Tải xuống một chương trình từ S7-200 có dễ không? Hay không quá nhiều?

Ngày: **2012-06-22**
Đã thêm: **Alexey Dmitriev**
Chủ đề: **Khó**

Lời nói đầu.

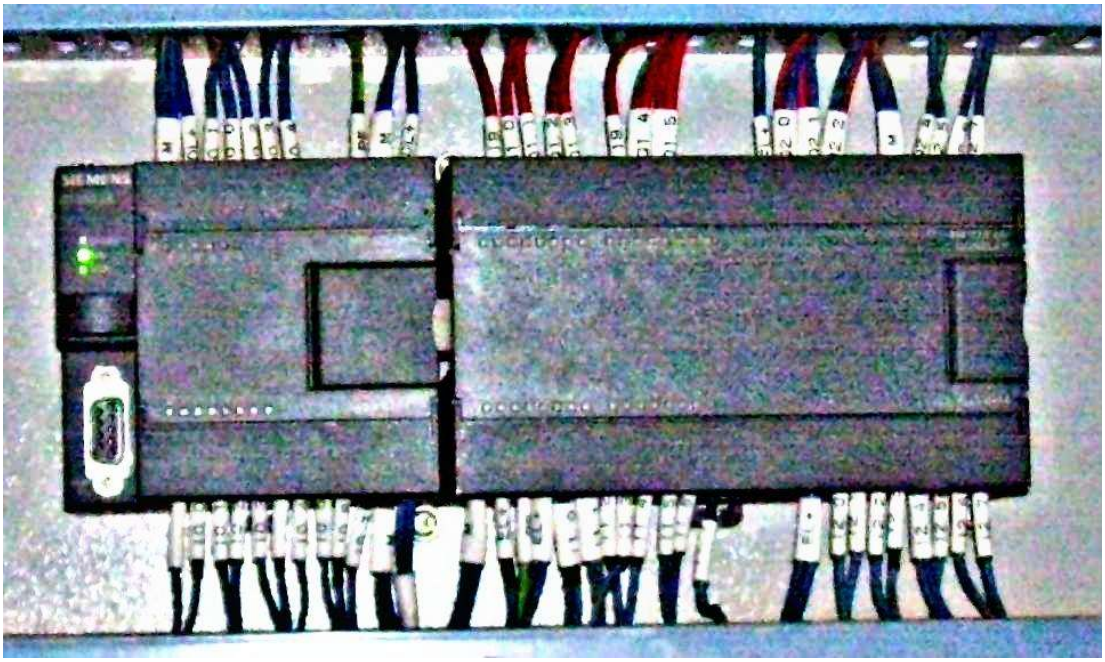
Tôi đã được thôi thúc viết bài này bởi tình huống xảy ra với máy cắt vật liệu dạng tấm bằng tia nước "ALBA" được mua tại cơ sở sản xuất thử nghiệm của chúng tôi, do các đồng nghiệp Trung Quốc của chúng tôi chế tạo máy từ Sunrise sản xuất. Máy hoạt động hoàn hảo trong một vài năm, và đột nhiên thông báo “Dừng khẩn cấp” xuất hiện trên màn hình của hệ thống CNC và máy từ chối thực hiện tất cả các loại hành động.
Đồng thời, hai đèn LED đỏ nhấp nháy đẹp mắt trên bảng điều khiển ở chế độ bộ đếm nhị phân. Vì không có tài liệu kỹ thuật thông thường, họ đã gọi cho trung tâm bảo hành của người bán. Họ trả lời - gửi đơn, nộp tiền, sau đó chúng tôi sẽ đến xem. Đề nghị, lẽ ra, đã được chấp nhận, nếu doanh nghiệp chưa ngồi tủ tài liệu, đương nhiên không có tiền.
Sau đó, nhà chức trách yêu cầu tôi xem xét, mặc dù nhiệm vụ chính thức của phó giám đốc thiết kế hệ thống điều khiển quá trình của viện thiết kế không bao gồm việc bảo trì khu máy sản xuất thử nghiệm.

Bảng điều khiển máy.

Quá trình.

Giai đoạn đầu là chuẩn bị.

