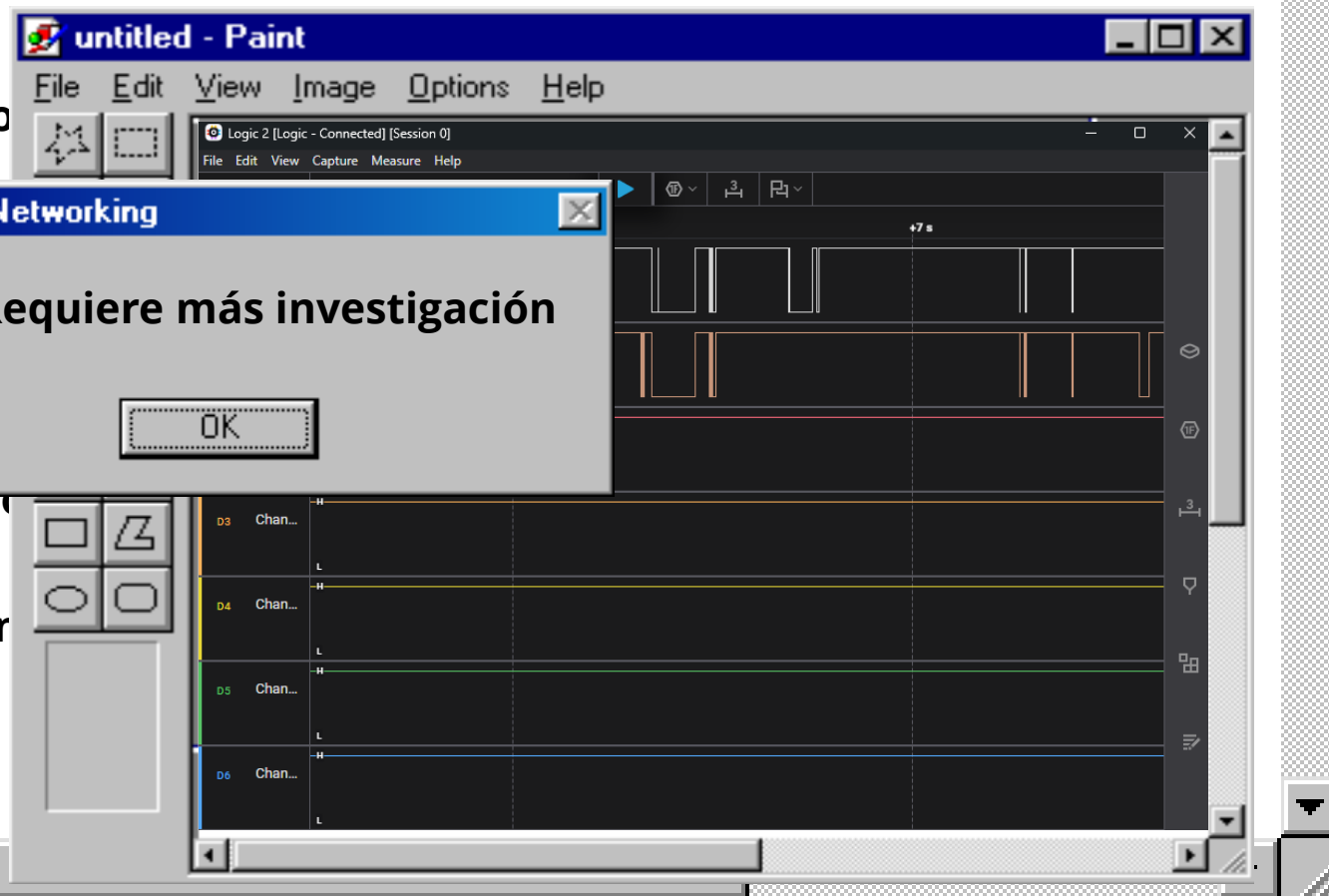


- Módulo



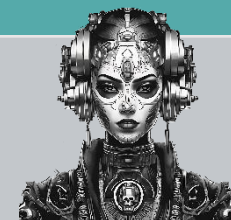
- Tiene t

- UART ir





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

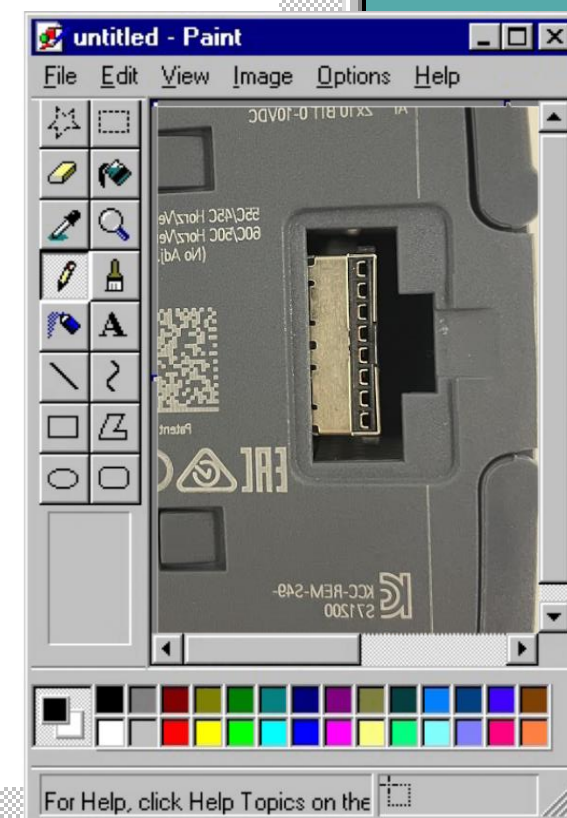


File Edit Search Help

Puerto derecho

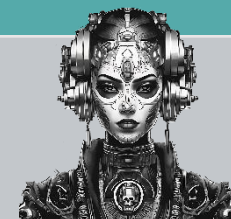
SIEMENS

- Módulos de señales
- Entradas/Salidas digitales y analógicas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

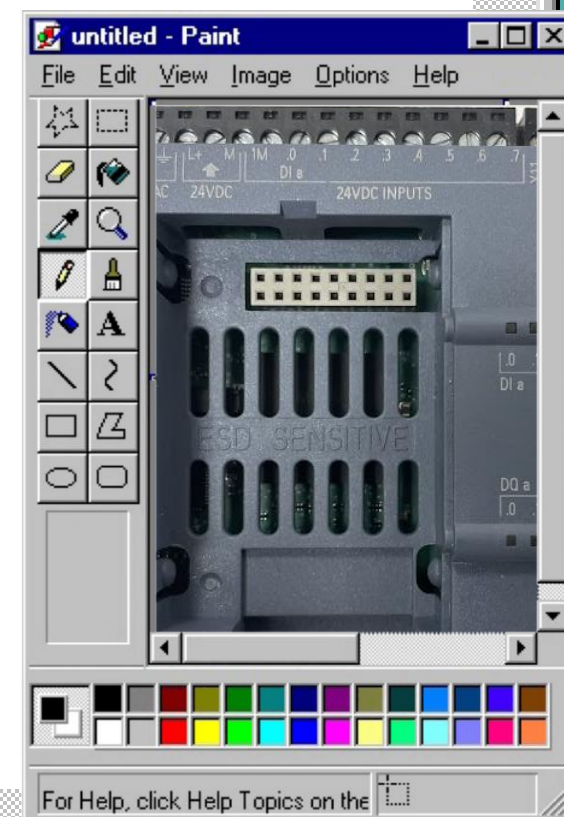


File Edit Search Help

Puerto central

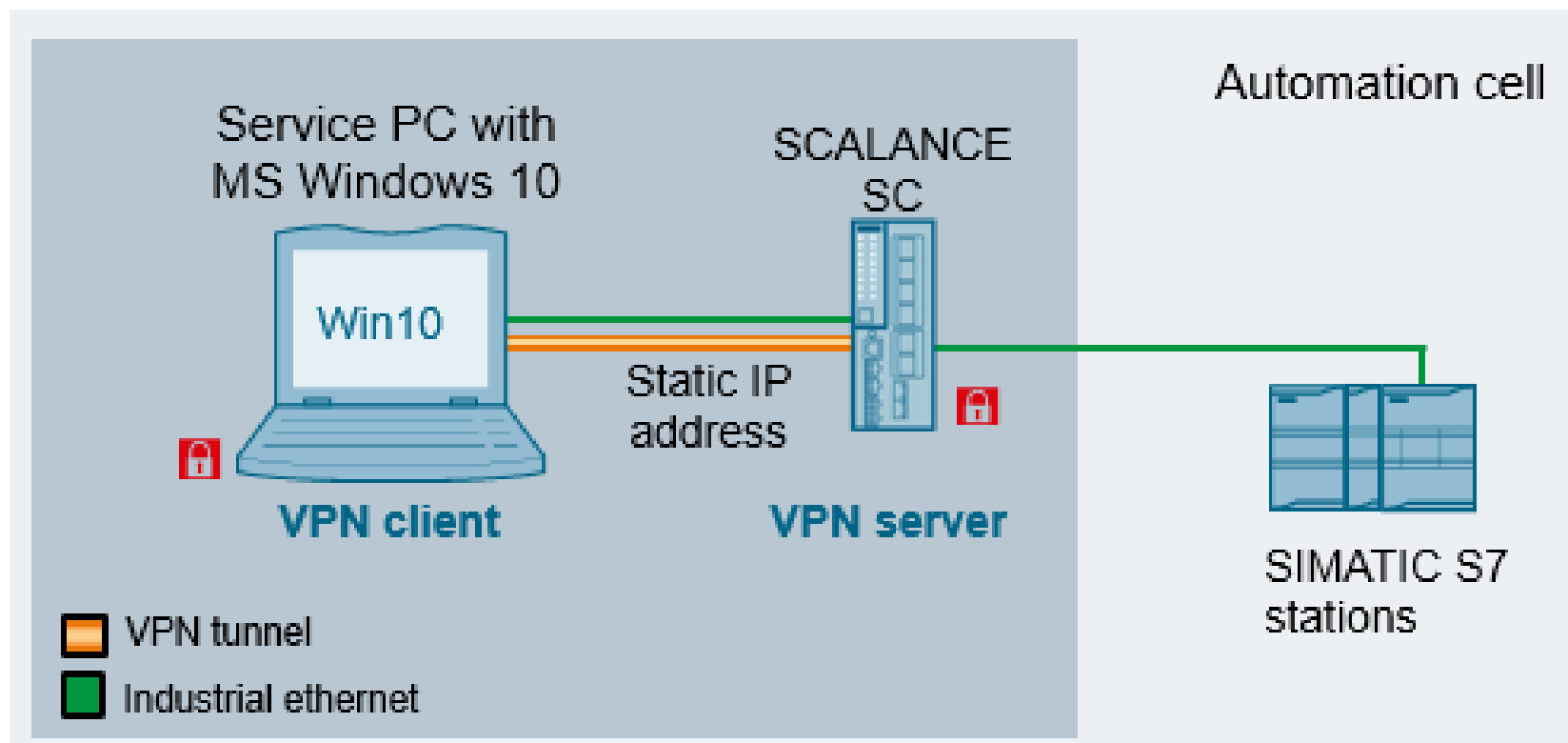
SIEMENS

- Módulos de señales
- Entradas/Salidas digitales y analógicas (menos)



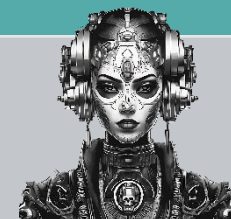


Fun fact





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



SIEMENS ▶

B&R

BECKHOFF ▶

PHOENIX CONTACT ▶

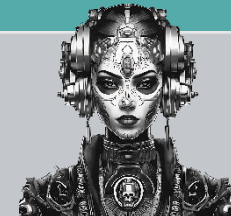
OMRON

Run...

Shut Down...



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

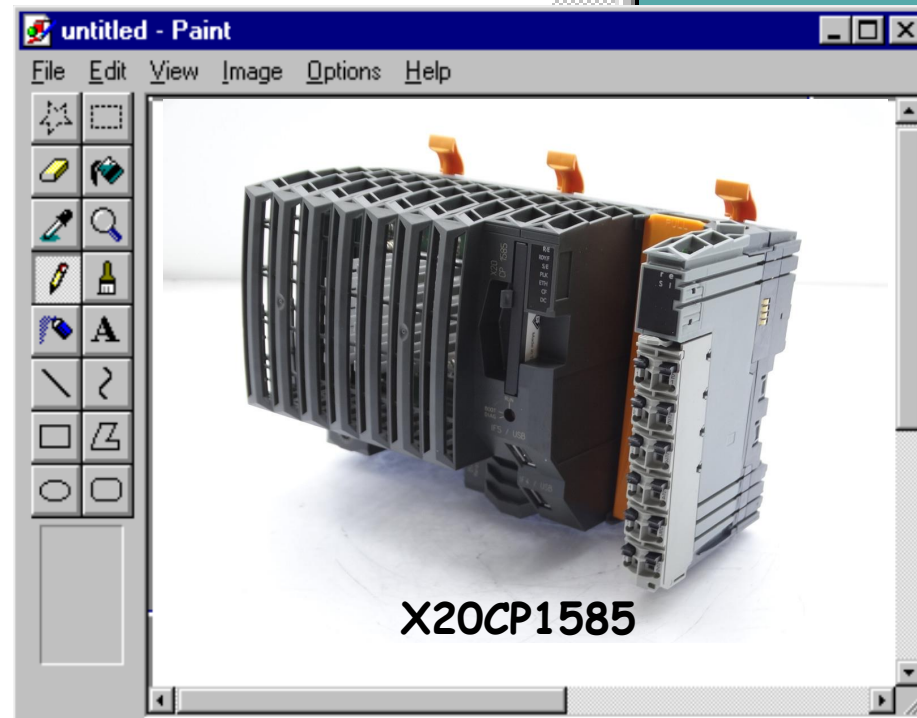


File Edit Search Help

Breakthrough

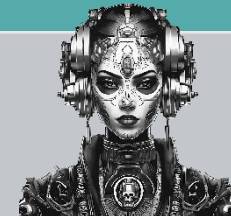
- **Protocolos POWERLINK y OPENSafety** (Downstream)
- **Protocolo AR** (Upstream)
- **Extracción del firmware**
- **Creación de módulos cargables**
- **Sistema X20** (Lateral)

B&R





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Ficha técnica

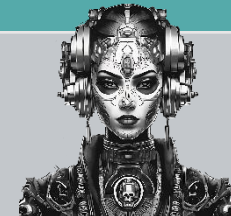


- **Arquitectura:** x86_64
- **OS base:** RTOS propietario de B&R
- **Entorno de programación:** B&R Automation Studio
- **Interfaces:** Ethernet, USB, POWERLINK, Sistema X20
- **Comunicaciones:** POWERLINK, OPENSafety, MODBUS TCP, AR





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

POWERLINK (Downstream)

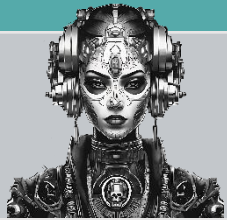


- **Protocolo Ethernet determinista por B&R con ethertype dedicado**
- **Basado en maestro-esclavo con ciclos temporizados**
- **Transmite datos en dos fases: tiempo real y asíncrona**
- **Soporte para IP en fase asíncrona (UDP)**





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



My Computer

WordPad

MS-DOS Prompt

Recycle Bin

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
124...	45.351128	B&RIndustria_20:e2...	B&RIndustria_00:49...	POWERLINK	88 240-> 2 PReq [64] F:RD=1,EA=0 V:0.0
124...	45.351128	B&RIndustria_00:49...	EPLv2_PRes	POWERLINK	176 2->255 PRes [152] F:RD=1,EN=0,RS=0,PR=0 V=0.0 NMT_CS_OPERATIONAL
124...	45.351128	B&RIndustria_20:e2...	B&RIndustria_00:49...	POWERLINK	88 240-> 3 PReq [64] F:RD=1,EA=0 V:0.0
124...	45.351128	B&RIndustria_00:49...	EPLv2_PRes	openSAFETY/Powerlink	240 SPDO Data with Time Response - 0x002, 0x003
124...	45.351128	B&RIndustria_20:e2...	B&RIndustria_00:49...	POWERLINK	88 240-> 4 PReq [64] F:RD=1,EA=0 V:0.0
124...	45.351128	B&RIndustria_20:e2...	EPLv2_SoA	POWERLINK	60 240->255 SoA (NO_SERVICE)->255 F:EA=0,ER=0 NMT_MS_OPERATIONAL
124...	45.353144	B&RIndustria_20:e2...	EPLv2_SoC	POWERLINK	60 240->255 SoC
124...	45.353144	B&RIndustria_20:e2...	B&RIndustria_1f:62...	openSAFETY/Powerlink	69 SPDO Data only - 0x006, 0x007
124...	45.353144	B&RIndustria_1f:62...	EPLv2_PRes	openSAFETY/Powerlink	130 SPDO Data only - 0x001, 0x009, 0x00A, 0x00B, 0x00C, 0x00D
124...	45.353144	B&RIndustria_20:e2...	B&RIndustria_00:49...	POWERLINK	88 240-> 2 PReq [64] F:RD=1,EA=0 V:0.0
124...	45.353144	B&RIndustria_00:49...	EPLv2_PRes	POWERLINK	176 2->255 PRes [152] F:RD=1,EN=0,RS=0,PR=0 V=0.0 NMT_CS_OPERATIONAL
124...	45.353144	B&RIndustria_20:e2...	B&RIndustria_00:49...	POWERLINK	88 240-> 3 PReq [64] F:RD=1,EA=0 V:0.0
124...	45.353144	B&RIndustria_00:49...	EPLv2_PRes	openSAFETY/Powerlink	240 SPDO Data with Time Response - 0x002, 0x003
124...	45.353144	B&RIndustria_20:e2...	B&RIndustria_00:49...	POWERLINK	88 240-> 4 PReq [64] F:RD=1,EA=0 V:0.0
124...	45.353144	B&RIndustria_20:e2...	EPLv2_SoA	POWERLINK	60 240->255 SoA (NO_SERVICE)->255 F:EA=0,ER=0 NMT_MS_OPERATIONAL
124...	45.354999	B&RIndustria_20:e2...	EPLv2_SoC	POWERLINK	60 240->255 SoC
124...	45.354999	B&RIndustria_20:e2...	B&RIndustria_1f:62...	openSAFETY/Powerlink	69 SPDO Data only - 0x006, 0x007
124...	45.354999	B&RIndustria_1f:62...	EPLv2_PRes	openSAFETY/Powerlink	130 SPDO Data only - 0x001, 0x009, 0x00A, 0x00B, 0x00C, 0x00D

> Frame 124351: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \

> Ethernet II, Src: B&RIndustria_20:e2:f7 (00:60:65:20:e2:f7), Dst: B&RIndustria_00:49:0

> Ethernet POWERLINK

.000 0011 = MessageType: PollRequest (PReq) (3)

Destination: 4 (0x04) (Controlled Node)

Source: 240 (0xf0) (Managing Node)

> Flags: 0x01, RD (Ready)

0... = FLS (First Link Status): False

.0.. = SLS (Second Link Status): False

PD0Version: 0.0

Size: 64

> PD0 - 2020:01

[Index: 2020]

[SubIndex: 01]

> Data (12 bytes)

Data: 1e03020000000000000000168

[Length: 12]

> PD0 - 2020:02

> PD0 - 2021:01

> PD0 - 2021:02

0000 00 60 65 00 49 04 00 60 65 20 e2 f7 88 ab 03 04 ..e.I... e

0010 f0 00 01 00 00 00 40 00 1e 03 02 00 00 00 00@.....

