Hacking the Farm: Breaking Badly Into Agricultural Devices.

DEF CON 30
Prime focus areas

- Food security
- ICS
  - Food & Agriculture
- Supply chain wake up call (hopefully)
Main take aways

- I should do this to my ________
This talk is suitable for

- People who eat food
OVH fire: while police investigate the cause, OVHcloud promises free backups in future

"I believe this incident will change the standards of the industry" says founder Octave Klaba

March 17, 2021   By: Peter Judge   Comment
Before hitting the Information Superhighway...

Consider the RISKS!
YOU WOULDN'T UPLOAD THE SUPPLY CHAIN
YOU WOULDN'T UPLOAD THE SUPPLY CHAIN

...OR WOULD YOU
John Deere
http://deere.com

Reports resolved: 94
Assets in scope: 15

Vulnerability Disclosure Program
Launched on Aug 2021

Managed by HackerOne
Reminder

- Today is a good day
- Wow that looks easy
- I should do this to my ________
- I can drive a tractor now!
Never give up
Never
Never give up
So I got another one

I bought yet another MTG

Not tested on TV
Never give up
Feat. (but not limited to)

OVH
John Deere
Samsung
Wind River
Yocto
John Deere
AgCo
Case, New Holland
Red Hat
CISA
John Deere
Molex
Micron
Disclaimer

- None of research was paid for
- All research was done in good faith
- Nothing today represents our employers, past employers, or future employers
- None of us are under gag orders
- All content in the slides is CC0
- All trademarks, logos and brand names are the property of their respective owners.
Sick Codes - good faith hackerman

https://github.com/sickcodes
https://twitter.com/sickcodes
https://linkedin.com/in/sickcodes
https://sick.codes
Want to do business?

Hardware/IoT/Firmware Embedded.

info@sick.codes

sick.codes/contact
chainsaw boi
gps controlled chainsaw boi
The Machine
(Tractor, Combine, etc.)

Touch Display

MTG Gateway
(Wifi, Satellite, Radio)
The Gateway

All 3 parts can control the other

Go hard or go home

1800 Display

2600 Display

2630 Display

4640 Display
Brown Box

https://www2.ljworld.com/news/2008/apr/26/new_technology_makes_farming_more_profitable_produc/
• Early 2000’s

• Still in use

• Lifetime unlocks

John Deere Brow

Location:
Auction: Mar 30, 2022

https://www.bigiron.com
Rare
John Deere 1800 Green Star 2 Monitor

ID#
Location:
Auction: Aug 10, 2022
Closing: 11d 21h 40m

US $775

Last minute bids extend item close by 3 mins

9 Bids

https://www.bigiron.com
GreenStar™ 2 2600 computer display on the John Deere 9770 STS. Credits: Rebecca Barocco, UF/IFAS
GreenStar™ 2 2600 computer display on the John Deere 9770 STS. Credits: Rebecca Barocco, UF/IFAS
John Deere 2600 Display

ID#
Location:
Auction: Jul 13, 2022

SOLD! US $5,600

63 Bids

https://www.bigiron.com/Search?historical=true&search=2600&searchMode=All&tab=&page=2&itemsPerPage=20&filter=Sold
2630 “The Workhorse”

- https://www.youtube.com/watch?v=wFv-fTItc2M
2630 "The Workhorse"

- https://www.sae.org/
2630 “The Workhorse”

- Windows Embedded CE

btw

https://www.sae.org/
The Workhorse

>$8,000

EOL

John Deere 2630 GreenStar 3 Display

Location: Ashland, NE
Auction: Jul 27, 2022

SOLD! US $8,500

John Deere 2630 GreenStar 3 Display

Location:
Auction: Jul 27, 2022

SOLD! US $8,000
<table>
<thead>
<tr>
<th></th>
<th>Born</th>
<th>Support end date</th>
<th>Support end date Pro</th>
<th>EOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Embedded CE 6.0</td>
<td>30&lt;sup&gt;th&lt;/sup&gt; Nov 2006</td>
<td>9&lt;sup&gt;th&lt;/sup&gt; April 2013</td>
<td>10&lt;sup&gt;th&lt;/sup&gt; April 2018</td>
<td>28&lt;sup&gt;th&lt;/sup&gt; Feb 2022</td>
</tr>
<tr>
<td>Windows Embedded Compact 7</td>
<td>15&lt;sup&gt;th&lt;/sup&gt; Mar 2011</td>
<td>12&lt;sup&gt;th&lt;/sup&gt; Apr 2016</td>
<td>13&lt;sup&gt;th&lt;/sup&gt; Apr 2021</td>
<td>28&lt;sup&gt;th&lt;/sup&gt; Feb 2026</td>
</tr>
<tr>
<td>Windows Embedded Compact 2013</td>
<td>11&lt;sup&gt;th&lt;/sup&gt; Aug 2013</td>
<td>9&lt;sup&gt;th&lt;/sup&gt; Oct 2018</td>
<td>10&lt;sup&gt;th&lt;/sup&gt; Oct 2023</td>
<td>31&lt;sup&gt;st&lt;/sup&gt; May 2028</td>
</tr>
</tbody>
</table>
Credit due:

- WinCE 6.0 keeps the food chain rolling
Credit due:

- Still works perfectly though.

Farms:
- Put seeds in ground
- Wait for seeds to grow
- Pick result
- Sell result
- Buy more seeds
Infinite money glitch IRL

Farms:
- Put seeds in ground
- Wait for seeds to grow
- Pick crop
- Sell crop
- Buy more seeds
21. Third Party Software Notifications and Licenses. The copyrights for certain portions of the Software may be owned or licensed by other third parties ("Third Party Software") and used and distributed under license. The Third Party Software Appendix (viewable at this link) includes the acknowledgements, notices and licenses for the Third Party Software. The Third Party Software is licensed according to the applicable Third Party Software license notwithstanding anything to the contrary in this License Agreement. The Third Party Software contains copyrighted software that is licensed under the GPL/LGPL or other copyleft licenses. A copy of those licenses are included in the Third Party Software Appendix. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of the Software by sending a money order or check for $5 to:

Deere Open Source Compliance Team
P.O. Box 1202
Moline, IL 61266-1202
USA

Please write "source for John Deere Generation 4-Series Display Unit Software" and your name and member of the software
The 4240 & 4640
The 4240 & 4640

John Deere 6000 Gen 4 4240 Universal Display
ID#
Location: Parlin, NJ
Auction: Jun 22, 2022

SOLD! US $4,500

62 Bids
Farmers prefer the old equipment

- Reliability/Productivity
- Proven
- Familiar
- Less device restrictions
Why am I hacking the 4240?

- Choosing the device with most longevity
- 2nd Hand fleet market
● Agricultural tech adoption is unique

● Equipment lasts for a LONG time
Ultra compatibility

• Brown Box *works* in brand new combine

• ISOBus VT: it’s in the name

• CAN, RS232, Analog, Digital, GPIO, WiFi

• GPS, RTCM, RTK Radio, NTRIP, USB, TCP, HSAL2...
Wind River Partner Ecosystem

Wind River works closely with Arm® to ensure that Wind River OSes, tools, and simulation offerings are optimized for use by Arm licensees. With Arm and Wind River, software developers and architects can utilize the full potential of Arm-based SoC designs.

Learn More »

A broad range of Intel® products and solutions are enabled for use with Wind River Studio, Wind River Linux, and VxWorks, providing compute platforms for critical workload consolidation and software-defined infrastructure.

