

Formalisasi dan verifikasi spesifikasi sistem kontrol persimpangan jalan raya dengan rel kereta api satu jalur satu arah

Achmad Ridok

Deskripsi Dokumen: <http://lib.ui.ac.id/opac/themes/libri2/detail.jsp?id=75653&lokasi=lokal>

Abstrak

Keberadaan perangkat lunak sebagai pengontrol suatu sistem, yang termasuk ke dalam kategori sistem tercangkok (embedded system) semakin meningkat, sejalan dengan pemanfaatan komputer dalam berbagai sektor kehidupan. Dalam sistem semacam itu, perangkat lunak ditempatkan pada sebuah atau beberapa komputer yang dihubungkan ke sensor-sensor dan aktuator-aktuator untuk mengontrol perilaku dari lingkungan sistem

.

Sistem tercangkok umumnya berinteraksi dengan lingkungannya secara terus-menerus sehingga disebut juga sistem reaktif (reactive system). Rika sistem tersebut diharapkan bereaksi dengan lingkungannya dalam batas waktu yang spesifik, sistem tersebut disebut sistem waktu nyata (real-time system). Contrail sistem terakhir adalah sistem pengatur lampu lalu lintas, sistem pengontrol pembakaran gas, dan pengontrol pintu perlintasan persimpangan rel kereta api dengan jalan raya. Sistem seperti ini harus memenuhi kriteria terpercaya (reliable); dalam arti, untuk menjamin keamanan sistem, waktu respon dari sistem terhadap lingkungannya hams sesuai dengan yang disyaratkan. Kegagalan sebuah sistem dalam merespon lingkungannya dapat menyebabkan terjadinya situasi kritis yang dapat berakibat fatal bagi manusia atau lingkungannya.

Sistem seperti di atas harus dirancang dengan presisi yang cukup tinggi. Penggunaan bahasa alami dalam proses pengembangannya, terutama pada tahap analisis untuk menentukan persyaratan yang dibutuhkan oleh sistem, dapat menimbulkan pernyataan-pernyataan yang ambigu sehingga persyaratan-persyaratan maupun spesifikasi sistem kurang terekspresikan secara akurat.

Salah satu teknik untuk mengembangkan perangkat lunak yang diharapkan memenuhi kriteria terpercaya adalah metoda formal. Terminologi 'metoda formal' menggambarkan suatu deskripsi umum dari penggunaan konsep matematika seperti logika dan teori himpunan untuk menggambarkan spesifikasi dan rancangan perangkat lunak beserta teknik-teknik validasi dan verifikasinya. ide dasar dari metode formal adalah menyediakan bahasa spesifikasi yang tidak ambigu untuk tahap perancangan selama pengembangan sistem sedemikian sehingga rancangan dapat dijustifikasi melalui langkah-langkah pembuktian formal [Franz96]. Bahasa spesifikasi tersebut biasanya terdiri dari tiga komponen utama, yaitu:

Sintaks

Semantik

Himpunan relasi yang mendefinisikan aturan-aturan yang menunjukkan objek-objek yang pantas memenuhi spesifikasi tersebut.

Dengan menggunakan matematika sebagai kerangka dalam perancangan sistem, ide-ide yang ada dapat diformulasikan dengan lebih tepat, sehingga sistem yang lebih terpercaya dapat dihasilkan.

Salah satu formalisasi sistem seperti di atas adalah Duration Calculus (atau disingkat DC) [Zho93, 71-IR91, ZHR92]. DC dikembangkan pertama kali oleh C. Thou, C.AR. Hoare, dan AP. Ravn sekitar tahun 1991.

Dalam DC, waktu dimodelkan sebagai bilangan nyata atau real (R), dan keadaan sebuah sistem dimodelkan oleh sejumlah variabel state. Setiap variabel state memiliki nilai Boolean yang direpresentasikan sebagai $(0,1)$. Pada dasarnya, variabel state yang bernilai deskrit dapat dimodelkan oleh sekelompok n -variabel Boolean. Keadaan sebuah variabel state dari waktu ke waktu dimodelkan oleh sebuah step function dengan domain R dan range $\{0,1\}$. Dengan melakukan integrasi terhadap sebuah step function dalam interval waktu tertentu, kita bisa mendapatkan total durasi di mana variabel state yang dimodelkan oleh fungsi tersebut berada dalam keadaan true (1). Teknik integrasi banyak digunakan dalam DC untuk menggambarkan persyaratan dan rancangan sistem-sistem yang kritis terhadap waktu (time-critical systems), tanpa menyebutkan waktu absolut secara eksplisit. Dalam penelitian ini dilakukan eksperimen untuk melihat bagaimana metode ini diterapkan untuk masalah aktual, yaitu dengan mencoba melakukan perancangan sistem pada suatu studi kasus.