Quá trình kiểm tra cho thấy toàn bộ thiết bị (ngoại trừ máy CNC) được điều khiển bởi một S7-200 nhỏ với một mô-đun I / O bổ sung. Mặc dù chúng tôi không sử dụng sê-ri thứ 200 trong thiết bị của mình (ngày càng có nhiều hơn về sê-ri thứ 300), nhưng bộ điều hợp PPI đã có sẵn (còn lại từ cấu hình của một số bảng điều khiển). Thật đơn giản - bạn cần tải xuống phần mềm từ bộ điều khiển và xem điều gì gây ra lỗi trên hệ thống CNC, vì chỉ một đầu ra của bộ điều khiển bị cháy và khi nó bị xé ra khỏi bộ điều khiển, lỗi từ màn hình CNC sẽ biến mất. , tuy nhiên, không cho phép máy hoạt động.



Đây là bộ điều khiển.

Hơn nữa, mọi thứ dường như rất tầm thường. Tôi đã cài đặt Step-7 Micro / Win trên máy tính xách tay của mình, kết nối bộ điều khiển, cấu hình giao diện, Tải lên và sau đó .... Cửa sổ nhập mật khẩu. Những nỗ lực của ALBA, SUNRISE, SUNSHINE và CHINA đã không đem lại kết quả gì :).
Một cuộc gọi đến bộ phận hỗ trợ kỹ thuật của người bán có phần nản lòng - “Chúng tôi không có mật khẩu, người Trung Quốc không cung cấp. Nếu có điều gì đó với bộ điều khiển, chúng tôi gửi nó đến thiên đường! ” -... ??? Thật khó tin, và nghi vấn về sự rạn nứt của toàn bộ nền kinh tế này đã trở thành một vấn đề danh dự nghề nghiệp.

Tôi đã xem xét trình đánh hơi cổng những gì được truyền / nhận trong quá trình ủy quyền. Bộ điều khiển truyền mật khẩu ở dạng mã hóa, vì vậy thông tin ít được sử dụng, vì thuật toán mã hóa không xác định và có thể có số lượng tùy chọn không giới hạn.

Giai đoạn hai là thu thập thông tin.

Đã đến văn phòng để hút Internet. Tôi tháo bộ điều khiển khỏi tủ máy và mang theo bên mình. Có rất nhiều điều thú vị, chủ yếu là trên http://plcforum.uz.ua. Trang web rất hữu ích, tôi rất muốn giới thiệu nó cho mọi người!

Chương trình giải mật mã dự án S7 -
Liên kết # 1:
http://plcforum.uz.ua/viewtopic.php?
f=1&t=9426&hilit=unpassword

Thật tốt, nó thực sự hoạt động (kiểm tra sau), nhưng chúng tôi không có dự án!

Các tìm kiếm sâu hơn đã dẫn đến một phương pháp đọc kết xuất từ chip 24C64 - bộ nhớ truy cập tuần tự. Có một kết xuất, bạn cũng có thể trích xuất mật khẩu.

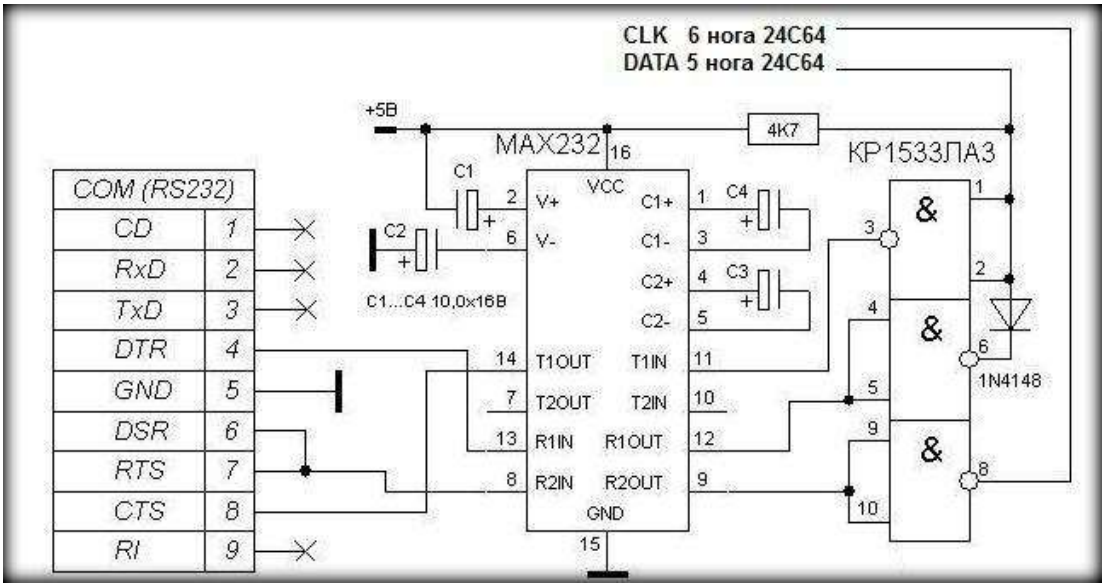
Link # 2:
http://plcforum.uz.ua/viewtopic.php?f=1&t=4648&hilit=%D0%BE%D0%B1%D1%80%D0%B0%D0%B7+S7+200
Xin cảm ơn rất nhiều CoMod để biết thông tin chi tiết.

