IEEE 1149.1-2013 puts an end to IC counterfeiting

CJ Clark, Intellitech CEO

Chairman, IEEE 1149.1-2013

IEEE 1149.1-2013 Executive Summary

- Standardizes a plug-n-play test interface to on-chip IP

Mission IP

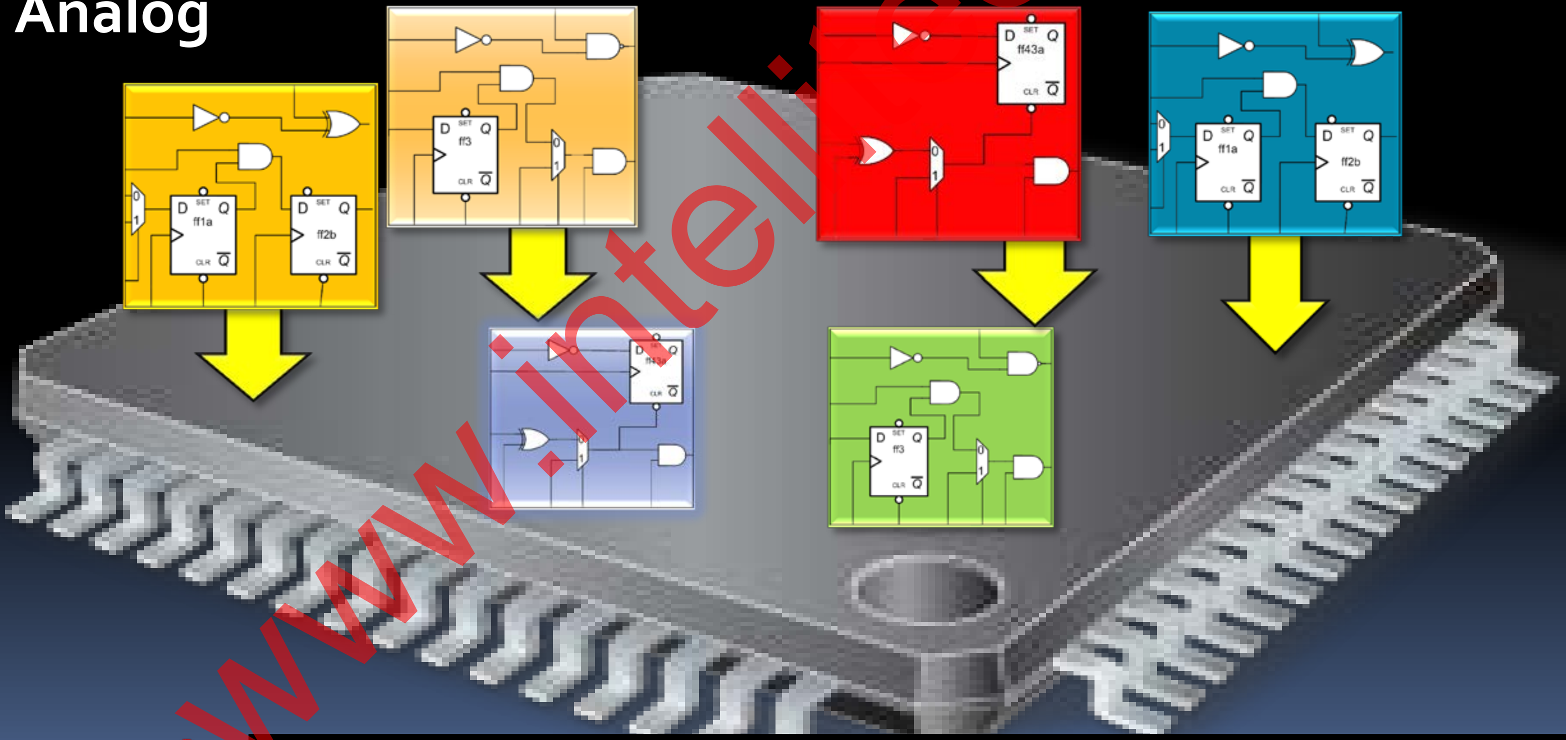
CPU
DSP
Memory
Analog

Graphics
Connectivity
Etc.