Learn More »

Wind River partners with NXP to enable optimized VxWorks and Wind River Linux OSes, compilation tools, and Wind River Simics® simulation support for the NXP QorIQ, i.MX, and S32 families of Arm and Power Architecture-based MPUs.

Learn More »
## Wind River in Aerospace and Defense

<table>
<thead>
<tr>
<th>Air</th>
<th>Commercial Aviation</th>
<th>Land</th>
<th>Sea</th>
<th>Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache Helicopter</td>
<td>Airbus A318</td>
<td>Abrams Tank</td>
<td>AEGIS</td>
<td>A2100 Satellite</td>
</tr>
<tr>
<td>AWACS</td>
<td>Airbus A319</td>
<td>Challenger Tank</td>
<td>AN/AQS20/X Sonar</td>
<td>EGNOS</td>
</tr>
<tr>
<td>Airbus A330M</td>
<td>Airbus A320</td>
<td>CHALS-X</td>
<td>AN/SQQ-89 ASW</td>
<td>HOPE-X Space Plane</td>
</tr>
<tr>
<td>Airbus A400M</td>
<td>Airbus A340</td>
<td>CIBADS II</td>
<td>Astute Class Sub.</td>
<td>Mars Rovers</td>
</tr>
<tr>
<td>B-1B</td>
<td>Airbus A380</td>
<td>Fuchs Spürpanzer</td>
<td>Harpoon Missile</td>
<td>Mars Odyssey</td>
</tr>
<tr>
<td>B-2</td>
<td>ATIDS</td>
<td>GIG-E Program</td>
<td>Mark 48 GMVLS</td>
<td>Mars Pathfinder</td>
</tr>
<tr>
<td>B-52</td>
<td>Boeing 777</td>
<td>Hellfire Missile</td>
<td>MK41 5 inch gun</td>
<td>Mars Recon Orbiter</td>
</tr>
<tr>
<td>Boeing 767 Tanker</td>
<td>Boeing 787</td>
<td>JCAD</td>
<td>NCSSS</td>
<td>MTSAT-2 Satellite</td>
</tr>
<tr>
<td>Boeing C-130 AMP</td>
<td>EC-225 Helicopter</td>
<td>JTRS</td>
<td>NAVMACS</td>
<td>MUBLCOMM Satellite</td>
</tr>
<tr>
<td>EC-725 Helicopter</td>
<td>GlobalStar 2100</td>
<td>MEADS Missile</td>
<td>Phalanx – CIWS</td>
<td>NASA Space Shuttle</td>
</tr>
<tr>
<td>F-15</td>
<td>VICTORIA</td>
<td>Patriot Missile</td>
<td>SGS</td>
<td>NPOESS</td>
</tr>
<tr>
<td>F-16</td>
<td>WAAS</td>
<td>PDCUE</td>
<td>SSDS</td>
<td>ORBCOMM</td>
</tr>
<tr>
<td>F-18</td>
<td></td>
<td>Sentinel Missile</td>
<td>Tomahawk Missile</td>
<td>Phoenix Mars Lander</td>
</tr>
<tr>
<td>F-22</td>
<td></td>
<td>Stinger Missile</td>
<td>Trident Missile</td>
<td>PROBA Satellite</td>
</tr>
<tr>
<td>F-35 (JSF)</td>
<td></td>
<td>TDOA System</td>
<td>Type 45 Destroyer</td>
<td>SBIRS</td>
</tr>
<tr>
<td>Global Hawk UAV</td>
<td></td>
<td>THAAD Missile</td>
<td></td>
<td>SORCE Satellite</td>
</tr>
<tr>
<td>Jaguar</td>
<td></td>
<td>TRC 4000</td>
<td></td>
<td>X-38 Space Lifeboat</td>
</tr>
<tr>
<td>nEUROn</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Section Control

Demo
Time Remaining: 15 of 15 Hrs

Demo Off

Enter Activation Code
## Dollar bills

### AUTO TRAC PRICES

**GS3 AUTOTRAC PRICES**

<table>
<thead>
<tr>
<th>SF1 WITH GS 3 2630</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOTRAC ACTIVATION</td>
<td>$3,500.00</td>
</tr>
<tr>
<td>GS3 DISPLAY</td>
<td>$5,895.00</td>
</tr>
<tr>
<td>SF1 SF6000 RECEIVER</td>
<td>$3,895.00</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$13,290.00</strong></td>
</tr>
</tbody>
</table>

**SF1 HAS 9” ACCURACY**

**SF3 HAS 1.2” ACCURACY**

<table>
<thead>
<tr>
<th>GS3 2630 SF3 KIT</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOTRAC ACTIVATION</td>
<td>$3,500.00</td>
</tr>
<tr>
<td>GS3 DISPLAY</td>
<td>$5,895.00</td>
</tr>
<tr>
<td>SF3 SF6000 RECEIVER</td>
<td>$7,895.00</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$17,290.00</strong></td>
</tr>
</tbody>
</table>

**RTK HAS SUB INCH ACCURACY**

<table>
<thead>
<tr>
<th>GS 3 2630 RTK KIT</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOTRAC ACTIVATION</td>
<td>$3,500.00</td>
</tr>
<tr>
<td>GS3 DISPLAY</td>
<td>$5,895.00</td>
</tr>
<tr>
<td>SF3 SF6000 RECEIVER</td>
<td>$7,895.00</td>
</tr>
<tr>
<td>RTK ACTIVATION</td>
<td>$3,500.00</td>
</tr>
<tr>
<td>RTK RADIO BUNDLE</td>
<td>$1,795.00</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$22,585.00</strong></td>
</tr>
</tbody>
</table>

### USED AUTOTRAC PRICES

<table>
<thead>
<tr>
<th>SF1 WITH GS2 2600</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOTRAC ACTIVATION</td>
<td>$3,500.00</td>
</tr>
<tr>
<td>USED GS2 DISPLAY</td>
<td>$1,500.00</td>
</tr>
<tr>
<td>USED SF1 SF3000 RECEIVER</td>
<td>$2,500.00</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$7,500.00</strong></td>
</tr>
</tbody>
</table>

### Gen IV Display Prices

#### Gen IV 4600 Activations
- AutoTrac Activation: $1,000.00
- Premium Activation (AT, Swath, Doc): $3,000.00

#### Gen IV 4640 Prices
- 4640 Universal Display: $3,985.00
- 1 Yr AutoTrac Subscription: $850.00
- 1 Yr Precision Ag Core Subscription (AT, Swath, Doc): $1,700.00
- 5 Yr AutoTrac Subscription: $4,000.00
- 5 Yr Precision Ag Core Subscription (AT, Swath, Doc): $8,000.00

### Other Items and Upgrades to GS2 and GS3 Equipment

<table>
<thead>
<tr>
<th>GS2 Upgrades</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWATH CONTROL PRO</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>AUTOTRAC ACTIVATION</td>
<td>$3,500.00</td>
</tr>
<tr>
<td>ROWSENSE ACTIVATION</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>RTK ACTIVATION</td>
<td>$3,500.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GS3 Upgrades</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Sync Activation</td>
<td>$1,500.00</td>
</tr>
<tr>
<td>SWATH PRO ACTIVATION</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>AUTOTRAC ACTIVATION</td>
<td>$3,500.00</td>
</tr>
<tr>
<td>AUTOTRAC ROWSENSE</td>
<td>$3,000.00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Misc</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>RATE CONTROLLER 2000</td>
<td>$2,350.00</td>
</tr>
<tr>
<td>ATU 200</td>
<td>$1,395.00</td>
</tr>
<tr>
<td>SF1 TO SF2 RECEIVER UPGR</td>
<td>$4,000.00</td>
</tr>
<tr>
<td>RTK RADIO BUNDLE</td>
<td>$1,795.00</td>
</tr>
</tbody>
</table>
### RTK HAS SUB INCH ACCURACY

