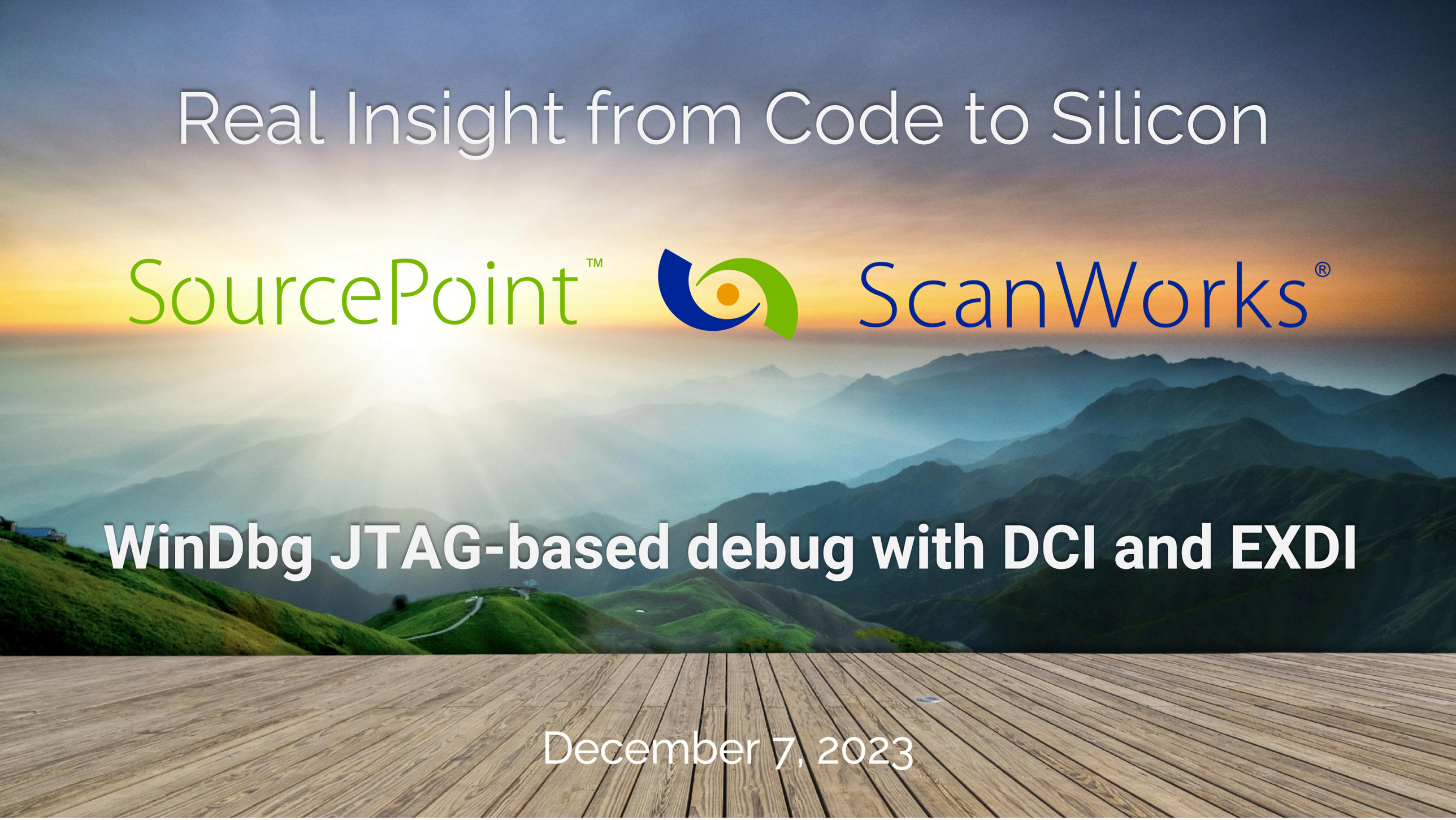
