Research on Model-based IMA Resources Allocation

Xiao Zhang[1, a], Lisong Wang[2, b]

[1]School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, 210016, China

[2]School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, 210016, China

[a]email:lovelyfly91@sina.com, [b]email:553690638@qq.com

Keywords: Integrated Modular Avionics; Resource Allocation; Meta-Model; Constraint

Abstract. The ever increasing complexity of avionics system and amount of platform devices makes allocating the IMA resources more error-prone and harder to evaluate. This paper proposes a method of preliminary design of IMA platform based on models. The definition of system and platform respectively bases on meta-model of system structure and platform structure, thus specific format of system and platform makes the definition clearer, providing conditions to extract constraints and evaluate the allocation strategy automatically. The constraints can be extracted from the general requirements and safety requirements. Candidate allocation strategies can be generated from ILOG solver by inputting constraints described by OPL format. After safety analysis of candidate strategies, the system designers can accept or reject the proposed allocation.

Introduction

Integrated Modular Avionics System is a significant architecture of avionics system. IMA resource allocation should be considered before IMA system development. It can be learned from DO-178B [1] standard that IMA system consists of a series of configurable resources, which can ensure hosted functions execute with adequate memory capacity, computing time, communication capabilities, I/O resources and interfaces with other bus connections [2].

Different groups of staff are responsible for each part pf IMA system development phase. System designers' responsibility is analyzing the aircraft function, inputting functional requirements and safety requirements for system integrating. With the usage domain description from IMA platform designers, the IMA integrators can generate the IMA topology，allocate I/O resource ,CPU resource and communication resource. The allocating process is iterative until allocation satisfying the hosted function requirements. Because of involving numbers of complex structure of system and resource, lacking of accurate model of system and platform architecture, the resource allocating experts usually need to spend great energy collecting information. Hardly interpenetrating manually makes a lot of trouble to evaluate whether defined architectures are valid [3]. Furthermore, civil aviation as a safety-critical area puts forward higher requirements to safety. Resource allocation, as the first-phase preparation of IMA designing, not only need distributing shared resources suitably, but also need ensuring the integrity and availability of functions. Against the proposed issues, this paper proposes a method of preliminary design of IMA platform based on models.

Framework of preliminary design of IMA platform based on model

IMA architecture consists of one or more cabinets with a core processing module and a data transmitting network with other subsystems of the aircraft, in order to provide computing, communications, I/O and other resources for the hosted functions. Through these shared resources IMA can realize the function of data processing, data transmission and simple data format conversion. According to hierarchical structure proposed by ASAAC [4], the main component can summarize as: integrated processing module (IPM), avionics full duplex switched Ethernet (AFDX), remote data collector (RDC), non-IMA device (controller, sensor, etc.) and partition application [5].

Avionics platform composed of shared computing and communication resource can not only support safety-critical applications but also non-safety-critical applications. Because of designing has not begun, platform designers and system designers can easily choose optimal allocation strategy form a number of strategies. In this paper, satisfaction of qualitative and quantitative safety requirements can be as the main objective in the allocation of resources. The method of combining safety analysis technology with constraint based resource allocation can be used to generate a preliminary design strategy of IMA system. The framework of IMA resource allocation and verification is shown in Fig.1 . The three main steps of the process are:

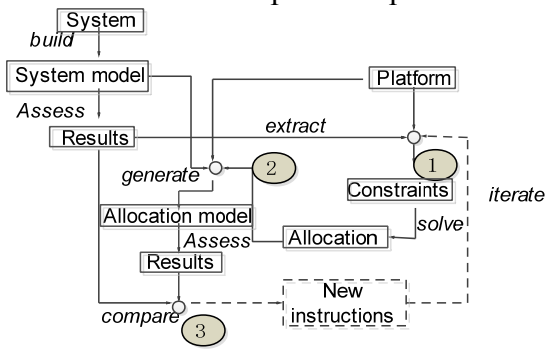

Fig.1. The framework of IMA resource allocation and verification

STEP1: Safety analysis of system model provided by system designers is executed using safety analysis method (such as fault tree analysis) in order to get the minimal cut sets of failure condition (FC) listed by FHA. From view of safety, segregation and aggregation constraints can be extracted because basic events of the minimal cut sets cannot be hosted on resources which have common cause failure in order to achieve the safety requirement. A series of allocation constraints can be extracted from the system model with the platform model provided by platform designers. These constraints are called constraints model which described by a set of equations and inequalities.