<table>
<thead>
<tr>
<th>GS 3 2630 RTK KIT</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOTRAC ACTIVATION</td>
<td>$3,500.00</td>
</tr>
<tr>
<td>GS3 DISPLAY</td>
<td>$5,895.00</td>
</tr>
<tr>
<td>SF3 SF6000 RECEIVER</td>
<td>$7,895.00</td>
</tr>
<tr>
<td>RTK ACTIVATION</td>
<td>$3,500.00</td>
</tr>
<tr>
<td>RTK RADIO BUNDLE</td>
<td>$1,795.00</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$22,585.00</strong></td>
</tr>
</tbody>
</table>

*Dollar bills*
### Gen IV 4640 Prices

- **4640 Universal Display with Documentation and Autotrac**: $8,495.00
- **Premium 3.0 Subscription - 1 Year (Swath, RowSense, Data Share)**: $850.00
- **Automation 3.0 Subscription - 1 Year (Prem 3.0 +Turn Automation, Imp Guide, Machine Sync)**: $1,350.00

### Gen IV 4240 Prices

- **4240 Display with Documentation and AutoTrac**: $5,495.00
- **Subscription - 1 Year (Swath, Data Sync)**: $600.00
## Gen IV Display Prices

### Gen IV 4600 Activations

<table>
<thead>
<tr>
<th>Service</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoTrac Activation</td>
<td>$1,000.00</td>
</tr>
<tr>
<td>Premium 3.0 (AT, Swath, Doc, RowSense, Data Share)</td>
<td>$3,750.00</td>
</tr>
<tr>
<td>Premium 1.0 to 3.0 Upgrade</td>
<td>$750.00</td>
</tr>
<tr>
<td>Premium 2.0 to 3.0 Upgrade</td>
<td>$250.00</td>
</tr>
<tr>
<td>Automation 3.0 (Prem 3.0 + Turn Automation, Imp Guide, Machine Sync)</td>
<td>$5,250.00</td>
</tr>
<tr>
<td>AutoTrac to Automation 3.0 Upgrade</td>
<td>$4,250.00</td>
</tr>
<tr>
<td>Premium 1.0 to Automation 3.0 Upgrade</td>
<td>$2,250.00</td>
</tr>
<tr>
<td>Premium 2.0 to Automation 3.0 Upgrade</td>
<td>$1,750.00</td>
</tr>
<tr>
<td>Premium 3.0 to Automation 3.0 Upgrade</td>
<td>$1,500.00</td>
</tr>
<tr>
<td>Automation 3.0 to Automation 3.0 Upgrade</td>
<td>$500.00</td>
</tr>
<tr>
<td>Pin Number</td>
<td>Circuit Code</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
</tr>
<tr>
<td>1</td>
<td>922C</td>
</tr>
<tr>
<td>2</td>
<td>n/a</td>
</tr>
<tr>
<td>3</td>
<td>209B</td>
</tr>
<tr>
<td>4</td>
<td>n/a</td>
</tr>
<tr>
<td>5</td>
<td>n/a</td>
</tr>
<tr>
<td>6</td>
<td>925B</td>
</tr>
<tr>
<td>7</td>
<td>924B</td>
</tr>
<tr>
<td>8</td>
<td>182</td>
</tr>
<tr>
<td>9</td>
<td>998</td>
</tr>
<tr>
<td>10</td>
<td>n/a</td>
</tr>
<tr>
<td>11</td>
<td>211B</td>
</tr>
<tr>
<td>12</td>
<td>915</td>
</tr>
<tr>
<td>13</td>
<td>914</td>
</tr>
<tr>
<td>14</td>
<td>070C</td>
</tr>
<tr>
<td>15</td>
<td>n/a</td>
</tr>
<tr>
<td>16</td>
<td>n/a</td>
</tr>
<tr>
<td>17</td>
<td>n/a</td>
</tr>
<tr>
<td>18</td>
<td>904C</td>
</tr>
<tr>
<td>19</td>
<td>905C</td>
</tr>
<tr>
<td>20</td>
<td>n/a</td>
</tr>
<tr>
<td>21</td>
<td>n/a</td>
</tr>
<tr>
<td>22</td>
<td>n/a</td>
</tr>
<tr>
<td>23</td>
<td>n/a</td>
</tr>
<tr>
<td>24</td>
<td>n/a</td>
</tr>
<tr>
<td>25</td>
<td>n/a</td>
</tr>
<tr>
<td>26</td>
<td>n/a</td>
</tr>
</tbody>
</table>
# Pinout Information

## Continuation of PF90687

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Circuit Code</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>922C</td>
<td>Switched Power</td>
</tr>
<tr>
<td>2</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>3</td>
<td>209B</td>
<td>Implement Status Signal</td>
</tr>
<tr>
<td>4</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>5</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>6</td>
<td>925B</td>
<td>CCD +</td>
</tr>
<tr>
<td>7</td>
<td>924B</td>
<td>CCD</td>
</tr>
<tr>
<td>8</td>
<td>182</td>
<td>Unswitched Power</td>
</tr>
<tr>
<td>9</td>
<td>998</td>
<td>Audio Mute</td>
</tr>
<tr>
<td>10</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>11</td>
<td>211B</td>
<td>Radar Ground Speed Signal</td>
</tr>
<tr>
<td>12</td>
<td>915</td>
<td>Vehicle CAN Bus - Lo</td>
</tr>
<tr>
<td>13</td>
<td>914</td>
<td>Vehicle CAN Bus - Hi</td>
</tr>
<tr>
<td>14</td>
<td>070C</td>
<td>Ground</td>
</tr>
<tr>
<td>15</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>16</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>17</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>18</td>
<td>904C</td>
<td>Implement CAN Bus - Hi</td>
</tr>
<tr>
<td>19</td>
<td>905C</td>
<td>Implement CAN Bus - Lo</td>
</tr>
<tr>
<td>20</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>21</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>22</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>23</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>24</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>25</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>26</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>
## Pinout Information

### Continuation of PF90687

<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Circuit Code</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>922C</td>
<td>Switched Power</td>
</tr>
<tr>
<td>2</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>3</td>
<td>209B</td>
<td>Implement Status Signal</td>
</tr>
<tr>
<td>4</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>5</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>6</td>
<td>925B</td>
<td>CCD +</td>
</tr>
<tr>
<td>12</td>
<td>915</td>
<td>Vehicle CAN Bus - Lo</td>
</tr>
<tr>
<td>13</td>
<td>914</td>
<td>Vehicle CAN Bus - Hi</td>
</tr>
<tr>
<td>14</td>
<td>070C</td>
<td>Ground</td>
</tr>
<tr>
<td>15</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>16</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>17</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>18</td>
<td>904C</td>
<td>Implement CAN Bus - Hi</td>
</tr>
<tr>
<td>19</td>
<td>905C</td>
<td>Implement CAN Bus - Lo</td>
</tr>
<tr>
<td>20</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>21</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>22</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>
RS232 Pin Out
Connector:
D-Sub Male 9 pins

Pin Out
01 DCD  Data Carrier Detect
02 RXD  Receive Data
03 TXD  Transmit Data
04 DTR  Data Terminal Ready
05 GND  Ground