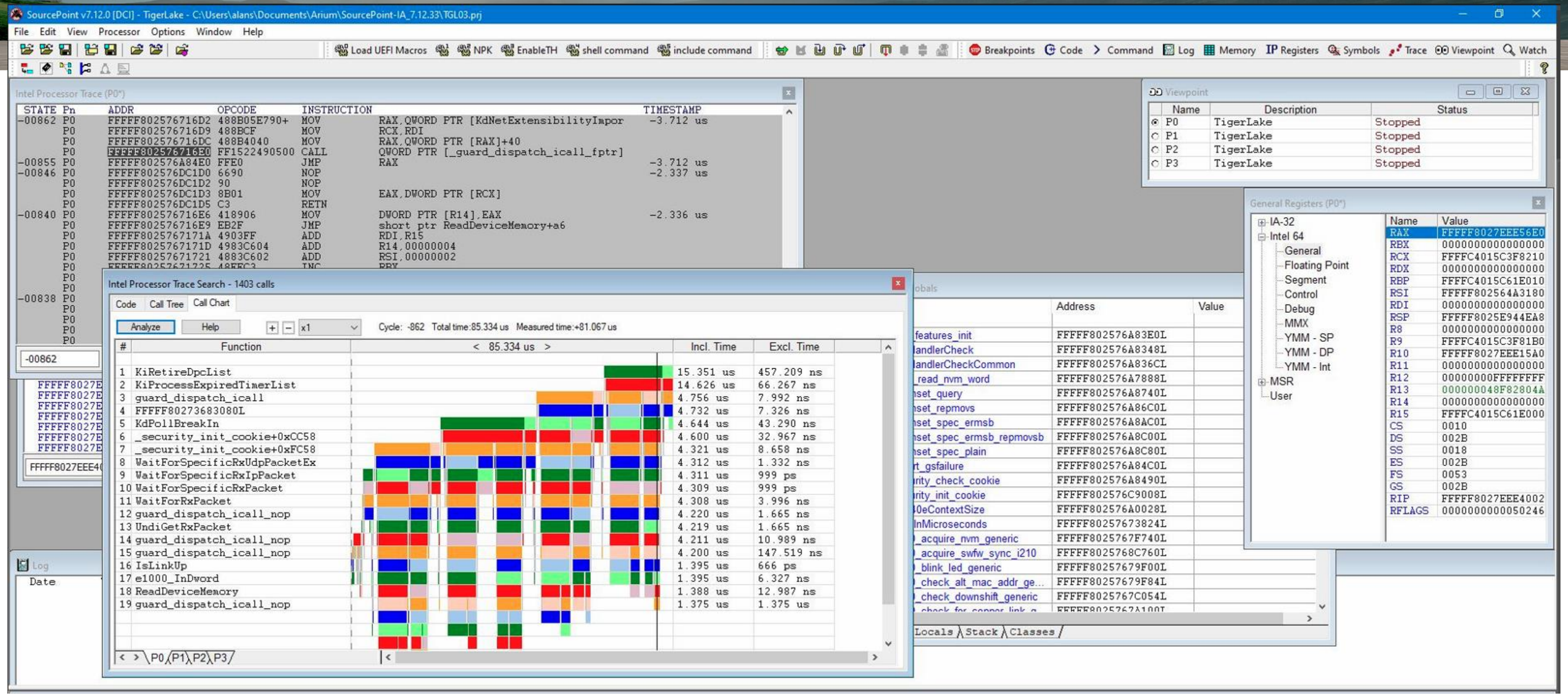

