

フェイルソフトな社会情報システムのための デュアルユース型冗長構成方式

久野 巧[†]

日常生活に密着した社会情報システムには耐フォールト性の向上と構築コストの抑制という相反する要求が突き付けられている。

本論文では、耐フォールト性を確実に向上させるためにデータの生成部分からデータの最終出力部分までを一貫して多重化し、所要リソース(構築コスト)の増大を抑制するために情報量を縮減したデータを利用するフェイルソフトな冗長システムの構成方式を提案する。正常時にはシステムの機能検証を実行し、フォールト発生時に機能縮退する。システム冗長化のために付加した部分を、機能縮退だけでなく、未発見のバグや潜在的輻輳箇所等の検出を目的にして正常時にも利用するという点で「デュアルユース」になっている。

Dual-Use Redundant System Architecture for Fail-Soft Social Information System

HISANO Takumi[†]

In this paper we describe a new redundant system architecture, which involves multiplexing of all modules to improve fault tolerance and using abstract data to reduce the amount of redundant modules.

The social information system based on the architecture would perform dual functions(system verification in the normal state and graceful degradation in the fault state).

1 はじめに

個人の日常生活あるいは企業の社会活動に密接な関わりを持つ、社会性の強い情報システムが「社会情報システム」である。

今後、ユビキタスコンピューティングの浸透に伴って、世の中のあらゆる場面で社会情報システムからの情報支援が受けられるようになると思われる。一方で、社会情報システムの存在があたりまえになった社会では、システムの障害(フォールト)が近代的な生活の営みをすべて停止させてしまう危険性もはらんでいる。そのような危険を顕在化させないために、耐フォールト性の高い冗長システムの構築と運用が重要になる。

従来の冗長システムでは、ハードウェア故障

の発生確率に基づいて多重化すべき箇所を限定し、フォールトの発生しやすい部分あるいはフォールトの発生がシステム機能に致命的な影響を与える部分だけを多重化することが多かった。部分的な冗長構成であっても、フォールト発生の予測が正しければ耐フォールト性は確かに向上する。ところが、広義の障害(ハードウェアの故障はもちろん、ソフトウェアのバグ、設計ミス、過負荷、輻輳等を含む障害)までを想定した場合には、フォールト発生確率の見積もりに誤差が増えるため、部分的な冗長構成では運用の継続を保証することが難しくなる。

社会情報システムの遍在を前提にした社会においては、システム全体の耐フォールト性が高く、かつ、システム構築に要するハードウェアやソフトウェア(リソース)の増大を抑えることのできる冗長構成方式がより一層求められる。

本論文では、そのような冗長構成方式の候補として、耐フォールト性を確実に向上させるためにデータの生成部分からデータの最終出力

[†] 独立行政法人 産業技術総合研究所知能システム研究部門 (National Institute of Advanced Industrial Science and Technology)

部分までを一貫して多重化し、所要リソースの増大を抑制するために情報量を縮減したデータを利用するフェイルソフトな冗長システムの構成方式を提案する。正常なときにはシステムの機能検証を実行し、フォールトが発生したときに機能縮退する。システム冗長化のために付加した部分を、フォールト発生時の機能縮退だけでなく、正常時にも未発見のバグや潜在的輻輳箇所等の検出を目的にして利用するという点で「デュアルユース」となっている。

2 フェイルソフトな社会情報システム

社会情報システムに対しては、従来から情報通信ネットワークの進展に合わせるように高度情報通信社会実現に向けた取り組みがなされてきた。

初期の社会情報システムの目標は、経済活動・社会活動における各種手続きの情報化であった。書類を介在させていた作業を通信ネットワーク経由のやりとりで置き換えることによって、事務処理効率を大幅に改善した。行政情報システムや地理情報システムあるいは科学技術情報や経済産業情報等の各種データベースシステムがその代表例である [1]。その後、物理世界からのリアルタイムデータを収集／加工／蓄積して情報提供する社会情報システムが実現された。代表例が気象情報システム、交通情報システム、地震情報システムである。