Có một liên kết khác ở đó, được thiết kế để đọc mật khẩu trực tiếp từ bộ điều khiển thông qua giao diện PPI tiêu chuẩn.

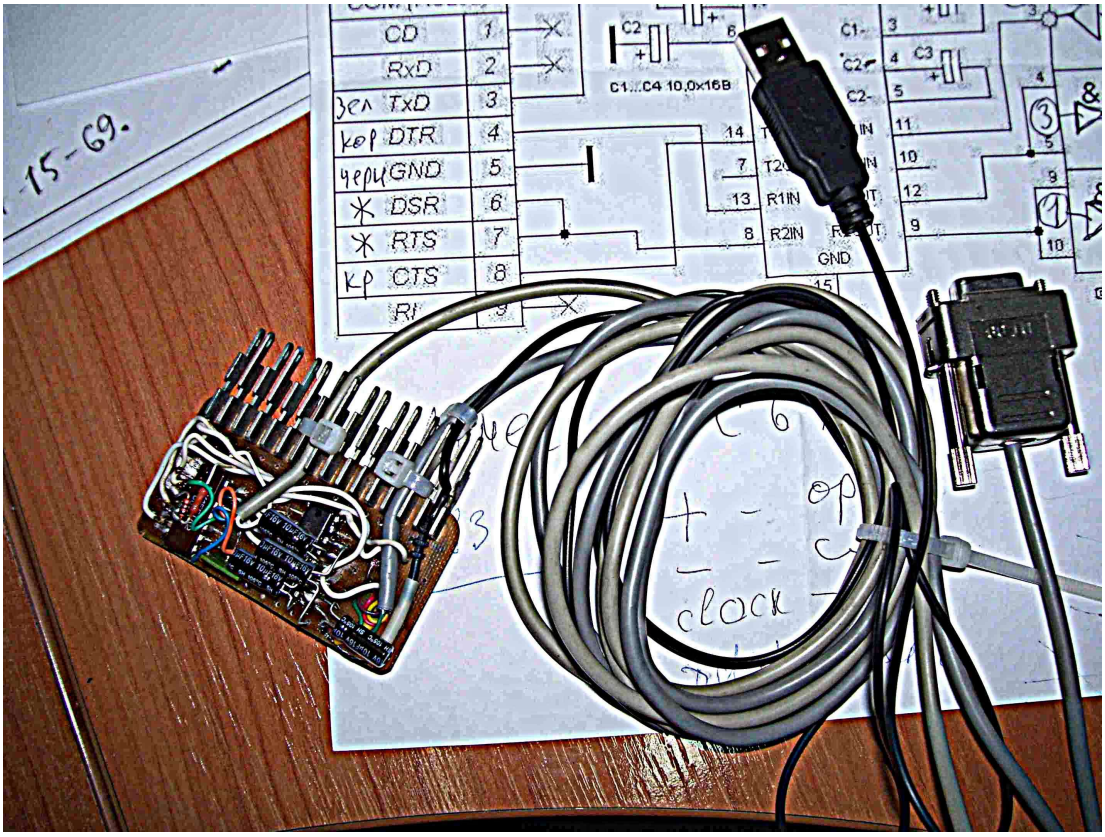
Liên kết số 3: http://rapidshare.com/files/3337879/S7-200.exe.html Chương trình thực sự truy cập bộ điều khiển, thậm chí đọc loại CPU và phiên bản phần sụn, nhưng, than ôi, nó không hiển thị mật khẩu - cánh đồng trống rỗng. Tôi nghi ngờ điều này đã từng hoạt động, nhưng trên các phiên bản đầu tiên của phần sụn CPU.
Chương trình thực sự đã lỗi thời và không còn phù hợp với các bộ vi xử lý mới.