Real Insight from Code to Silicon
SourcePoint™
ScanWorks®
WinDbg JTAG-based debug with DCI and EXDI
December 7, 2023



© 2023, ASSET InterTech, Inc.

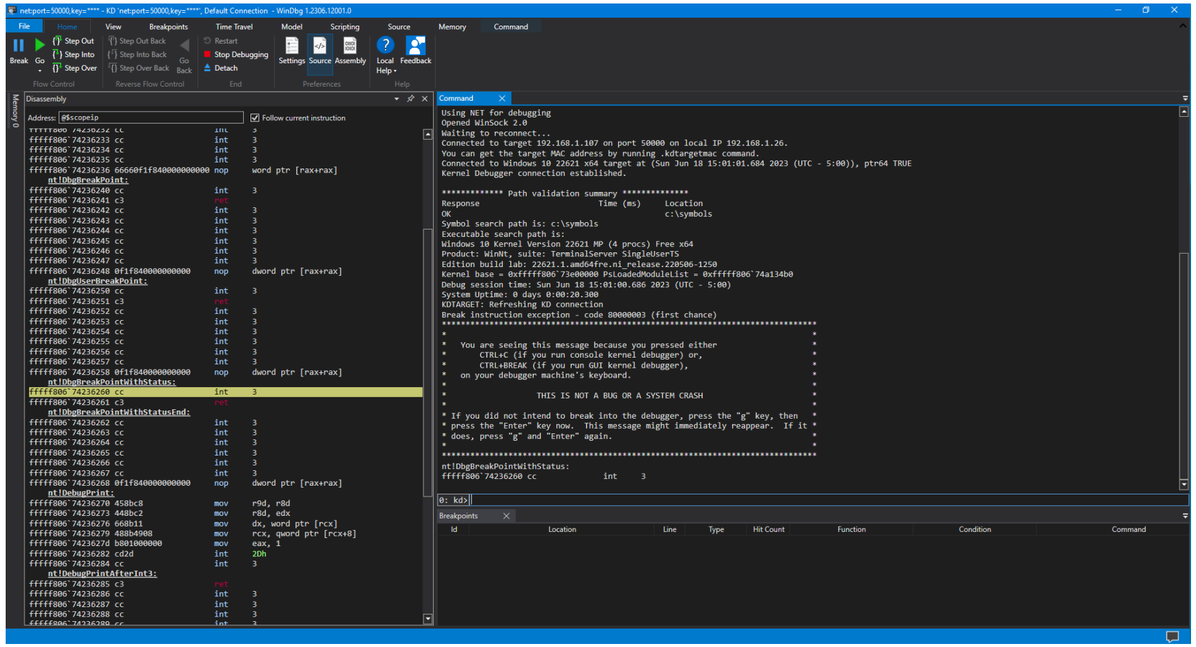
Agenda

- WinDbg
- SourcePoint
- Why combine the two?
  - Enhancing WinDbg with JTAG-based run-control and trace features
  - “Debugging the Undebuggable”
- Demo configuration
  - What you’ll see in the demo
- Demo
- Wrap-Up

© 2023, ASSET InterTech, Inc.

WinDbg

- WinDbg is a kernel-mode and user-mode debugger that's included in Debugging Tools for Windows
- De facto standard for Windows system-level programming/ debugging
- Very powerful: OS-aware (processes, threads, jobs, kernel symbols, etc.)



SourcePoint™
Platform for Software Debug and Trace

© 2023, ASSET InterTech, Inc.

