

SOLID ソフトウェア開発環境をアップデートし、 QEMU 仮想マシンを同梱して提供開始

2021 年 8 月 5 日 京都マイクロコンピュータ株式会社

京都マイクロコンピュータ株式会社(以下 KMC と記載)は、本日 2021 年 8 月 5 日から KMC のリアルタイム OS ベースの組込みソフトウェア開発プラットフォーム SOLID(以下、SOLID と記載)にQEMU 仮想マシンを同梱した、アップデート版の提供を開始したことを発表します。

1 SOLID-IDE と QEMU 仮想マシンの統合

KMC は、RTOS を含んだ組込みソフトウェア開発プラットフォーム "SOLID"を 2018 年より提供開始しており、現在多くのお客様にご使用いただいています。この SOLID に「Windows® PC だけでビルドから実行まで完結できる」ことを実現するため、SOLID を構成する開発環境に QEMU 仮想マシンを追加・同梱して提供することになりました。SOLID に QEMU 仮想マシンを同梱することにより、ターゲットボードなどがなくても、PC 上で SOLID-OS や SOLID 開発プラットフォームの様々な機能を体験することができます。また、SOLID が提供する実行時デバッグ機能も QEMU 仮想マシン上で使用できるので、開発製品ファームウェアの単体デバッグなど、初期段階のデバッグに有効です。

2 QEMUとは

QEMU は、オープンソースプロジェクトにより開発・運用管理されている汎用的な CPU マシンエミュレータであり、x86, Power-PC, Arm®プロセッサや RISC-V プロセッサ向けなど、多くの CPU の仮想化に対応しています。また近年では、PC 上で Arm CPU 用 Android 機器開発を行うための SDK にQEMU が採用され、QEMU の性能が大幅に向上しました。

QEMU の仮想化の特徴は、基本的なインタプリタ実行だけでなく、中間コードと JIT による動的コンパイルで、比較的高速に実行できる点です。

KMC では 2007 年から QEMU の社内利用を開始し、Visual Studio® 上で顧客仮想ハードウェア環境を構築するツール "HARVEST" のリリース(2008 年)、デバッガとの連携など、QEMU に関する製品の提供実績があります。



3 SOLID 版 QEMU 仮想マシンの仕様

SOLID では、次のような QEMU 仮想マシンを提供します。

- · Windows 用にビルドしたバイナリの QEMU ARM を同梱します。
- · 対象のプロセッサ

Arm®v7-A アーキテクチャ:Arm®Cortex®-A9 プロセッサ(シングルコア/デュアルコア) Arm®v8-A アーキテクチャ:Arm®Cortex®-A53 プロセッサ(シングルコア/デュアルコア)

· RTOS を動作させるためのハードウェア

メモリ

GICv2(割り込みコントローラ)

Timer (Arm Generic Timer)

UART (Arm PL011)

また、対象となるリアルタイム OS は現在リリースされている TOPPERS/AMP3、TOPPERS/FMP、TOPPERS/FMP3 に全て対応します。

4 QEMU 仮想マシンを使ってできること

QEMU 仮想マシンには、上記のようにプロセッサ、割り込みとタイマが含まれているので、RTOS の API 仕様に従って作成されたモジュール(タスク)が実ハードウェアと同様に起動・遷移していく様子が確認できます。

さらに、実ハードウェアが無い場合、デバッグ手段は SOLID の静的解析機能である文法チェックや構 文解析などの利用に限られていましたが、QEMU 仮想マシンを利用することで以下のような実行時デ バッグも可能となります。

- ・ MMU 自動設定機能を利用したスタックオーバーフローなどのメモリ領域不正アクセス自動検出 や、読み出し専用領域への不正書き込みアクセスの自動検出
- · アドレスサニタイザ機能による、配列オーバーなどのメモリアクセスバグの自動検出
- ・ コードカバレッジ表示、関数トレース表示
- ・ローダー機能を使った、多拠点で開発されたアプリを結合した実行モジュールの構築とデバッグ
- · プロセッサの内部リソースを含むトレース情報の取得および解析