Giai đoạn ba - phần cứng (phần cứng).

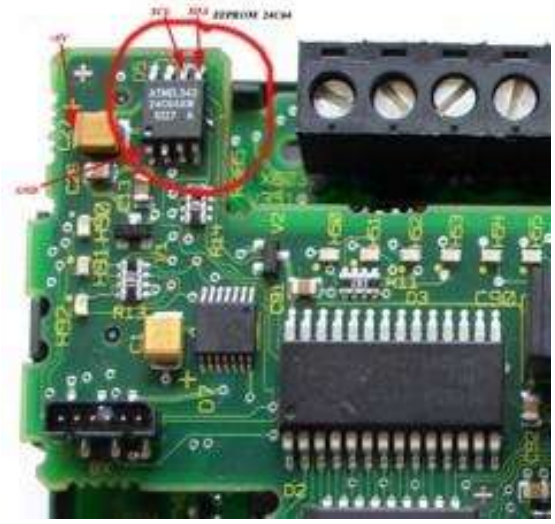
Bước tiếp theo là xây dựng lập trình viên. Không cần suy nghĩ kỹ, tôi hàn với một bản cài đặt có bản lề mà CoMod đã đề xuất trong tài liệu tham khảo số 2 dựa trên cổng LPT. Hai KT315, bốn điện trở. Tôi đã hàn dây vào chip ROM, cài đặt PonyProg http://www.lancos.com/prog.html và ... không hoạt động!
Khiêu vũ với tambourine và thăm dò tín hiệu bằng đồng hồ vạn năng không cho kết quả nào. Hóa ra sau này, tôi không cảm thấy nó tốt với đồng hồ vạn năng, nhưng nhiều hơn về điều đó sau đó.
Đã đi hút Internet hơn nữa để tìm kiếm một giải pháp. Kết quả là, tôi đã giải quyết bằng chương trình lập trình viên EXTRAPIC http://www.5v.ru/extrapic.htm trong một phiên bản đơn giản hóa - tôi đã loại bỏ mọi thứ không cần thiết để đọc 24C64 và điều này là rất nhiều. Có hai vi mạch MAX232 và 555LA3 (tôi đặt 155TL3), bốn tụ điện, một điện trở và một diode. Khi tôi đến cửa hàng để mua MAX232 (phần còn lại của thùng rác đã có mặt), tôi quyết định mua 24C64 để thử nghiệm với lập trình viên. Tôi lấy nguồn điện 5 volt từ USB. Tôi đã hàn dây vào chip ROM (đã có trong gói DIP mới), khởi chạy PonyProg và ... không hoạt động!
Mẹ kiếp!



Đây là sơ đồ lập trình viên:



Nó trông giống như một thiết bị được hàn vội vàng.