Infrastructure IP

Embedded Test
Memory BISR
SerDes BIST

Voltage/Temp
Security
Process monitors



Intellitech®

See Yervant Zorian: "*Infrastructure IP for SoCs*" and "*What is Infrastructure IP?*"
BIST = Built In Self-Test BISR = Built-in Self-Repair

1149.1-2013 adds depth to the other half of the standard
- Standard Test Access Port and Boundary Scan architecture

"Boundary Scan" has always been a misnomer, it's only a part of the standard.

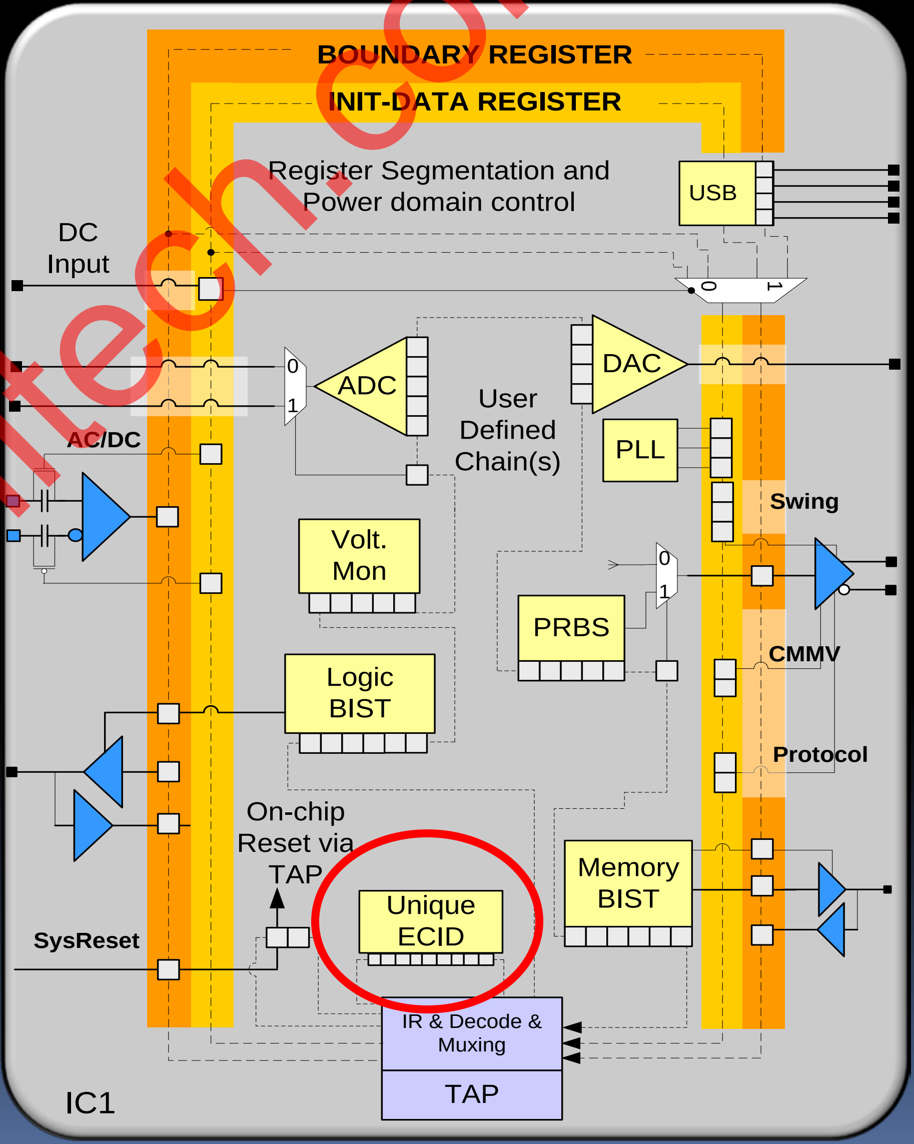
Standardization now available for all internal JTAG registers via the Test Access Port

