



Sommaire :

- SQUIRT BGA RGH montage sur X360 SLIM
- SQUIRT BGA RGH montage sur X360 FAT
- Installer la partie software du reset glitch hack (RGH)
- Diagnostic des pannes et suggestions
- Installation en DUAL NAND sur SLIM
- Installation en DUAL NAND sur FAT
- Diagnostic des pannes et suggestions

Site officiel :

<http://www.360squirt.com/>

Tutos :

<http://www.xavbox360.com/>

Forrum :

<http://www.xavboxforum.com/index.php/forum/220-360squirt/>

MANUEL v.1.3

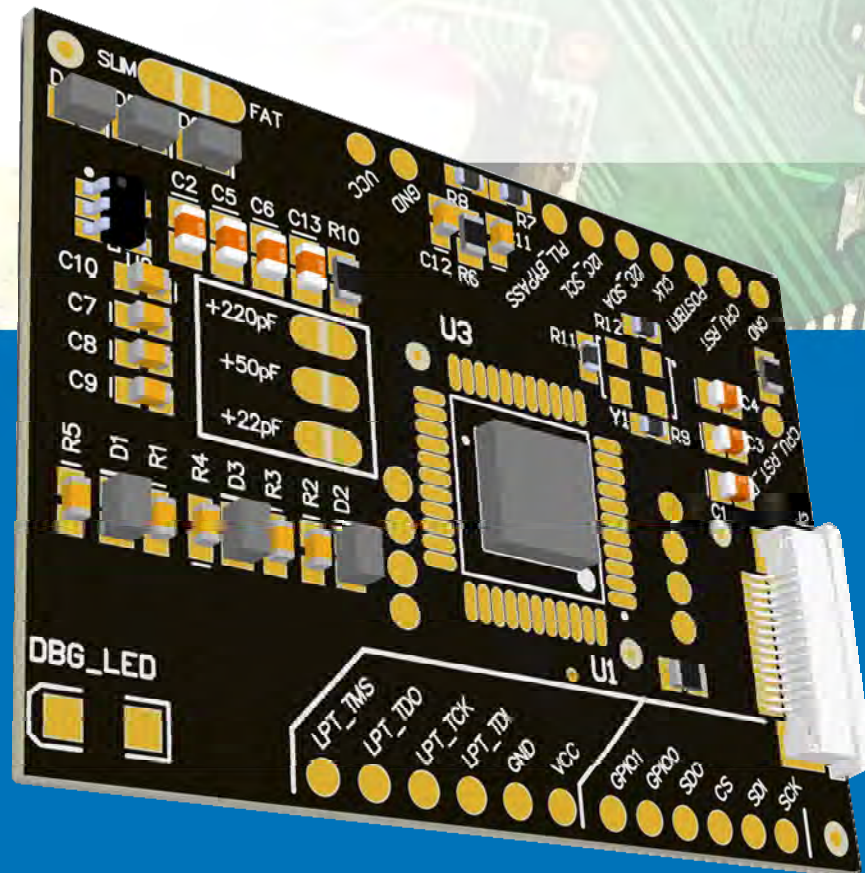
22/04/2012

360SQUIRT

Tout ce dont vous avez besoin pour le RGH

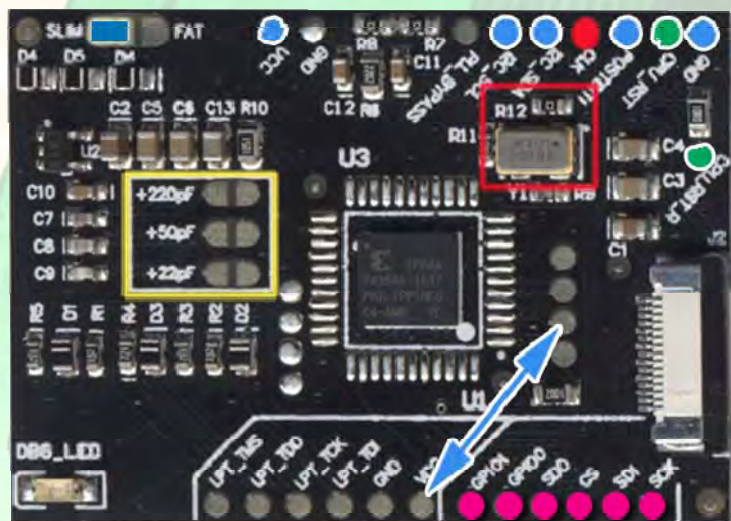
Décharge :

Dans la plupart des pays il est légal d'installer et d'utiliser un Modchip (une puce) dans votre console de jeu personnelle. Cependant ... la copie de jeux est illégale dans de nombreux pays (si ce n'est tous les pays). Dans certains pays les lois ne vous autorisent pas d'utiliser des sauvegardes de jeux, même si vous possédez l'original, vous devez vérifier les lois en vigueur dans votre propre pays et les respecter. Si vous avez le droit de faire des sauvegardes, cela signifie que vous avez acheté la licence originale pour utiliser ce jeu. SQUIRT ou n'importe quelle autre des sociétés associées ne pardonnent pas la reproduction illégale et/ou la distribution de logiciel pour les consoles de jeu ou un autre format. Vous devez agir conformément aux lois de votre pays! Respectez les lois, Respectez l'industrie du jeu et utilisez nos produits en conséquence dans son état originel. Le but destiné de notre Modchip est de vous permettre d'utiliser votre console de jeu pour jouer aux jeux imports et aux sauvegardes des jeux que vous possédez légalement ou développés par vous, pour la conservation, la maintenance et les buts de service autorisés par la loi.