0020 00 00 01 68 9b 00 00 00 00 00 00 00 00 00 00 ...h.....

0030 00 00 00 00 00 00 00 00 1e 03 02 00 00 00 00S.....

0040 00 00 01 53 9b 00 00 00 00 00 00 00 00 00 00S.....

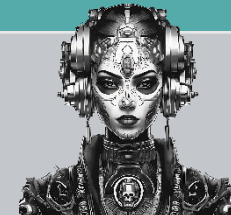
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00

No hay cifrado ni autenticación
Susceptible a:

- DoS
- Injection
- Spoofing



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

OPENSafety (Downstream)



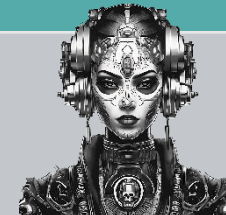
- Encapsulado en UDP sobre POWERLINK (fase asíncrona)
- Transmite datos críticos con redundancia
- Seguridad funcional SIL 3

Safety Integrity Level	Safety	Probability of Failure on Demand	Risk Reduction Factor
SIL 4	> 99,99 %	0,001 % - 0,01 %	100.000 - 10.000
SIL 3	99,9 % - 99,99 %	0,01 % - 0,1 %	10.000 - 1.000
SIL 2	99 % - 99,9 %	0,1 % - 1 %	1.000 - 100
SIL 1	90 % - 99 %	1 % - 10 %	100 - 10





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
105...	41.211181	B&RIndustria_20:e2...	B&RIndustria_1f:62...	openSAFETY/Powerlink	69 SPDO Data only - 0x006, 0x007
105...	41.211181	B&RIndustria_1f:62...	EPLv2_PRes	openSAFETY/Powerlink	130 SPDO Data only - 0x001, 0x009, 0x00A, 0x00B, 0x00C, 0x00D
105...	41.211181	B&RIndustria_20:e2...	B&RIndustria_00:49...	POWERLINK	88 240-> 2 PReq [64] F:RD=1,EA=0 V:0.0
105...	41.211181	B&RIndustria_00:49...	EPLv2_PRes	POWERLINK	176 2->255 PRes [152] F:RD=1,EN=0,RS=0,PR=0 V=0.0 NMT_CS_OPERATIONAL
105...	41.211181	B&RIndustria_20:e2...	B&RIndustria_00:49...	POWERLINK	88 240-> 3 PReq [64] F:RD=1,EA=0 V:0.0
105...	41.211181	B&RIndustria_00:49...	EPLv2_PRes	openSAFETY/Powerlink	240 SPDO Data only - 0x002, 0x003

> Frame 105560: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \

> Ethernet II, Src: B&RIndustria_20:e2:f7 (00:60:65:20:e2:f7), Dst: B&RIndustria_1f:62:5

> Ethernet POWERLINK

> openSAFETY, SPDO; Producer: 0x006 (6)

[Byte Offset: 0x0019]

[SCM UDID Auto Detect: 00:60:65:01:a2:e5]

[SCM UDID Valid: True]

> SN send from: 0x0006

[Safety Node: 0x0006]

[Safety Domain: 0x0001]

> [110. = Type: openSAFETY SPDO (0x6)]

Message: SPDO Data only (0xc0)

.... 0... = Send to: Consumer

.... .1.. = Connection Valid Bit: Set

[Consecutive Time: 0x56F8 [22264] (Complete)]

> SPDO Feature Flags: 0x00

> Data (2 bytes)

Data: 030f

[Length: 2]

Length: 2

> CRC for subframe #1: 0x008A

[Is Valid: True]

CRC Type: CRC8 (1)

> CRC for subframe #2: 0x0077

[Is Valid: True]

> openSAFETY, SPDO; Producer: 0x007 (7)

[Byte Offset: 0x0028]

[SCM UDID Auto Detect: 00:60:65:01:a2:e5]

[SCM UDID Valid: True]

> SN send from: 0x0007

> [110. = Type: openSAFETY SPDO (0x6)]

Length: 2

> CRC for subframe #1: 0x0090

> CRC for subframe #2: 0x00A5

0000 00 60 65 1f 62 5f 00 60 65 20 e2 f7 88 ab 03 01 ..e.b..e.....

0010 f0 00 01 00 00 00 2d 00 00 06 c4 02 f8 03 0f 8aw.....

0020 07 a4 33 01 a2 e6 0f 77 07 c4 02 f7 00 0f 90 06 ..3.....

0030 a4 34 01 a2 e5 0f a5 00 00 00 00 00 00 00 00 ..4.....

0040 00 00 00 00 00

Frame (69 bytes) openSAFETY Frame (15 bytes) openSAFETY Frame (15 bytes)

Mejoras:

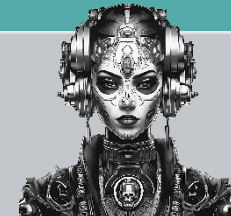
- Redundancia de datos
- Integridad (checksums)

Siguen igual de mal:

- Cifrado (ninguno)
- Autenticación (nada)
- Resistencia a DoS



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Automation Runtime (Upstream) TCP:11169



- Acceso en tiempo real a variables, memoria y config
- Permite descarga de módulos, actualizaciones y firmware
- Permite diagnóstico, monitoreo y comandos remotos





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Automation Runtime (Upstream) TCP:11169



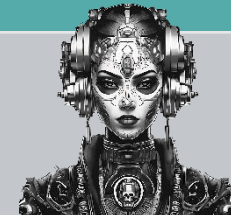
- Acceso en tiempo real a variables, memoria y config
- Permite descarga de módulos, actualizaciones y firmware
- Permite diagnóstico, monitoreo y comandos remotos
- **POR DEFECTO SE MANDA TODO EN TEXTO PLANO SIN CIFRADO NI**

AUTENTICACIÓN





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Automation Runtime (Upstream) TCP:11169



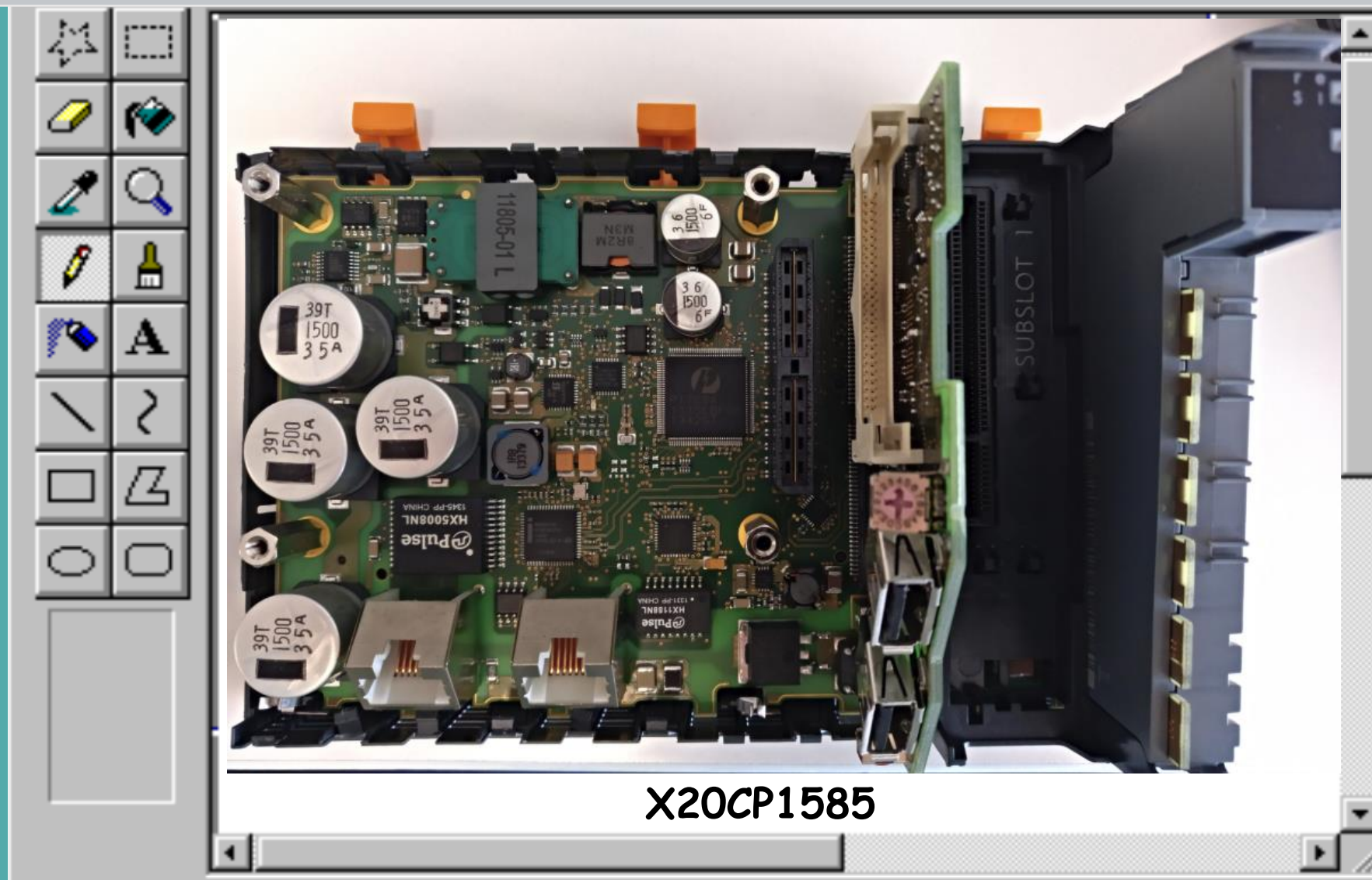
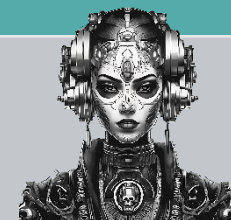
Comandos disponibles

- **GetSymbol**
- **GetSymbolTable**
- **ReadVar**
- **WriteVar**
- **ExecuteCommand**
- **DownloadObject**
- **UploadObject**
- **GetConfig**
- **SetConfig**
- **InvokeFunction**



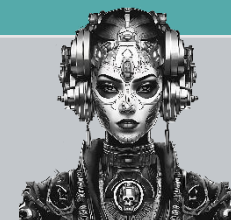


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



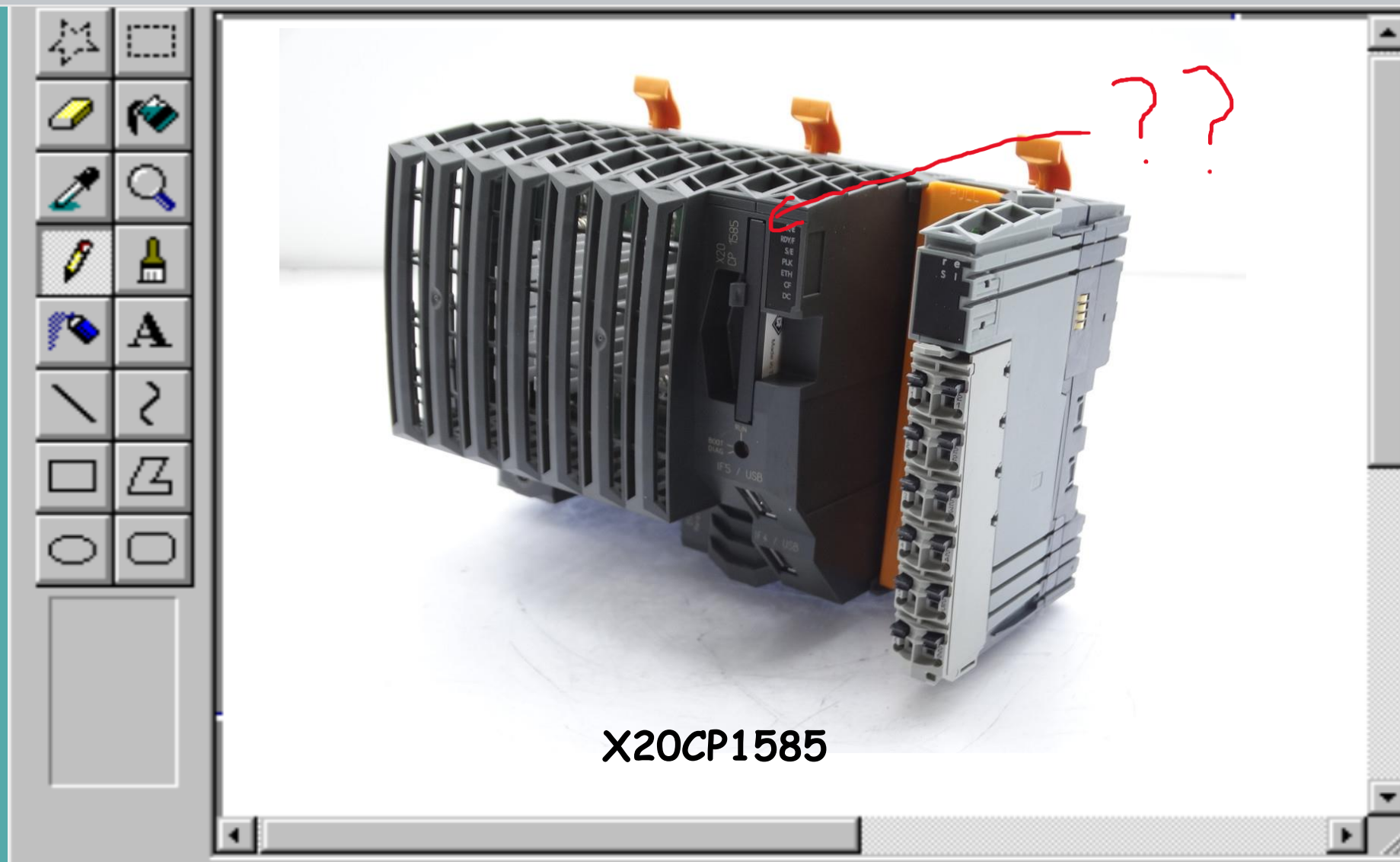
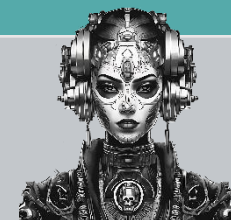