Hierarchical descriptions of on-chip IP

Hierarchical operational language for On-chip IP

Synergy with IEEE 1500 and IEEE 1801
- re-use popular IEEE 1500 structures
- TDRs can cross power domains

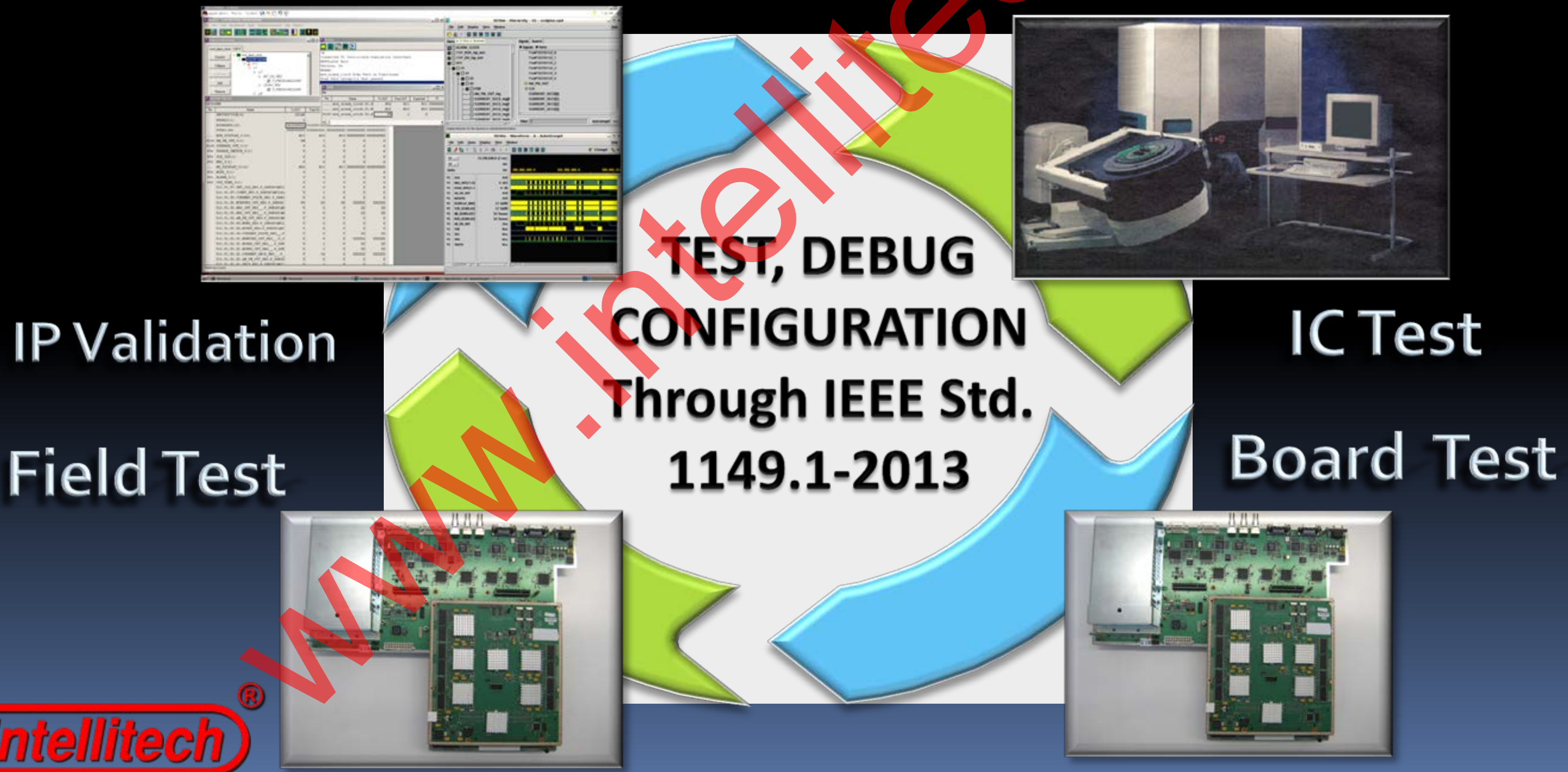