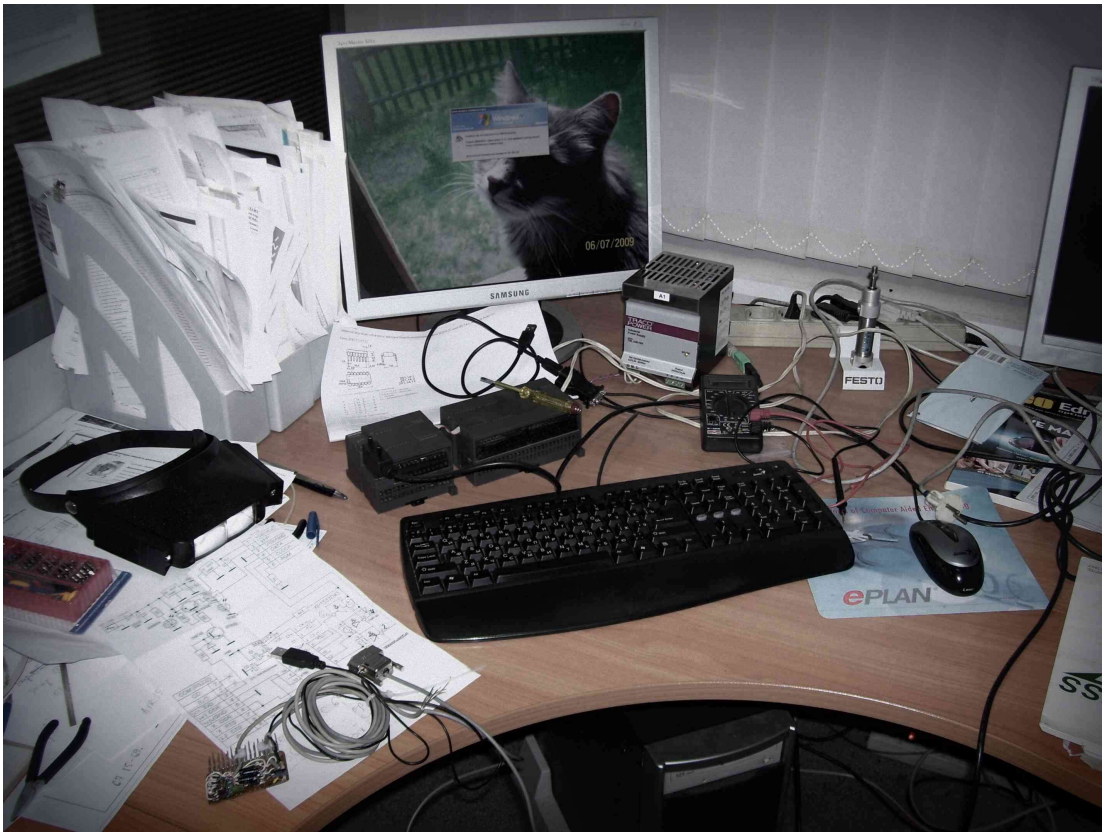


Đây là vị trí của chip trên bảng điều khiển S7-200.

Hình ảnh của bảng điều khiển từ http://plcforum.uz.ua/ được cung cấp bởi CoMod, rất cảm ơn anh ấy.

Giai đoạn bốn - khiêu vũ với tambourine.

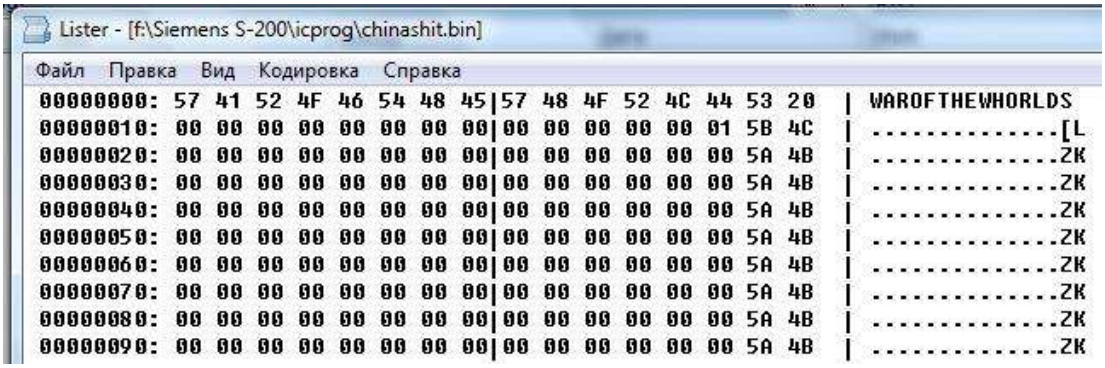
Đã tải xuống http://www.winpic800.com/. Chương trình này rất hữu ích để thiết lập và kiểm tra lập trình viên - bạn có thể chọn tín hiệu của các cổng được kết nối với chip ROM và chuyển đổi chúng theo chương trình ở trạng thái tĩnh, do đó kiểm tra sự truyền và bình thường của tín hiệu. Trên đường đi, tôi đã kiểm tra kỹ lưỡng nhãn hiệu của 24C64 đã mua và không tìm thấy bất cứ điều gì tương tự trên vỏ máy. ??? Không phải thứ gì đó bị trượt trong cửa hàng (có thể do vô tình, có thể là một thiết bị tương tự) ...? Tôi đã đến một cửa hàng khác và mua 24C08 ở đó (đó chính xác là những gì nó ghi trên đó), kết nối nó ...
Không có phản hồi từ chip ROM! Tôi bắt đầu thăm dò các tín hiệu bằng đồng hồ vạn năng và ... Tôi phát hiện thấy một đoạn ngắn mạch, không hẳn là ngắn, nhưng vẫn còn, của các dây tín hiệu với nhau trong cáp kết nối bộ lập trình với chip ROM. Cáp này đã bị cắt một ngày trước từ một con chuột chết (đó là lý do tại sao con chuột không hoạt động!)! Cắt bỏ một nửa - phần còn lại đã biến mất. Đã kết nối và ... lo và kìa - ĐÃ LÀM VIỆC! Tôi kết nối dây với chip 24C64 của bộ điều khiển S7-200, khởi chạy WinPic800 - đọc và ... 256 byte số không đã được đọc ... !!! ???
Mẹ kiếp!