現在では、利用者の状況（現在位置や嗜好）に応じて社会生活に必要な情報内容を提供しようとする情報支援システム実現への取り組みが活発になされている [2]。将来的には、個別の社会情報システムが自律的に情報を収集／更新しながら、リアルタイムの分散型コンピュータネットワークで連結され、相互に有機的に機能するような社会情報システムが実現されるであろう [3] [4]。

しかし、社会情報システムの普及は我々の社会生活を便利で豊かにしてくれる反面、いくつかのリスクを抱え込むことになる。そのリスクの一つがシステムの停止による社会的な混乱で

ある。そのような混乱の顕在化を避けるためには、耐フォールト性を向上させた冗長化社会情報システムの構築と運用が重要になる。

このとき、耐フォールト性向上のためには、技術的な側面だけでなく、構築コストの抑制という制約も乗り越えなければならない。特殊な分野（安全保障や人命に関わる用途）を除いて、構築コストが機能や性能の高度化と同程度に重要な設計条件となる。今後は特に耐フォールト性と構築コストの両立が可能なフェイルソフト社会情報システムが重視される。

3 デュアルユース型冗長システム構成方式の概要

3.1 従来の冗長システム

計算機システムの構成要素にフォールトが発生しても、外から見る限りそのシステムの機能が正常に維持されるシステムをフォールトトレラントシステムという。一方、フォールトの発生によってシステムの正常な機能をすべて維持することができなくても、その機能の一部を保持して運用を継続するシステムをフェイルソフトシステムという。フォールトトレラントシステムあるいはフェイルソフトシステムを構築するための技術の総称がフォールトトレランス技術である。フォールトトレランス技術の基本は、多重化による冗長構成である。ハードウェア上の多重化には、静的冗長方式や動的冗長方式があり、ソフトウェア上の多重化には、Nバージョン法がある [5]。

多重化による冗長構成では、同一仕様の構成要素を複数用意し、そのうち1つを稼働させながら、別の少なくとも1つを並列稼働あるいは待機させる場合が多い。故障の発生した構成要素の切替えや切離しを容易にするのが理由である。

また、従来の冗長構成方式は、システムのすべての構成要素を多重化するのではなく、フォールトの発生しやすい部分、あるいはフォールトの発生がシステム機能に致命的な影響を与える部分だけを多重化する。理由は、第一に、すべての構成要素を多重化すると所要リソース

が増大してシステム構築のコストが大幅に上昇するためであり、第二に、ハードウェアの故障発生確率等をもとにして多重化すべき箇所を限定したとしても耐フォールト性の向上に一定の効果があるためである。

3.2 デュアルユース型冗長システム構成方式の特徴

提案する新しい冗長構成方式は次のような特徴を持つ。

- 耐フォールト性を高めるため、データの生成部分からデータの最終出力部分までのすべての処理ユニットに冗長部分を付加して多重化する。所要リソース(システム構築に必要なハードウェアとソフトウェア)を抑えるために、冗長部分では情報量を縮減したデータを扱う。冗長部分は、フォールト発生時にシステム主要部分の予備要素となつて、機能縮退のために利用可能なデータを供給する。
- システム設計の段階で定義した望ましい動作と稼働中のシステムの動作が一致しているか否かを常時照合して機能検証する。
- フォールトを検出したときに、より確かしいデータの選択して機能縮退する。

3.3 多階層モデル表現法とマルチレベルシミュレーション

情報量を縮減し、その縮減したデータ(抽象データ)を扱う技術として、多階層モデル表現法とマルチレベルシミュレーション法を適用する。フォールトトレランスとは直接関連しない技術であったが、複数の抽象レベルで表現する手法がデュアルユース型冗長システムの構築と制御に適していることが分かってきた。

3.3.1 多階層モデル表現法の概要

多階層モデル表現法は、計算機システムの構造と動作を抽象的な表現レベル(抽象的な属性

を表す変数の領域)と具体的な表現レベル(具体的な属性を表す変数の領域)で記述するための手法である[6]。通常、具体的な表現レベルの構造記述と現実の計算機システムの構成要素とが一対一対応するように表現される。抽象的な表現レベルの構造記述は、上位下位対応関係の記述を通して、間接的に計算機システムの構成要素と対応づけられる。主に論理装置の設計の分野で用いられた。