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





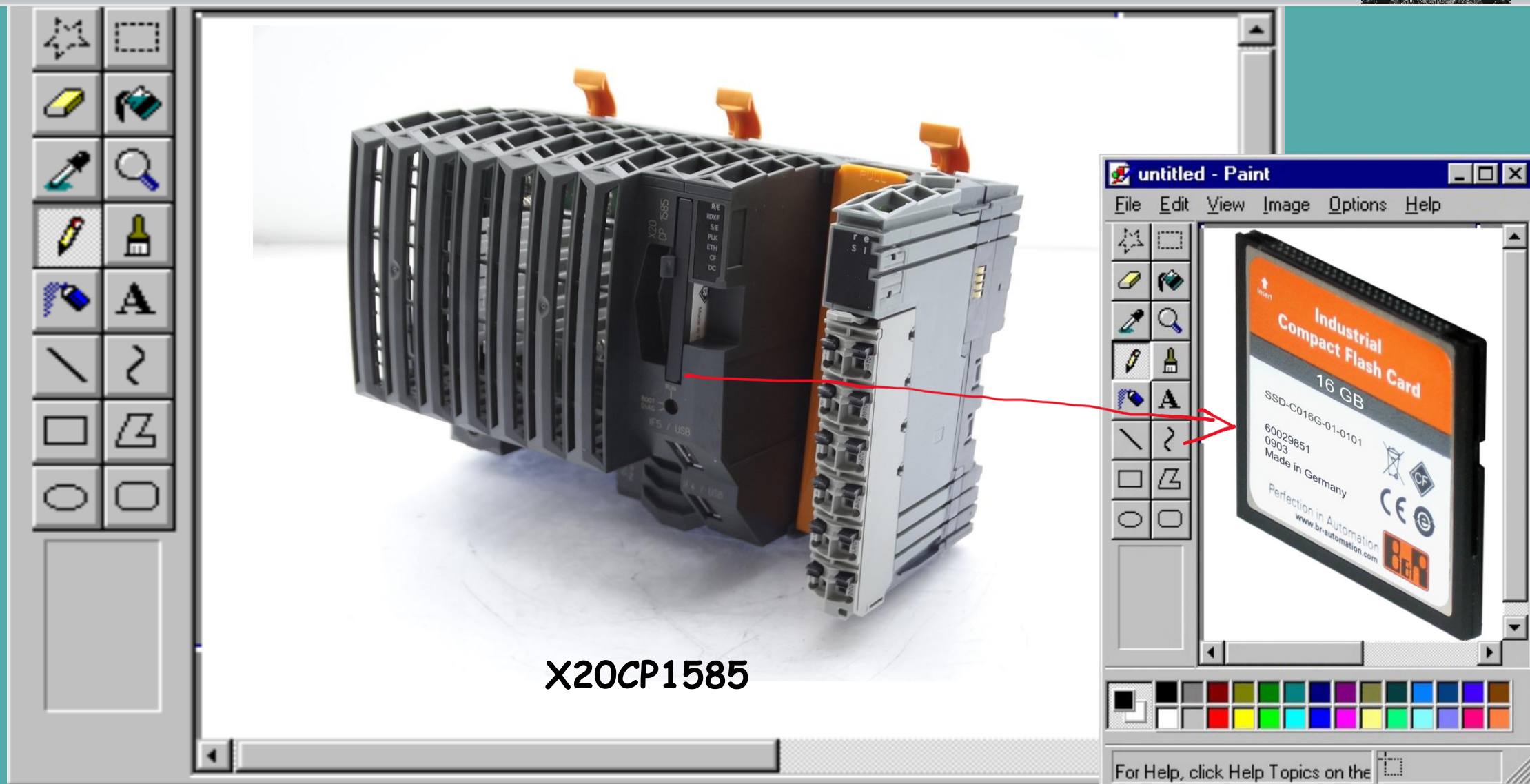
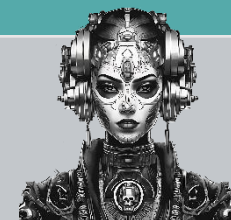
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



X20CP1585



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



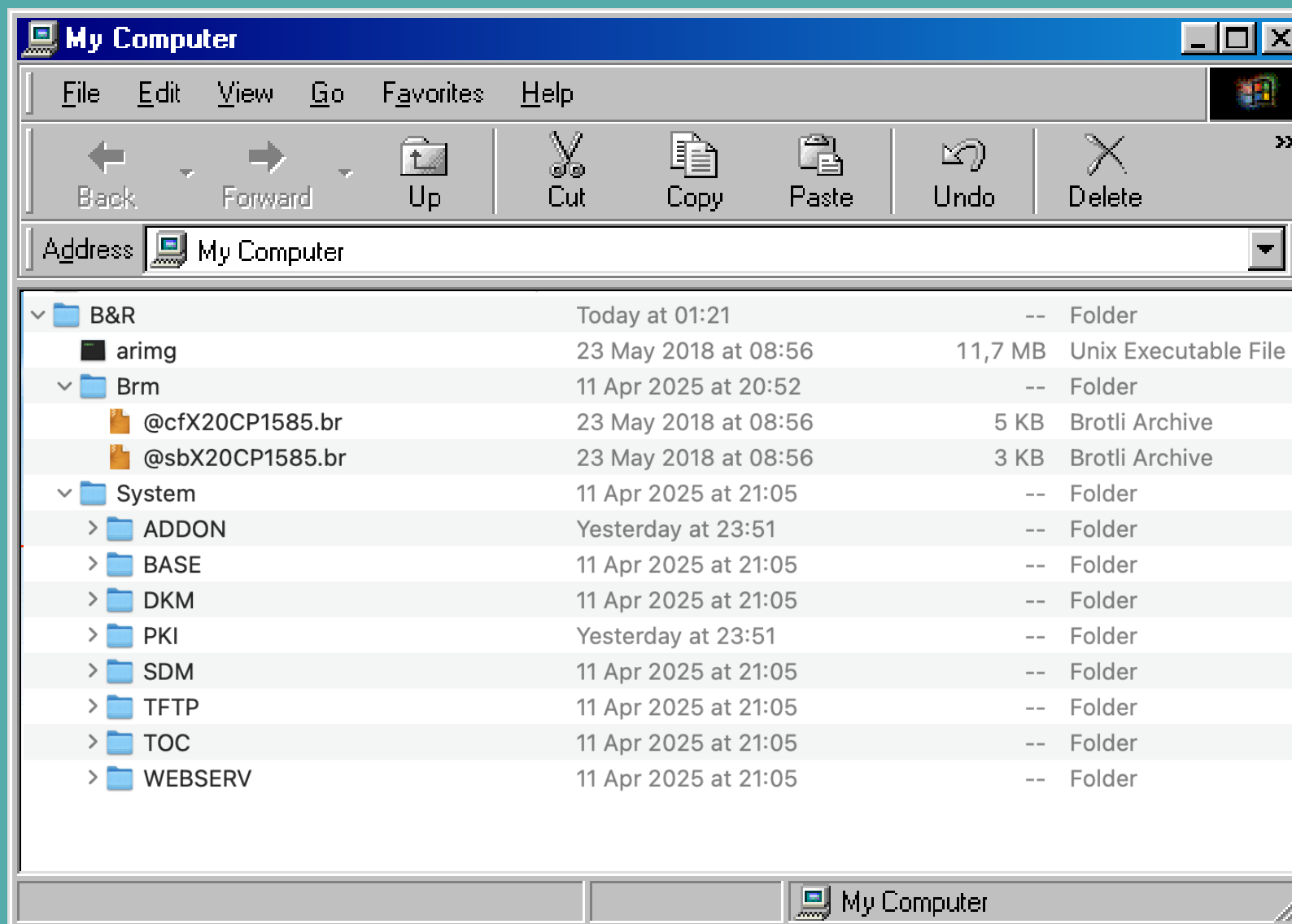
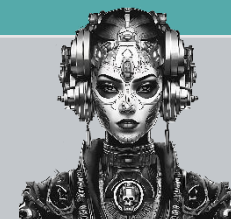


Fun Fact:



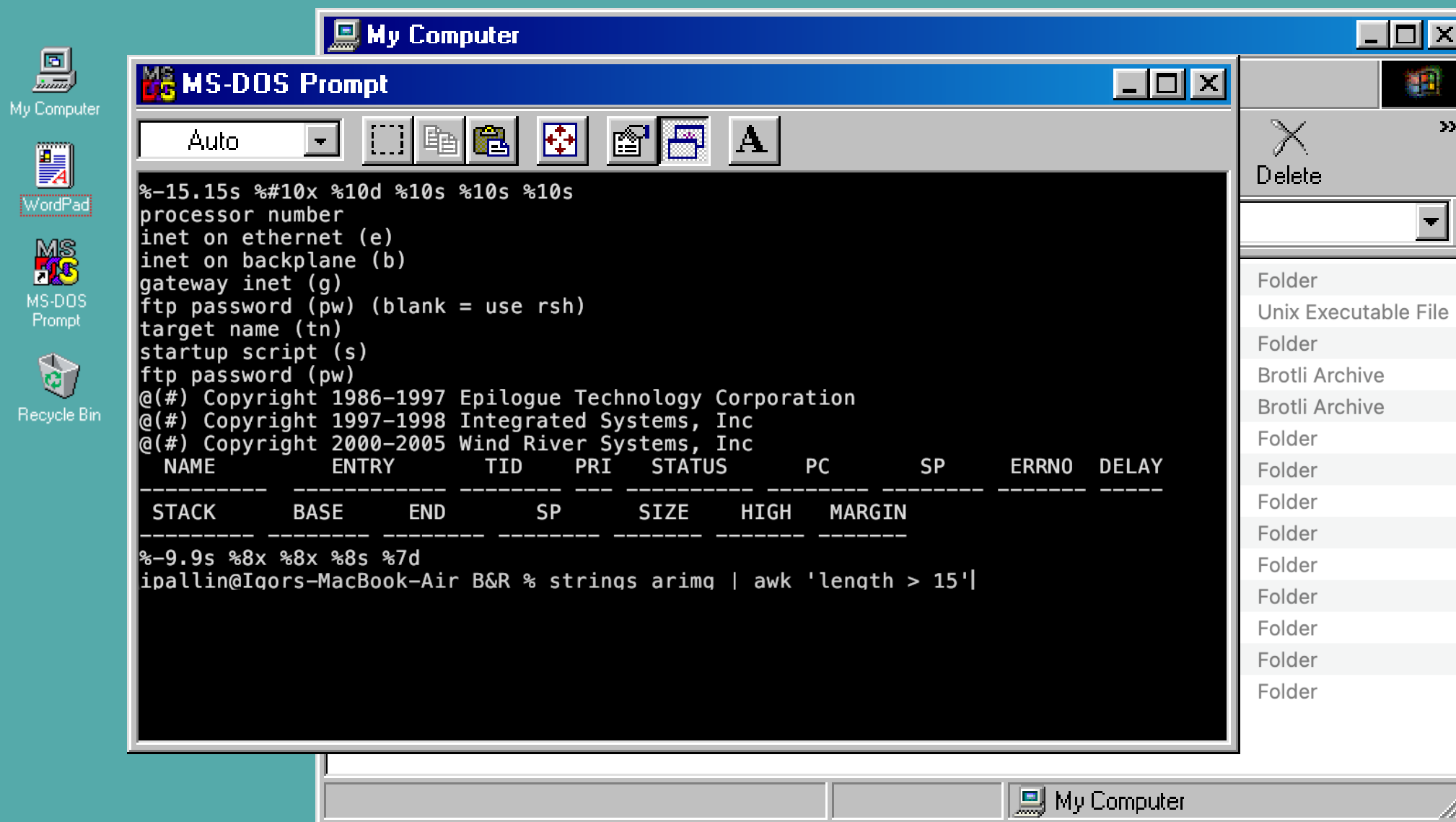
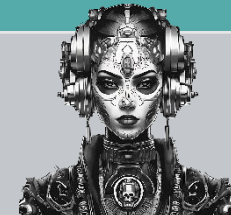


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



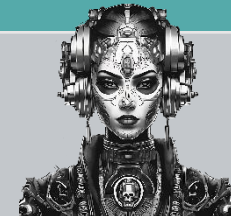


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Descubrimientos principales

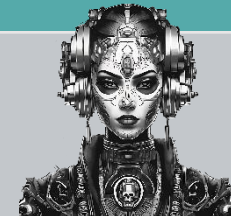


- RTOS base: VxWorks 6.9 (Wind River Systems - 2011)
- Automation Runtime de B&R sobre el RTOS
- Módulos cargables (DKM) ← !!!
- Drivers modulares: Powerlink, CAN, Modbus, Profibus
- Hardware tree jerárquico con descriptores XML





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Descubrimientos principales (Servicios)

B&R

- **FTP: Wind River FTP**
- **Telnet y shell VxWorks con login**
- **HTTP: servidor AsHttp con posible configuración web**
- **SNMP v1/v2/v3 con tablas y usuarios**
- **SMB/CIFS: servidor de archivos con contraseña por defecto**





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Desarrollo de módulos cargables

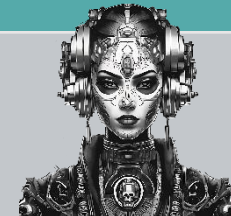


- Crear el modulo en C/C++
- Compilar .o compatible con el target B&R
- Ubicar el modulo en C:/SYSTEM/DKM/
- Editar el descriptor C:/SYSTEM/DKM/dkms.xml
- Para la prueba creamos un TCP listener en el puerto 4096





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit **Borland C++ - hello** View Project Script Tool Debug Options Window Help

Desarrollo

- Crear
- Configurar
- Utilizar
- Ejecutar
- Paquetes

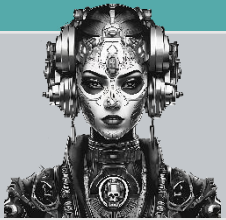
```
B&R > C dkm_tcp_listener.c > ...
38 void listenerTask(void) {
46     serverAddr.sin_family = AF_INET;
47     serverAddr.sin_port = htons(PORT);
48     serverAddr.sin_addr.s_addr = INADDR_ANY;
49
50     if (bind(g_sock, (struct sockaddr*)&serverAddr, sizeof(serverAddr)) < 0) return;
51
52     while (1) {
53         int recvLen = recvfrom(g_sock, recvBuf, BUF_SIZE - 1, 0, (struct sockaddr*)&clientAddr, &addrLen);
54         if (recvLen > 0) {
55             recvBuf[recvLen] = '\0';
56             processCommand(recvBuf);
57         }
58     }
59 }
60
61 DINT dkmInitialize(void) {
62     g_taskId = sysTaskCreate(g_taskName, 10, 4096, (UDINT)listenerTask);
63     return (g_taskId != 0) ? 0 : 1;
64 }
65
66 DINT dkmTerminate(void) {
67     if (g_sock > 0) close(g_sock);
68     sysTaskDelete(g_taskId);
69     return 0;
70 }

dkms.xml x
B&R > System > DKM > dkms.xml
1 <?xml version="1.0" encoding="utf-8"?>
2 <DKMS>
3 <DKM PATH="C:/SYSTEM/DKM/dkm_opcua_partialImage.o" INIT="opcuaInit" SUCCESS="0"/>
4 <DKM PATH="C:/SYSTEM/DKM/dkm_dev_gdbserver_partialImage.o" INIT="dkm_dev_gdbserver_Init" SUCCESS="0" SUPPRESS_WARNING="1"/>
5 <DKM PATH="C:/SYSTEM/DKM/dkm_scm_partialImage.o" INIT="ScmScRegister" SUCCESS="0"/>
6 <DKM PATH="C:/SYSTEM/DKM/dkm_arUTFramework_partialImage.o" INIT="dkm_arUTFrameworkInit" SUCCESS="0" SUPPRESS_WARNING="1"/>
7 <DKM PATH="C:/SYSTEM/DKM/dkm_arUT_partialImage.o" INIT="dkm_arUT_Init" SUCCESS="0" SUPPRESS_WARNING="1"/>
8 <DKM PATH="C:/SYSTEM/DKM/dkm_gdbserver_x86_partialImage.o" INIT="dkmGdbserverX86Init" SUCCESS="0" SUPPRESS_WARNING="0"/>
9 <DKM PATH="C:/SYSTEM/DKM/dkm_rbac_partialImage.o" INIT="dkm_rbac_Init" SUCCESS="0" SUPPRESS_WARNING="0"/>
10
11 <DKM PATH="C:/SYSTEM/DKM/dkm_tcp_listener.o" INIT="dkmInitialize" SUCCESS="0"/>
12 </DKMS>
```





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

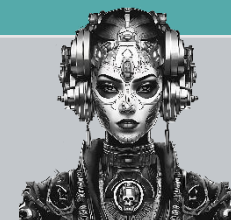
Módulos extra (Físicos)

B&R





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Módulos extra
(Físicos)

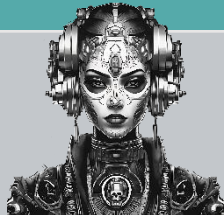
X20

B&R





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Sistema X20

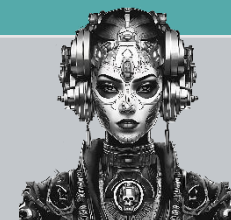


Pin	Señal	Dirección	Descripción
1	+24V	Entrada	Alimentación del módulo
2	GND	—	Tierra
3	CLK	CPU → módulo	Señal de reloj del sistema (sincronización)
4	DATA_OUT	CPU → módulo	Datos enviados por la CPU
5	DATA_IN	módulo → CPU	Datos enviados por el módulo
6	SYNC	CPU → módulo	Pulso de sincronización por ciclo
7	SLOT_ID	módulo ← CPU	Identificación lógica de slot
8	MOD_ID	módulo → CPU	Tipo de módulo y características
9	RESET	CPU → módulo	Restablecer estado del módulo (si aplica)