444 Pgs vs. 208 pgs in 1149.1-2001



Intellitech

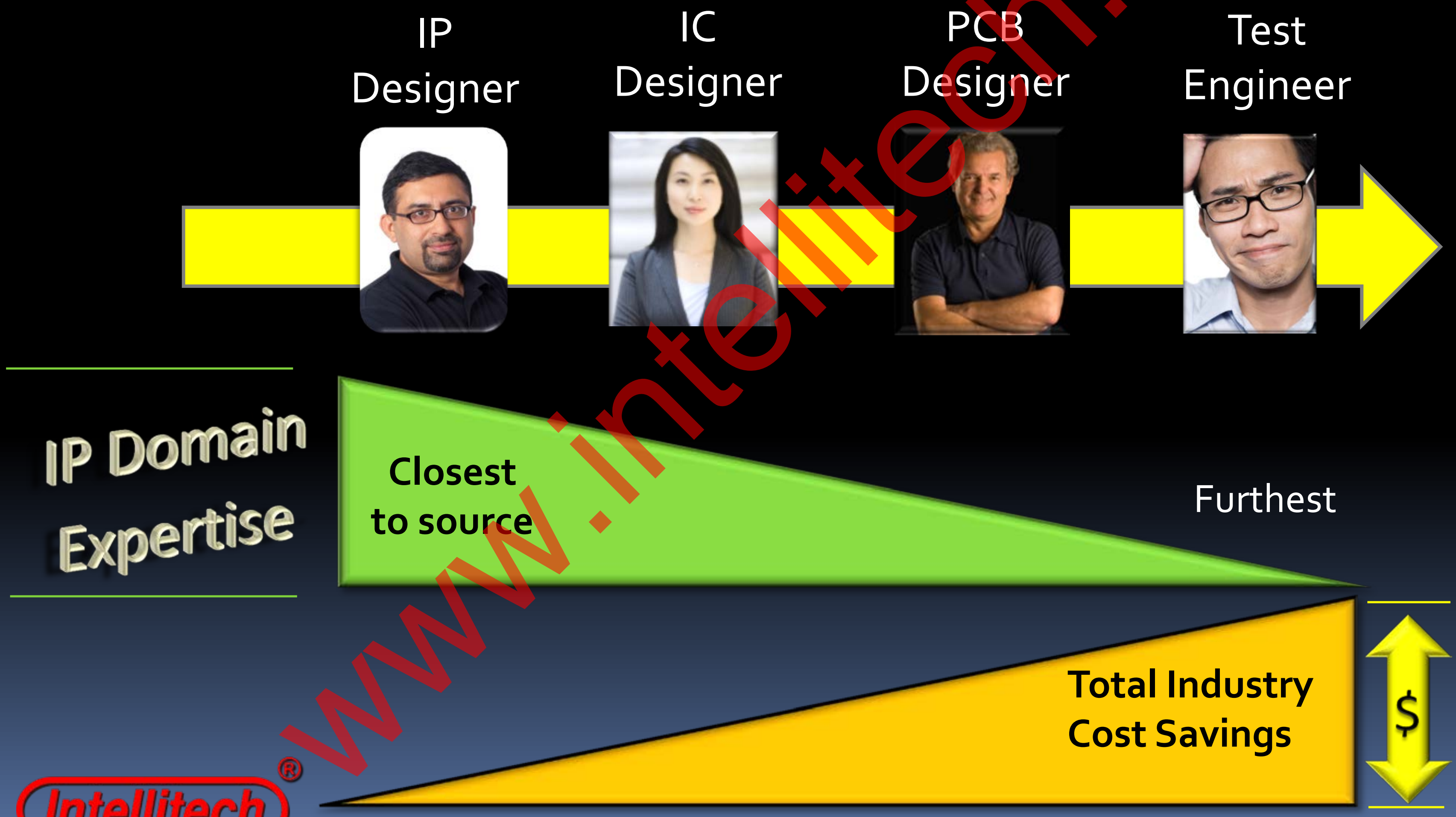
IEEE Std. 1149.1-2013 lowers industry costs by enabling test re-use through all phases of the IC life-cycle