3.3.2 マルチレベルシミュレーションの概要

マルチレベルシミュレーションは、多階層モデルの記述の一貫性を確かめるための検証法である[7]。多階層モデルの記述に一貫性があれば、その表現対象である計算機システム(論理装置)の設計は正しいことになる。

マルチレベルシミュレーションの検証手順の概要は次のとおりである。前提として、検証の対象となる論理装置の多階層モデルの記述が存在しているものとする。すなわち、論理装置は、多階層モデル表現法に基づいて2つの表現レベル(抽象的な上位表現レベル;例えばレジスタトランスファレベル、および下位表現レベル;例えばゲートレベル)で構造と動作が記述され、さらに、それら2つの表現レベル間の論理装置の入出力および状態の上位下位対応関係(上位表現レベルの変数と下位表現レベルの変数との対応関係)も明確に記述されているものとする。多階層モデルに3つ以上の表現レベルがある場合には、上位下位対応関係の記述された2つの(隣り合う)表現レベルに注目した検証を複数回繰り返す。

まず、下位表現レベルの(構造記述を変換して得られた)動作記述から、特定のテストパターンに対する出力結果R1をシミュレーションにより得る。次に、テストパターンを上位下位対応関係を使って上位表現レベルの入力データに変換し、上位表現レベルの論理装置の動作記述からそのデータに対する出力結果R2をシミュレーションにより得る。一方、出力結果R1は、テストパターンの変換と同様に、上位下位対応関係を使って出力結果R1'に変換される。その後で、この変換された出力結果R1'と出力結果

R1 とが照合される。複数の適切なテストパターンに対して照合が成功したとき、(論理装置の)多階層モデルの記述には一貫性があると判断される。

通常のシミュレーションでは設計者がシミュレーション結果を逐一観察して論理装置の正しさを判断しなければならないが、マルチレベルシミュレーションを利用すればその観察と判断を自動的に行えるという利点がある。

3.4 デュアルユース型冗長システム構成手順

まず、デュアルユース型冗長システムの説明で使う用語を次のとおり定義する。

抽象化 元のデータから特定の属性に関する情報を抽出する操作あるいは特定のパターン情報を特定のシンボル情報で代表する操作等の適用により、データの情報量を減らす変換が「抽象化」である。抽象化したデータを元のデータに対して「抽象データ」という。また、データの流れが抽象化と逆方向になる変換を「逆抽象化」という。逆抽象化したデータを「復元データ」という。

第1レベルモジュール 本構成方式が適用された計算機システムにおいて、冗長的な構成にする前段階のシステムの各部分が「第1レベルモジュール」である。当然ながら、フォールトの発生を想定しなければ第1レベルモジュールだけでシステムの機能のすべてを実現できる。「第1レベルデータ」は、主に第1レベルモジュールにおいて処理あるいは通信されるデータをいう。

第2レベルモジュール 第1レベルデータを抽象化したデータが「第2レベルデータ」である。主に第2レベルデータを処理または通信するモジュールを第2レベルモジュールという。

デュアルユース型冗長システム構成手順は次のとおりである。

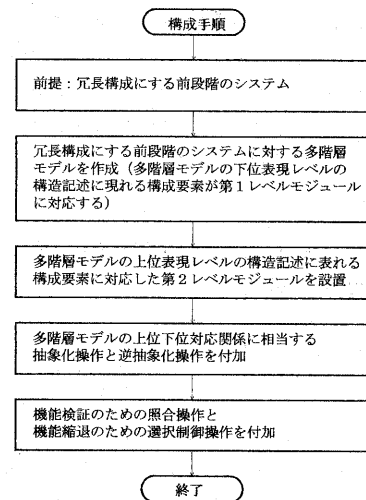


図 1: デュアルユース型冗長システム構成手順

1. 冗長構成にする前段階のシステムの多階層モデルを作成する。このとき、多階層モデルの下位表現レベルの構造記述に表れる各構成要素が第1レベルモジュールとなる。
2. 多階層モデルの上位表現レベルの構造記述に表れる各構成要素に対応した、実体のある第2レベルモジュールを設置する。
3. 多階層モデルの上位下位対応関係の記述に相当する抽象化操作と逆抽象化操作を用意する。
4. 機能検証のための照合操作と機能縮退のための選択制御操作を用意する。