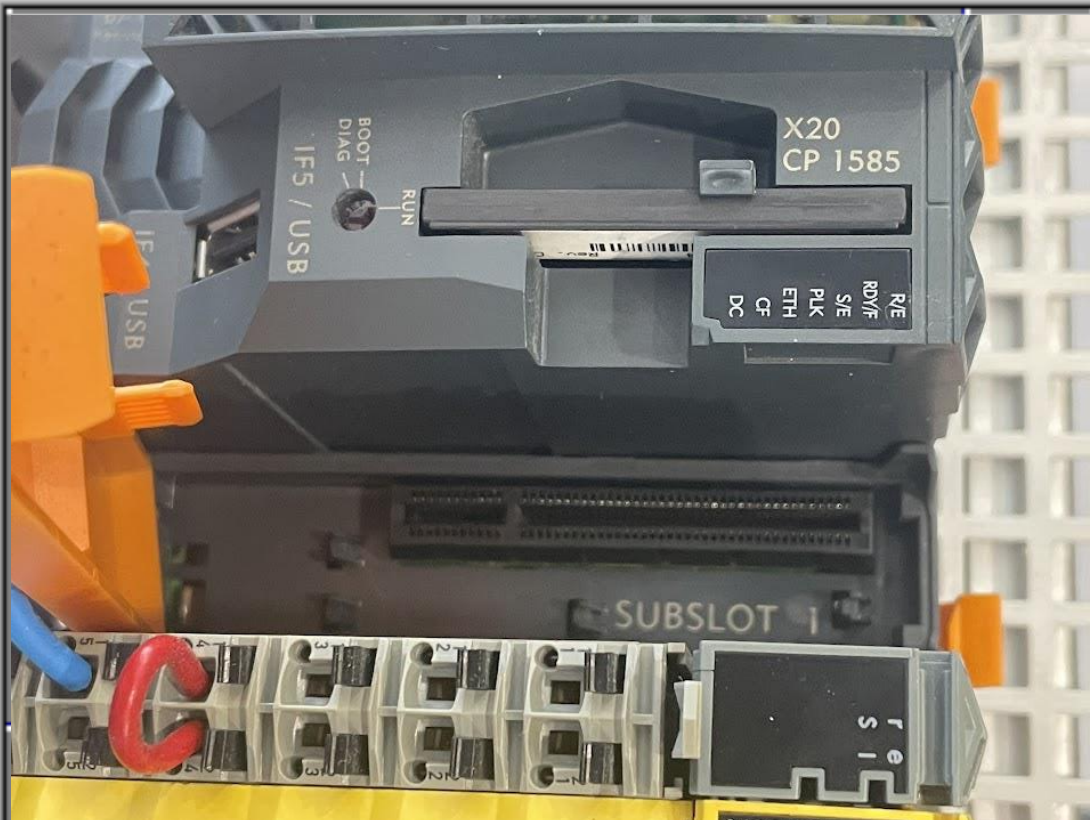
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

untitled - Paint

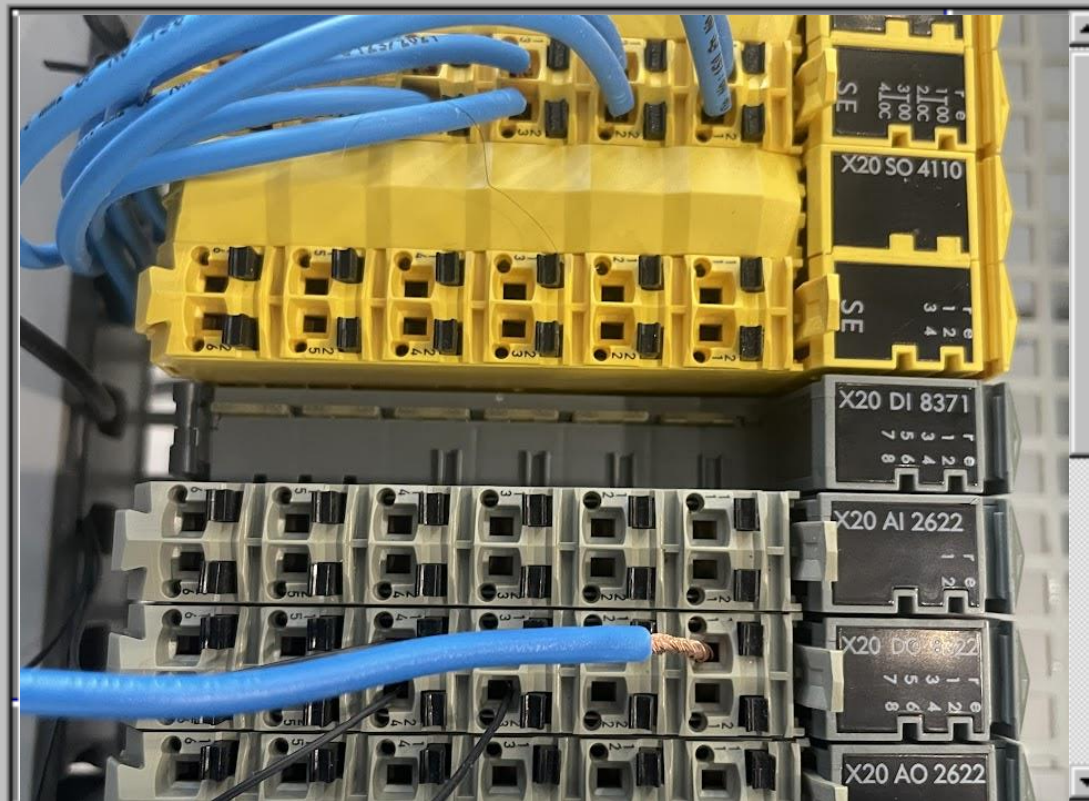
File Edit View Image Options Help



R-D

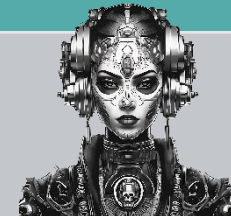
titled - Paint

Edit View Image Options Help



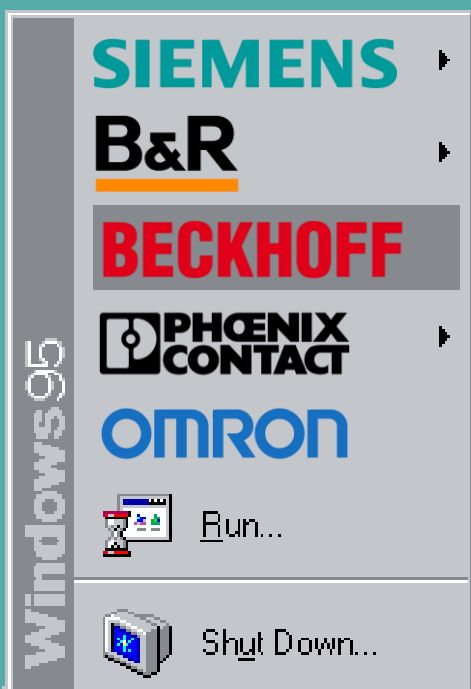
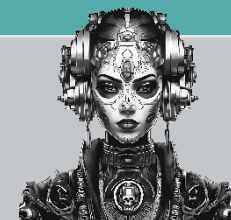


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



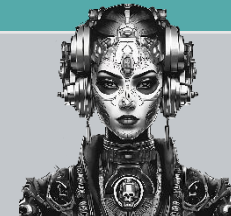


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

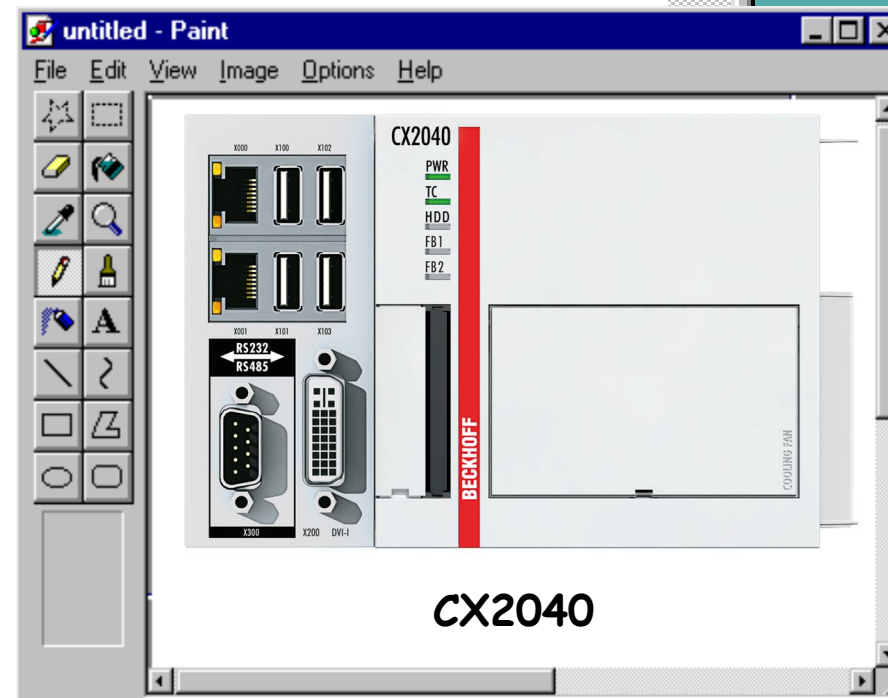


File Edit Search Help

Breakthrough

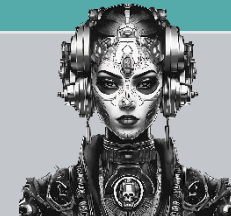
- **Protocolo ETHERCAT** (Downstream)
- **Creación de esclavos**
- **Extracción del firmware?**
- **Virtualización de PLCs**
- **K-Bus / E-Bus** (Lateral)

BECKHOFF





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Ficha técnica

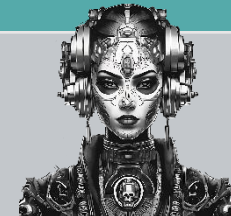
BECKHOFF

- **Arquitectura:** x86_64
- **OS base:** Windows ce
- **Entorno de programación:** TwinCAT 2
- **Interfaces:** Ethernet, USB, DVI, RS232/RS485, K-bus/E-bus
- **Comunicaciones:** ADS, Modbus/TCP, OPC UA, EtherCAT, Profinet, CANopen





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

ETHERCAT

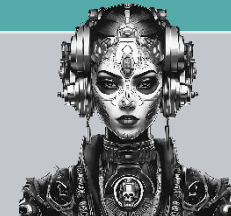
BECKHOFF

- Utiliza capa 2 directamente (Ethertype 0x88A4)
- Topología en cadena o Anillo (La misma trama pasa por todos los nodos secuencialmente)
- Cada esclavo lee y escribe sus datos en tiempo real dentro de una única trama





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
120	0.236431	MS-NLB-PhysServer...	Broadcast	ECAT	116 7 Cmds, SumLen 16, 'FPWR'...
121	0.246657	Oracle_23:98:cf	Broadcast	ECAT	198 11 Cmds, SumLen 50, 'FPRD'...
122	0.246678	MS-NLB-PhysServer...	Broadcast	ECAT	198 11 Cmds, SumLen 50, 'FPRD'...
123	0.246919	Oracle_23:98:cf	Broadcast	ECAT	116 7 Cmds, SumLen 16, 'FPWR'...
124	0.246933	MS-NLB-PhysServer...	Broadcast	ECAT	116 7 Cmds, SumLen 16, 'FPWR'...
125	0.257144	Oracle_23:98:cf	Broadcast	ECAT	198 11 Cmds, SumLen 50, 'FPWR'...
126	0.257165	MS-NLB-PhysServer...	Broadcast	ECAT	198 11 Cmds, SumLen 50, 'FPWR'...
127	0.257385	Oracle_23:98:cf	Broadcast	ECAT	122 7 Cmds, SumLen 22, 'FPRD'...

> Frame 121: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits)

> Ethernet II, Src: Oracle_23:98:cf (00:14:4f:23:98:cf), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> EtherCAT frame header

- 000 1011 0110 = Length: 0x0b6
- 0... .. = Reserved: Valid (0x0)
- 0001 = Type: EtherCAT command (0x1)

> EtherCAT datagram(s): 11 Cmds, SumLen 50, 'FPRD'...

- > EtherCAT datagram: Cmd: 'FPRD' (4), Len: 10, Adp 0x1001, Ado 0x502, Cnt 0
 - > Header
 - Cmd : 4 (Configured address Physical Read)
 - Index: 0xf8
 - Slave Addr: 0x1001
 - Offset Addr: 0x0502
 - > Length : 10 (0xa) - No Roundtrip - More Follows...
 - Interrupt: 0x0000
 - Working Cnt: 0

> EtherCAT datagram: Cmd: 'FPWR' (5), Len: 4, Adp 0x1004, Ado 0x502, Cnt 0

> EtherCAT datagram: Cmd: 'FPWR' (5), Len: 4, Adp 0x1000, Ado 0x502, Cnt 0

> EtherCAT datagram: Cmd: 'FPRD' (4), Len: 10, Adp 0x1003, Ado 0x502, Cnt 0

> EtherCAT datagram: Cmd: 'FPRD' (4), Len: 10, Adp 0x1002, Ado 0x502, Cnt 0

> EtherCAT datagram: Cmd: 'BRD' (7), Len: 2, Adp 0x0, Ado 0x130, Cnt 0

> EtherCAT datagram: Cmd: 'APRD' (1), Len: 2, Adp 0x0, Ado 0x130, Cnt 0

> EtherCAT datagram: Cmd: 'APRD' (1), Len: 2, Adp 0xffff, Ado 0x130, Cnt 0

> EtherCAT datagram: Cmd: 'APRD' (1), Len: 2, Adp 0xfffe, Ado 0x130, Cnt 0

> EtherCAT datagram: Cmd: 'APRD' (1), Len: 2, Adp 0xfffd, Ado 0x130, Cnt 0

> EtherCAT datagram: Cmd: 'APRD' (1), Len: 2, Adp 0xfffc, Ado 0x130, Cnt 0

0000 ff ff ff ff ff ff 00 14 4f 23 98 cf 88 a4 b6 10 0#.....

0010 04 f8 01 10 02 05 0a 80 00 00 00 00 00 00 00

0020 00 00 00 00 00 00 05 f9 04 10 02 05 04 80 00 00

0030 00 01 46 00 00 00 05 fa 00 10 02 05 04 80 00 00 F.....

0040 00 01 44 00 00 00 04 fb 03 10 02 05 0a 80 00 00 D.....

0050 00 00 00 00 00 00 00 00 00 00 00 00 04 fc 02 10

0060 02 05 0a 80 00 00 00 00 00 00 00 00 00 00 00

0070 00 00 07 fd 00 00 30 01 02 80 00 00 00 00 00 00 0.....

0080 01 fe 00 00 30 01 02 80 00 00 00 00 00 01 ff 0.....

0090 ff ff 30 01 02 80 00 00 00 00 00 00 01 01 fe ff 0.....

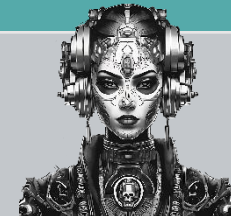
00a0 30 01 02 80 00 00 00 00 00 00 01 02 fd ff 30 01 0.....

00b0 02 80 00 00 00 00 00 00 01 03 fc ff 30 01 02 00 0.....

00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Creación de esclavos

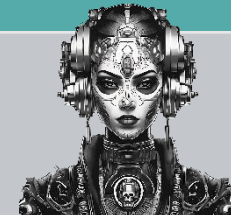
BECKHOFF

- A efectos prácticos un ataque de replay
- Permiten generar un entorno simulado más complejo
- Meter valores anómalos de forma manual





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File

Borland C++ - hello

File Edit Search View Project Script Tool Debug Options Window Help

ethercat_fake_slave > src > main.rs > ...