- Specifies best practices for Infrastructure IP test interfaces
- Specifies rules for describing IP operation
- Enables one description to be used in all test stages
- Enables defect correlation between system failures and IC ATE
  - ECID used to track IC from wafer to grave



1149.1-2013 enables knowledge transfer

Through the standard hierarchical PDL/Tcl languages of 1149.1-2013, IP and IC designers can transfer critical expertise to customers through pre-written routines



IP Designer

IC Designer

PCB Designer

Test Engineer

IP Domain Expertise

Closest to source

Furthest

Total Industry Cost Savings

$

Intellitech®

IEEE 1149.1-2013 ECID - Electronic Chip ID

New Instruction Optional ECIDCODE

- Targets a test data register known as "ECID"

Unique per die value to be either programmed at Wafer/Package Test or possibly from PUF (Physically Unclonable Function)

Requires TAP pins, Compliance Enable pins and optionally specified System Clocks to retrieve data from ECID register.

There is no specified length. ECID TDR can be of any desired length

New **Attributes** enable the description of the mnemonics and fields associated with each bit of the TDR

1149.1 Standard provides for new PDL (Procedural Description Language) proced
called "ecid"

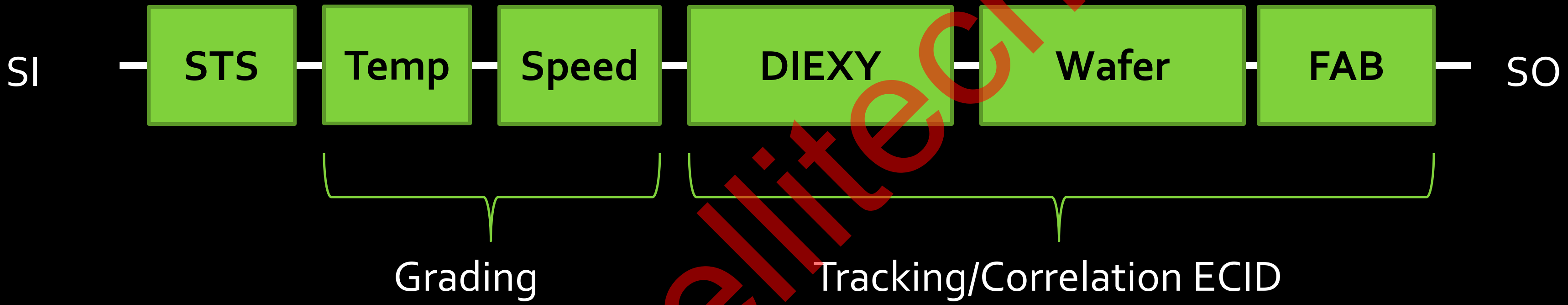
- tools can automatically execute described procedure for any IC

1149.1 Standard enables but does not define how to program efuse/NVM values

ECID to prevent Counterfeiting by re-marking

Problem: Supply chain re-marking of parts to alter speed grade or Temp (C/I)
- 3rd parties have little resources to test/validate

Solution: IEEE 1149.1-2013 ECID programmed with rated temp/speed in OTP efuse/NVM



```
Tracking/Correlation ECID can be defined or made private
       - shown for convenience
       - Can also be encrypted/scrambled

Grading information should be made public

Values programmed during test/binning/burn-in by trusted
OSAT (Out Sourced Assembly and Test) house
```