上記の構成手順に従って構築したデュアルユース型冗長システムのブロック図を図2に示す。情報量を縮減したデータを扱う冗長部分(第2レベルモジュール)を設置し、データの生成部分からデータの最終出力部分までを一貫して多重化する。第1レベルモジュールとその抽象的な動作(すなわちシステムの機能)を実現した第2レベルモジュールが同時並行的に実行可能な状態で存在するため、システム稼働中にマルチレベルシミュレーション相当の機能検証を常時実行することができる。さらに、検証時の照合の失敗に基づいてフォールトを検出し、

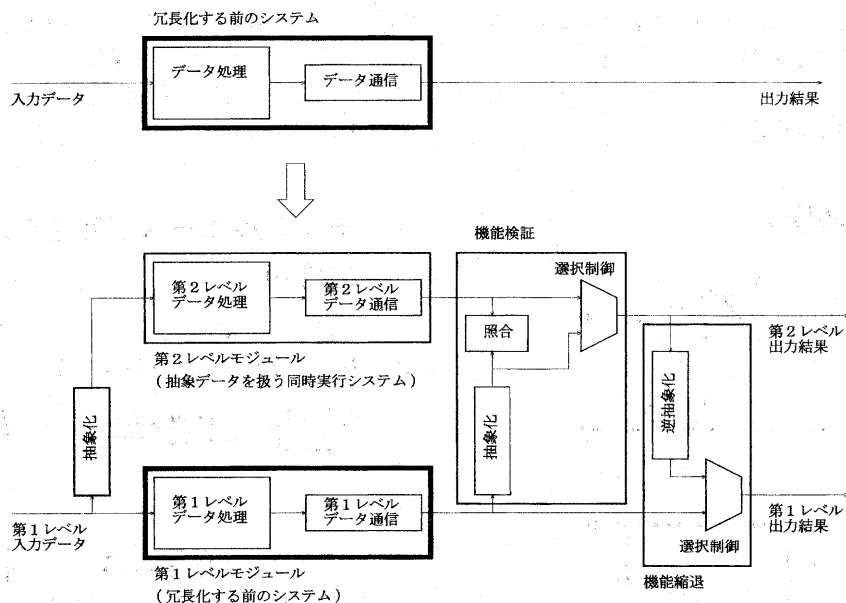


図 2: デュアルユース型冗長システムのブロック図

機能縮退を実行することができる。

3.5 機能検証と機能縮退

図2のデュアルユース型冗長システムにおいて実行される、機能検証と機能縮退について説明する。

3.5.1 機能検証

機能検証は、2組の等価な処理ユニットに等価なデータを入力すれば等価な出力データが得られるという原理を利用する。抽象化によって等価なデータに変換し、照合操作が等価性を調べる。等価な出力データが得られなかった場合、2組の処理ユニットのいずれかにフォールトが発生したとみなす。

図2の第1レベルモジュールと第2レベルモジュールは扱うデータの情報量の違いを除いて等価である。特定の入力データが第1レベルモジュールに入力されると、それと同時に入力データは抽象化されて第2レベルモジュールにも入力される。第1レベルモジュールと第2レ

ベルモジュールが同時並行的に動作した後、第1レベルモジュールの出力データと第2レベルモジュールの出力データが照合される。

照合は、第1レベルモジュールの出力データを抽象化した抽象データと第2レベルモジュールの出力データに対して実行される。照合が成功すれば「フォールトなし」、照合が失敗すれば「フォールトあり」となる。

ここで、入力データの処理結果を抽象化したデータと入力データを抽象化したデータの処理結果を照合する手順はマルチレベルシミュレーションのそれと同じである。マルチレベルシミュレーションでは、下位表現レベルの構造の動作が上位表現レベルの動作(すなわち機能)を満足しているか否かを確認している。