ScanWorks®
Platform for Embedded Instruments

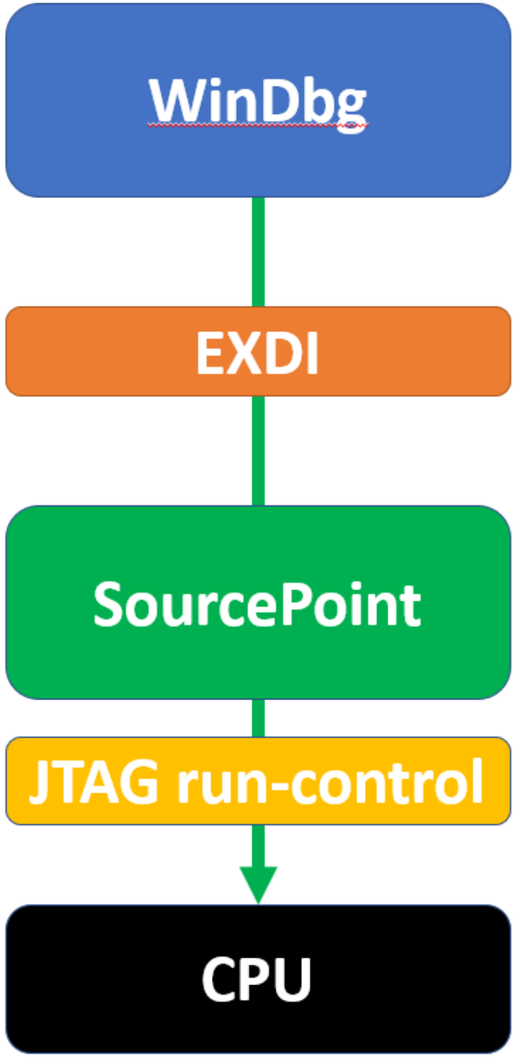
SourcePoint

- Best-in-class UEFI debugger
- Support for x86: Intel (all CPUs) and AMD (EPYC)
- Source-level symbolic debugger, full run-control (stop, go, single-step, breakpoints, etc.)
- Supports Advanced (Conditional) Breakpoints on AMD
- Supports innovative Trace features on Intel

© 2023, ASSET InterTech, Inc.

Why combine WinDbg and SourcePoint?

- Microsoft released update to EXDI (Extended Debug Interface)
- EXDI is an adaptation layer between a software debugger and a debugging target.
- Extends WinDbg by adding support for hardware-based debuggers (i.e. JTAG-based)
- WinDbg is the controller; SourcePoint is the worker
- “Debugging the Undebuggable” https://www.andrea-allievi.com/blog/debugging-the-undebuggable-part-1/
  But on steroids!



© 2023, ASSET InterTech, Inc.

Why combine SourcePoint with WinDbg?

Take advantage of powerful features of both applications:

WinDbg

- *OS-aware*
- *Extensible*
- *Go-to tool for kernel debugging*

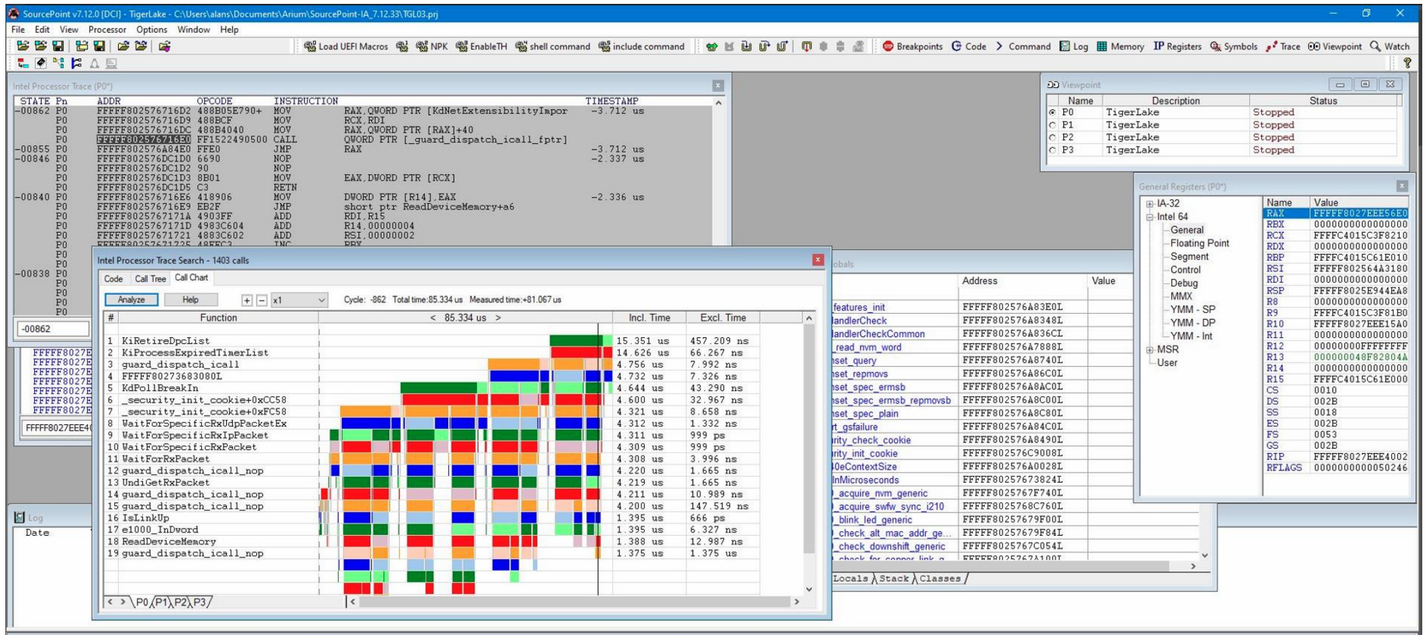
SourcePoint

- *Advanced breakpoint support (SMM entry/exit/data access, machine check, etc.)*
- *Intel Processor Trace*
- *Trace Hub*
- *Architectural Event Trace (AET)*

© 2023, ASSET InterTech, Inc.