STEP2: The constraint model is transformed into the format which can be recognized by the constraint solver. The results provided by constraint solver can generate the allocation model with function model and platform model.

STEP3: Safety analysis of the allocation model is executed using safety assessment tools in order to provide safety results which can be compared with the results obtained by STEP1. From the comparison, system designer can decide whether the allocation is accepted or rejected. If the strategy is rejected, new constraints can be sent in order to find an optimal allocation strategy.

System model

The system model defines the logical structure, functional properties and requirements of hosted functions. The main items of system model are task, signal, and part of constraints of system. This paper uses meta-model to define the system model in order to ensure the definitions of system architecture be in unified format. Meta-model consists of classes, relations, attributes, methods and so on. The meta-model definition of system model is shown in Fig.2 .

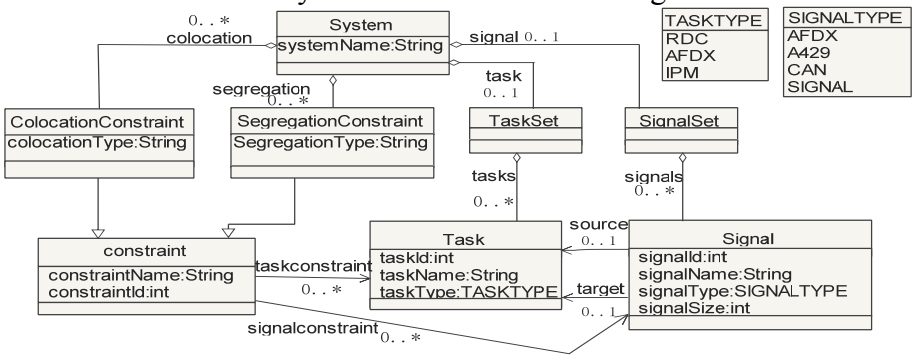

Fig.2. Meta-model of system model

The system model is consisted of task set, signal set, segregation constraints, and aggregation

constraints. There are a number of tasks in TaskSet. Task refers to the software that can be executed on the IMA hardware. Every task associated with a task type has ID and name. The value of enumeration field TASKTYPE is {RDC, IPM, AFDX}. There are a number of signals in SignalSet. Signal is the data exchanged between two tasks. Every signal associated with a signal type has ID, name and size. The value of enumeration field SIGNALTYPE is {AFDX, A429, CAN, SIGNAL}. A signal and two tasks associate by associations *target* and *source*.

Platform model

Hardware layer refers to the topology of IMA platform, including hardware devices and the connection between devices. They can provide computing resources, communicating resources, I/O resources. The meta-model of IMA platform is shown as Fig.3 .

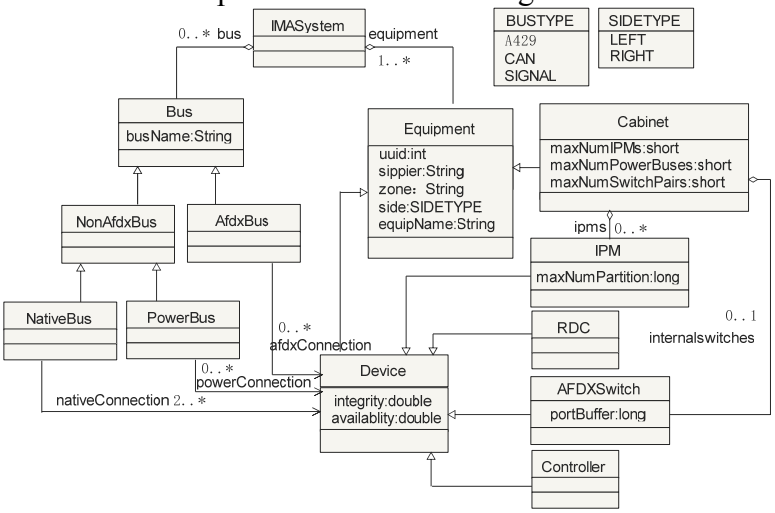

Fig.3. Meta-model of platform model

In the meta-model of IMA platform, the devices are divided into IPM, RDC, AFDX Switch, Controller and so on. Different types of devices can host different types of application, and the type of device is relative to the task type. In the aircraft the devices have fixed installation location, side and zone can be considered as hardware attributes in order to provide allocation constraints. IMA system contains a number of devices which can be connected by bus to achieve data exchanging between devices. The signal of system model will be mapped onto the bus.