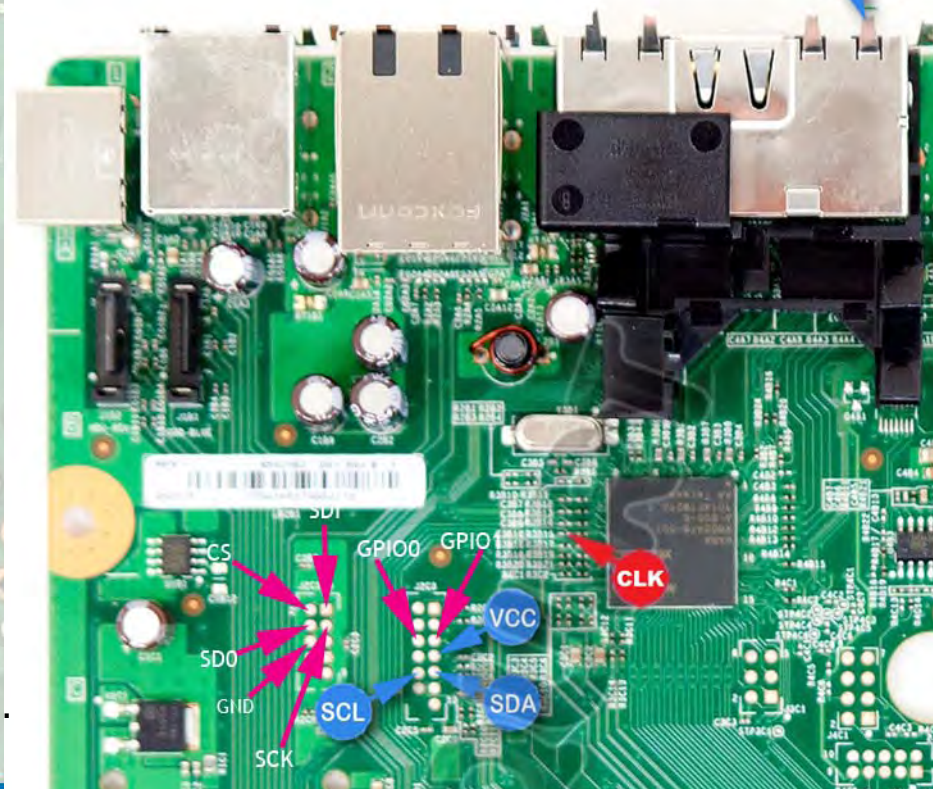


SQUIRT BGA RGH montage sur X360 SLIM



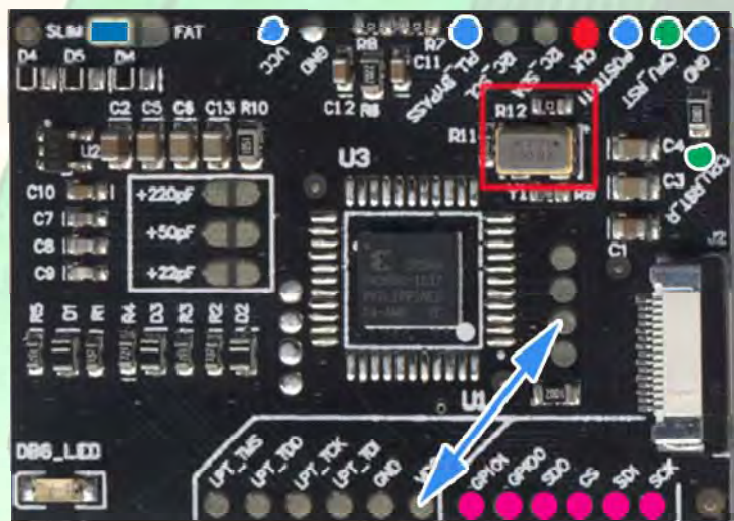
"SPI" CONNEXION FACULTATIVE :
Nous vous suggérons ces points
ainsi vous pourrez accéder à la
NAND en utilisant le câble FCC à
15 broches.
En utilisant le câble FCC, vous
n'aurez plus besoin de ré-ouvrir la
console quand il sera nécessaire
de faire une mise à jour.
(Même si vous avez besoin de
dumper/programmer la NAND ou
le CLPD)

- 1- Pontez les points SLIM en haut à gauche de la puce, pontez le point 4 et VCC si vous installez le SQUIRT BGA 1.2 sans le DUAL NAND.
- 2- Soudez les points CPU_RST, le POSTE, GND, VCC, SCL, SDA et facultativement CLK
- 3- Les meilleurs résultats de RGH sur SLIM ont été atteints en utilisant CPU_RST_R (CPU_RST avec une résistance en série de 10 Ohm) et 220pF
Vous pouvez tester et voir ce qui fonctionne le mieux pour votre console
(Le carré jaune sur la photo de la puce) :
+220pF = 220pF
+220pF / +50pF = 270pF
+220pF / +50pF / +22pF = 292pF
(Ce sont les résultats obtenus en pontant les 2 points en face de chaque valeur NDT)
- 5- SQUIRT BGA intègre un oscillateur 48Mhz, ceci lui permet d'être plus stable dans la réalisation du glitch et d'être aussi compatible avec de nouvelles consoles. Il est possible que dans quelques modèles de consoles il puisse être préférable de mettre hors-service l'OSC et d'utiliser le point CLK de la console.
Pour utiliser le CLK de la X360 vous devez enlever la résistance R12 sur la puce.
Ceci mettra hors-service l'oscillateur intégré.





SQUIRT BGA RGH montage sur X360 FAT



- 1- Soudez les points PLL_BYPASS, I2C_SCL, I2C_SDA, POSTBIT, CPU_RST, GND et facultativement le CLK (voir ci-dessous)
- 2- Pontez le point 4 et VCC comme sur l'image si vous n'avez pas besoin des fonctions de DUAL NAND (fonction uniquement sur les fat avec NAND de 16Mb NDT).
- 3- Important! Depuis le 6 avril 2012 tous les bits treams FAT fonctionnent correctement avec les points SLIM ponté même si vous allez l'installer sur une FAT. Ceci améliore le temps de boot dans des consoles FAT.
- 4- utilisez le point CPU_RST pour souder le point RST sur la carte mère. Sur la console FAT la résistance de 10 Ohm supplémentaire n'est pas nécessaire sur la point CPU_RST_R.
- 5- SQUIRT BGA intègre un oscillateur 48Mhz, ceci lui permet d'être plus stable dans la réalisation du glitch et d'être aussi compatible avec de nouvelles consoles. Il est possible que dans quelques modèles de consoles il puisse être préférable de mettre hors-service l'OSC et d'utiliser le point CLK de la console.

Pour utiliser le CLK de la X360 vous devez enlever la résistance R12 sur la puce.

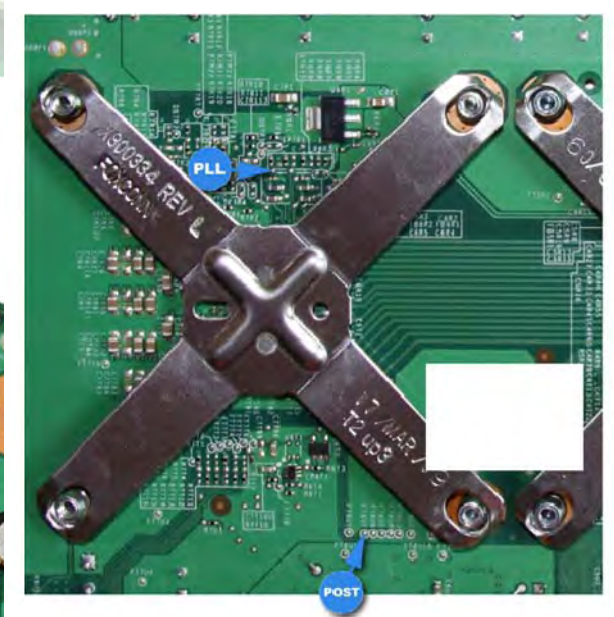
Ceci mettra hors-service l'oscillateur intégré.