Đây là nơi quá trình diễn ra.

Giai đoạn 5 - Chiến thắng!

Đã tải xuống chương trình http://www.ic-prog.com/. Ra mắt và ..., lo và kìa, tôi đã đọc được kết quả. Có vẻ khá tuyệt khi bắt đầu!



Sau đó, đó là vấn đề kỹ thuật, vì nó được viết trong liên kết số 1. Chúng tôi sử dụng Unlocks7_200and300.exe để giải nén mật khẩu từ kết xuất. Chúng tôi tải xuống dự án Step-7 Micro / Win và nghiên cứu kỹ lưỡng. Chiến thắng!

Giai đoạn thứ sáu là nghiên cứu về mật mã từ thời Trung Vương quốc.

Trên thực tế, chương trình điều khiển không đại diện cho bất cứ điều gì phức tạp. Điều khiển "rơ le" thông thường của tất cả các loại, chẳng hạn như thủy lực, máy bơm, van và rác khác, nhưng ... Có một mã hẹn giờ cho 360 ca làm việc 8 giờ. Bộ đếm thời gian chỉ đếm khi một số đầu ra được bật, chẳng hạn như bật bơm thủy lực của bộ tăng áp, tức là khi máy đang chạy. Khi bộ đếm thời gian đếm đến cuối, lá cờ có địa chỉ M13.0 được thiết lập :), thích, tất cả các chàng trai, hãy trả tiền! Đây là gì nếu không phải là tống tiền! Không thể đặt lại cờ theo bất kỳ cách nào, ngoại trừ việc kết nối trình gỡ lỗi, yêu cầu mật khẩu!
Nó xấu đến mức nào và ai đã lập trình nó, tất nhiên là người Trung Quốc hoặc người trung gian của chúng tôi từ Moscow, tôi không biết ... Nhưng tôi muốn nói: Chà, các người là đồ dê xồm!

PS: Thật thú vị, 360D được viết trên vỏ PLC với một điểm đánh dấu. Lúc đầu, tôi lấy nó để làm mật khẩu, sau đó, tất nhiên, ý nghĩa thực sự của dòng chữ này trở nên rõ ràng :).

Nhân tiện, phiên bản đầu tiên của lập trình viên, rất có thể, đã hoạt động. Thật đáng trách!

Dmitriev Alexey
Yaroslavl, 2011.

Các công cụ cần thiết (tải xuống 2,5Mb)

Lượt xem: 75481

Nhận xét về tài liệu

Đã thêm: **Ilya** Ngày: **2012-07-15**

Những cuộc phục kích như vậy là tiêu chuẩn. Tôi có một bộ điều khiển S5 khởi động 2500 giờ một lần và yêu cầu mật khẩu. Mật khẩu rất khó tạo, cần phải gọi mỗi lần và tìm ra mật khẩu. Đầu tiên, tôi phá mật khẩu, sau đó họ chuyển S5 sang Siemens mới và xóa khối mật khẩu.

Đã thêm: **komatic** Ngày: **2012-07-15**

2Ilya, chia sẻ khối mật khẩu nếu bạn đã rời khỏi, tôi tự hỏi ...

Đã thêm: **Dmitry** Ngày: **2012-08-31**

Và có ai đã tự Unlocks7_200and300.exe không?
Và sau đó, nó không còn nằm trong bãi rác, cũng như chính bãi rác.

Đã thêm: **komatic** Ngày: **2012-09-07**

Đã thêm một liên kết đến bài viết

Đã thêm: **Nicholas** Ngày: **2012-12-07**

Các chàng trai cuối cùng, bạn biết làm thế nào! bạn có thể! ;)
Chà, nói chung là rất tuyệt! Tốt lắm

Đã thêm: **Nicholas** Ngày: **2012-12-07**

Ai không hiểu cụm từ đầu tiên - đó là từ đây:
http://www.yapfiles.ru/show/232666/127e56360f0b740f8bd328289ada3496.flv.html?autoplay=1