Pin Out
Data Set Ready  DSR 06
Request To Send  RTS 07
Clear To Send  CTS 08
Ring Indicator  RI 09

Cable Tester
Copyright ©
www.cable-tester.com
- RS232
<table>
<thead>
<tr>
<th>Pin Number</th>
<th>Circuit Code</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>911B</td>
<td>n/a</td>
</tr>
<tr>
<td>2</td>
<td>907</td>
<td>RS232 Com Bus 1 - TXD</td>
</tr>
<tr>
<td>3</td>
<td>909</td>
<td>RS232 Com Bus 1 - RXD</td>
</tr>
<tr>
<td>4</td>
<td>911C</td>
<td>n/a</td>
</tr>
<tr>
<td>5</td>
<td>070A</td>
<td>Ground</td>
</tr>
</tbody>
</table>
SR INSTALLATION of PCGUMIA00552B - 1.1

English: Your system has entered System Recovery. Please contact your John Deere Dealer to attempt data recovery and software reinstallation. Dealers please refer to latest machine or display technical manual for more information.

Español: Su sistema ha entrado en modo de Recuperación. Por favor comuníquese con el concesionario John Deere para intentar la recuperación de datos y la reinstalación del software. Los concesionarios deben consultar el manual técnico más reciente de la máquina o de la pantalla.

Français: Votre système a démarré une récupération du système. Veuillez contacter votre concessionnaire John Deere pour tenter une récupération de données et une réinstallation du logiciel. Concessionnaires : veuillez vous reporter au manuel technique le plus récent de la machine ou de la console pour plus d’informations.

Deutsch: Ihr System befindet sich in Systemwiederherstellungsmodus. Bitte wenden Sie sich an Ihren John Deere-Händler, um eine Datenwiederherstellung und Neuinstallation der Software zu versuchen. Händler sollten das neueste technische Handbuch der Maschine oder des Displays heranziehen, um weitere Informationen zu erhalten.


Italiano: Il sistema in uso è entrato in fase Recupero sistema. Rrivolgersi al concessionario John Deere di zona per procedere al recupero dei dati ed alla reinstallazione del software. Per ulteriori informazioni i concessionari possono consultare il manuale tecnico della macchina o del display più recente.
Welcome to minicom 2.8

OPTIONS: I18n
Compiled on Jan 9 2021, 12:42:45.
Port /dev/ttyUSB0, 06:52:12

Press CTRL-A Z for help on special keys

my_load:667: do
HOTPLUG: mounted sda1 at /tmp/mnt/usbLYU3Gf
/dev/mmcb1k0p2: recovering journal
/dev/mmcb1k0p2: clean, 17026/130048 files, 243487/520192 blocks
SetupNormalPartitions IN_PROGRESS 36
fsck from util-linux 2.26.2
SetupUserDataAccess SUCCESS 100
10 Reboots = Dealer lock...

- Ok let’s desolder the eMMC
- Reduce the bootcount, increase max to 9999
[user@hostname 0]$ cat bootcount.cfg
BOOT_MODE=NORMAL
MAX_BOOT_COUNT=10
RECOVERY_BOOT_COUNT=6

[user@hostname 0]$
The Magic Check File

# DESCRIPTION
# Spawns login prompt on serial port, does not return.

SpawnSerialLogin()
{
    while true; do
        setsid /sbin/agetty -c -L 115200 ttyS_debug vt100
done
}
**Size** 16 GB (15,535,702,016 bytes)  
**Auto-clear** [ ]  
**Mounting File** /run/media/user/970EVO-1TB/master/4240.img  
**Partitioning** Master Boot Record  

### Volumes

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Filesystem</th>
<th>Filesystem</th>
<th>Filesystem</th>
<th>Extended Partition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Partition 1</td>
<td>Partition 2</td>
<td>Partition 3</td>
<td>Partition 4</td>
</tr>
<tr>
<td>Free Space</td>
<td>17 MB</td>
<td>17 MB Ext2</td>
<td>2.1 GB Ext4</td>
<td>13 GB</td>
</tr>
<tr>
<td></td>
<td>Partition 5</td>
<td>Partition 6</td>
<td>Partition 7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.1 GB Ext4</td>
<td>2.1 GB Ext4</td>
<td>8.5 GB Ext4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Partition 8</td>
<td>Partition 9</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>268 MB Ext2</td>
<td>268 MB Ext2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Size** 17 MB (16,777,216 bytes)  
**Contents** Unallocated Space  
**Device** /dev/loop0 (Read-Only)
รีการติดตั้ง
Fail

SetupUser: DataAccess SUCCESS 100

Wind River Linux 8.0.0.30 (none) ttyS_debug

(none) login:
Wind River Linux 8.0.0.30 (none) ttyS_debug

(none) login: a
Password:
Login incorrect
(none) login: @+Entering system recovery (Reached max allowed boot count of 10).
Entering System Recovery Mode
Attempting system recovery launch from /dev/mmcblk0p8.
socket: Function not implemented

System Recovery BootCount On Entry: 9999

CTRL-A % for help | 115200 8N1 | NOR | Minicom 2.8 | VT102 | Offline | ttyUSB0
Your system has entered System Recovery. Please contact your John Deere Dealer to attempt data recovery and software reinstallation.

Follow instructions if system recovery message is displayed.

System Recovery tries to protect and potentially save user data. System Recovery initiates when the system detects a conflict that might corrupt the intended functions. For more information about System Recovery, contact your John Deere dealer.
English: Your system has entered System Recovery. Attempt data recovery and software reinstallation or display technical manual for more information.

Please contact your John Deere Dealer to.

Dealers please refer to latest machine.
What if you don’t have a John Deere Dealer?
John Deere Asia's virtual showroom at your fingertips. Click and explore!
Find a dealer near you

Thailand
14 hr 59 min (1,113.4 km) via Route 4
Google

14 hr 59 min (1,)

LOOK AT ME

I AM THE DEALER NOW
Official public software manager
ncdu 2.1.2 ~ Use the arrow keys to navigate, press ? for help
--- /home/user/.wine/drive_c/users/user/Application Data/JDSync ---

12.2 GiB [################################] /working
492.0 KiB [ ] gsixRsync.log
4.0 KiB [ ] settings.cfg
● armv7hl
● atom
● corei7_64
● armv7h1v2
● noarch
#!/bin/bash

# param 1 - devnode
# param 2 - mount point

scriptName=${0##*/}
appsUsbScriptFile='/opt/GSix/bin/usbmanager.sh'
reprogramImageCheckFile='root/JDeereBootableUSBFlag87657'
unitBootedFile='/tmp/uDevVUnitBooted'
isoSecurityDeveloperFile='/opt/persistent/43434.001'
isoSecurityFactoryFile='/opt/persistent/43434.002'

if [ $# -ne 2 ]; then
    /usr/bin/logger "${scriptName}: ERROR - Missing parameter"
    exit 1
fi

devnode=$1
usbMountPath=$2
```
if [ ! -z ${MOUNT_POINT:-} ]
then
    local readonly REPROGRAM_IMAGE_CHECK_FILE="${MOUNT_POINT}/root/JDeereBootableUSBFlag87657"
    if [ -e ${REPROGRAM_IMAGE_CHECK_FILE} ]
    then
        isoKernelPath=$(find ${MOUNT_POINT}/boot -name vmlinuz -o -name zImage -o -name uImage)
        if [ ! -z ${isoKernelPath:-} ]
        then
            isoKernelPath=$(dirname ${isoKernelPath})
        fi
    fi
fi
```

```
echo ${isoKernelPath}
```
<table>
<thead>
<tr>
<th>Name</th>
<th>Owner</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>JD-Display-Updates-JD5</td>
<td>user</td>
<td>48.0 KiB</td>
</tr>
<tr>
<td>Trash-1000</td>
<td>user</td>
<td>16.0 KiB</td>
</tr>
<tr>
<td>dealerAuth</td>
<td>user</td>
<td>0 byte</td>
</tr>
<tr>
<td>43434.002</td>
<td>user</td>
<td>0 byte</td>
</tr>
<tr>
<td>JDeereBootableUSBFlag87657</td>
<td>user</td>
<td>0 byte</td>
</tr>
</tbody>
</table>
SR INSTALLATION of PCGUMUA005528 - 1.1

English: Your system has entered System Recovery. Please contact your John Deere Dealer to attempt data recovery and software reinstallation. Dealers please refer to latest manual or display technical manual for more information.