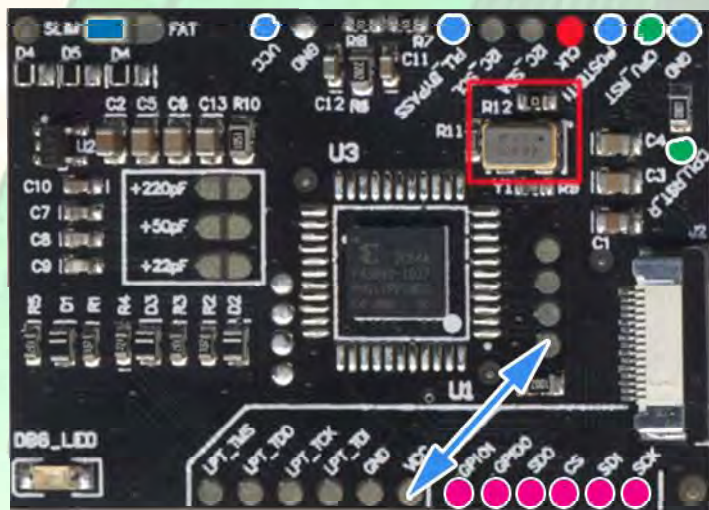
"SPI" CONNECTION FACULTATIVE :

Nous vous suggérons ces points ainsi vous pourrez accéder à la NAND en utilisant le câble FCC à 15 broches.

En utilisant le câble FCC, vous n'aurez plus besoin de ré-ouvrir la console quand il sera nécessaire de faire une mise à jour. (Même si vous avez besoin de dumper/programmer la NAND ou le CLPD)



SQUIRT BGA RGH sur X360 FAT XENON



"SPI" CONNEXION FACULTATIVE :

Nous vous suggérons ces points ainsi vous pourrez accéder à la NAND en utilisant le câble FCC à 15 broches. En utilisant le câble FCC, vous n'aurez plus besoin de ré-ouvrir la console quand il sera nécessaire de faire une mise à jour. (Même si vous avez besoin de dumper/programmer la NAND ou le CLPD)

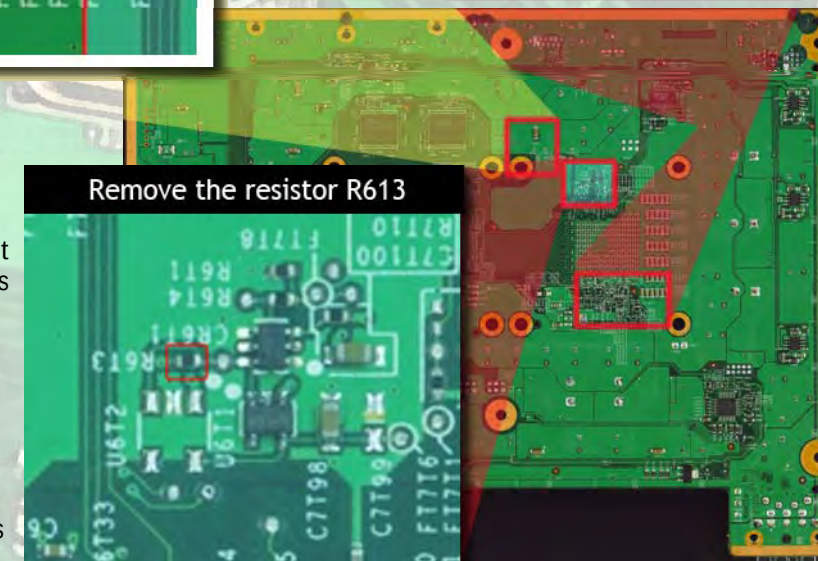
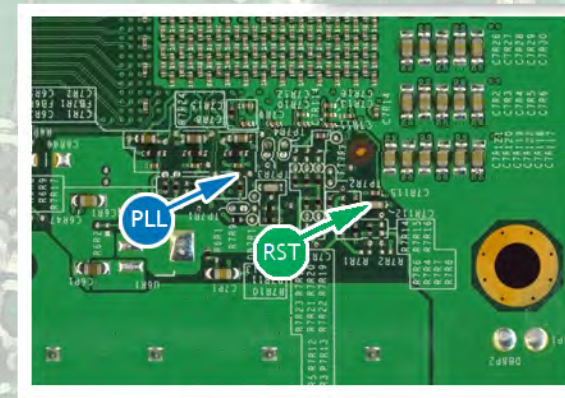
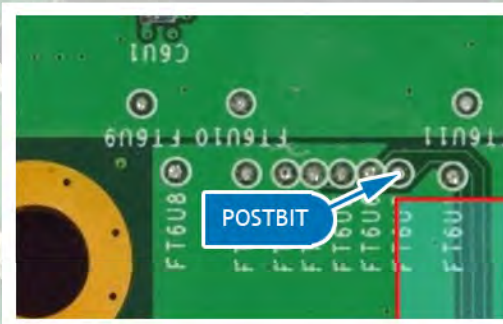
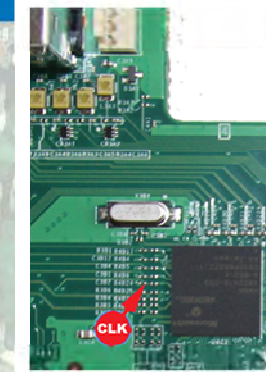
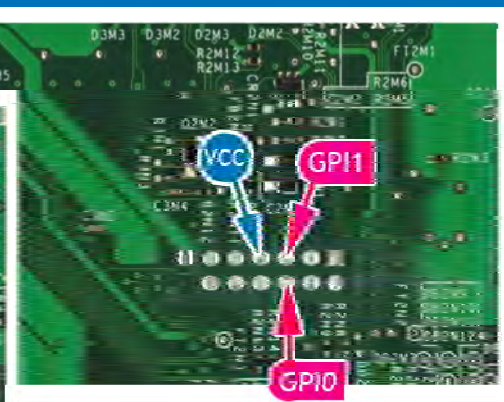
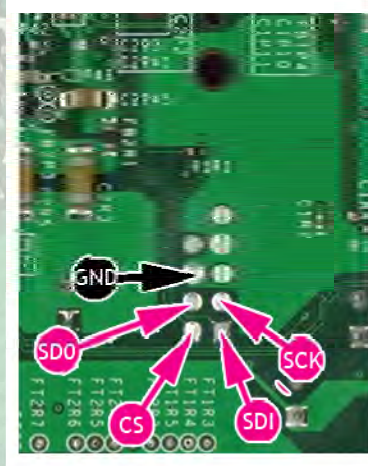
- 1-Soudez les points PLL_BYPASS, I2C_SCL, I2C_SDA, POSTBIT, CPU_RST, GND et facultativement le CLK (voir ci-dessous)
- 2-Pontez le point 4 et VCC comme sur l'image si vous n'avez pas besoin des fonctions de DUAL NAND.
- 3-Important! Depuis le 6 avril 2012 tous les bitstreams FAT fonctionnent correctement avec les points SLIM ponté même si vous allez l'installer sur une FAT. Ceci améliore le temps de boot dans des consoles FAT.
- 4-utilisez le point CPU_RST pour souder le point RST sur la carte mère. Sur la console FAT la résistance de 10 Ohm supplémentaire n'est pas nécessaire sur le point CPU_RST_R.
- 5-SQUIRT BGA intègre un oscillateur 48Mhz, ceci lui permet d'être plus stable dans la réalisation du glitch et d'être aussi compatible avec de nouvelles consoles. Il est possible que dans quelques modèles de consoles il puisse être préférable de mettre hors-service l'OSC et d'utiliser le point CLK de la console.
Pour utiliser le CLK de la X360 vous devez enlever la résistance R12 sur la puce.
Ceci mettra hors-service l'oscillateur intégré.