Mathematical representation of resource allocation constraints

The system is composed of software blocks and the signal. The software block which is regarded as a block box, can be a controller application or a data processing application.

Definition 1(System function description): Let $orig: S_i \to T_i(S_i \in Signal, T_i \in Task)$ be data flow and its original task, $dest: S_i \to T_i(S_i \in Signal, T_i \in Task)$ be data flow and its destination task, where,

(1) $Signal = \{S_1, S_2, ..., S_m\}(m \geq 0)$, *signal* is the signal set of system model;

(2) $Task = \{T_1, T_2, ..., T_n\}(n \geq 0)$, *task* is the task set of system model.

Data flow can be viewed as path from the task generating the signal to the task using the signal. Data flow should be hosted on a path of platform model. Path is a finite set of resources of platform.

Definition 2(Available path of platform resources) $P_i = (\{r_1, r_2, \ldots, r_n\}, type)$ $(n \geq 1, P_i \in Path, type \in SINGNALTYPE, r_1, r_2, ..., r_n \in Res)$, where,

(1) $Res = device \bigcup bus$, *Res* is resource set of platform model, where, *device* is the hardware set, and *bus* is the bus set;

(2) $\{r_1, r_2, ..., r_n\}$ is a resource set, which means that r_i connects r_{i-1} and r_{i+1} in the platform model. All the paths which have the length 1 are *Res*.

(3) *type* is the type of signal which can be transformed by the path, the value of enumeration field

SIGNALTYPE is *{AFDX, A429, CAN, SIGNAL}*.

Resource allocation not only refers to the function hosted on device, but also includes signal can be transformed from the device hosted its original task and the device hosted its destination task. Resource allocation is a mapping between the system items and the platform resources.

Definition 3(Resource allocation): $allo:(Task \bigcup Signal) \to Path$. $allo(x) \to y$ means that task or signal *x* is hosted on resource *y*.

Allocation refers to a computing resource assigning with task, and sequence of communication devices assigning with data flow. A series of constraints can be extracted from system model and platform model in order to find the optimal allocation.

a) Allocation uniqueness constraint

Allocation uniqueness constraint refers to one and only one device (resp. communication path) can host a task (resp. signal).The mathematical representation of allocation uniqueness constraint is:

$$\forall t:Task, \exists! d:device, allo(t)=d \,\&\&\, t.TaskType = d.type \quad (1)$$

$$\forall s:Signal, \exists! p:Path, allo(s)=p \,\&\&\, s.SignalType = p.type \quad (2)$$

where, symbol $\exists!$ in formula (1) and (2) means one and only one.

b) Path and signal consistency constraint

If a signal can be hosted on a communication path, this means the original task of the signal is hosted on the first device of the path and the destination task of the signal is hosted on the last device of the path. The mathematical representation of path and signal consistency constraint is:

$$\forall s:Signal, \exists p:Path\ if\ allo(s)\ then\ allo(orig(s)) = first(p) \,\&\&\, allo(dest(d)) = last(p) \quad (3)$$

where, in formula(3), $orig(s)$ is the original task of signal *s*, $dest(s)$ is the destination task of signal *s*, $first(p)$ is the first device of the path *p*, $last(p)$ is the last device of path *p*.