Thêm bởi: **Serj Balabay** Ngày: **2013-02-07**

Tôi nghĩ rằng tôi đã có một trường hợp cá biệt. Máy ép dừng không có lý do, trên bảng điều khiển viết "CALL ME" bằng tiếng Trung Quốc. Dự án trong bộ điều khiển đã được bảo vệ bằng mật khẩu. Do tính đơn giản của nhiệm vụ, dự án đã được viết lại.
Câu hỏi chính là Unlocks7_200and300.exe là Unlock_and_converter_MMC_Image_S7.exe? Có điều gì đó không hiển thị trong tệp lưu trữ đính kèm (simatic_s7-200_s7-300_mmc_password_unlock_2006_09_11.rar) của tệp này

---

Đã thêm: **komatic** Ngày: **2013-02-07**

2Serj
vâng, nó là, chỉ là một cái tên hơi khác (Unlock_and_converter_MMC_Image_S7.exe)

Đã thêm: **Mikle** Ngày: **2013-02-22**

Vào khoảng năm 2000, một chiếc điện thoại cố định MT-201 "Irbis" đã được mua. Ba năm sau, nó bắt đầu hiển thị 64 phút trên màn hình và thông tin về các cuộc gọi không được lưu lại. Thiết bị đã được sửa chữa bởi các đại lý. Ba năm sau vấn đề tái diễn. Nhà sản xuất vào thời điểm đó đã phá sản và hóa ra điều này là điển hình cho tất cả các thiết bị của mô hình này. Phần mềm cơ sở từ một thiết bị khác đã được cài đặt, điều này đã giải quyết được sự cố.

Đã thêm: **delsnos** Ngày: **2013-03-24**

Xin gửi lời chúc mừng đến tác giả!

Đã thêm: **Kolyan** Ngày: **2013-07-25**

Vùng nhớ M biến động. Có lẽ họ muốn rút phích cắm của máy ít nhất một lần một năm và do đó thiết lập lại bit M13.0 này? .. và sau đó họ suy nghĩ và quyết định - tại sao không tự thiết lập lại nó vì tiền, hehe))

Đã thêm: **Vitaly** Ngày: **2013-11-13**

Rất cám ơn Tác giả! Làm theo hướng dẫn của anh ấy, tôi đã nhận được mật khẩu và tải lên dự án từ CPU-224CN, chỉ CPU này có chip ROM 4256BWP, nhưng sơ đồ chân tương tự

Đã thêm: **Tác giả** Ngày: **2013-12-20**

Vùng nhớ M - không thay đổi. Số lượng byte không bay hơi được đặt trong bộ cấu hình bộ điều khiển.

Đã thêm: **Kirill** Ngày: **2015-01-22**

Rất cám ơn Tác giả! Tôi đã nhận được mật khẩu và tải lên dự án từ CPU-224. CPU này có chip ROM AT24S128T (Atmel). Tôi đã sử dụng một lập trình viên khác, nhưng nguyên tắc là giống nhau.

Đã thêm: **dekor** Ngày: **2015-01-30**

Hoan hô!
Tài liệu rất đầy đủ.
cảm ơn nhiều.

Đã thêm: **Anatoly** Ngày: **2015-02-13**

Vùng nhớ M, được chọn trong bộ cấu hình bộ điều khiển, thực sự dễ bay hơi, được cung cấp năng lượng bằng pin bên trong.
Đó là trường hợp sau khi chiếc điều khiển rơi xuống sàn, bộ nhớ này không còn lưu trữ, hóa ra cục pin đã bị rơi mất.

Đã thêm: **Vova** Ngày: **2016-03-27**

Cảm ơn Bratva

Đã thêm: **Alexey** Ngày: **2016-06-16**

Mọi người ơi, tôi gặp sự cố tương tự trên bộ điều khiển S300, Siemens chưa được đào tạo và tôi không biết nó ăn vào cái gì, mong các cơ quan chức năng giải quyết vấn đề!
Ai không thờ ơ thì viết e-mail cho tôi metaaleks@mail.ru
giúp tôi, ấm trà, đối phó với con lobuda này

Đã thêm: **Alexey** Ngày: **2016-07-12**

Với S7-300 thì dễ dàng hơn - lắp thẻ MMC từ bộ điều khiển vào bộ lập trình và sử dụng Unlocks7_200and300.exe để lấy mật khẩu.

Thêm bởi: **Diego** Ngày: **2016-07-19**

Chip cpu của tôi là 224xp 4256bwp nhưng không thể đọc bin thông qua eeprom của lập trình viên. Ai đó có thể giúp tôi.