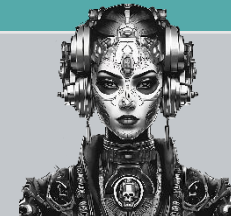
Cre

```
8 fn main() {
23     match rx.next() {
24         Ok(packet: &[u8]) => {
25             let eth_packet: EthernetPacket<'_> = EthernetPacket::new(packet).unwrap();
26             if eth_packet.get_ethertype().0 == ETHERCAT_TYPE {
27                 println!("[+] EtherCAT packet captured from {}", eth_packet.get_source());
28
29                 let payload: &[u8] = eth_packet.payload();
30                 println!("Payload ({} bytes): {:x?}", payload.len(), payload);
31
32                 let source_mac: MacAddr = eth_packet.get_destination();
33                 let dest_mac: MacAddr = eth_packet.get_source();
34                 let mut buffer: [u8; 1500] = [0u8; MAX_PACKET_SIZE];
35                 let mut response: MutableEthernetPacket<'_> = MutableEthernetPacket::new(packet: &mut buffer).unwrap();
36
37                 response.set_source(val: source_mac);
38                 response.set_destination(val: dest_mac);
39                 response.set_ethertype(val: pnet::packet::ethernet::EtherType(ETHERCAT_TYPE));
40
41                 let ethercat_data: [u8; 20] = [
42                     0x01, 0x10,           // EtherCAT Type: LRW
43                     0x00, 0x00,           // Reserved / Index (0)
44                     0x01, 0x00,           // Address Position (ADP) (0x0001)
45                     0x00,                 // Address Offset (ADO)
46                     0x00,                 // Reserved
47                     0x04, 0x00,           // Length: 4 bytes
48                     0x00, 0x00,           // Interrupt enable / reserved
49                     0x00, 0x00,           // Data (4 bytes) - dummy
50                     0x11, 0x22, 0x33, 0x44, // Example data
51                     0x04,                 // Working Counter (WKC)
52                     0x00,                 // FCS padding (not CRC)
53                 ];
54
55                 response.set_payload(vals: &ethercat_data);
56
57                 match tx.send_to(response.packet(), dst: Some(interface.clone())) {
58                     Some(Ok(_)) => println!("[+] Respuesta EtherCAT (LRW) enviada a {}", dest_mac),
59                     Some(Err(e: Error)) => eprintln!("Error sending response: {}", e),
60                     None => eprintln!("No transmitter available"),
61                 }
62             }
63         }
64     }
65 }
```

FF



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Entorno simulado

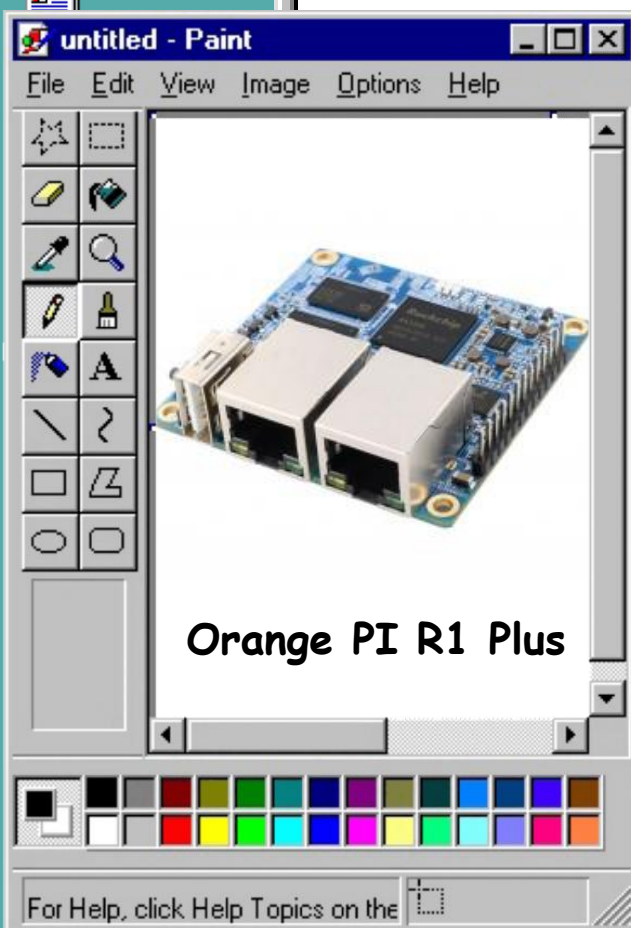
BECKHOFF

PLC

SL 1

SL 3

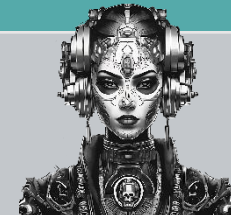
SL 2



Orange PI R1 Plus



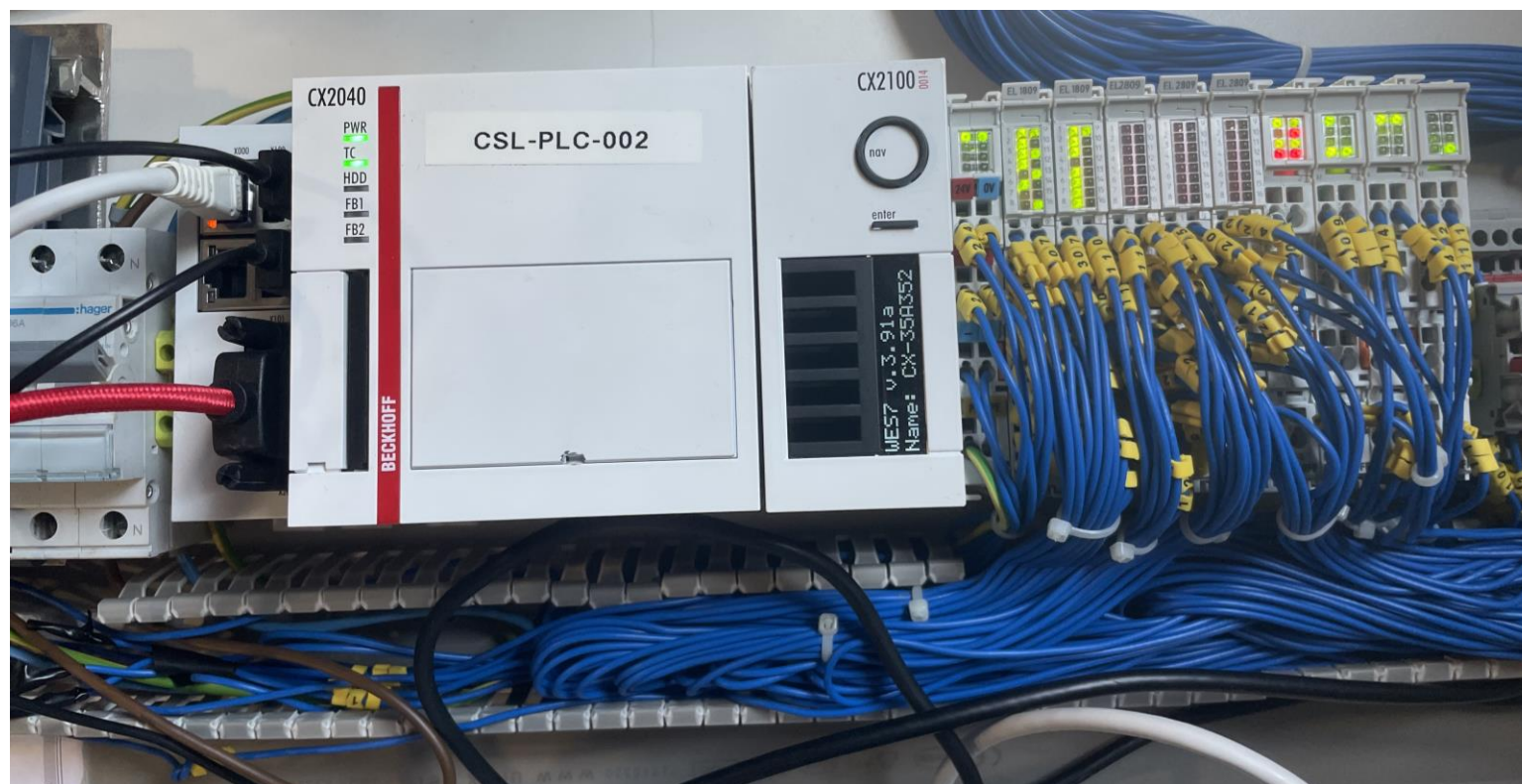
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

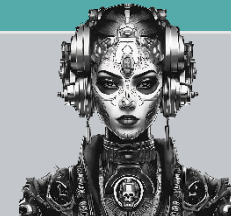
Superficie de ataque

BECKHOFF





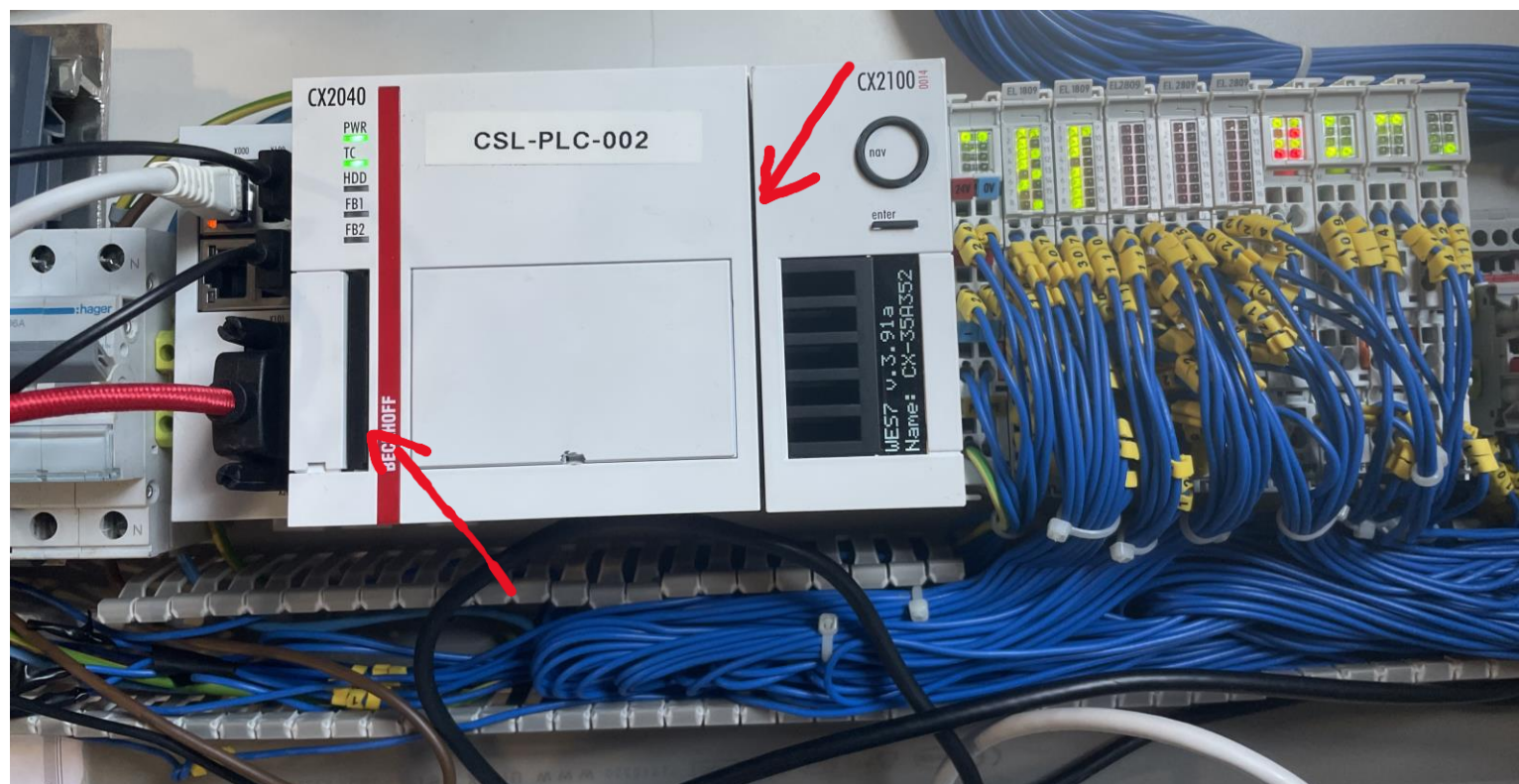
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

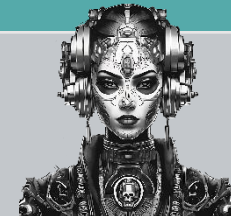
Superficie de ataque

BECKHOFF





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Extracción de firmware?

BECKHOFF

Es un Windows CE con runtime propietario

(Curiosamente también tarjeta flash para cámaras)



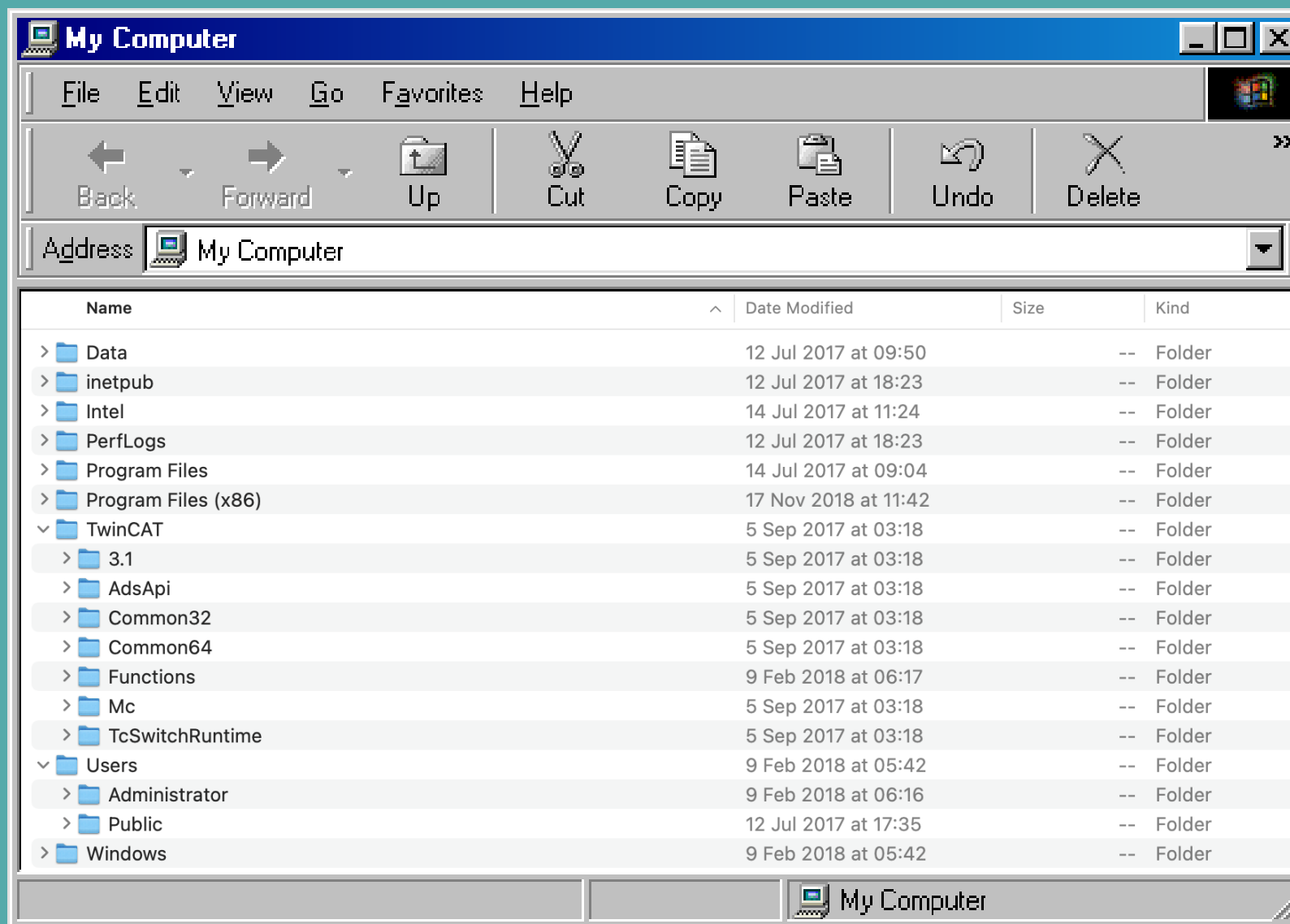
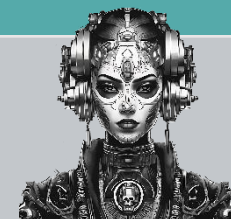


Fun Fact:



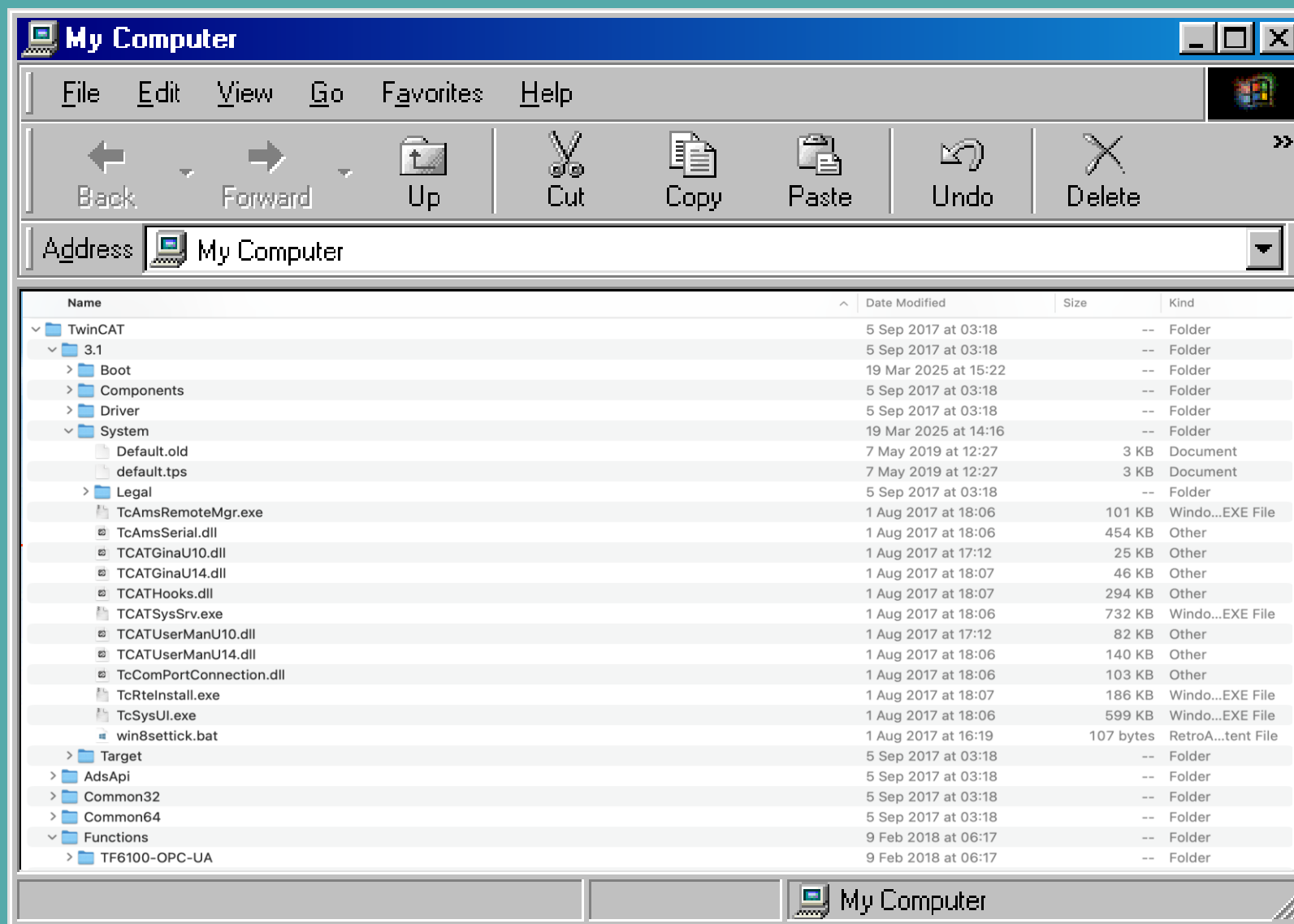
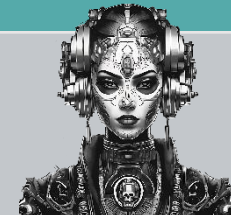


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



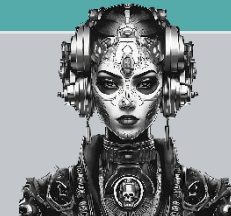


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Virtualización del PLC

BECKHOFF

- **Windows:**

Un Windows cualquiera con TwinCAT Runtime

- **BSD:**

ISO de TwinCAT/BSD con runtime incluido

(Ambos descargables de forma gratuita desde la web)



My Computer



WordPad



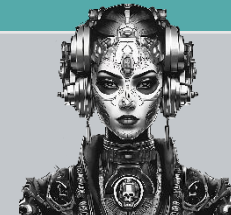
MS-DOS Prompt



Recycle Bin



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

E-Bus / K-Bus (Lateral)

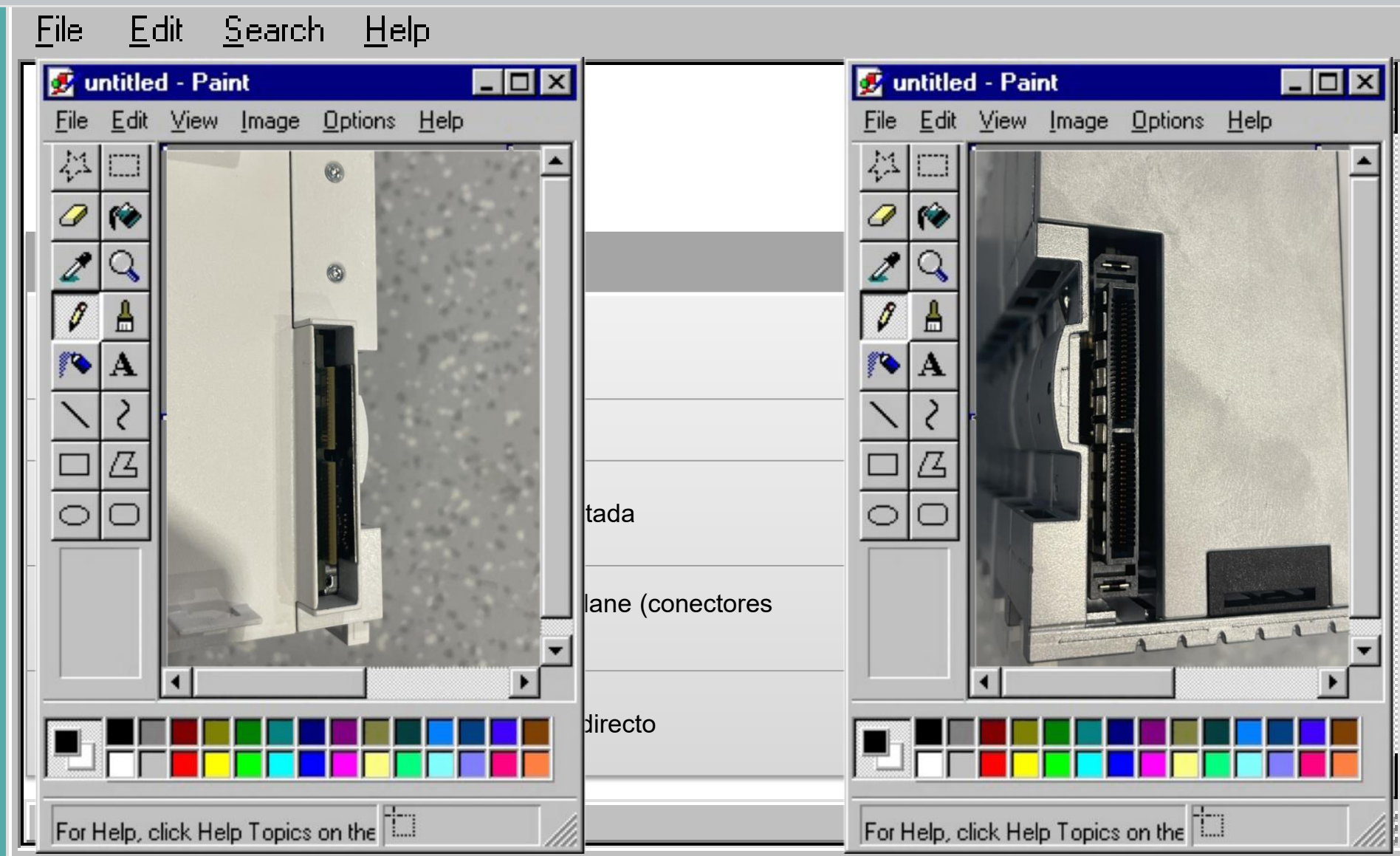
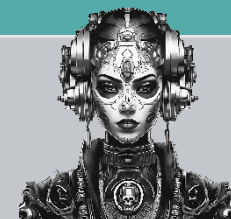
BECKHOFF

	K-Bus	E-Bus (EtherCAT-Terminal-Bus)
Tecnología	Bus paralelo propietario	Basado en EtherCAT (serie, tiempo real)
Velocidad	Baja-media	Muy alta (tiempo real determinista)
Configuración	Manual o automática limitada	Completamente automática con TwinCAT
Conexión física	Pines de cobre en backplane (conectores especiales)	Pines para EtherCAT interno (misma mecánica)
Ataques posibles	Necesario acceso físico directo	Sniffing/MITM posibles vía red EtherCAT



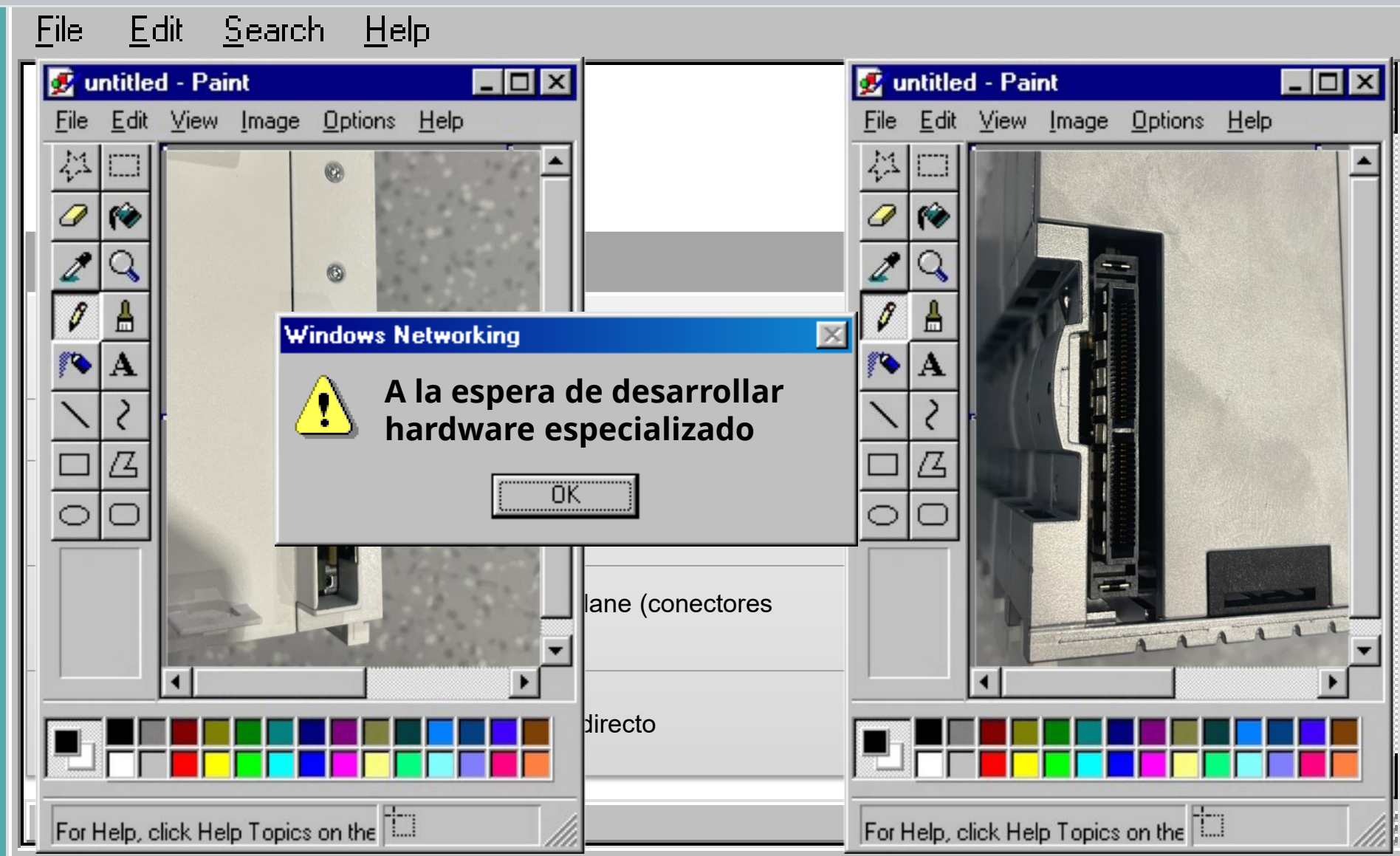
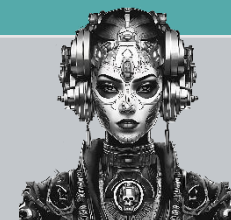


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



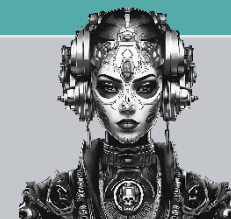


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



SIEMENS ▶

B&R ▶

BECKHOFF ▶

PHOENIX
CONTACT

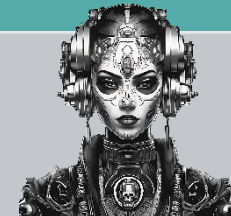
OMRON

Run...

Shut Down...



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

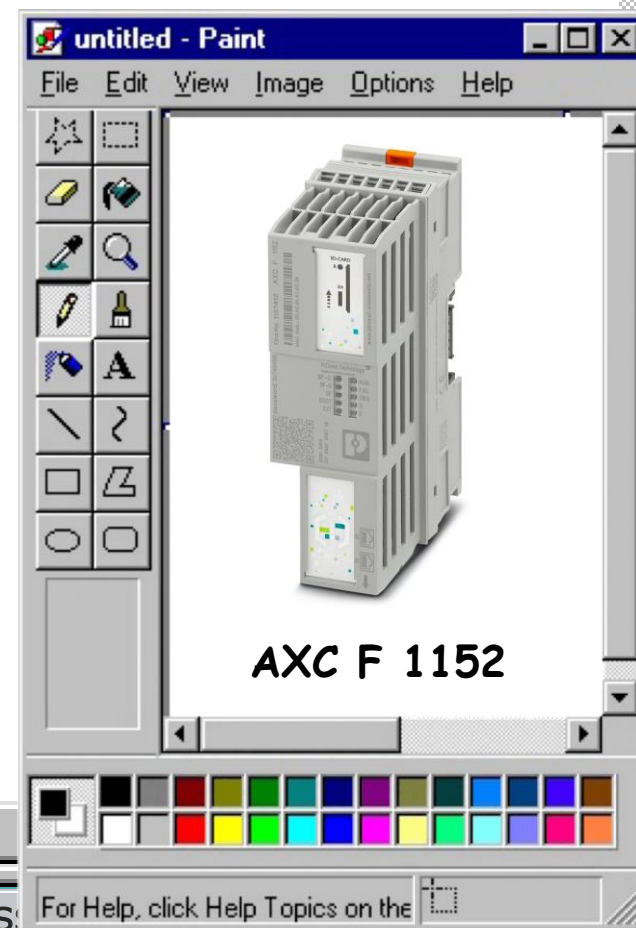


File Edit Search Help

Breakthrough

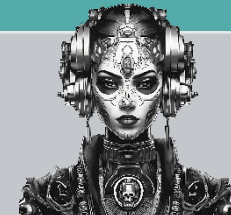
- Extracción de firmware
- Ingeniería inversa
- Virtualización

PHOENIX CONTACT





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Ficha técnica

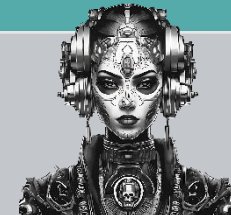


- **Arquitectura:** ARM Cortex-A8
- **OS base:** Linux embebido
- **Entorno de programación:** PLCnext Engineer
- **Interfaces:** Ethernet, SD interna, USB, microSD
- **Comunicaciones:** OPC UA, Profinet, Modbus TCP, Ethernet/IP, MQTT





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Reconocimiento previo

PHOENIX
CONTACT

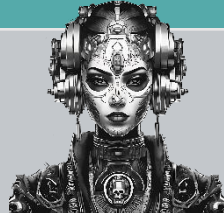


```
MS-DOS Prompt
Auto
root@CPU00556:~# nmap -p- 10.200.102.12
Starting Nmap 7.80 ( https://nmap.org ) at 2025-06-17 09:24 CEST
Nmap scan report for 10.200.102.12
Host is up (0.0097s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp < ----- Firmware
80/tcp    open  http < ----- Admin web
1962/tcp  open  biap-mp < ----- Interacción con procesos
41100/tcp open  unknown < ----- Conexión PLCnext engineer

Nmap done: 1 IP address (1 host up) scanned in 2055.32 seconds
```



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Reconocimiento previo



Deutsch English

AXC 1050
2700988

+ Information

+ Diagnostics

- Administration

Password

Factory Defaults

Updates via SD card

WebVisu

Diagnostic Archive

	Message	Time	System
i	Diagnostic archive saved	06.05.2049 12:29:29	System
i	Buffer battery charged	06.05.2049 12:00:54	System
i	Diagnostic archive saved	05.05.2049 21:29:29	System
i	Controller has changed to RUN state.	05.05.2049 20:59:32	PLC
i	Controller started	05.05.2049 20:59:31	PLC
i	Ready	05.05.2049 20:59:31	Axioline F
i	Switch on the controller has been set to RUN/PROG position.	05.05.2049 20:59:31	PLC
i	Charging of buffer battery started	05.05.2049 20:59:31	System

Refresh Diagnostic Archive

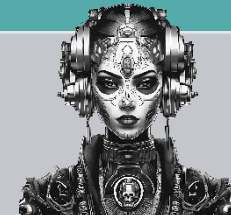
Device Name: ilc-131-eth1
Project Name: Vicomtech

HW: 04 FW: 3.0.1.5

*No requiere auth



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Extracción del firmware



- Descarga desde la web
- Obtención desde el FTP
- Archivo tipo RAUC

```
MS-DOS Prompt
Auto
ipallin@Igors-MacBook-Air AXC_F_1152_FW_2025_0_2 % unsquashfs axcf1152-2025
.0.2-25.0.2.86.rauch
Parallel unsquashfs: Using 8 processors
9 inodes (4827 blocks) to write

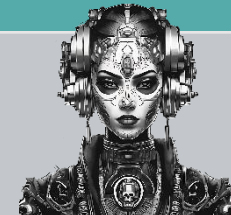
[=====/] 4836/4836 100%

created 9 files
created 1 directory
created 0 symlinks
created 0 devices
created 0 fifos
created 0 sockets
created 0 hardlinks
```