Intel Processor Trace

- Execution Trace
- Real-time (nominal performance impact)
- Stored in system memory (post-MRC)
- Call Tree, Call Chart, all with Search capability
- Up to 2GB instruction trace



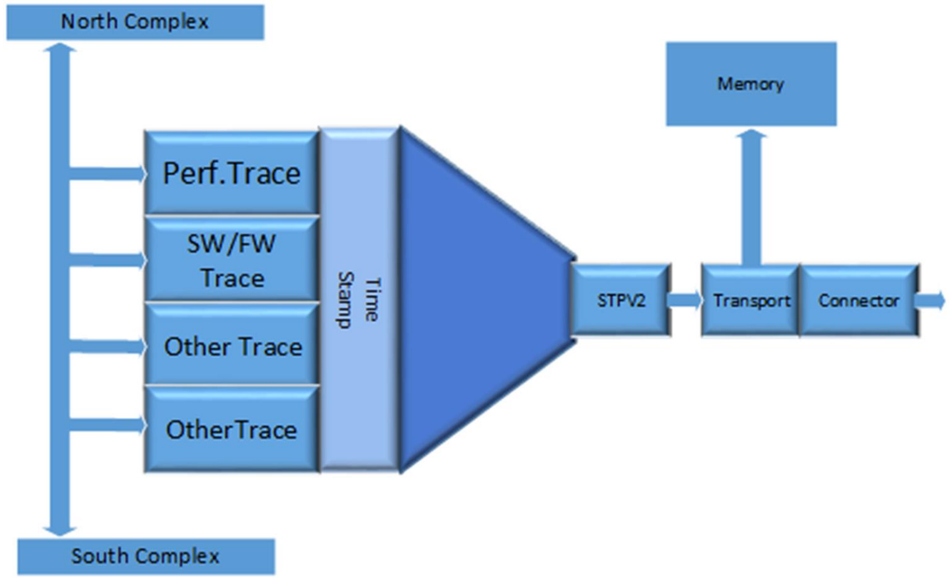
© 2023, ASSET InterTech, Inc.

SourcePoint™
Platform for Software Debug and Trace

ScanWorks®
Platform for Embedded Instruments

Intel Trace Hub

- Logic that comprises trace sources, a global hub with timestamp, trace destinations, and a trigger unit
- A slave device for writes from cores and any other trace sources
- Acts as a PCI device, and aligned with industry standards
- Sources include Architectural Event Trace (AET), ME Trace, SW/FW Trace, etc.
- Trace destinations include:
  - MTB (8kB, out of reset)
  - System Memory (after MRC)
  - ***Direct Connect Interface (out of reset, supports streaming trace)***



© 2023, ASSET InterTech, Inc.

Architectural Event Trace (AET)

Event Trace, that complements Instruction Trace. Requires JTAG.

Event Type	Event SubTypes	Description
HW/SW Interrupt	HW_INTR	HW interrupt trace
IRET	IRET	IRET trace
Exception	Exception	Exception, fault, trap trace
MSR	RDMSR, WRMSR	MSR trace
IO	PORT_IN, PORT_OUT, PORT_IN_ADDR	IO trace
SGX	AEX, EENTER, ERESUME, EEXIT	SGX trace
CODE_BP	CODE_BP	Code breakpoint trace
DATA_BP	DATA_BP	Data breakpoint trace
FIXED_INT	SMI, RSM, NMI	“Fixed” interrupt trace
SW_POWER	MONITOR/MWAIT	MONITOR/MWAIT trace
WBINVD	WBINVD_BEGIN, WBINVD_END	Write-back invalidate trace

© 2023, ASSET InterTech, Inc.