Español: Su sistema ha entrado en modo de Recuperación. Por favor comuníquese con el concesionario John Deere para intentar la recuperación de datos y la reinstalación del software. Los concesionarios deben consultar el manual técnico más reciente de la máquina o de la pantalla.
SR INSTALLATION of PCGUMUA00552B - 1.2

Preparing to read disk
SR INSTALLATION of PCGUMUA005528 - 3.1

Gen 1 OS and AMS Applications not found on USB drive.
Still bootlooped
SR INSTALLATION of PGMN00552B - 1.5

Backing up data to USB drive...

(??) Maintain electrical power
(??) Do not remove USB drive
John Deere Dealer auth bypass

- touch ./dealerAuth.txt
- Ty Gusutec BR
1.7.1 Preparing to install software.
Installing System Update

Please wait. Installation may take up to an hour to complete.

Maintain Electrical Power
FINALIZING SOFTWARE UPDATES
Do NOT power OFF display or machine
John Deere Display Software License Agreement

Attention! Your use of this Display and the associated software and services are governed by the John Deere Display License Agreement, which is an enforceable legal contract that governs your use of the system and software. Among other important terms, the license agreement:

- Binds you, and any company or other legal organization that you represent, to comply with its terms.
- Protects Deere’s intellectual property rights.
- Limits your rights with respect to the system and software.
- Limits Deere’s liability for damages and injuries.
- Limits Deere’s warranty obligations.
- Obligates you to indemnify Deere for certain damages and injuries.
- Specifies the forum and governing law for any disputes arising under this license agreement.

Please read the entire license agreement before accepting it. The entire license agreement is available at the link below. The license agreement can also be found on the About tab under Information & Settings within each Application.

IF YOU ARE UNWILLING OR UNABLE TO ACCEPT THE TERMS OF THE LICENSE,

Scroll to view entire agreement

I Decline

I Accept
Bonus!

- Logs
- Logs
- Logs!

Post update...

[shell output]

[user@hostname PCGUMUA005528]$ find .
./SRLogs
./SRLogs/yum.log
./SRLogs/sr.log-2013-01-01-00-25-28
./SRLogs/recovery.log
./SRLogs/lastlog
./SRLogs/SRInError.txt
./BSPLogs
./BSPLogs/yum.log.11
./BSPLogs/dmesg.1
./BSPLogs/syslog.13.gz
./BSPLogs/MIBDump
./BSPLogs/syslog.17.gz
./BSPLogs/wtmp
./BSPLogs/syslog.12.gz
./BSPLogs/Xorg.0.log.old
./BSPLogs/yum.log.10
./BSPLogs/ospl-error.log
./BSPLogs/dmesg.4
./BSPLogs/syslog.14.gz
./BSPLogs/syslog.10.gz
./BSPLogs/syslog.18.gz
./BSPLogs/dmesg.3
./BSPLogs/CleanInstallLog.log.gz
./BSPLogs/ospl-info.log.15.gz
19.5 MiB [############################] usrdatal.tar-6
19.5 MiB [############################] usrdatal.tar-5
19.5 MiB [############################] usrdatal.tar-4
19.5 MiB [############################] usrdatal.tar-3
19.5 MiB [############################] usrdatal.tar-2
19.5 MiB [############################] usrdatal.tar
14.1 MiB [############################] usrdatal.tar-82
  1.1 MiB [#] /PCGUMUA005528
  752.0 KiB [ ] /SRLogs
  8.0 KiB [ ] /BSPLogs
  8.0 KiB [ ] systemConf.txt

Total disk usage:  1.6 GiB  Apparent size:  1.6 GiB  Items:  150
Starting kernel ...

Booting system...(BootCount is 2)
my_load:667: do
ifdown: socket: Function not implemented
[MonitorAutoUpdate] Checking if monitors need to be updated

Wind River Linux 8.0.0.30 PCGUMUA005528.local.domain tty_console

PCGUMUA005528 login:
Wind River Linux 8.0.0.30 PCGUMUA005528.local.domain tty_console

PCGUMUA005528 login:
Wind River Linux 8.0.0.30 PCGUMUA005528.local.domain tty_console

PCGUMUA005528 login:
Wind River Linux 8.0.0.30 PCGUMUA005528.local.domain tty_console

PCGUMUA005528 login:
Wind River Linux 8.0.0.30 PCGUMUA005528.local.domain tty_console

PCGUMUA005528 login:
Wind River Linux 8.0.0.30 PCGUMUA005528.local.domain tty_console