1149.1-2013 ECID Package definitions

```
attribute REGISTER_MNEMONICS of ECID : entity is
 "Temp (Comm  (0B00) < Commercial >, "&
 "      Ind   (0B10) < Industrial >, " &
 "      AEC   (0B01) < AEC-Q100 >), "&
 "Speed (S1    (1),  " &
 "       S2    (0) )," &
 "Stat  ( Ready     (1), " &
 "        Not_Ready (0)) ";

attribute REGISTER_FIELDS of ECID : package is
"ECID [35]( "&
 "( Status [1] IS (34 )        CAPTURES(Stat  (Not_Ready)) ), "&
 "( Temp [2] IS (33 DOWNTO 32) CAPTURES(Temp  (-)) ), "&
 "( Speed[1] IS (31)           CAPTURES(Speed (-)) ), "&
 "( Die   [9] IS (30 DOWNTO 22 ) ), "&
 "( Wafer[20] IS (21 DOWNTO 2) ), "&
 "( Fab   [2]  IS (1 DOWNTO 0) ) )";
```

1149.1-2013 ECID Procedural Definition Language

PDL Description of how to read ECID temp/speed

```
# ECID.pdl
iPDLLevel 1 -version STD_1149_1_2013
iProcGroup ECID
iProc ecid {} {

iRunLoop 10000 -sck Sysclock_200MHz
iLoop
iRead Status Ready
iApply -nofail
iUntil -match -maxloop 10 “ECID timed out”

Set t [iGet -so -mnem Temp]
Set s [iGet -so -mnem Speed]
puts "This IC grading is Temp:$t and Speed:$s\n"
}
```

1149.1-2013 ECID Procedural Definition Language

Setup that public/3rd parties can use to validate IC grades match the package markings.

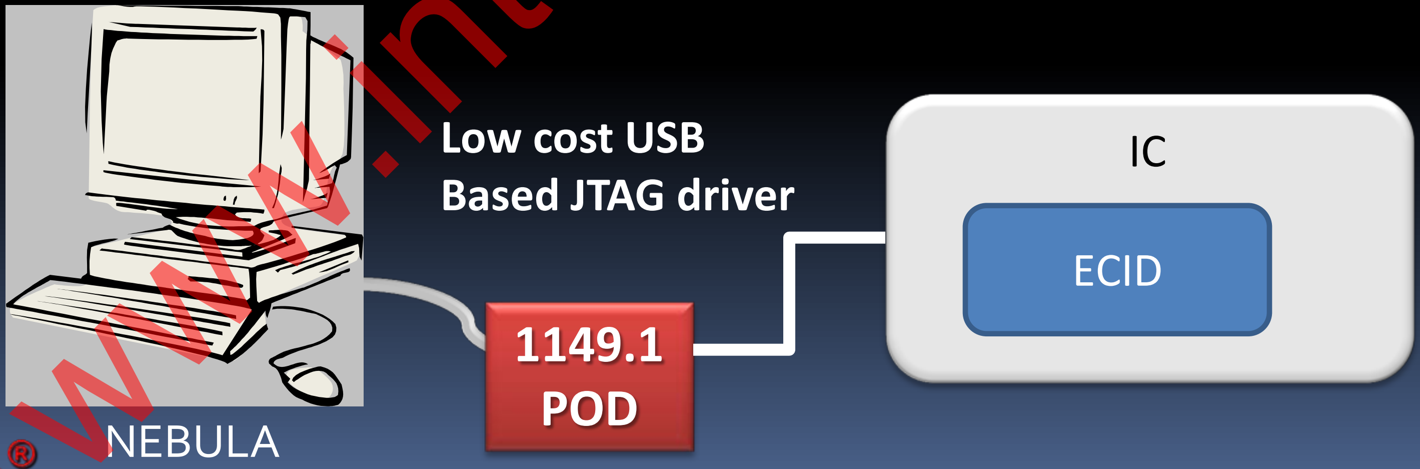
- Key is making source PDL publicly available for use with free 1149.1-2013 compliant software