NOTE : Sur les XENON, les temps de boot du RGH sont très longs, parfois plus d'une heure.

Si vous voulez essayer, nous vous suggérons d'enlever le condensateur C7R112 proche du point RST sur la carte mère de la X360.

S'il vous plaît veuillez noter que ce hack n'est pas disponible sur les consoles avec les dashboards des mises à jour 14717 ou 14719 (à vérifier dans les paramètres systèmes de la console).

Il n'y a que les bitstreams du RGH 2.0 qui puisse glitcher ces dashboards





Installer la partie software du reset glitch hack (RGH)

- 1- Téléchargez depuis la section « support » de SQUIRT360.COM ou 360SQUIRT.COM l'archive rar : SQUIRT SOFTWARE COLLECTION (360squirt.com/support.php NDT). À l'intérieur vous trouverez les logiciels suivants :
 urJTAG = c'est le logiciel nécessaire pour le programmer le bitstreams RGH à l'intérieur du XILINX IC sur le SQUIRT BGA 1.2 via USB. (urJTAG supporte aussi la programmation via LPT avec le port LPT intégré au SQUIRT BGA)
 squirter.exe = c'est le logiciel nécessaire pour lire et écrire la mémoire SPI nand de la X360. Super rapide! 1'20" pour un dump de 16 Mb :) (Nous vous rappelons que vous pouvez utiliser aussi un autre programmeur NAND SPI du marché)



installation typique du SQUIRT BGA avec la configuration DUAL NAND



connectez le câble plat 15 broches FCC du SQUIRT BGA au PROGRAMMEUR comme sur l'image. Vous aurez un accès facile à la programmation du JTAG XILINX et SPI ! Plug and Play sans soudure !

- 2- Installez le logiciel urJTAG, téléchargez le bon bitstream ".svf" pour la version de la console que vous

allez modifier. Mettez le fichier .svf dans le dossier "data" du chemin d'installation d'urJtag. Lancez l'urJTAG par l'invite de commande CMD (dans WINDOWS), nous suggérons de le faire avec les droits d'administrateurs et entrez ces simples commandes :
 "cable ft2232" << cette commande contrôle que le SQUIRT PROGRAMMER (NDT le programmeur SQUIRT) est connecté à l'USB
 "detect" << cette commande contrôle que le SQUIRT BGA est correctement connecté.
 "svf xxxxx.svf" << Cette commande autorise à flasher le XILINX avec le bitstream

- Si la commande "cable ft2232" échoue et qu'une erreur apparaît sur l'écran il est possible que les driver du SQUIRT PROGRAMMER ne sont pas reconnus par votre installation WINDOWS. Dans ce cas allez sur <http://www.ftdichip.com/Drivers/VCP.htm> pour téléchargez les drivers
- Si vous obtenez des erreurs après la commande DETECT, il est possible que votre SQUIRT BGA soit endommagé ou non connecté correctement.
- Si vous obtenez des erreurs avec la commande SVF assurez-vous que vous exécutez urJTAG avec les droits administrateurs.

```

C:\Windows\system32\cmd.exe - jtag.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Raz>cd C:\Program Files (x86)\UrJTAG
C:\Program Files (x86)\UrJTAG>jtag.exe

UrJTAG 0.10 W1502
Copyright (C) 2002, 2003 ETC s.r.o.
Copyright (C) 2007, 2008, 2009 Kolja Waschk and the respective authors

UrJTAG is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
There is absolutely no warranty for UrJTAG.

WARNING: UrJTAG may damage your hardware!
Type "quit" to exit, "help" for help.

jtag> cable ft2232
Connected to libttd2xx driver.
jtag> detect
IR length: 8
Chain length: 1
Device Id: 000001101100101101000010010011 <0x000000006E5D093>
Manufacturer: Xilinx
Part(0): XC2C64-CP56
Stepping: 0
Filename: c:\program files (x86)\urjtag\data\xilinx\xc2c64a-cp56\xc2c64a-c
p56
jtag> svf trinity.svf
jtag>
    
```

NDT : pour ouvrir l'invite de commande CMD, maintenez le bouton Windows enfoncé (à gauche de votre barre espace sur le clavier : il est généralement entre Alt et Fn). Si votre clavier n'est pas équipé, dans la barre des tâches, cliquer sur démarrer (le bouton rond Windows) et entrez cmd dans la recherche des programmes et fichiers.



Installer la partie software du reset glitch hack (RGH)

3-Nous allons maintenant procéder à la lecture du NAND SPI avec le SQUIRT PROGRAMMER nous vous rappelons que vous pouvez le connecter par le câble plat FCC SQUIRT ou aussi directement au BUS SPI sur la console (les schémas sont disponibles sur le site de SQUIRT à la page téléchargements (360squirt.com section SQUIRT DIAGRAMS COLLECTION NDT)

Nous vous suggérons de le connecter via le câble plat FCC SQUIRT, ceci permet d'accéder à la NAND et au JTAG sans ouvrir la console ou avoir besoin de souder à nouveau des fils! Nous vous rappelons que vous devez laissez la console en standby pendant le read/write des NANDS et le câble d'alimentation branché (En gros vous allumez la console et vous la laissez tranquille jusqu'à la fin, pensez à enlever la veille automatique, NDT)

Après que le programmeur soit correctement connecté nous continuons par lire la NAND avec cette simple commande (selon la taille de la NAND de votre console NDT):

" SQUIRTER.exe ftdi :-r16 xxxxxx.bin "(xxxxxx = nom de fichier)

" SQUIRTER.exe ftdi :-r64 xxxxxx.bin "(la commande r64 est pour des consoles avec NAND de Mo 256/512) (Ne mettez pas les apostrophes NDT)

4-Installez le programme Multi Builder 0.83 ci-dessus.