Đã thêm: **Andrey** Ngày: **2016-10-01**

Vấn đề là tôi có một kết xuất s-200 226cn v 2. 01, nhưng không có một phương pháp nào giúp giải mã. Xin hãy giúp tôi giải mã

Đã thêm: **Hamed** Ngày: **2016-11-22**

HI SIR
Tôi không thể tải xuống s7200.exe từ trang web này:
http://rapidshare.com/files/3337879/S7-200.exe.html
bạn có thể giúp tôi và gửi tệp exe đến email của tôi không?
email của tôi là hamed.keshtkar6805@gmail.com
cảm ơn bạn

Đã thêm: **Ivan** Ngày: **2016-12-15**

Cảm ơn bạn đã đăng kho lưu trữ với các chương trình. Và sau đó, trong nhiều năm, nó đã bị xóa khỏi tất cả các tài nguyên Internet

---

Đã thêm: **79225593111@yandex.ru** Ngày: **2018-02-21**

s7-200 smart sr60
eprom - 25p10vp

дамп снял расшифровать не могу, если знаете как сделать напишите на почту плз

Добавлен: **79225593111@yandex.ru** Дата: **2018-02-21**

подскажите что можно предпринять?
Если нажимаю получить пароль то выдает такой пароль: O: "{aKы
Если нажимаю преобразовать в wld то получаю размер файла = 0

Добавлен: **Oleg** Дата: **2018-08-02**

Я в шоке! Заместителю главного конструктора видимо делать нехер целыми днями, как только заниматься хаком plc. Где бы работу такую найти?

Добавлен: **Shahzaib** Дата: **2018-09-09**

Sir kindly explain me the procedure of S7 300 password break

Добавлен: **Boris** Дата: **2019-03-31**

I do not know how the "Vot Schema Scheme" scheme is connected to the PC and to the PLC S7-200. Does the CLK and DATA wires have to connect directly to the 5 and 6 pin of the chip? And where is the USB port connecting, and where is DB9 (whether male or female)? We kindly ask you to answer.

Добавлен: **Алекс** Дата: **2019-04-21**

А подскажите пожалуйста пароль на архив, который выложил автор 😕

Добавлен: **Naveed** Дата: **2019-10-20**

Yeh kp1533 Kaya hy. Ager ic hy to kitny pin ka hy. Es ki jaga koi or chal Jay ga

---

Добавлен: **Собеседник** Дата: **2019-11-01**

Спасибо, парни.
Молодцы.

Добавлен: **Simon** Дата: **2020-07-13**

Вам СПАСИБО ОГРОМНОЕ, тоже помыкался, к стати пароль был J ANUS

Добавлен: **Aleksandr** Дата: **2020-07-24**

Коллеги, будте так добры.
У кого осталась Unlocks7_200and300 - поделитесь пожалуйста линком.

Заранее примного благодарен.

Добавлен: **PICStarter** Дата: **2020-10-10**

Могу помочь с 4 уровнем защиты всем желающим.
Подробнее в видео: https://www.youtube.com/watch?v=tpVHFoZIeI8&t=347s

---

Добавлен: **Сергей** Дата: **2020-12-06**

У меня получилось, спасибо огромное автору!!! Мой cpu 224xp, память 24c256. Сливал PonyProg. Пароль оказался SHANGHAI (Шанхай).

Добавлен: **фы** Дата: **2021-05-14**

S7-200 CN - Взломать не сломаем, но понизить с 4 до третьего уровня с известным паролем можем

Добавлен: **фы** Дата: **2021-05-14**

S7-200 CN - Взломать не сломаем, но понизить с 4 до третьего уровня с известным паролем можем. даже если защита от апрлоада

Добавлен: **x200881** Дата: **2021-07-27**

Спасибо за проги и инфу. ПЛК 224, память 24c128n. Перебирал пароль онлайн 1,5 года, скорость 9,6 кбод не нашел в первых 4 разрядах, начал 5. Через прищепку без демонтажа не вышло. Выпаял считал AsProgrammer через перешитый usbasp, пароль оказался "VICOL".

Добавлен: **в** Дата: **2021-07-30**

ФЫ, ДАВАЙ СПИШЕМСЯ. НУЖНА ПОМОЩЬ.fpdtlb@inbox.ru

Добавить комментарий

Ваше имя:

Текст комментария (4000 max):

Введите сумму с картинки:

1+2

bình luận

danh bạ mail
RSS