Constraint a) and b) are general basic constraints for any system. In order to achieve the safety requirements listed in FHA and optimal allocation, other constraints should be extracted.

c) Segregation constraint

Qualitative objective describes any combination of events less than the number of N cannot result in FC, N is related to the safety severity. Obtained from the safety analysis, if the safety severity is catastrophic, basic events of the minimum cut set with number 2 cannot be hosted on a group of devices with a common cause failure. It is generally believed that a group of devices with shared power supply, devices in the same zone or on the same side can cause the common cause failure. The mathematical representation of segregation constraint is:

$$\forall t_1,...,t_n : segT, not(commonT(allo(t_1),...,allo(t_n))), n \geq 2 \quad (4)$$

$$\forall s_1,...,s_n : segT, not(commonT(allo(s_1),...,allo(s_n))), n \geq 2 \quad (5)$$

where, $segT(t_1,...,t_n)$ means that tasks or signals $t_1,...,t_n$ cannot be hosted on a group of devices with common cause failure type T (power, zone and so on).For formula (4), $allo(t_1)=d_1,...,allo(t_n)=d_n$, if $T(t_1)=...=T(t_n)$, then the value of $commonT(d_1,...d_n)$ is true. For formula (5), $allo(s_1)=p_1,...,allo(s_n)=p_n$ if $\exists\, p_1^{'}:p_1,...,p_n^{'}:p_n, T(p_1^{'})=...=T(p_n^{'})$, then the value of $commonT(p_1,...,p_n)$ is true.

d) Aggregation constraint

Aggregation constraints are dual constraints of separation constraints. Aggregating a set of tasks and signals means that they should reside on a set of devices with a common cause failure. The mathematical representation of aggregation constraint is:

$$\forall t_1,...,t_n : ccolocT, (commonT(allo(t_1),...,allo(t_n))), n \geq 2 \quad (6)$$

where, $colocT(t_1,...,t_n)$ means that tasks or signals $t_1,...,t_n$ should be hosted on a group of devices with common cause failure type T.

e) Allocation group constraint

Allocation group constraint means that the tasks and signals are divided into several subsets, the range of the hosted resource of a certain subsets must be a subset of platform. After making sure the

allocation groups, it can be in a smaller range to search the allocation strategies, thereby reducing the search scale. The mathematical representation of allocation group constraint is:

$$\forall t : subF, exists\ p : subPath, allo(t) = p \tag{7}$$

where, $subF$ is a subset of the system model, $subPath$ is a subset of the platform model.

f) Allocation exclusion constraint

Allocation exclusion constraint means that range of the hosted resource of some subsets must not be some subsets of platform. The mathematical representation of allocation exclusion constraint is:

$$\forall t : subF, \forall p : subPath, not(allo(t) = p) \tag{8}$$

g) Peripheral device constraint

Peripheral equipment is not configured, non-IMA device, and belongs to a system. There is a task having the same name with peripheral device, meaning that the task should be hosted on the peripheral device. The mathematical representation of peripheral device constraint is:

$$\forall d_1 : Controller, \exists t : Task, \exists d_2 : Device, t.name = d_1.name \,\&\, \&allo(t) = d_1 \tag{9}$$

where, *Controller* is the collection of all peripheral devices. Formula (9) means that all peripheral devices in platform model has its corresponding task, the device task hosted on is IMA hardware equipment the peripheral device should be wired.

In addition to the general constraints and safety constraints listed above, other constraints also need to be considered. This paper doesn't take as a key consideration, so no longer tautology.

Extraction of resource allocation constraints

The allocation strategies search algorithm has three inputs, which are system model, platform model, allocation constraints supplement inputted by designers. Meta-models of system and platform are both descripted by EMF (Eclipse Modeling Framework). ILOG solver which taking OPL as input language is a mathematical tool which can solve constraint problems. System model and platform model have unified format, and the allocation constraints inputted are XML format, therefore, a toolset is developed to extract constraints from models, and automatically transformed into OPL format input file. The allocation strategies search algorithm is shown as Fig.4 .

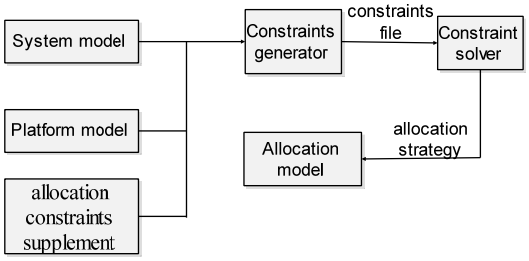

Fig.4. Allocation strategies search algorithm

The results

CDS (Cockpit Display System) is complex. For the convenience of research, this paper selected the function of providing attitude and altitude as a main function for simplifying. The safety requirements can be made sure through FHA and PSSA. The safety requirements are: (1) loss of attitude (altitude) displays is classified as hazardous; (2) display of misleading attitude (altitude) information is classified as catastrophic. Redundant architecture can improve availability and command/monitor architecture can improve integrity. The CDS architecture is shown as Fig.5 .

