Applying TRIZ/USIT to A Social & Technical Problem: Auto-locking Door System of Apartment Building

Toru Nakagawa and Arata Fujita

Osaka Gakuin University, Japan

Abstract

Students' discussions were guided with TRIZ and USIT to solve an everyday problem. The security problem of auto-locking door system of apartment building needed to be solved in the human psychology and social behaviour first and then must be ensured in the technology. Mechanical & physical system of door has been shifted to IT & logical system.

1. INTRODUCTION

This is a case study report of solving an everyday problem by guiding students' discussions and constructing a system of conceptual solutions. TRIZ and its simplified & unified process USIT have been used in this study in a rather informal manner.

In my thesis-work class of Osaka Gakuin University, every student is required to find and solve an everyday problem for his/her thesis. Since our undergraduate students in the Faculty of Informatics do not have technological specialty yet, we think common and familiar problems in our daily life are suitable to address. I advise the students to have problems individually but to discuss and work on the problems together for stimulating ideas and understanding more deeply.

The present problem is related to the security of an auto-locking door system at the entrance of an apartment building. Arata Fujita is living in a big apartment building with his parents in Osaka City and feels some insecurity with the door system. It is widely known that the current standard technology of auto-locking door system does not prevent unauthorized persons from entering. Any person can enter the door simply following a resident by pretending to be a resident.

In the seminar class, I guided the discussions by Fujita and other four students on the causes of the problem and on possible solution ideas. Discussions were mostly recorded with Post-it Notes and summarised step by step. The thesis work by Arata Fujita was posted in [1].

Then Toru Nakagawa worked further to build up the conceptual solution. The whole process of analyzing the problem, generating ideas, and constructing a solution was reported by Nakagawa and Fujita in the 3rd TRIZ Symposium in Japan, 2007 [2]. Presentation slides in Japanese and in English, and a full paper in Japanese are presented/published in the Proceedings and are also posted in my Web site "TRIZ Home Page in Japan".

The present paper is based on the work [2] and rewritten in English so as to clarify our thinking.

2. SETTING THE PROBLEM

2.1 Start of the work

Arata Fujita brought in this problem as his thesis topic. At that time there were several criminal news stories broadcast on TV. A child had been fallen from a high storey of an apartment building; a girl was injured by somebody in the corridor of a high-rise residence, etc. Unknown criminals are supposed to enter the residential building even though the entrance door has a standard auto-locking door system.

Everybody knows from their experience that typical auto-locking door systems are not secure enough for preventing unauthorized persons from entering. Any person can easily slip in through the open door just after a preceding resident. It is difficult for us to stop such a person, even if we are on the spot and suspicious about the person.

So we have chosen this as a good problem to solve.

2.2 Confirming the focus of the problem

Typical apartment buildings have various security means. Not only the entrance door locking system, but also the overall structure of the building, structure of elevators and staircases, concierge and monitoring system, interphone between entrance and flats, door locks of each flat, etc. For the nature of security, we have to maintain all these means one by one.

Nevertheless, we have found in discussion that the entrance door lock system is the most important means and yet has the commonly known defect.

In a typical auto-locking door system, the residents are requested to show authentication of entering the door by means of keys, ID cards, or even finger prints. Visitors, on the other hand, are typically requested to talk on the interphone with the resident in the flat for obtaining temporary authentication. The resident, talking (and viewing) through the (video-)interphone, may send the unlock-door order to the system.

However, an unauthorized person can slip in through this entrance simply by following a preceding resident who opened the door. A closing door will open again when the person pushes it lightly. Once such a person enters there can be various forms of risks.

With this understanding, we have decided to focus our efforts on the problem of solving the security defects of the auto-locking door system at the entrance of the apartment building.

2.3 Problem definition

We have used USIT (Unified Structured Inventive Thinking) [3] as the main process for problem solving. The discussions at the initial stage may be summarized in the style of Problem Definition in USIT.

(a) Unwanted effect

At the entrance of an apartment building, unauthorized persons can easily enter through the auto-locking door system and threaten security.

(b) Task/goal

To ensure the security of the apartment building by preventing unauthorized persons from entering the auto-locking door.