PCGUMUA005528 login:
Wind River Linux 8.0.0.30 PCGUMUA005528.local.domain tty_console
```bash
# The device names in this file were setup during the install process.

<table>
<thead>
<tr>
<th>File System Path</th>
<th>Mount Point</th>
<th>Filesystem Type</th>
<th>Options</th>
<th>Dump</th>
<th>Pass</th>
</tr>
</thead>
<tbody>
<tr>
<td>dev/mmcb1k0p2</td>
<td>/</td>
<td>ext4</td>
<td>ro, noatime</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>dev/mmcb1k0p1</td>
<td>/boot</td>
<td>ext2</td>
<td>ro, noatime</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dev/mmcb1k0p3</td>
<td>/opt/persistent</td>
<td>ext4</td>
<td>rw, noatime, data=journal</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>dev/mmcb1k0p5</td>
<td>/opt/GSix</td>
<td>ext4</td>
<td>ro, noatime</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>dev/mmcb1k0p6</td>
<td>/var</td>
<td>ext4</td>
<td>rw, noatime, data=journal</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>dev/mmcb1k0p7</td>
<td>/opt/usr_data</td>
<td>ext4</td>
<td>rw, noatime, data=journal</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>mpfs</td>
<td>/run</td>
<td>tmpfs</td>
<td>rw, nodev, nosuid, noexec, mode=1777</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mpfs</td>
<td>/logging</td>
<td>tmpfs</td>
<td>size=20M, nodev, nosuid, noexec, mode=1777</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Decision to make

● Risk the LBGA100 chip by hot air again (requires risk)

● Root the device naturally

● Try another USB method
Cool white-listed devices

# BSP rules for IAVS

3  KERNEL="eeprom",     GROUP="bsp"
4  KERNEL="spi_dma",     GROUP="bsp"; MODE="0660"
5  KERNEL="rtc0",        GROUP="bsp"; MODE="0660" SYMLINK+=="rtc"
6  KERNEL="watchdog",    GROUP="bsp"; MODE="0660"
7  KERNEL="i2c-0",       GROUP="bsp"; MODE="0660"
8  KERNEL="video0",      GROUP="bsp"; MODE="0666"
9  KERNEL="fb0",         GROUP="bsp"; MODE="0666"
10 KERNEL="fb1",         GROUP="bsp"; MODE="0666"
#!/bin/bash

source /usr/sbin/RunOnceHelpers.sh

# The SSH keys must be generated while the unit is mounted in rw mode. An easy way to do this is starting and stopping the SSH daemon

_ /etc/init.d/sshd start
_ /etc/init.d/sshd stop

exit ${RetVal}
ReadOnly=unknown

# Determine if root is read-only, remount if so
HandleReadOnly()
{
    if [[ ${ReadOnly} == "unknown" ]]; then
        # System recovery is not read-only
        ReadOnly=false
        if grep " / " /etc/fstab | awk '{ print $4 }'  
            ReadOnly=true
            mount -o remount,rw /
        fi
    fi
}
• Attempt at data rw without hot air

• Fail (btw)
Desoldered again.

- BOOT_COUNT 9999 fails checksum
- There's a `RebootClearBootCount` command anyway
- Add cron task
Display Monitor cannot communicate with processor (DTC: VTU 516843.09)
Just in case...
Improvise
2 mins later
Need more paths

PATHS=('/bin'
    '/etc/bspd/sbin'
    '/usr/lib mono/xbuild/12.0/bin'
    '/usr/lib mono/xbuild/14.0/bin'
    '/usr/lib mono/msbuild/Current/bin'
    '/usr/lib mono/msbuild/Current/bin/Roslyn'
    '/usr/lib pm-utils/bin'
    '/usr/lib rpm/bin'
    '/usr/bin']
    '/usr/sbin'
    '/usr/local/bin'
    '/usr/local/sbin'
    '/sbin'
    '/run/tmp/root_tmp/mnt/usb/usb-0.1/usb/bin')

for NEW_PATH in "${PATHS[@]}"; do
    export PATH="${NEW_PATH}:${PATH}"
Need more paths

- Bonus bins

root@PCGUMUA005528:/root>
Display all 1072 possibilities? (y or n)
root@PCGUMUA005528:/root> . path.sh
root@PCGUMUA005528:/root>
Display all 1105 possibilities? (y or n)
"System rollback"

- `cat 4240.img > /dev/sde`
- **Root password change**
- **Permit root login over SSH**
- `rw disk`
- **Add terminal**
- **Remove udev rules for usb ethernet**
Root password change

sudo chmod 644 shadow
sudo chmod 644 shadow-
sudo chmod 600 shadow-
sudo chmod 400 shadow
Root password change

de93739bc876dd4d8d5e36427c8446f
./SystemRecoveryWithSRApp.1.1.346-9.armv7hlv2.iso
Permit root login over SSH

- ./1/etc/init.d/sshd
- ./1/etc/rc1.d/K09sshd
- ./1/etc/rc0.d/K09sshd
- ./1/etc/default/volatiles/99_sshd
- ./1/etc/rc3.d/S09sshd
- ./1/etc/rc5.d/S09sshd
- ./1/etc/rc6.d/K09sshd
- ./1/etc/ssh/sshd_config
- ./1/etc/ssh/sshd_config_readonly
- ./1/etc/pam.d/sshd
- ./1/etc/rc2.d/S09sshd
- `edit /etc/fstab`

```bash
1 # <file system> <mount point>  <type>  <options>  <dump>  <pass>
2 proc /proc  proc  nodev,noexec,nosuid  0  0
3
4 # the device names in this file were setup during the install process.
5 /dev/mmcblk0p2 /  ext4  ro,noatime  0  1
6 /dev/mmcblk0p1 /boot ext2  ro,noatime  0  0
7 /dev/mmcblk0p3 /opt/persistent ext4  rw,noatime, data=journal  0  2
8 /dev/mmcblk0p5 /opt/GSix ext4  ro, noatime  0  2
9 /dev/mmcblk0p6 /var ext4  rw, noatime, data=journal  0  2
10 /dev/mmcblk0p7 /opt/usr_data ext4  rw, noatime, data=journal  0  2
11
12 tmpfs /run tmpfs  rw, nodev, nosuid, noexec, mode=1777  0  0
13 tmpfs /logging tmpfs  size=20M, nodev, nosuid, noexec, mode=1777  0  0
14
15
```
Add terminal

- */2 * * * * root DISPLAY=:0 /usr/bin/x-terminal-emulator
- */2 * * * * root DISPLAY=:1 /usr/bin/x-terminal-emulator
- etc/cron.d/logrotate.cron
- `lib/udev/rules.d`

- Find udev rules to allow ethernet adapter

- Either remove deny list or allow all

Remove udev rules for usb ethernet for wired usb nic
<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>Administrator</td>
<td>1</td>
<td>11111</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>Operator</td>
<td>2</td>
<td>11111</td>
<td>0</td>
</tr>
</tbody>
</table>
Can we emulate this?
Can I use JD rpms on Fedora?
emulating the reMarkable tablet (i.MX6 ARMv7) with Qemu

I'm trying to emulate the reMarkable tablet with Qemu in order to create a proper development environment for it, instead of cross-compiling and sending to the hardware device.

The firmware flasher repo contains the rootfs, kernel, DTB and u-boot files. I've created an .img file from the rootfs in order to boot it in Qemu with the following command:

```
qemu-system-arm \
-M sabrelite \ 
-bios "files/u-boot.imx" \ 
-kernel "zImage" \ 
-append "console=ttymxc0 rootfstype=ext4 root=/dev/mmcblk1p2 rw rootwait init=/bin/init -dtb "zero-gravitas.dtb" \ 
-drive file="floppy.img",format=raw,id=mmcblk1p2 \ 
-device sd-card,drive=mmcblk1p2
```
The Windows reflash toolkit used by the manufacturer to unbrick, unlock and reflash your Remarkable Tablet.
Booting Linux on physical CPU 0x0
Linux version 4.1.28-zero-gravitas-01866-ge0b823726ea4-dirty (sandmark@meruval) (gcc version 5.3.0 (GCC) ) #82 Thu Apr 27 14:27:47 CEST 2017
CPU: ARMv7 Processor [410fc090] revision 0 (ARMv7), cr=10c5387d
CPU: PPI / VIP nonaliasing data cache, VIP nonaliasing instruction cache
Machine model: reMarkable Prototype 1
Reserved memory: failed to allocate memory for node 'linux,cma'
cma: Reserved 32 MiB at 0x10000000
Memory policy: Data cache writeback
On node 0 totalpages: 32768
free_area_init_node: node 0, pgdat 8080fa24, node_mem_map 85ee7000
Normal zone: 256 pages used for mmemp
Normal zone: 0 pages reserved
Normal zone: 32768 pages, LIFO batch:7
CPU: All CPU(s) started in SVC mode.
pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
pcpu-alloc: [0] 0
Built 1 zonelists in Zone order, mobility grouping off. Total pages: 32512
Kernel command line: console=ttyS0 rootfstype=ext4 root=/dev/mmcblk0p2 rw rootwait init=/bin/bash loglevel=8 bootmem-debug earlyprintk
PID hash table entries: 512 (order: -1, 2048 bytes)
Dentry cache hash table entries: 16384 (order: 4, 65536 bytes)
Inode-cache hash table entries: 8192 (order: 3, 32768 bytes)
Memory: 88292K/131072K available (5361K kernel code, 218K rwdata, 2448K rodata, 196K init, 353K bss, 10012K reserved, 32768K cma-reserved, OK highmem)
Virtual kernel memory layout:

vector: 0xffff0000 - 0xffff1000 ( 4 KB)
fixmap: 0x0f000000 - 0xffff0000 (3072 KB)
vmalloc: 0x08800000 - 0xff000000 (1896 MB)
lowmem: 0x08000000 - 0x80000000 (128 MB)
map: 0x7fe00000 - 0x80000000 ( 2 MB)
.text: 0x80000000 - 0x807a89dc (7811 KB)
.init: 0x807a9000 - 0x807da000 ( 196 KB)
data: 0x807da000 - 0x80810980 (219 KB)
.bss: 0x80810980 - 0x80868f2c (354 KB)
SLUB: Halign=64, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
NR_IRQS:16 nr_irqs:16 16
LZC-310 erratum disabled
LZC-310 full line of zeros enabled for Cortex-A9
LZC-310 cache controller enabled, 8 ways, 64 KB
LZC-310: CACHE_ID 0x00000000, AUX_CTRL 0x00000000
mxc_clocksource_init 6000000
Switching to timer-based delay loop, resolution 15Ns
Trial & error