同様に、上記照合もシステム設計の段階で定義した望ましい動作(すなわち機能)と稼働中のシステムの動作が一致しているか否かを確認していることになる。

また、照合によるフォールト検出に加えて、第1レベルモジュールと第2レベルモジュールにそれぞれ独立して設けた誤り検出ユニットもフォールト検出を行う。

照合と誤り検出ユニットの結果を組み合わせることにより、各種のフォールト（ハードウェア故障、ソフトウェアのバグ、設計ミス、過負荷、輻輳等）を検出する。

3.5.2 機能縮退

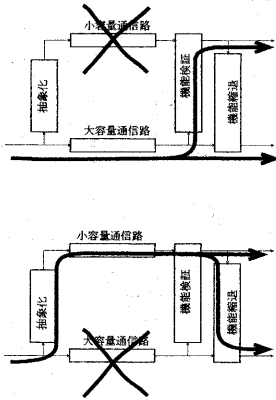


図 3: 機能縮退

フォールト検出に基づいてより確からしいデータの選択制御を行い、その結果として機能縮退する。

選択制御のため、処理対象のデータにはメタデータを付与する。メタデータは抽象化や逆抽象化およびフォールト発生に基づいて単調に減少する値である。

機能縮退に関しては、第1レベルデータの出力が重要になる。第1レベルデータの出力結果として、第1レベルモジュールにフォールトが検出されなければ第1レベルモジュールの出力データをそのまま選択し、第1レベルモジュールにフォールトが検出されれば逆抽象化によって第2レベルデータから復元されたデータを選択するように制御される。

注意すべき点は、復元データの情報は、抽象化と逆抽象化を伴っているもので、本来の第1レベルモジュールのデータのそれに比べて少ないことである。そのため、それ以降の処理または通信によって得られた結果にはより多くの誤差が含まれるようになる。

すなわち、システムは、上記のような選択制

御によって、第1レベルモジュールでフォールトが発生したときに出力結果に誤差が増える状態に移行という意味で機能を縮退させながら、動作を継続する。

4 デュアルユース型冗長システムの応用

デュアルユース型冗長システムの代表的な応用場面は、次の2つに分類される。

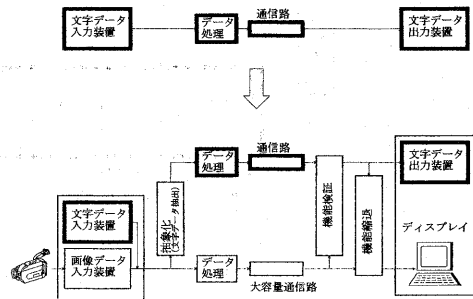


図 4: テキスト情報処理を主体にしたデュアルユース型冗長システム構成

1. 情報量が比較的小さいテキスト情報処理を主体としたシステムにおいて、補助的な画像情報を付加することで情報支援環境を高度化した応用（図4参照）。フォールトが発生してもテキスト情報処理だけは継続するような耐フォールト性を提供する。
2. 情報量が比較的多いセンサ情報処理や画像情報処理を主体としたシステムにおいて、処理される情報内容の重要度に違いがある応用。フォールト発生時には重要な項目だけを選択的に処理することで機能縮退する。

4.1 実験例

デュアルユース型冗長システムの冗長化の効果を調べる目的で上記「画像情報処理を主体としたデュアルユース型冗長システム構成」に基

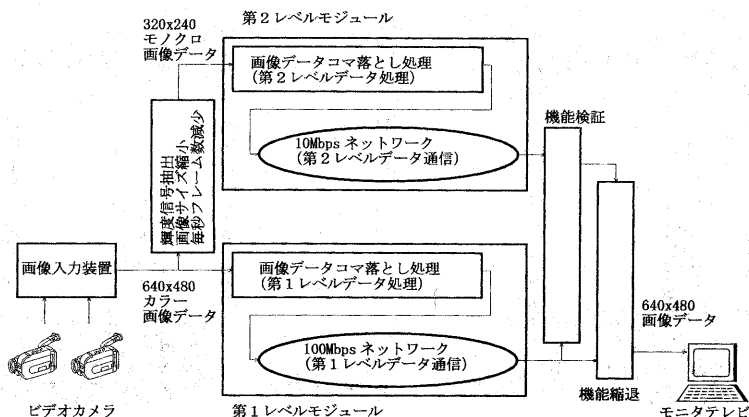


図 5: 冗長化した実験システムの構成

づく実験を行い、機能検証と機能縮退の有効性を確認した。

4.1.1 実験システムの構成と環境

冗長化するシステムは「特定の施設への来客者を知るために施設入口に複数のビデオカメラを設置し、距離的に離れた受付や待機場所に置いたモニタテレビに来客者の姿を表示させるシステム」である。