- use low cost ~US$250.00 Xilinx pod

Output:

```
This IC grading is Temp:AEC and Speed:S2
```

Free 1149.1-2013 compliant software

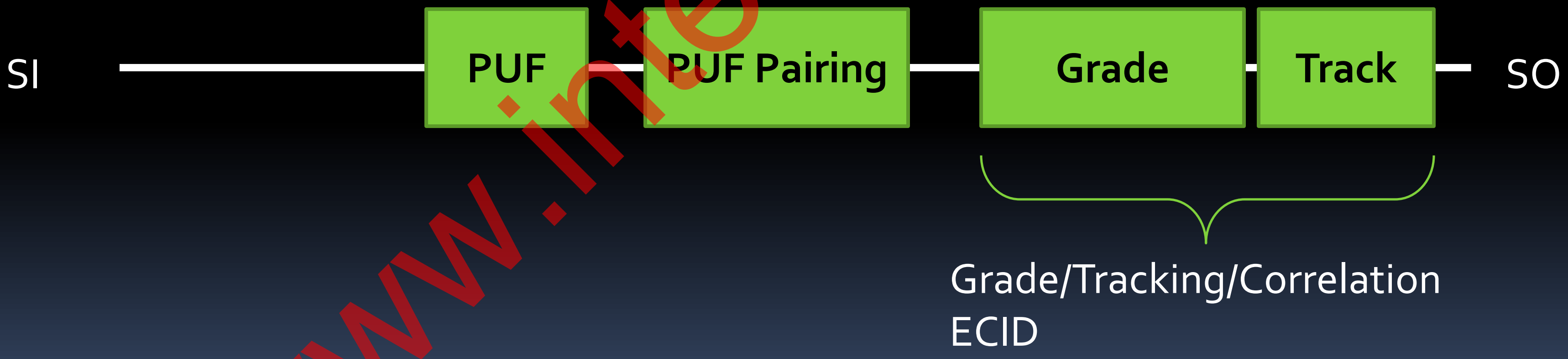


ECID to prevent Counterfeiting by Cloning

Problem: It's possible with well funded counterfeiter to clone by imaging IC layer by layer.

We'll accept that as fact and not discuss difficulties in cloning 14nm FinFet designs, anti-fuses, various oxide based NVM storage that is Difficult to clone or slowed by SEM microscope via by via inspection.

Solution: IEEE 1149.1-2013 ECID captures PUF value
At production SHA256 Hashed PUF Pair value programmed in OTP



Intellitech®

1149.1-2013 Additional ECID Package definitions

```
attribute REGISTER_MNEMONICS of ECID : entity is
 "Temp (Comm  (0B00) < Commercial >, "&
 "      Ind   (0B10) < Industrial >, " &
 "      AEC   (0B01) < AEC-Q100 >), "&
 "Speed (S1    (1),  " &
 "       S2    (0) )," &
 "Stat  ( Ready     (1), " &
 "        Not_Ready (0)) ";

attribute REGISTER_FIELDS of ECID : package is
"ECID [547]( "&
 "( PUF  [256] IS (546 DOWNTO 291) ), "&
 "( PUFHASH  [256]  IS (290 DOWNTO 35) ), " &
 "( Status [1] IS (34 )        CAPTURES(Stat  (Not_Ready)) ), "&
 "( Temp [2] IS (33 DOWNTO 32) CAPTURES(Temp  (-)) ), "&
 "( Speed[1] IS (31)           CAPTURES(Speed (-)) ), "&
 "( Die  [9] IS (30 DOWNTO 22 ) ), "&
 "( Wafer[20] IS (21 DOWNTO 2) ), "&
 "( Fab  [2]  IS (1 DOWNTO 0) ) )";
```

1149.1-2013 ECID with PUF and HASH

With a uniform language, IC vendor or ECID IP provider can
Supply software routines (encrypted/remote) to authenticate on-chip PUF and HASH values returned by ECID call

```
# ECID.pdl
iPDLLevel 1 -version STD_1149_1_2013
iProcGroup ECID
iProc ecid {} {

iRunLoop 10000 -sck Sysclock_200MHz
iLoop
iRead Status Ready
iApply -nofail
iUntil -match -maxloop 10 “ECID timed out”

Set PUF [iGet -so PUF]
Set PUFHash [iGet -so PUFHASH]
Puts "PUF and HASH:\n$PUF\n$PUFHash\n" ;# 256 bit hex values
iCall CheckValues $PUF $HASH   ;# call vendors external program
}

iProc  CheckValues {puf  hash} {

#Extern call SecretSauce $puf $hash
```

1149.1-2013 ECID with PUF and HASH

IC can be validated as authentic over its lifetime without direct support/communication to IC vendor

Public can validate using 1149.1-2013 compliant software

Severe obstacle for cloner to duplicate just one pair.   Hard coded pairs to mimic cloned device would show up to the public in simple sampling as having the same values.