```bash
qemu-system-aarch64 -machine virt -cpu cortex-a57 \
  -device virtio-net-device,netdev=net0 -netdev user,id=net0 \
  -m 512 \n  -bios qemu-u-boot-bcm-2xxx-rpi4.bin \n  -device virtio-gpu-pci -serial stdio \n  -device qemu-xhci -device usb-tablet -device usb-kbd \n  -drive id=disk0,file=boot-image-qemu.hddimg,if=none,format=raw 
  -device virtio-blk-device,drive=disk0
```
What happens when you?

- Mix & match kernels, device trees (DTB files), architectures, disks...
Jul 04 11:10:00.883873 hostname kernel: qemu-system-aarch [191949]: segfault at a0 ip 000056298699d0bb sp 00007fe2bb9fde30 error 4 in qemu-system-aarch64[5629863bc000+97c000]

Jul 04 11:10:00.883965 hostname kernel: Code: 48 89 06 c7 46 08 01 00 00 04 89 66 20 0f 11 46 10 e8 b8 ff ff 48 8b 74 24 30 eb 53 90 4 8 8b 6c 24 28 0f 1f 00 48 89 ca <48> 8b 89 a0 00 00 00 48 85 c9 75 f1 80 7a 30 00 0f 84 9f 00 00 00

Jul 04 11:10:00.884009 hostname kernel: audit: type=1701 audit(1656933...
<table>
<thead>
<tr>
<th>CVE-ID</th>
<th>Learn more at National Vulnerability Database (NVD)</th>
<th>Description</th>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2022-35414</td>
<td>• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information</td>
<td>softmmu/physemem.c in QEMU through 7.0.0 can perform an uninitialized read on the translate_fail path, leading to an io_readx or io_writex crash.</td>
<td><strong>Note:</strong> References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.</td>
</tr>
</tbody>
</table>

- MISC:https://github.com/qemu/qemu/blob/f200ff158d5abcb974a6b597a962b6b2fbea2b06/softmmu/physemem.c
- MISC:https://github.com/qemu/qemu/blob/v7.0.0/include/exec/cpu-all.h#L145-L148
- MISC:https://github.com/qemu/qemu/commit/3517fb726741c109cae7995f9ea46f0cab6187d6#diff-82e563ed6329dc5d49876f1116c7519b5c16654bba6b4b4e2e928f5833d576f4b42
[user@hostname 0]$ cd ..
[user@hostname 4240_RESTORED]$ find | grep SecurityChipPassword
./1/usr/share/Deere/SecurePassword/7.10.1044/SecurityChipPassword
[user@hostname 4240_RESTORED]$ cd ./1/usr/share/Deere/SecurePassword/
[user@hostname SecurePassword]$ ls
7.10.1044  SavedPasswordHash
[user@hostname SecurePassword]$ ls -lha
total 16K
drwxr-xr-x  3 user  root  4.0K Jan  1 2013 7.10.1044
-rw-r--r--  1 user  root  35 Jan  1 2013 SavedPasswordHash
[user@hostname SecurePassword]$ cat SavedPasswordHash
$1$sffRhdI$tpMglXkj6BAXW3O7YB.sy1
[user@hostname SecurePassword]$
# If we are on IAVS, also set the u-boot password