フォールトは、通信路の切断（ネットワークケーブルの切断や通信装置の故障）を想定する。

冗長化したシステムの構成を図5に示す（なお、図5は代表的な応用場面の中の画像情報処理を主体とした構成の例となっている）。

第1レベルモジュールは、動画から静止画に変換した画像データを蓄積し転送する機能を持つ。第1レベルモジュールの通信路は100Mbpsを上限とするネットワークである。第1レベルデータは640x480画素カラー画像データである。

抽象化は、次の3つの操作によって行う。

- ・ カラーデータから輝度信号を抽出してモノクロデータへ変換
- ・ 1秒当たりのフレーム数を1/10に縮減
- ・ 画面サイズをXY軸方向に1/2に縮減

第2レベルモジュールは、第1レベルデータの画像データから情報量を縮減した、320x240

画素モノクロ画像データを処理する。第2レベルモジュールの通信路は10Mbpsを上限とするネットワークである。

逆抽象化は、次の2つの操作によって行う。

- ・ 1秒当たりのフレーム数が10倍に補間
- ・ 画素数をXY軸方向に2倍に拡大

モニタテレビは機能縮退モジュールの選択制御の出力結果を映像として表示する。

4.1.2 実験結果

実験システムの典型的な動作例を次に示す。

（動作例1 [機能検証]）

フォールトが検出されていない場合（正常時）：モニタテレビはビデオカメラからの映像を640x480カラーで表示。機能検証のための画像データの照合を常時実行し、「フォールトなし」をコンソールに出力。

（動作例2 [機能縮退]）

第1レベルモジュールでフォールトが発生した場合（100Mbpsネットワークケーブルの切断）：モニタテレビはビデオカメラからの映像を（320x240モノクロデータから復元して）640x480モノクロで表示。「第1レベルモジュールにフォールトあり」をコンソールに出力。

（動作例3）

第2レベルモジュールでフォールトが発生した場合（10Mbpsネットワークケーブルの切断）：モ

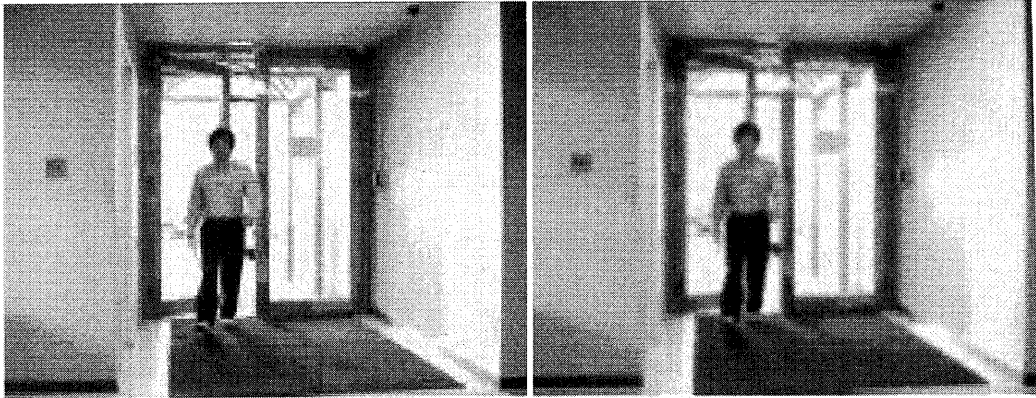


図 6: 正常時の画像 (左: 640x480 カラー) と縮退した画像 (右: 320x240 → 640x480 モノクロ)

ニタテレビはビデオカメラからの映像を 640x480 カラーで表示。「第 2 レベルモジュールにフォールトあり」をコンソールに出力。

上記のとおり、実験環境において機能検証と機能検証は目標どおりに動作した。

5 おわりに

デュアルユース型冗長システムの利点を整理すると次のようになる：

- 情報量を縮減したデータを扱う冗長モジュールを多重化することで、所要リソースの増大は抑制される。
- 個別に設置した誤り検出ユニットおよび抽象データの等価性の検証結果を利用することによって、ハードウェアの故障はもちろん、ソフトウェアのバグ、設計ミス、過負荷、輻輳等を含む広義の障害を検出することができる。
- フォールトが検出された場合に、その発生要因や発生箇所に応じて、抽象データから復元されたデータを出力結果とすることで、広義の障害に対して機能縮退することができる。