5-Copiez le fichier dumpé de votre NAND dans Data\my360 (le dossier à l'intérieur du dossier d'installation de Multi Builder 0.83 o).

Après la copie, renommez le nanddump (faites en une sauvegarde ailleurs, on ne sait jamais NDT)

6-Lancez Multi Builder et choisissez votre modèle de console. Le logiciel nous averti que la CPU KEY (la clé CPU NDT) est manquante (avertissement normal puisque à cette étape nous n'avons pas la clé CPU). Le logiciel, après cet avertissement, commence à générer automatiquement le fichier pour lancer le RGH « image_0000000000.ecc »

```
C:\WINDOWS\system32\cmd.exe -SQUIRTER0.2.exe ftdi: -r16 nanddump.bin
D:\Xavbox\SQUIRTER SPI NAND SOFTWARE>SQUIRTER0.2.exe ftdi: -r16 nanddump.bin
SQUIRTER v0.2 beta
Init USB->FTDI->SPI
Flash Config: 0X023010
Start Read NAND:
4.9%
```

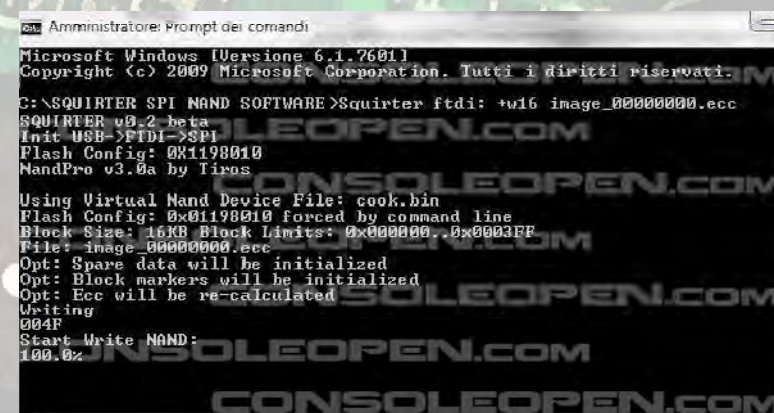


Installer la partie software du reset glitch hack (RGH)

- 6- Copiez le fichier généré "image_0000000.ecc" à l'intérieur du dossier du logiciel SQUIRTER.
Avec l'invite de commande entrez s'il vous plaît ces commandes :
Squirter ftdi : +w16 image_00000000.ecc---> si vous avez une Nand de 16Mb
Squirter ftdi : +w64 image_00000000.ecc---> si vous avez une Nand de 256 ou 512Mb

- 7-Maintenant nous pouvons démarrer notre console avec XELL RELOADED et lancer notre RGH.

- 8-Avec XELL vous pouvez récupérer le CPU KEY (la clé CPU NDT) de votre console. Ceci vous permet d'installer le dashboard de votre choix. De nombreux tutoriaux sont disponibles en ligne



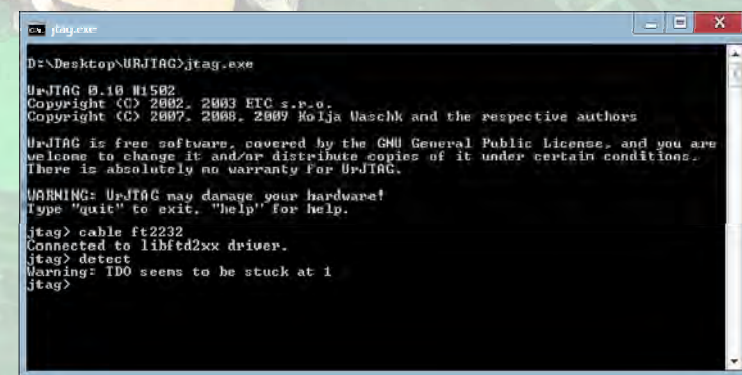
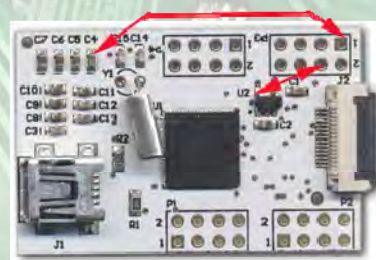
Diagnostic des pannes et suggestions

- Si la commande DETECT montre l'erreur "TDO seems to be stuck at 1" comme sur l'image il y a 99 % de possibilités que la puce SQUIRT BGA soit endommagée, l'urJtag ne peut pas écrire le XILINX IC. Demandez s'il vous plaît un remplacement de votre SQUIRT BGA
- Si vous avez un programmeur BLANC (première production beta) et vous avez des ennuis dans la programmation du SPI ou du JTAG, vérifiez s'il vous plaît s'il y a des courts-circuits sur ces points (vérifiez la continuité avec votre testeur NDT):
SCK < > SDI
3.3V < > CS
1.8V < > SCK

Si vous trouvez un court-circuit demandez s'il vous plaît un remplacement, votre programmeur est défectueux

- Si pendant le démarrage de XELL ou de votre dashboard personnalisé vous obtenez l'erreur E71, des leds rouges etc...

Il est possible que votre NAND secondaire ait des BAD BLOCKS, s'il vous plaît reportez vous à la page 11 pour régler ce problème.