AET Tips #1

- ***Probe-mode (JTAG) needed to initialize AET – use outside of probe mode (i.e. BIOS, device driver) causes #GP.***
- AET is implemented in CPU microcode and does not modify the architectural behavior of the processors – no need to instrument code!
  - ** Enabling CODE/DATA_BP changes the behavior of normal breakpoints – causes a trace event rather than a debug exception. Great for critical sections of code, concurrency issues, debugging memory accesses, etc.*
- This is event trace, not instruction trace: source code/ symbols not required (but it's great if you have them!)

© 2023, ASSET InterTech, Inc.

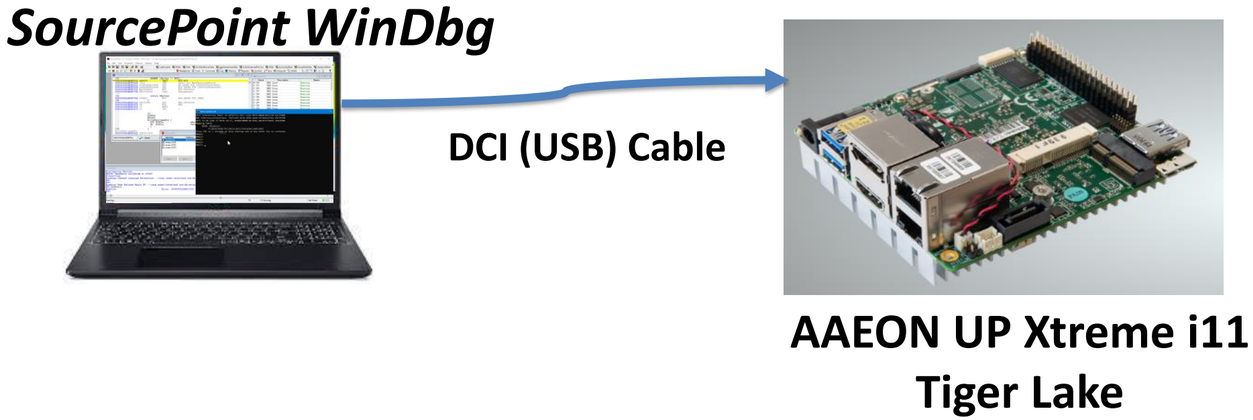
AET Tips #2

- A Last Branch Record (LBR) instruction trace stack can be added to all event traces – a fast way to trace back ~ 300 instructions
  - *LBR uses MSRs to track from_address and to_address pairs, so operates out of reset – no need for system memory*
- Intel Processor Trace and AET can run concurrently
  - *Intel PT places trace data in system memory*
- On Ice Lake processors and later, both AET LBR tracing and Intel Processor Trace can be enabled at the same time

© 2023, ASSET InterTech, Inc.

The Demo – what you'll see

1. SourcePoint makes JTAG connection at reset vector with DCI
2. COTS Tiger Lake target booted from reset vector to Windows desktop
3. SourcePoint launches WinDbg, makes EXDI connection
4. Symbols visible in both WinDbg & SourcePoint
5. Demonstrate run-control, symbolic debug (stop, go, set breakpoint, single-step, etc.), Intel Processor Trace, AET, etc.



© 2023, ASSET InterTech, Inc.

Demo

© 2023, ASSET InterTech, Inc.

Resources

- SourcePoint Academy: https://www.asset-intertech.com/resources/academy/sourcepoint-academy/
  - *SourcePoint WinDbg Getting Started Guide*
  - *Getting Started Guide for the AAEON UP Xtreme i11*
  - *Videos, Online Help, Release Notes, etc.*

© 2023, ASSET InterTech, Inc.

Questions and Contact Information

alan.sguigna@asset-intertech.com

X DM @AlanSguigna

© 2023, ASSET InterTech, Inc.

Real Insight from Code to Silicon

SourcePoint™
Platform for Software Debug and Trace

© 2023, ASSET InterTech, Inc.,

ScanWorks®
Platform for Embedded Instruments