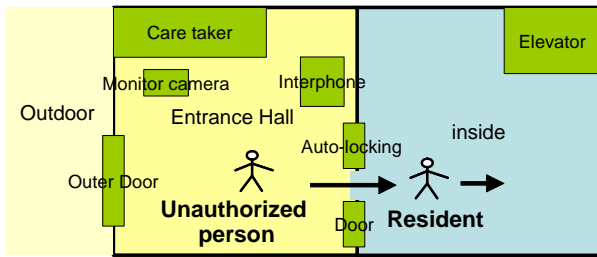*(c) Sketch of the problem situation*

Fig. 1. Problem situation

(d) Plausible root causes

The unauthorized person, behaving like a resident, can enter the open door by simply following a resident.

(e) Minimum set of relevant objects

Entrance door, lock control system, an unauthorized person, a resident who goes ahead

3. ANALYSIS OF THE PROBLEM

In the stage of problem analysis, we have used various methods in a flexible way. The analysis processes are described in a logical way as follows:

3.1 Space and time characteristics analysis

Typical characteristics in space are drawn in the sketch, Fig. 1. The inner door has the auto-locking system. While the door is open after the entrance of a resident, an unauthorized person can enter by walking a few meters behind.

The duration of the door opening is typically about 10 seconds. The resident, sometimes with baggage and with children, can enter the door smoothly and safely. The heavy door opens and closes slowly. The closing door can be reopened easily by pushing it back lightly.

All these operations are performed for the sake of safety as well as security.

3.2 Current security methods in the auto-locking door system

Current security methods in common and in advanced systems are discussed and surveyed at this stage.

(a) Mrthods of identifying a resident

There are various ways of proving to be a resident for authentication. Possessing/showing keys, card keys, IC cards, RFID, etc. Biometric authentication with finger prints, palm vein patterns, face recognition, etc. may also be used in some advanced cases.

(b) Methods for visitors

Visitors are not allowed, as a rule, to enter without being approved by a resident. Typically, at the video-interphone just before the inner door, the visitor pushes the apartment number of the resident to be visited. The resident, talking with the visitor on the phone and checking the person through the video, may approve the entrance and send a signal to the control system to unlock the door. If the resident does not approve, the door will not be opened.

(c) Methods for opposing unauthorized entrance

As stated in 2.3, the present problem is the entrance of an unauthorized person through the 'already open door'. In some cases, a concierge or a guard watches and can prevent it. In many other cases, video monitors are set and the monitor screens are either viewed in real time or recorded for later reviewing. These devices are either expensive in human resources or are not effective if they are unattended for a period of time.

3.3 Thinking from the side of offenders

When we consider security, we usually think how to prevent from, protect or defend against something wrong. But thinking in the other way, i.e. from the side of offenders, is also useful. Such a way of thinking is called subversion analysis in TRIZ, but actually has been a well known method in the art of war since ancient China.

Thus in the class, I guided the students to temporarily take the position of offenders and to think how to enter the door without being suspected. I encouraged them to keep saying their ideas and recorded the ideas on Post-it Notes. Then the cards are posted on the whiteboard and are grouped and rearranged according to their intentions. This is a quick and informal application of the KJ Method (or Affinity Diagram Method) originally developed by Jiro Kawakita [4].

Such offending ideas may be summarized (in the upper-level summary cards of the KJ Method) as:

- Unauthorized person should behave just like a resident.
- He can slip in through the open door at the proper time.
- Once inside the door, the person can go anywhere and can do anything.

3.4 Root-cause analysis (1) duration of open door

As discussed in the space and time characteristics analysis, the rather long duration of the door being open is clearly one of the root causes of the present problem.

In the door operation, safety is the crucial criterion even over security; thus the door should not be shut quickly. This is the fundamental contradiction in this problem.

3.5 Root-cause analysis (2) psychology of the residents

From the beginning we noticed that the residents allow the unauthorized persons to slip in through the open door. The residents sometimes suspect such persons and some other times do not suspect them at all. So we need to analyze the root causes of the psychology of the residents.

I guided the students to talk about their own thoughts and feelings in such a situation, and I asked them 'why?' from time to time.