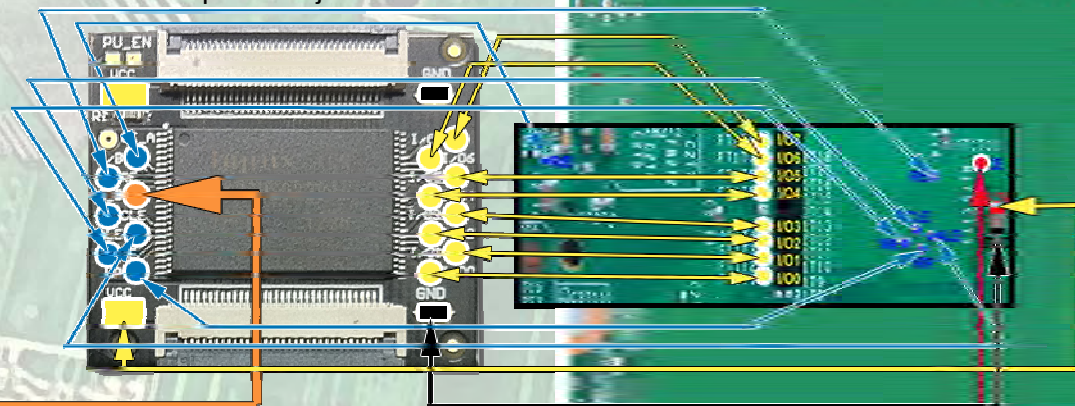
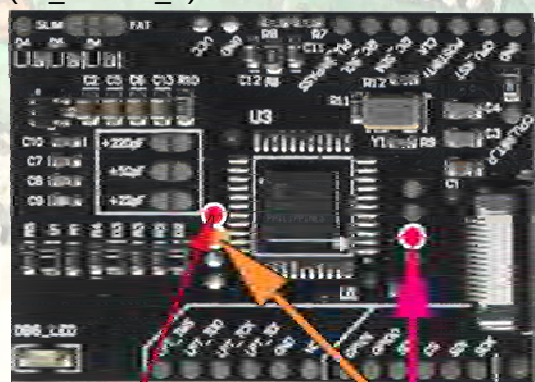
Installation en DUAL NAND sur SLIM

Préambule :

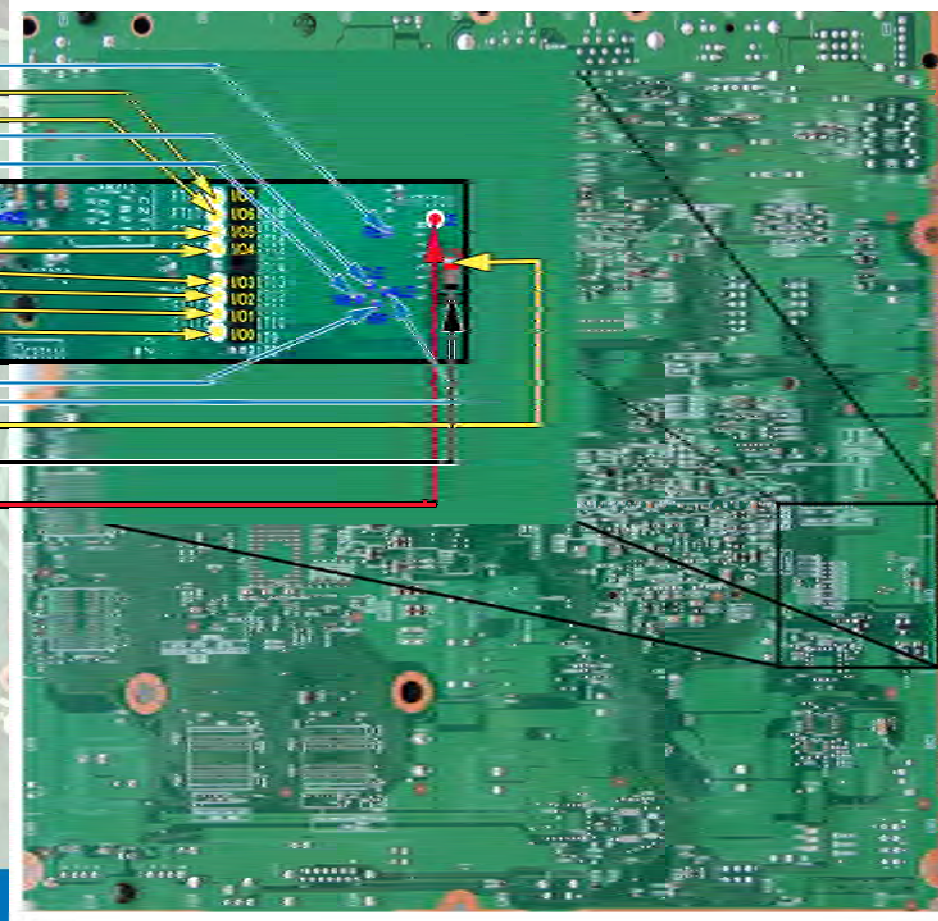
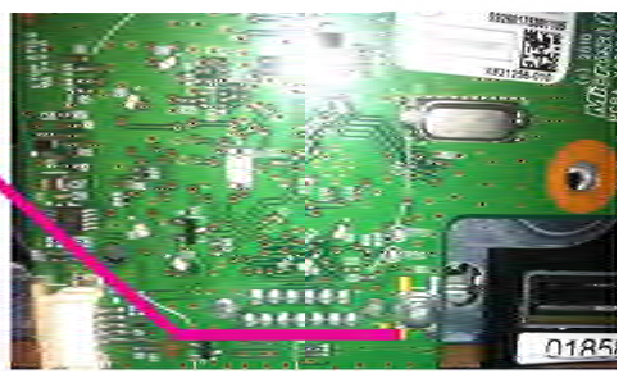
L'installation DUAL NAND permet de démarrer votre console avec le RGH ou le firmware ORIGINAL. Avec le SQUIRT, le DUAL NAND est facile à installer, moins cher et aussi plus facile à exécuter, en fait après l'installation, il suffit d'appuyer sur le bouton de SYNC de la console X360 pour commuter entre les NANDS et choisir le mode de boot de votre console X360 (le bouton en façade pour synchroniser les manettes et casques sans fils juste à côté du bouton power NDT)

Il est important de noter que XELL et les DASHBOARD FREEBOOT doivent être installés à l'intérieur de la NAND SECONDAIRE et de garder intacte la NAND d'original de la console.

- 1-Installez le SQUIRT BGA avec le RGH et la connexion SPI comme expliqué dans la page 2 de ce manuel et permettez la fonction de DUAL NAND en ne pontant pas les points VCC et PAD4.
- 2-Continuez maintenant à installer les fils de la NAND secondaire, la chip select (ce_a et ce_b) et le fil de bouton sur le bouton de SYNC pour l'injection.



- 3-Connectez le fil rose au bouton de SYNC sur la face avant de la X360.