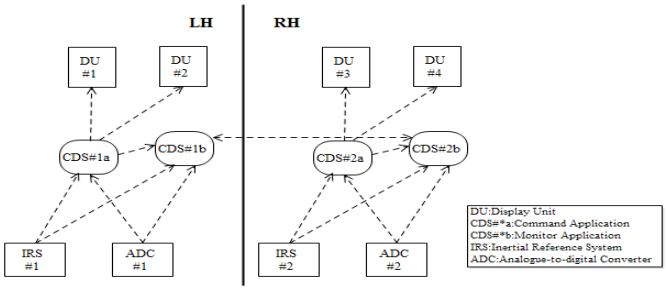

Fig.5. CDS architecture

Firstly, system and platform models should be built, using XML files to describe the models. Platform model is built based on the platform architecture provided by IMA platform designers. System model is built based on system architecture shown in Fig.5 and segregation and aggregation constraints. The result of safety analysis shows that {irs1, irs2}, {adc1, adc2} and other tasks or signals can not be hosted on the resources with common cause failure, and {adc1, irs1, cds1a, cds1b, dis1} should hosted on the same side. Through the tool designed for this paper, input file in OPL format can be automatically extracted from system and platform models.

The optimal goal of the experiment is using the least connection in the allocation process. Allocation model is shown in Fig.6 can be generated by combining the allocation strategy produced by ILOG Solver and system and platform models. The result of safety analysis shows that the probability of losing display attitude (altitude) is 1e-8 which can satisfy the safety requirement, and the probability of erroneous display attitude (altitude) is 1.22e-10 but no signal failure can cause the FC which satisfy the quantitative and qualitative safety requirements. Therefore, the system designer can accept the allocation strategy.

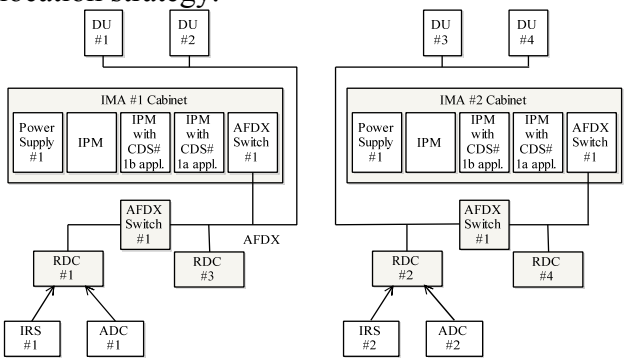

Fig.6. CDS recourse allocation

Conclusion

The proposed method can support dialog between system designers and IMA platform designers. Based on the general requirements of shared resources which are needed by analyzing the system to be hosted and the IMA platform and the safety requirements, a series of constraints can be extracted. Tool is designed to transform constraint expressions into OPL format input files. Multi-solutions can be generated by ILOG solver. Candidate allocation strategy can be performed safety analysis to decide whether it can meet other safety requirements. If the method will be applied to practical engineering application, a set of suitable IMA resource allocation tools should be developed.

Acknowledgement

In this paper, the research was sponsored by the National Key Basic Research Program of China (Project No.2014CB744900, 2014CB744903).

References

[1] Johnson L A.DO-178B, Software considerations in airborne systems and equipment certification[J].

[2] Watkins C B. Integrated Modular Avionics: Managing the allocation of shared intersystem resources. 25th Digital Avionics Systems Conference[C], 2006 IEEE/AIAA. IEEE, 2006: 1-12.

[3] Annighöfer B, Kleemann E. Model-based development of integrated modular avionics architectures on aircraft-level[J]. Deutscher Luft-und Raumfahrtkongress, Bremen, 2011.

[4] WANG Y, CHEN Y. Analysis of ASAAC Avionics Standards[J]. Telecommunication Engineering, 2007, 5: 041.

[5] Annighofer B, Kleemann E, Thielecke F. Automated selection, sizing, and mapping of integrated modular avionics modules. Digital Avionics Systems Conference (DASC)[C], 2013 IEEE/AIAA 32nd. IEEE, 2013: 2E2-1-2E2-15.