The main points may be summarized as:

- Residents allow the unauthorized persons to get in.
- Because I thought he/she would be a resident.
- Because I didn't think he/she a malicious person.
- Because we cannot distinguish whether a person is malicious or not.
- Because usually we assume our community is formed of good people.
- We don't know what to do even if we suspect the person to be malicious.
- If we suspect the person to be malicious, and he/she is not, we could be in trouble

In essence, the present system implicitly requests the residents to judge whether the unfamiliar person is malicious or not, and the residents do not want to take the

risk of misjudging and getting into a trouble. The essence of the difficulty is that the present system implicitly requests the residents to make an impossible judgement.

3.6 Root-cause analysis (3) happening of meeting two parties

In the above discussion, there arose a question 'Even though we understand the need to be aware of suspicious cases, we do not know what to do.'

So we went further to discuss 'what should we do when we happen to meet other people at the entrance door?' During this discussion it became clear to us that the (social) rule for the present auto-locking door system is not effective for (or does not cover) such a case. The present system does not clearly say what to do; this means that there is no standard social manner applicable in such a case.

Suppose we meet a person at the entrance whom we do not know to be a resident or not. In order not to allow an unauthorized person to enter, we should behave at least not to assist him to enter. But it means not behaving kindly and also means behaving unkindly.

Formally, we should say (either explicitly or implicitly) the person, "Please wait for a while till the door is closed. Then get the authentication on the control board and open the door for yourself." This statement is quite different from the kind/polite way we usually show in case of a public entrance. This difference is so large for ourselves and for the person that it would be possible to make the person angry and run into a trouble.

Thus one more root cause here is the lack of the social rule for the cases that two (or more) parties meet by chance at the auto-locking entrance door of apartment buildings.

3.7 Understanding the overall structure of the problem

During these analyses from multiple points of view, we have memorized various facts, observations, views, solution ideas, etc. in a large number of Post-it Notes. For the purpose of understanding the overall structure of the problem, we first applied the grouping technique of the KJ Method and obtained 20-30 higher-level cards.

Then we displayed them all on the board and tried to construct the overall structure of the problem. The KJ Method and the RCA+ Diagram Method [5] were useful in this process. The result is shown in Fig. 2 [1].

The cards (1) - (4) express some of the present methods. The cards (5) - (17) are related to the description of the present problem and its causes. The arrows among them show the cause-effect relationships in the way of RCA+ (though not rigorously). The cards (18) - (27) describe some solution ideas.

Fig. 2 contains rich information in a compact and yet structured form. The whole problem analysis can be understood by reading the cards in the order shown in ( ) together with the relationships between them.

3.8 Understanding the essence of the problem

Summarizing the whole analysis, the essence of the problem can be described as follows [by using the card numbers shown in Fig. 2].

The principal reason for the threat to the security of apartment buildings at the entrance door is the fact (7):

- '(7) Unauthorized person can enter the door easily at a good timing when it is open (by a preceding resident).'

This threat (7) is not avoidable due to three main reasons. They are:

- First, '(8) The auto-locking door is kept open/unlocked for about 10 seconds.'