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Extracción del firmware



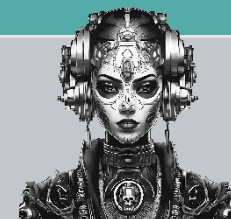
MS-DOS Prompt

```
ipallin@Igor's-MacBook-Air AXC_F_1152_FW_2025_0_2 % ls -la squashfs-root
total 1234008
drwx-----@ 11 ipallin  staff          352 Jun 16 13:41 .
drwx-----@  7 ipallin  staff          224 Jun 16 13:41 ..
-rw-r--r--@  1 ipallin  staff 631288832 Apr  6  2011 axcf1152-image-base-a
xcf2152.ext4
-rw-r--r--@  1 ipallin  staff      8170 Apr  6  2011 cleanOverlayFS
-rwxr-xr-x@  1 ipallin  staff       676 Apr  6  2011 hook
-rw-r--r--@  1 ipallin  staff       325 Apr  6  2011 manifest.raucm
-rwxr-xr-x@  1 ipallin  staff       242 Apr  6  2011 recoverType2
-rwxr--r--@  1 ipallin  staff    131072 Apr  6  2011 u-boot-env-pxc-axcf21
52.bin
-rwxr--r--@  1 ipallin  staff     65536 Apr  6  2011 u-boot-spl.sfp
-rwxr--r--@  1 ipallin  staff    297200 Apr  6  2011 u-boot.img
-rwxr-xr-x@  1 ipallin  staff       960 Apr  6  2011 updateBootloader
```





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Extracción del firmware

**PHOENIX
CONTACT**

untitled - Paint

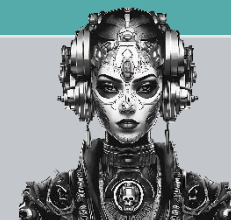
File Edit View Image Options Help

- axcf1152-image-base-axcf2152.ext4 - - 2a2783ab8b5c42668a4415d08acf4c0b
 - > boot
 - > dev
 - > etc
 - > home
 - lost+found
 - > media
 - mnt
 - > opt
 - proc
 - root
 - run
 - srv
 - sys
 - tmp
 - > usr
 - > var
 - bin
 - init
 - lib
 - sbin

```
FW_2025_0_2 % ls -la squashfs-root
352 Jun 16 13:41 .
224 Jun 16 13:41 ..
832 Apr 6 2011 axcf1152-image-base-a
170 Apr 6 2011 cleanOverlayFS
676 Apr 6 2011 hook
325 Apr 6 2011 manifest.raucm
242 Apr 6 2011 recoverType2
072 Apr 6 2011 u-boot-env-pxc-axcf21
536 Apr 6 2011 u-boot-spl.sfp
200 Apr 6 2011 u-boot.img
960 Apr 6 2011 updateBootloader
```



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Descubrimientos principales

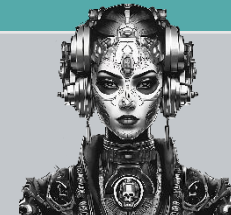


- **Linux embebido basado en Yocto-Debian**
- **Runtime de PLCNext**
- **Cadenas de confianza hechas**
- **Toolchain BitBake**





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Monatando una VM



```
ipallin@Igor's-MacBook-Air squashfs-root % qemu-system-arm \
-M vexpress-a9 \
-m 512M \
-kernel zImage \
-dtb vexpress-v2p-ca9.dtb \
-drive file=axcf1152-image-base-axcf2152.ext4,format=raw,if=sd \
-append "root=/dev/mmcblk0 rw console=ttyAMA0" \
-serial mon:stdio -nographic
```

Dockerfile 1 x

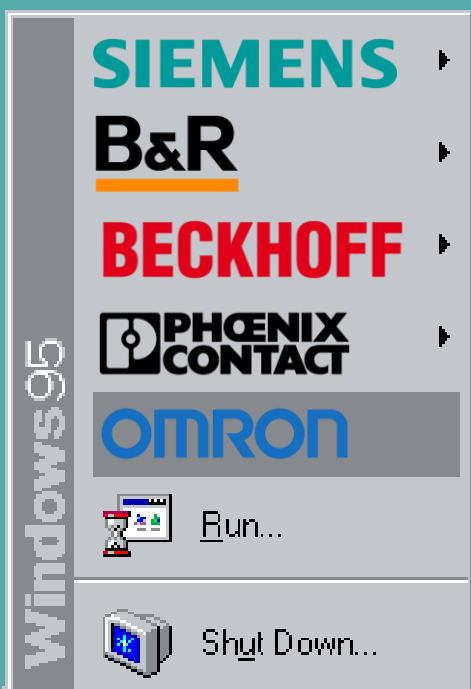
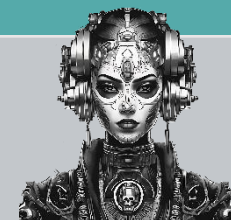
AXC_F_1152_FW_2025_0_2 > sq

```
1 FROM arm32v7/debian:bullseye
2 COPY rootfs/ /plcnext-rootfs/
3 RUN apt-get update && \
4     apt-get install -y --no-install-recommends \
5         ca-certificates \
6         libstdc++6 \
7         libgcc-s1 \
8         libatomic1 \
9         libssl1.1 \
10        libusb-1.0-0 \
11        libusb-dev \
12        libusb-1.0-0-dev && \
13        rm -rf /var/lib/apt/lists/*
14 COPY --from=plcnext/axc-f-1152-fw:2025.0.2 /plcnext-rootfs/ /plcnext-rootfs/
```



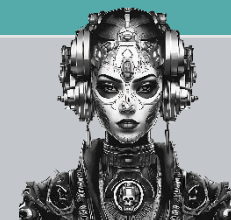


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

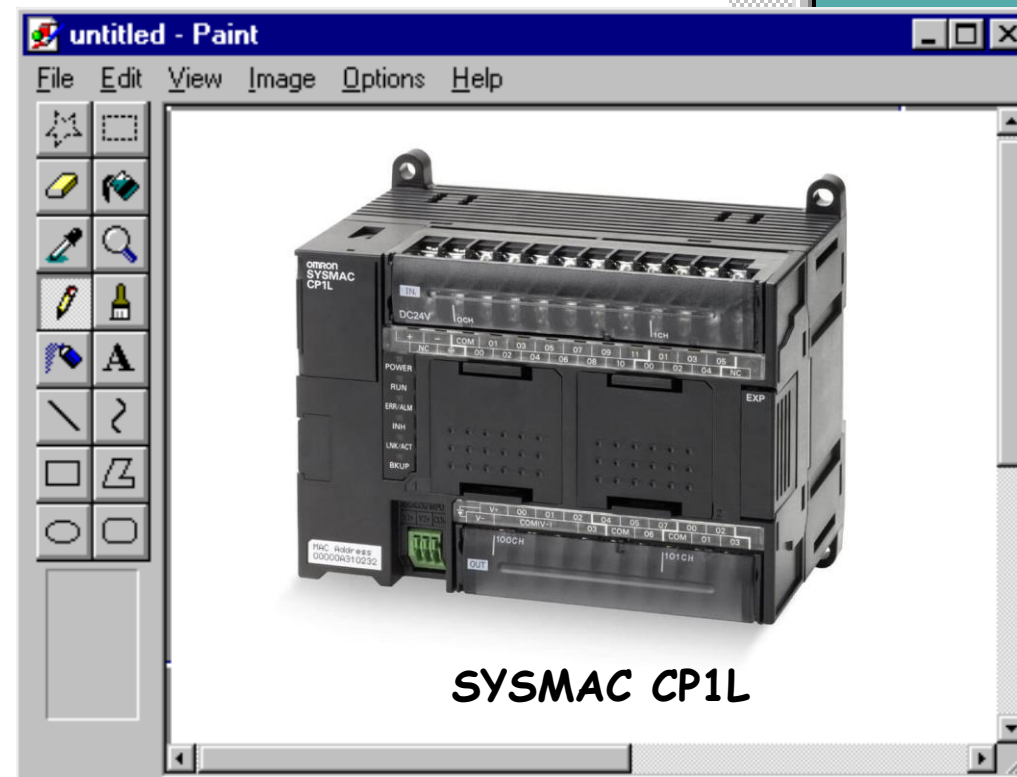


File Edit Search Help

Breakthrough

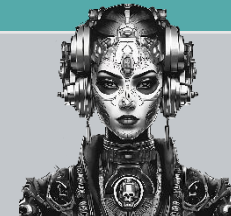
- Extracción de firmware
- Ingeniería inversa
- Virtualización

OMRON





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Breakthrough

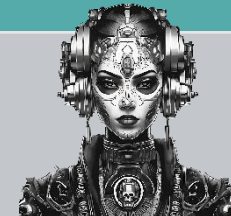
OMRON

- **Arquitectura:** ARM Cortex-A8
- **OS base:** RTOS propietario de omron
- **Entorno de programación:** Omron CX-One
- **Interfaces:** USB-B, Módulos de expansión propietarios
- **Comunicaciones:** Protocolo FINS (Requiere Ethernet)





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Identificación externa

OMRON

- **USB type B**
- **Puertos propietarios**
- **Pines de expansión**



My Computer



WordPad



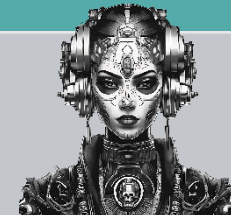
MS-DOS
Prompt



Recycle Bin



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

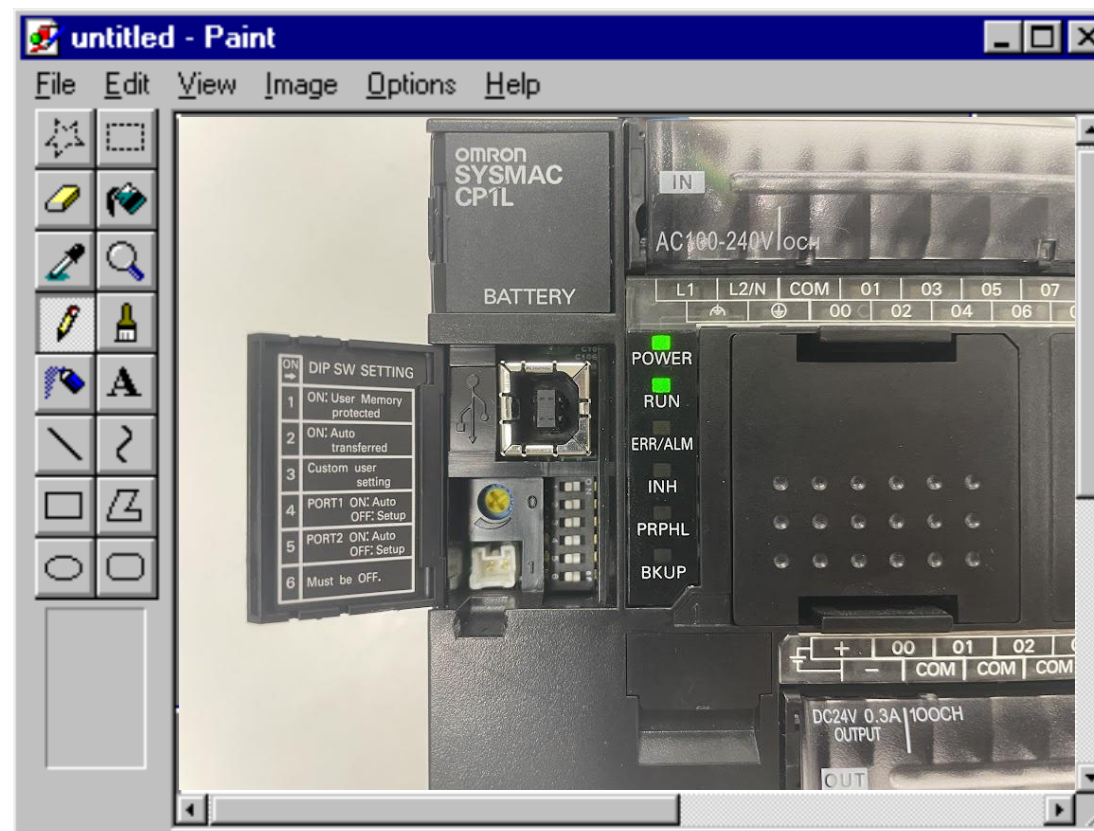


File Edit Search Help

Identificación externa

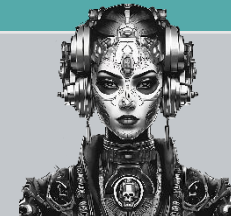
- USB type B
- Puertos propietarios
- Pines de expansión

OMRON





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

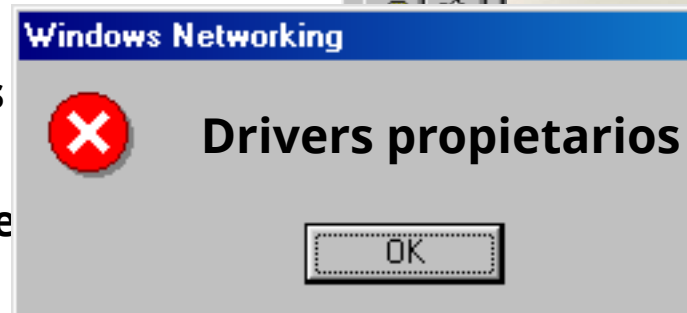


File Edit Search Help

Identificación externa

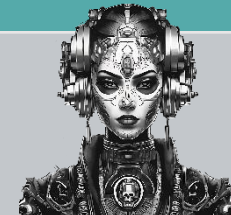
OMRON

- USB type B
- Puertos
- Pines de





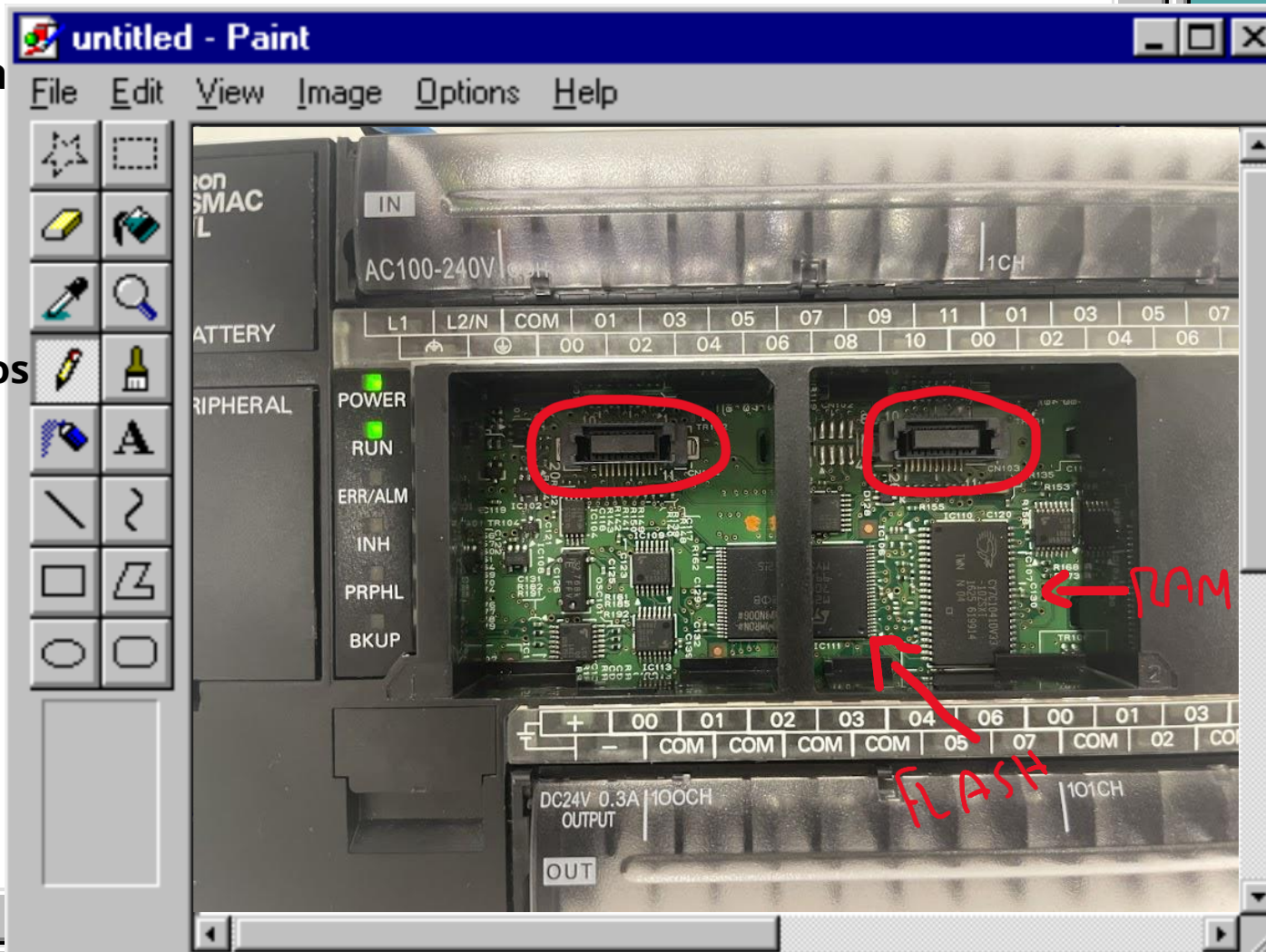
PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