ECID Security already in use!

Intellitech SystemBIST IC - a PCB anti-cloning root of trust

IC Fab

Wafer +
Package Test

Parts Shipped

Intellitech

Package Serial# Laser Mark

Program Serial#, Cust, CM Code,

Unique 128bit, SHA256

Re-test packaged part

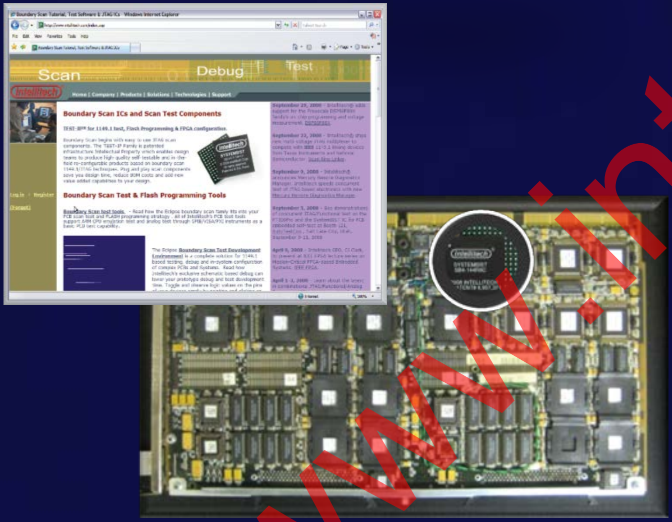
Scan
Debug
Test
Boundary Scan ICs and Scan Test Components
Boundary Scan Test & Flash Programming Tools

Each IC data logged

On www.intellitech.com

-Enter serial number to retrieve

Parts Shipped

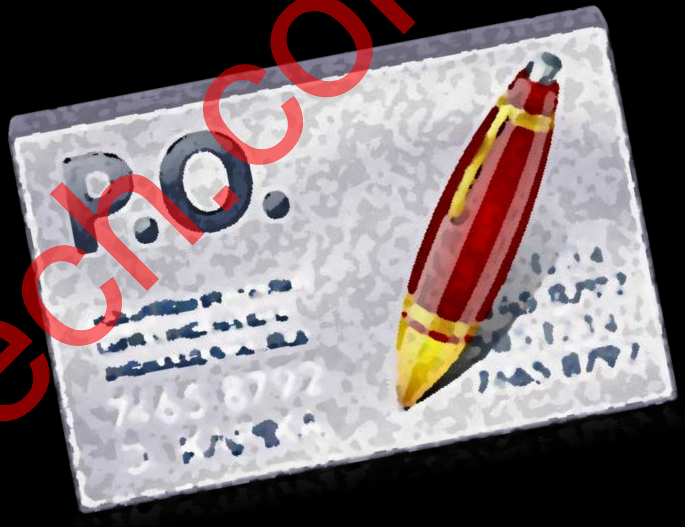

Scan
Debug
Test
Boundary Scan ICs and Scan Test Components
Boundary Scan Test & Flash Programming Tools

Optional: PCB data history by serial no#

On www.intellitech.com

For Fifteen or more years IEEE 1149.1 compliance has been a requirement for many ASIC and SoC contracts

Purchase Orders from Silicon vendors for on-chip infrastructure IP will also include requirements for IEEE 1149.1-2013 compliance



OEM Purchase Orders will include requirements for 1149.1-2013 compliance and IP with compliant documentation. OEM's will require the 1149.1- 2013 ECID based security for outsourced ASIC designs

The 1149.1 brand continues
To give assurances to
Customers that IP and ICs
Meet an acceptable
Level of simplicity for IC
Test operations

Intellitech®

IEEE 1149.1-2013 - "It's in there"