SOLID IDE からは 1 アクションで QEMU が簡単に起動でき、QEMU のコンソール表示画面に仮想マシンの UART 出力が表示できます(図 1)。

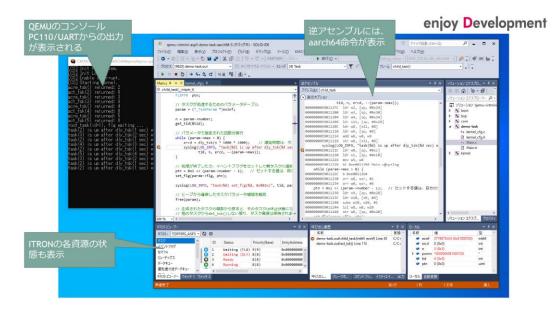


図1. QEMU コンソールで仮想ハードウェア UART 出力表示を確認する

5 QEMU 仮想マシン同梱版 SOLID の提供方法

SOLID Ver.2.1 以降、標準機能として QEMU 仮想マシンが同梱されます。既に SOLID のライセンス契約をしてご使用中の方は、追加費用無しでバージョンアップすることで QEMU 仮想マシンがご利用できるようになります。

なお、ハードウェア仕様決定とソフトウェアの評価を平行して進めなければいけない場合や、高価な評価ボードを開発者の人数分用意することが現実的ではない場合には、QEMU 仮想マシンをカスタマイズして、評価ボード相当のものを構築することが可能です。そのために次の2つの方法をご用意していますので、併せてご検討ください。

- (1) KMC 製 QEMU SDK(有償にて提供)
 Windows で独自の仮想ハードウェアを開発するためのフレームワーク、ドキュメントや仮想ハードウェア開発のための技術サポートを提供します
- (2) 仮想ハードウェアの開発受託 開発内容に応じて個別にお見積



【付録】開発プラットフォーム SOLID の概要

1) SOLID-IDE の特徴

SOLID-IDE は、Visual Studio をベースに開発した統合開発環境で、エディタやビルダーそしてデバッガが含まれます。SOLID-IDE には実績が豊富な KMC 製 GCC コンパイラ(exeGCC)の他、LLVM/Clang コンパイラを含んでいます。

- 2) ソフトウェア品質向上と、開発効率向上に有効なデバッグ・解析支援機能 SOLID では、SOLID-OS にデバッグ支援用として強化したランタイムと、SOLID-IDE に含まれる Clang コンパイラの持つ充実した解析機能を連携させることにより、アドレスサニタイザやデバッグ 用コードカバレッジ表示などを実現しています。スタック破壊などの実行時バグを自動検出する機能や、ソースコードの静的解析機能など、ソフトウェア品質向上と、開発効率向上に有効なデバッグ・解析支援機能を豊富にそろえています。
- 3) 大規模システム開発を効率よく行える支援機能

モジュール単体でのビルド・ロードおよびアンロードが行えるローダーを独自に開発しました。このローダーを利用することで、大規模ソフトウェアを多人数・多拠点で開発する場合に、他拠点のソースコードを共有することなく開発対象のソフトウェアだけのビルド・ロードをし、開発対象のソフトウェアを効率よくソースコードデバッグできます。

4) JTAG デバッガ PARTNER-Jet2 対応

当社の JTAG デバッガである PARTNER-Jet2 が使用できます。PARTNER-Jet2 はデバッグ対象の Arm Cortex v7-A 32bit/64bit プロセッサおよび Arm Cortex v8-A 64bit プロセッサに対応しています。 Arm Cortex v8-A 64bit プロセッサのデバッグでは、A64 命令セットの解析や 64bit アドレス空間表示 のほか、取得したトレース情報の 64bit アドレス空間表示が可能です。また Arm Cortex v8-A 64bit アーキテクチュアで定義された 4 つの Exception Level(EL0~EL3)と、セキュア/非セキュア状態での デバッグがしやすいよう、ブレーク条件やトレース結果に Exception level とセキュア状態が設定/表示できるようにしました。さらにマルチプロセッサ構成をふまえて、ブレーク条件やトレース結果にプロセッサ ID の設定/表示が可能です。

SOLID について: https://solid.kmckk.com/SOLID/

ここに記載されている製品名は各社の商標または登録商標です。