```bash
if [ $(GetPlatform) == $PLATFORM_GSI6_ARM ]; then
echo -n "$Password" | /usr/bin/md5sum > $tmpFile
md5Password=$(< /usr/bin/cut -c-32 $tmpFile)
rm $tmpFile
if ! /sbin/fw_setenv bootstopkey $md5Password; then
echo "Failed to set uboot password"
exit 1
fi
fi
```
Index of /demo_software/WANDBOARD/

../
wandboard-imx6/ 08-Dec-2021 09:27 -
<table>
<thead>
<tr>
<th>File Name</th>
<th>Size (Bytes)</th>
<th>Date and Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>archived/</td>
<td>0</td>
<td>03:13 20-Dec-2021</td>
</tr>
<tr>
<td>wandboard-all-ubuntu-16.04-sdcard-20171213.zip</td>
<td>907396015</td>
<td>05:57 19-Mar-2018</td>
</tr>
<tr>
<td>wandboard-android-7.1.1.1-20170726-sdcard.zip</td>
<td>411187847</td>
<td>09:16 03-Aug-2017</td>
</tr>
<tr>
<td>wandboard-imx6_yocto-3.0_x11_qca_20211018182250.&gt;</td>
<td>872458421</td>
<td>09:27 08-Dec-2021</td>
</tr>
</tbody>
</table>
3.3. Fast Ethernet

The Hobbitboard features a 10/100 Mbit/s Fast Ethernet MAC compliant with the IEEE802.3-2002 standard. The MAC layer provides compatibility with half- or full-duplex 10/100 Mbit/s Ethernet LANs.

Figure 11 - Hobbitboard RJ-45 Network Connector Location
<table>
<thead>
<tr>
<th>Model</th>
<th>ARMv7-A</th>
<th>ARM Cortex-A7</th>
<th>ARM Cortex-A9</th>
<th>ARM Cortex-A17</th>
<th>Frequency</th>
<th>GPU</th>
<th>Memory</th>
<th>Bus Width</th>
<th>Release</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>RK3188T</td>
<td>1.5</td>
<td>256</td>
<td>Mali-400 MP2</td>
<td>600[28]</td>
<td>10.8[28]</td>
<td></td>
<td>DDR3L-1333, LPDDR2/3-1066, up to 4 GiB</td>
<td>32-bit dual channel</td>
<td>?</td>
<td>Q3 2014</td>
</tr>
</tbody>
</table>
U-Boot 2015.04-00061-g442f623 (Dec 19 2016 - 14:10:19)

CPU: Freescale i.MX6UL rev1.0 at 396 MHz
CPU: Temperature 41 C
Reset cause: POR
DRAM size is 256MB
Board: PicoSOM i.mx6UL
I2C: ready
DRAM: 512 M1B
PMIC: PFUZE300 DEV_ID=0x30 REV_ID=0x11
MMC: FSL_SDHC: 0
*** Warning - bad CRC, using default environment

In: serial
Out: serial
Err: serial
flash target is MMC:0
Net: FEC1
can't find partition: misc, dump the partition table
idx 0, ptn 0 name='gpt' start=0 len=128
idx 1, ptn 0 name='bootloader' start=2 len=2046
rw_block, cannot get the partion info for misc
read_bootctl, rw_block read failed
read command failed
Fastboot: Normal
Hit any key to stop autoboott: 3
Key features

- The real cross platform. Linux, Windows, MacOS (not tested yet)
- Multi devices program support
- Daemon mode support
- Few dependencies (only libusb, zlibc, libbz2)
- Firmware (uboot/kernel) uses WCID to auto load the winusb driver on the Windows side. Windows 7 users need to install the winusb driver from https://zadig.akeo.ie/ Windows 10 will install the driver automatically.
Computer Science Is About Abstraction

Level of Abstraction

Structured Programming

Object-oriented Programming

GUI

Proc(i1, i2, o1)

DO I=1, 100
I=I+1

MOV R0, A1
BNE F32C

FORTRAN

Assembly Language

Machine Language

Time
- Works

- NXP: no GFX on the imx6UL
Welcome to the hell that is 3D in Qt.

To understand the problems that you are facing, you need to know a little history. Other users can perhaps provide additional insight or correct any errors, since my recollection and understanding of these matters is probably not perfect.

I know a little bit about the history. I've been hanging around Qt from the 4.5 days, or thereabouts.
Qt3D was introduced in 2016 to much fanfare and was going to be the primary
> 3D solution for Qt. The idea was that Qt3D would provide a high-performance
> core capable of modern 3D graphics. Then, in 2017, Qt Co. had a
> philosophical shift and realized that rather than offering 3D functionality
> through LGPL/C++ (which could also be used by those darned open-source
> users), they could make more money in the short-term by locking in John
> Deere/others into subscription-based commercial licensing to display their
> little tractor animations. Because of the KDE agreement, they could not
> simply modify the license on Qt3D going forward, so they had to start from
> scratch with a new GPL/QML package: enter QtQuick3D.
through LGPL/C++ (which could also be used by those darned open-source
users), they could make more money in the short-term by locking in John
Deere/others into subscription-based commercial licensing to display their
little tractor animations. Because of the KDE agreement, they could not
simply modify the license on Qt3D going forward, so they had to start from
scratch with a new GPL/QML package: enter QtQuick3D.
● Try Robert Feranec option
● imx6rex

Options?
• Pump the brakes
1 MILLION ERASE/WRITE CYCLES, with 40 YEARS DATA RETENTION
DUAL ORGANIZATION: 256 x 16 or 512 x 8
BYTE/WORD and ENTIRE MEMORY PROGRAMMING INSTRUCTIONS
SELF-TIMED PROGRAMMING CYCLE with AUTO-ERASE
READY/BUSY SIGNAL DURING PROGRAMMING
SINGLE SUPPLY VOLTAGE:
– 4.5V to 5.5V for ST93C66 version
– 3V to 5.5V for ST93C67 version
SEQUENTIAL READ OPERATION
5ms TYPICAL PROGRAMMING TIME
ST93C66 and ST93C67 are replaced by the M93C66

Figure 1. Logic Diagram
### Table 1. Signal Names

<table>
<thead>
<tr>
<th>Signal</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>Chip Select Input</td>
</tr>
<tr>
<td>D</td>
<td>Serial Data Input</td>
</tr>
<tr>
<td>Q</td>
<td>Serial Data Output</td>
</tr>
<tr>
<td>C</td>
<td>Serial Clock</td>
</tr>
<tr>
<td>ORG</td>
<td>Organisation Select</td>
</tr>
<tr>
<td>VCC</td>
<td>Supply Voltage</td>
</tr>
<tr>
<td>VSS</td>
<td>Ground</td>
</tr>
</tbody>
</table>

**Diagram of ST93C66 and ST93C67 pinouts**

AI01254C
tim0s/
MicrowireEEPROM

Read and write EEPROMs using the Microwire protocol, such as the ST93C66

Contributors 0
Issues 4
Stars 16
Forks 6
Microwire EEPROM Library for Arduino

This library enables you to read and write EEPROM chips which use the Microwire protocol. Examples are chips such as the ST93C66 or 93LC46. See the datasheets of these chips for a description of the protocol.

Why not just use SPI?

For some Microwire EEPROMS you could use the Arduinos SPI interface, however, this does not work in all cases --- some chips count the number of clock pulses between the start bit and the falling edge of the clock signal. SPI works on multiples of eight bits, so if the address width does not happen to be five (quite small) or thirteen (quite large) bits, it will not work.

Therefore this library bitbangs the Microwire protocol. This also means you have complete flexibility over which Arduino pins you want to use.
- SCLK: Serial Clock (output from master)
- MOSI: Master Out Slave In (data output from master)
- MISO: Master In Slave Out (data output from slave)
- CS /SS: Chip/Slave Select (often active low, output from master to indicate that data is being sent)
DRAM: 2 GB
MMC: status 0
FSI_ESDHC: 0
In: serial
Out: serial
Err: serial
FEC0 [PRIME]
autoboot in 1 seconds
mmc0(part 0) is current device

MMC read: dev # 0, block # 4096, count 20480 ... 20480 blocks read: OK

MMC read: dev # 0, block # 24576, count 8192 ... 8192 blocks read: OK
## Booting kernel from Legacy Image at 10800000 ...
   Image Name: Bootloader
   Image Type: ARM Linux Multi-File Image (uncompressed)
   Data Size: 3153530 Bytes = 3 MB
   Load Address: 10008000
   Entry Point: 10008000
   Contents:
     Image 0: 3153522 Bytes = 3 MB
## Loading init Ramdisk from Legacy Image at 12000000 ...
   Image Name: SR Bootloader Filesystem
   Image Type: ARM Linux RAMdisk Image (gzip compressed)
   Data Size: 2152759 Bytes = 2.1 MB
   Load Address: 11000000
   Entry Point: 11000000
   Loading Multi-File Image ... OK
OK
Home stretch

- Root term is sufficient.
- We can trivially remount the OS
- Boot partition edit = bad
- checksum had been changed

- Could edit /boot but in the spirit of stock
- “rooted”
USB exploit vs...

https://learn.adafruit.com/how-to-build-a-testingfixture
USB exploit vs...
Useless shell
- WiFi
- TL-WN725N
- Fail
- (unless MTG *cough*)
- Boot count fix
called

configuration
cando

canecho
cansend

consequence
● Grand finale
sh-3.2# mount -o remount,rw /
sh-3.2#
• No display?
• Xorg anyway
The "Jailbreak"

- `tee -a '/etc/cron.d/logrotate.cron' <<< '*/2 * * * * root DISPLAY=:0 /usr/bin/x-terminal-emulator'
- `mount -o remount,rw /`
Wait there’s more
@skelegant

https://forum.zdoom.org/viewtopic.php?t=61681
Only one problem

- I hadn’t asked *skelegant* if I could use her WAD context

- *aaaand it doesn’t run without DECORATE*
So we met up and sh created the ultimate solution...

Demo:
USB Drive Options

What would you like to do?

- Import Data
- Export Data
- Install Software
Thank you

https://github.com/sickcodes
https://twitter.com/sickcodes
https://linkedin.com/in/in/sickcodes
https://sick.codes
info@sick.codes

Special thanks @Skelegant

GUSETEC BRAZIL, Last Person
Alex the kangaroo
Kevin Kenney
Johannes Agra-GPS

Vlad, Aleksei, Mauro, Dudas, Alex 2, Alex 3