Installation en DUAL NAND sur FAT (NAND de 16 Mb)

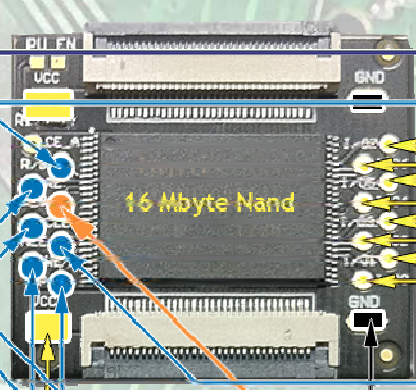
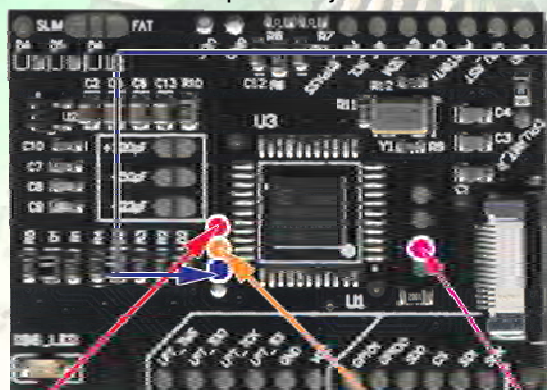
Préambule :

L'installation DUAL NAND permet de démarrer votre console avec le RGH ou le firmware ORIGINAL.

Avec le SQUIRT, le DUAL NAND est facile à installer, moins cher et aussi plus facile à exécuter, en fait après l'installation, il suffit d'appuyer sur le bouton de SYNC de la console X360 pour permuter entre les NANDS et choisir le mode de boot de votre console X360 (bouton de synchronisation des manettes en façade, à côté des ports carte mémoire NDT)

Il est important de noter que XELL et les DASHBOARD FREEBOOT doivent être installés à l'intérieur de la NAND SECONDAIRE et de garder intacte la NAND d'original de la console. SQUIRT ne permet le DUAL NAND que sur les consoles X360 FAT avec NAND de 16mb

- 1-Installez le SQUIRT BGA avec le RGH et la connexion SPI comme expliqué dans la page 3 de ce manuel et permettez la fonction de DUAL NAND en ne pontant pas les points VCC et PAD4.
- 2-Continuez maintenant à installer les fils de la NAND secondaire, la chip select (ce_a et ce_b) et le fil de bouton sur le bouton de SYNC pour l'injection.



- 3-Connectez le fil rose au bouton de SYNC sur la face avant de la X360.

- 4-La fonction DUAL NAND sur FAT exige de couper la piste du southbridge de la console comme sur la photo 1 et de connecter le fil BLEU piste du southbridge.

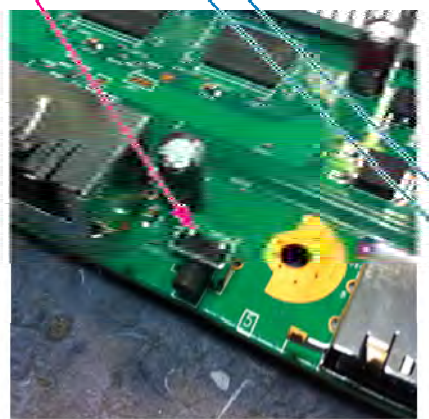
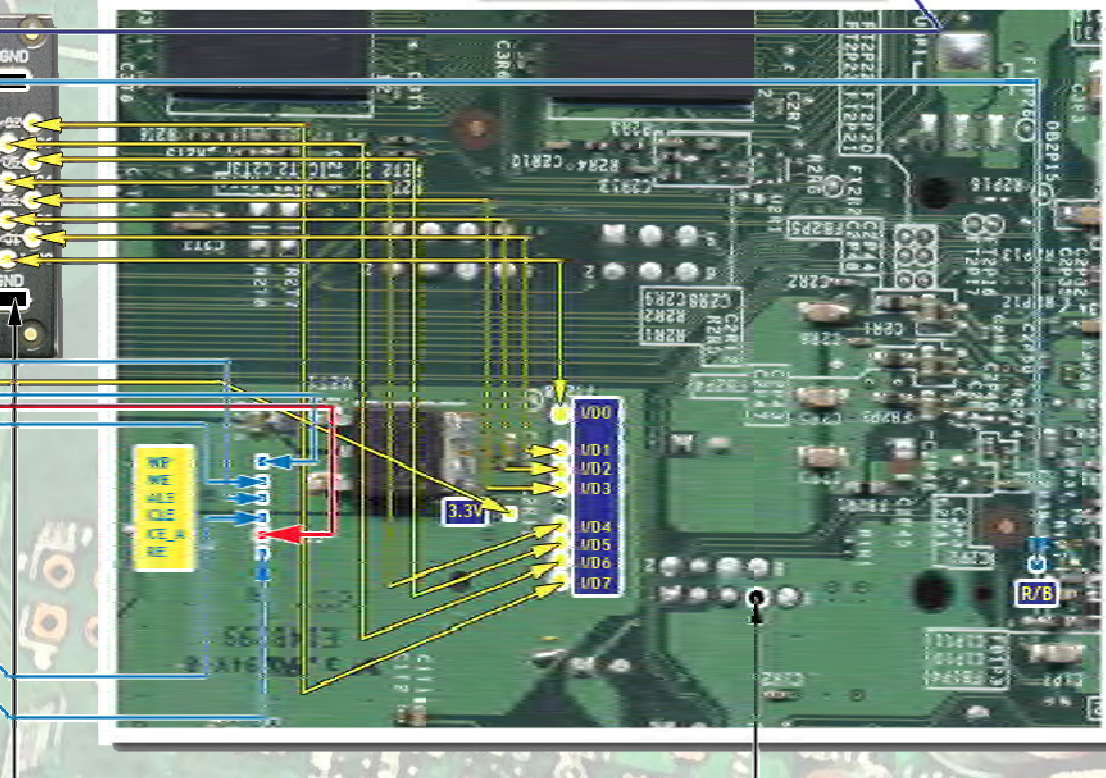
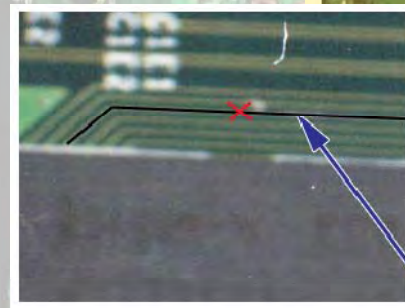


photo 1 :
coupez la piste du southbridge



■ Diagnostic des pannes et suggestions avec la fonction DUAL NAND

A la première lecture de la NAND (votre NAND secondaire est vide) :

- Pour permettre le premier reading/writing (la lecture et l'écriture) des NANDS primaires et secondaires (RGH OFF) :
 - > Débranchez et rebranchez le câble d'alimentation de votre console
 - > pressez le bouton SYNC sur votre console (il n'est pas nécessaire d'allumer la console, juste de la laisser en standby)
- Pour permettre le reading/writing SECONDAIRE (RGH ON) :
 - > Débranchez et rebranchez le câble d'alimentation de votre console
 - > Appuyez (et maintenez) le bouton SYNC et rebranchez le câble d'alimentation.
 - > Lâchez le bouton SYNC et allumer la console avec le bouton power (le gros bouton rond) ... l'amusement commencera très vite... Éteignez de nouveau la console
 - > Commencez le writing/reading de la NAND secondaire (la lecture/écriture).