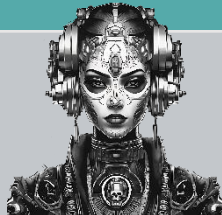
Identificación externa

- USB type B
- Puertos propietarios
- Pines de expansión





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Identificación externa



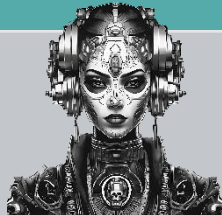
Pin	Señal	Función
1	+24 V	Alimentación CP1W
2	0 V (GND)	Tierra
3	TxD (CPU → módulo)	Datos serie transmitidos
4	RxD (módulo → CPU)	Datos serie recibidos
5	RTS	Request To Send
6	CTS	Clear To Send
7	RS-422/485 control (sel)	Selección entre RS-483/485 o RS-422
8	Tierra de señal (SG)	Referencia de señal para RS-422/485

Fuente: datasheet del PLC





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Identificación externa



Pin	Señal	Función
1	+24 V	Alimentación CP1W
2	0V (GND)	Tierra
3		Datos serie transmitidos
4		Datos serie recibidos
5		Request To Send
6	CTS	Clear To Send
7	RS-422/485 control (sel)	Selección entre RS-483/485 o RS-422
8	Tierra de señal (SG)	Referencia de señal para RS-422/485

Windows Networking

 **A la espera de desarrollar hardware especializado**

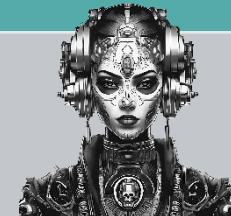
OK

Fuente: datasheet del PLC





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Identificación externa

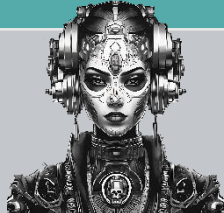
- USB type B
- Puertos propietarios
- Pines de expansión

OMRON





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



My Computer

untitled - Paint

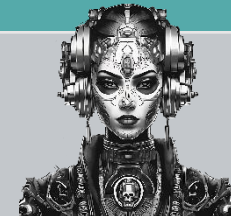
File Edit Search Help

Intento de lectura

Pin	Función	Pin	Función
1	+24 V (Power)	11	NC / ID detect
2	GND	12	NC
3	MCLK (Clock)	13	NC / Bus request
4	MDATA (Data)	14	NC
5	MSEL / Chip Select	15	NC
6	SG (Signal Ground)	16	NC
7	Reserved / Pullup	17	Reserved
8	Reserved	18	Reserved
9	Reserved	19	Reserved
10	Reserved	20	Reserved



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

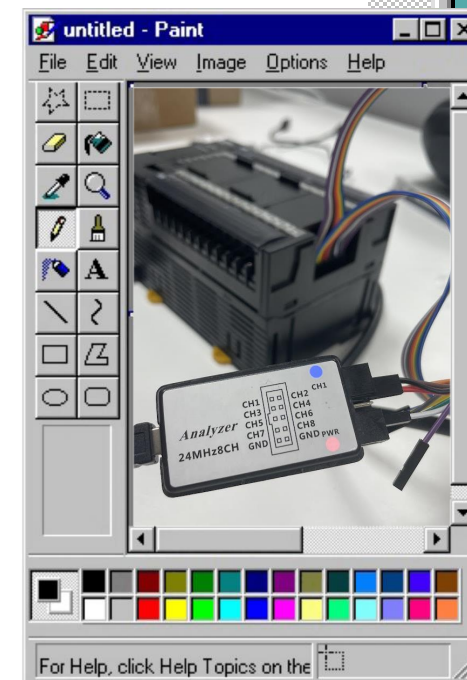


File Edit Search Help

Resultados

OMRON

- Si se conecta el analizador antes de encender el PLC el segundo no entra en modo run
- Si se conecta el analizador con el PLC en marcha el primero se convierte en una máquina de humo





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas

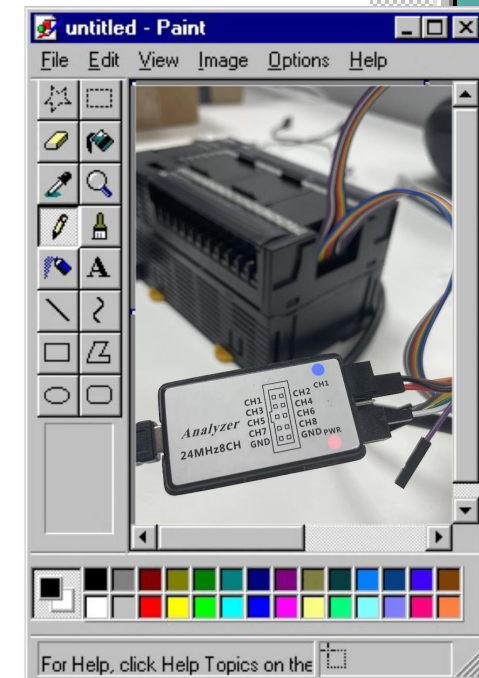
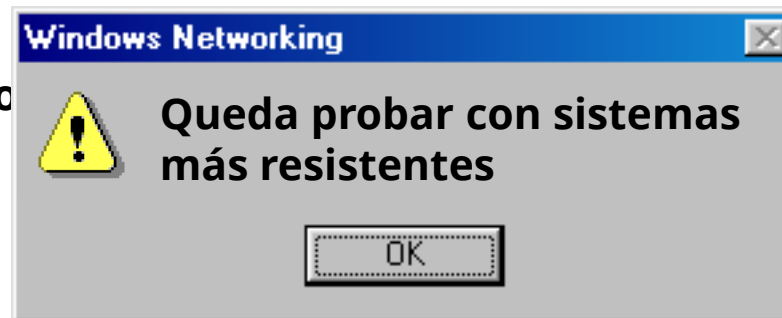


File Edit Search Help

Resultados

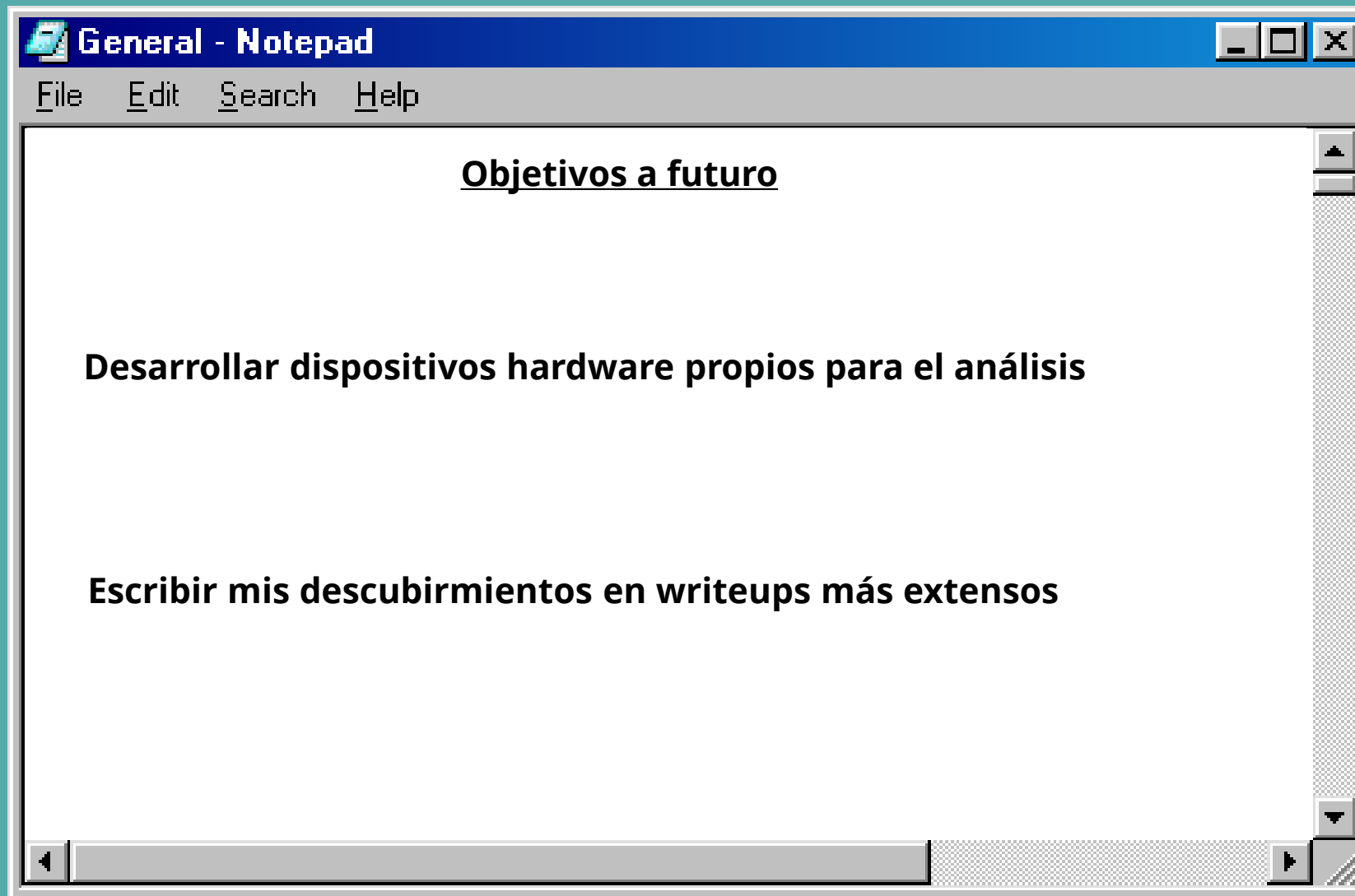
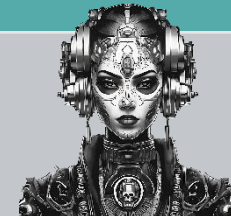
OMRON

- Si se conecta el analizador antes de encender el PLC el segundo
- Si se conecta el analizador con el PLC en marcha el primero se convierte en una máquina de humo



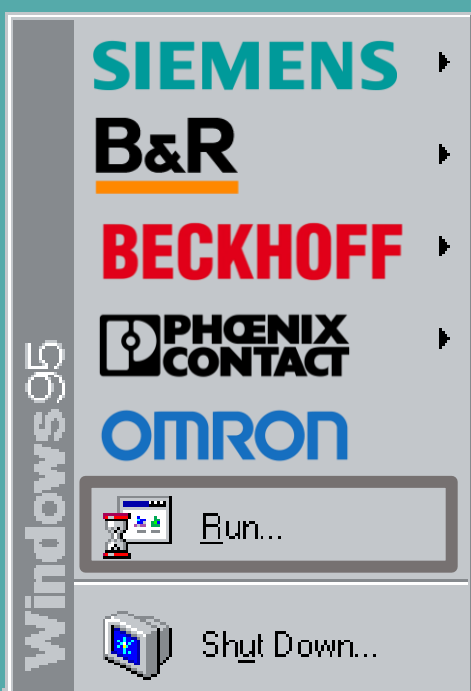
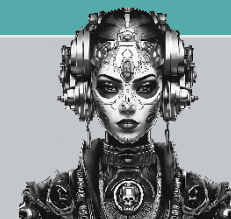


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



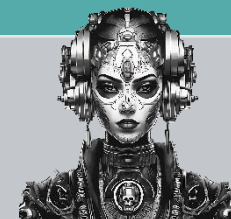


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Aquí se supone que iba la demo



My Computer



WordPad



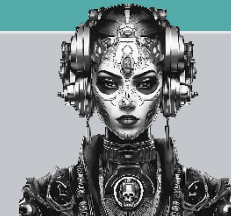
MS-DOS
Prompt



Recycle Bin



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Aquí se supone que iba la demo (pero al menos tengo una anécdota)
Y un pequeño ejercicio de lógica computacional



TP-1200



My Computer



WordPad



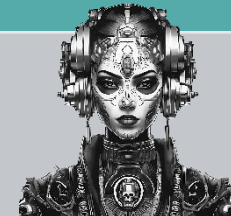
MS-DOS
Prompt



Recycle Bin



PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Aquí se supone que iba la demo (pero al menos tengo una anécdota)
Y un pequeño ejercicio de lógica computacional

Los PLCs funcionan a 220V

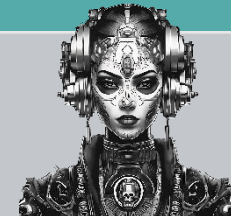


TP-1200





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Aquí se supone que iba la demo (pero al menos tengo una anécdota)
Y un pequeño ejercicio de lógica computacional

Los PLCs funcionan a 220V

Los IPCs se conectan igual que los PLCs

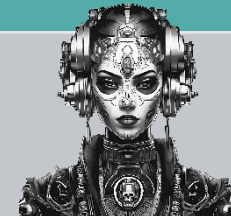


TP-1200





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Aquí se supone que iba la demo (pero al menos tengo una anécdota)
Y un pequeño ejercicio de lógica computacional

Los PLCs funcionan a 220V

Los IPCs se conectan igual que los PLCs

El TP-1200 es un IPC

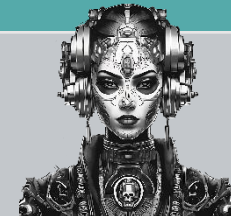


TP-1200





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Aquí se supone que iba la demo (pero al menos tengo una anécdota)
Y un pequeño ejercicio de lógica computacional

Los PLCs funcionan a 220V

Los IPCs se conectan igual que los PLCs

El TP-1200 es un IPC

Entonces el TP-1200 funciona a 220V

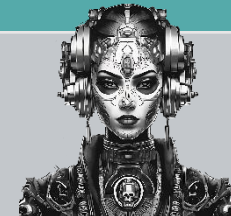


TP-1200





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Aquí se supone que iba la demo (pero al menos tengo una anécdota)
Y un pequeño ejercicio de lógica computacional

Los PLCs funcionan a 220V

Los IPCs se conectan igual que los PLCs

El TP-1200 es un IPC

~~**Entonces el TP-1200 funciona a 220V**~~

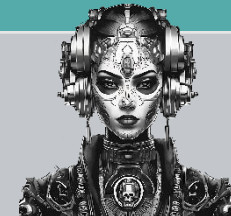


TP-1200





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Aquí se supone que iba la demo (pero al menos tengo una anécdota)
Y un pequeño ejercicio de lógica computacional

El TP-1200 Tiene pantalla

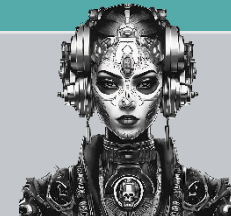


TP-1200





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



File Edit Search Help

Aquí se supone que iba la demo (pero al menos tengo una anécdota)
Y un pequeño ejercicio de lógica computacional

El TP-1200 Tiene pantalla

Si un dispositivo tiene pantalla...

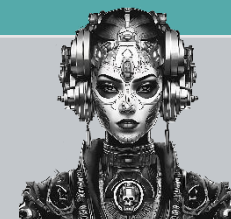


TP-1200





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



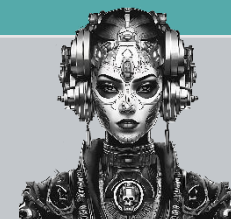
File Edit Search Help

El Siemens TP-1200 corre el Doom



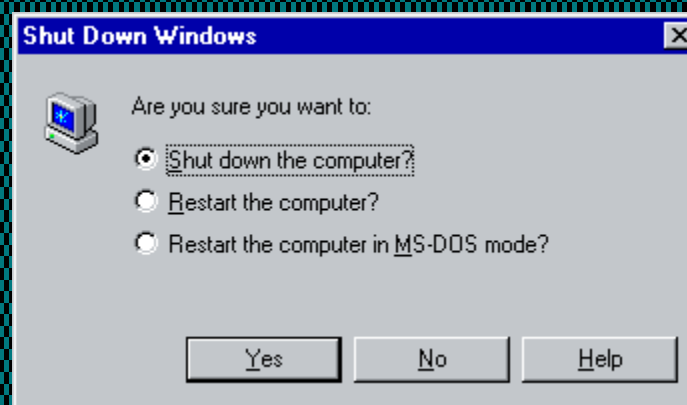
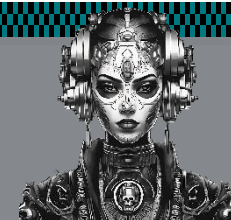


PLC LAN Party: Sistemas Obsoletos y Redes Caóticas





PLC LAN Party: Sistemas Obsoletos y Redes Caóticas



**It's now safe to turn off
your computer.**