以上の利点により、所要リソースを抑制して、正常時にシステム機能検証を実行しフォールト発生時に機能縮退を実行する冗長システムの構成が容易になる。

今後は、図 2 の基本構成を拡張して第 3 レベルモジュール構成や縦列接続構成とする方法について明らかにしたい。

参考文献

- [1] 上野滋. 情報化の進展と社会システム. 情報処理, 27(10):1098-1104, 1986.
- [2] 中島秀之, 石田亨, 西田豊明, and 久野巧. サイバーシティ計画. コンピュータソフトウェア, 16(5):484-490, 1999.
- [3] L. M. Branscomb and J. H. Keller. *Converging Infrastructures*. MIT Press, 1996.
- [4] N. R. Jennings and M. J. Wooldridge. *Agent technology*. Springer, 1998.
- [5] 当麻喜弘. フォールトトレラントシステム論. コロナ社, 1990.
- [6] 久野 巧. 設計問題解決のための多階層表現法. 電子技術総合研究所口報, 57(2):1-22, 1993.
- [7] 久野 巧. マルチレベルシミュレーションによる多階層モデルの検証. 電子情報通信学会論文誌, J76-D-II(4):908-913, 1993.

小型情報端末用 DataSlim2 の空間光通信方式

林 新[†] 伊藤 日出男^{†‡}

概要 空間光通信は、空間を伝播する光のエネルギーの一部を利用して信号を伝える通信方式である。従って、伝送用の光エネルギーが空間に存在する無線伝送の特徴と情報伝送媒体として光を使う光ファイバ通信の特徴を合わせ持つと言える。我々は、このような空間光通信技術と位置を基づく通信技術を使って、近距離閉空間での情報サービスによる行動支援できる携帯通信端末 MyButtonTMと室内レーザレーダ i-lidarTMについての研究を進めている。一方、DataSlim2 は反射型液晶ディスプレイを有する名刺サイズの PDA である。この PDA は、アドインアプリケーションソフトウェアを開発することにより、所望のプログラムを実行できる。そこで、液晶ディスプレイの光散乱反射板を、再帰光反射シートに変更して、画面をプログラムで制御すれば、空間光反射率変調機能を実現することができる。また、DataSlim2 は情報環境の中で、極めて低い消費電力で長時間動作できるため、室内レーザレーダ通信システム用の携帯情報端末 MyButton として用いることが考えられる。

キーワード: DataSlim2, 空間光通信, 反射率変調, データ伝送

Spatial optical communication technique of the DataSlim2 for compact information terminal

Xin LIN[†] and Hideo ITOH^{†‡}

Abstract: Spatial optical communication is a signal transmission technique by using optical energy. It not only has characteristics of wireless transmission, but also has characteristics using optical fiber communication. Based on the spatial optical communication technique and the location-based information service technique, an indoor laser radar communication system, i-lidarTM and its terminal equipment, MyButtonTM has been developing for human information support. On the other hand, the DataSlim2 is a compact Personal Data Assistant (PDA) with a liquid crystal display. It is used as a handheld communication terminal, MyButtonTM for data uploading in the indoor laser communication system. The spatial optical modulation function of the DataSlim2 has been achieved by using a software development kit, and changing its light-scattering-reflection sheet of the liquid crystal display into a corner-reflection liquid crystal display. Data transmission characteristics and reflectivity modulation characteristics of the DataSlim2 as a communication terminal are measured and evaluated.

Keywords: DataSlim2, optical communication, reflectivity modulation, data transmission.

[†] 産業技術総合研究所サイバーアシスト研究センター, Cyber Assist Research Center, AIST

E-mail: x.lin@aist.go.jp, hideo.itoh@aist.go.jp

[‡] 科学技術振興事業団 CREST, CREST, JST (Japan Science and Technology Corporation)