READING/WRITTING (lecture/écriture) des NANDS alors que FREEBOOT est déjà installé en NAND secondaire

- Pour permettre la lecture/écriture de la NAND SECONDAIRE (RGH OFF) :
 - > Débranchez et rebranchez le câble d'alimentation de votre console
 - > commencez à lire/écrire la NAND originale
- Pour permettre la lecture/écriture de la NAND PRINCIPALE (RGH OFF) :
 - > Sur la console avec le câble d'alimentation branché mais console éteinte, pressez le bouton SYNC
 - > Commencez à lire/écrire la NAND secondaire

PROCÉDURES STANDARD POUR L'UTILISATEUR FINAL (ce que nous expliquerons aux clients)

- > Allumez la console avec le bouton d'EJECT : mode RGH ON (démarrage sur Xell)
- > Allumez la console avec le bouton power : mode RGH ON + mode NAND SECONDAIRE choisi
- > Allumez la console avec le bouton de la manette : mode RGH ON + mode NAND SECONDAIRE choisi
- > Allumez la console et dans le même temps maintenez le bouton SYNC appuyé : mode RGH OFF + mode NAND ORIGINALE choisi.
- > Éteignez la console en mode RGH OFF : Quand la console est de nouveau allumée, par défaut le mode "RGH ON + le mode NAND SECONDAIRE" est choisi
- > Au redémarrage de la console : le mode RGH ON + mode NAND SECONDAIRE est choisi



Diagnostic des pannes et suggestions, Dual Nand

NOTIFICATION PAR LED DE LA NAND SELECTIONNEE :

Avec le nouveau bitstreams disponible depuis le 6 avril 2012 nous avons ajouté la notification par led de la nand sélectionnée qui permet de savoir quelle NAND est choisie. Il suffit de connecter un fil du SQUIRT BGA à une des leds du bouton power (le ROL).

Les deux fonctions:

LED ALLUMÉE = NAND PRINCIPAL choisie

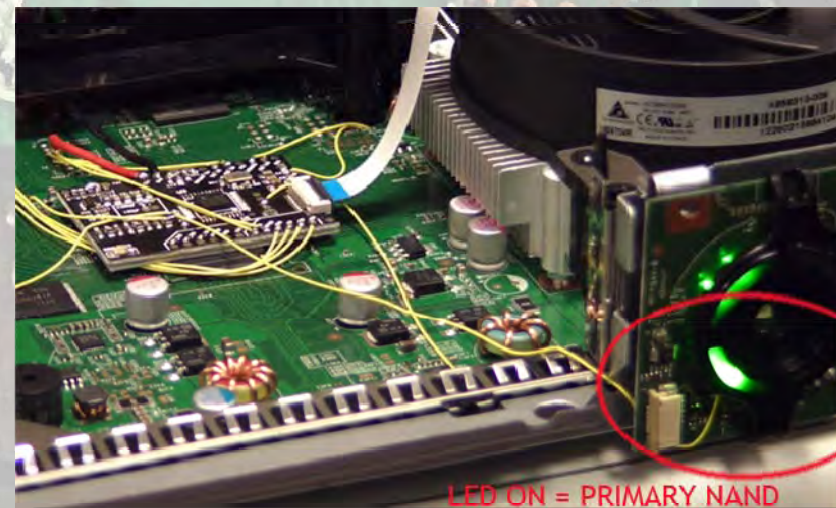
LED ÉTEINTE = NAND SECONDAIRE choisie

Cette fonction est très utile afin de savoir quelle Nand nous allons lire ou écrire.

Sur console FAT la LED est gérée par le bitstream avec la led 4 d'indication de la manette (attention à la position de la console) (voir l'image).

Sur consoles SLIM, la LED est simplement gérée en connectant un fil sur le point CE_B de la puce, ceci parce qu'il n'y avait plus de place dans bitstream de la SLIM.

La solution sur SLIM n'est pas parfaitement stable, nous suggérons de tester un peu la console avant de procéder à l'installation.

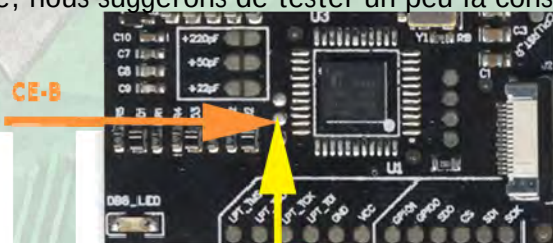


LED ON = PRIMARY NAND



CONSOLE
FAT

PHAT EXTERNAL LED
NOTIFICATION.



CONSOLE
SLIM



quand le bouton SYNC est pressé console en attente. La puce va passer à la Nand primaire et la led va s'allumer. Pour revenir à la Nand secondaire, allumez et éteignez la console.

■ Diagnostic des pannes et suggestions avec la fonction DUAL NAND

ERREUR 71 et PROBLÈMES AVEC le BOOT du RGH :

Si vous êtes dans la situation où la console ne peut pas démarrer même si RGH est ON et la NAND SECONDAIRE est correctement installée, il est possible que vous deviez remapper les bad blocks de la nand secondaire.

Pour résoudre ce problème nous suggérons cette procédure :

- 1-Programmez à l'intérieur de la nand secondaire le contenu du dump de la nand originale.
- 2-relisez la nand secondaire et procédez au patchage avec le XELL ou le Freeboot comme décrit sur les pages 5 et 6.
- 3-Écrivez alors de nouveau nand secondaire avec le microprogramme modifié (xell ou freeboot)

Avec ces procédures les outils de patch standard utilisés pour créer les firmwares xell ou freeboot sont capables de remapper les bads blocks et les problèmes devraient être résolus.

System Error. Contact Xbox Customer Support.
 Systemfehler. Wenden Sie sich an den Xbox Kundensupport.
 Service requis. Contactez le Support Technique Xbox.
 Errore di sistema. Rivolgersi all'Assistenza clienti Xbox.
 Error del sistema. Llama al Servicio de soporte al cliente de Xbox.
 Erro de sistema. Contate o Suporte ao Cliente Xbox.
 システムエラー。Xbox カスタマー サポートにお問い合わせください。
 시스템 오류. Xbox 고객 지원 센터에 문의하십시오.
 系統錯誤，請聯絡 Xbox 客服支援。
 Błąd systemu. Skontaktuj się z biurem obsługi klienta konsoli Xbox.
 Системная ошибка. Обратитесь в службу поддержки пользователей Xbox.

E 71

www.xbox.com/support