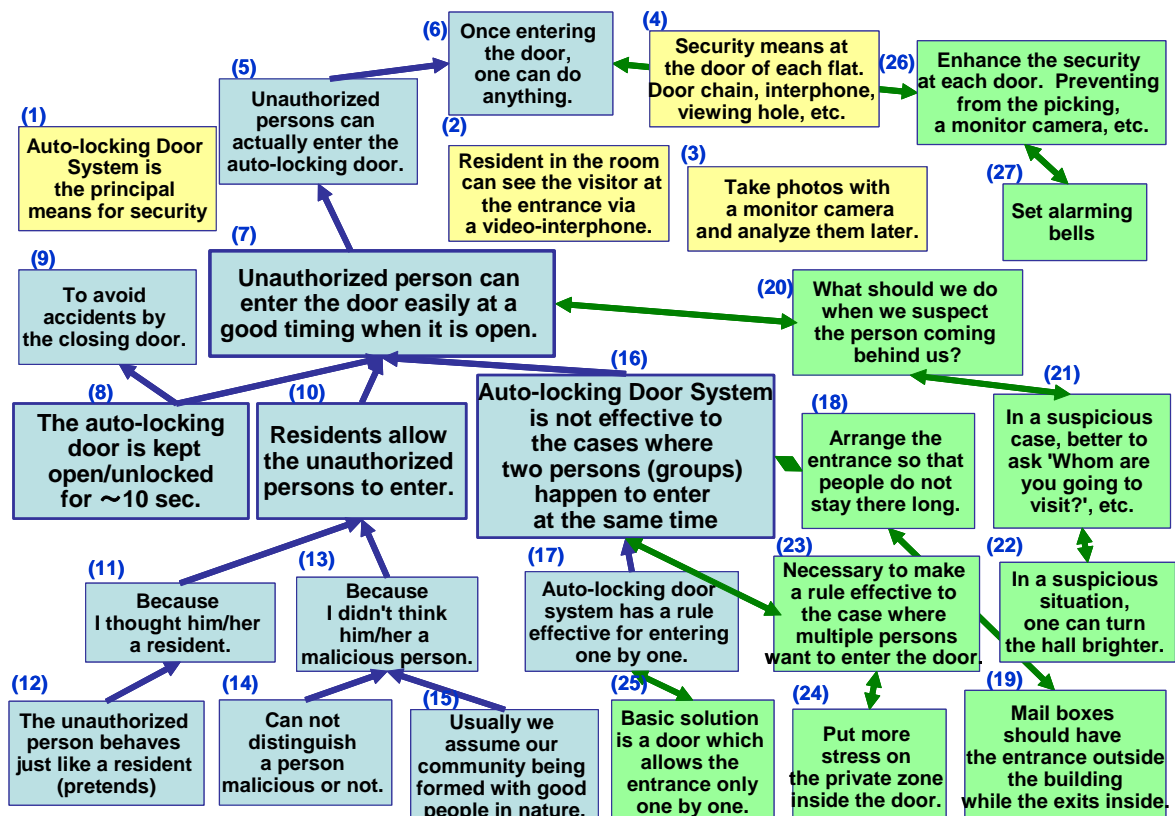- Second, '(10) Residents allow the unauthorized persons to enter.'

Fig. 2 Overall structure of the problem

- Third, '(16) Auto-locking door system is not effective to the cases where two persons (or groups) happen to enter at the same time.'

Thus, clearly, we have to eliminate all these defects in our design of a new solution system. The above three defects are related to technology, psychology, and social behaviour, respectively.

4. GENERATING IDEAS AND CONSTRUCTING SOLUTION CONCEPTS

During the analysis we have obtained various solution ideas as partly shown in Fig. 2. This kind of idea generation is a natural process, because when we find specific causes, defects, weak points, etc. we often find solution ideas, effective or not, as immediate reactions.

As the next step, we have examined such ideas more closely and expanded our range of solution ideas. During this stage we have tried to figure out ideas so as to expand the current state of technology and to think of new approaches in relation to our psychology and social behaviour.

We have used Post-it Notes again to memorize fragments of ideas and solution directions. By considering the relationships between such ideas, we have revealed possible logical structures among the solution ideas.

4.1 Solution ideas to the problem of 'Residents allow them to enter'

Among the three main causes of problem, we have found the problem related to the residents is most basic.
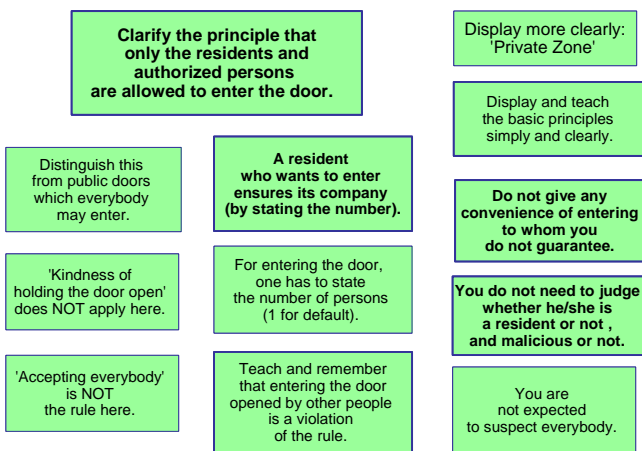
Fig. 3 shows the cards related to this problem.

Fig. 3. Solution ideas related to the residents

(a) Distinguishing Private Zone Entrance from public one

The real basis of the solution was found to clarify the principle of the Private Zone. 'Only the residents and authorized persons are allowed to enter the entrance door of the apartment building.'

Of course this principle is understood by residents and visitors to some degree, but it needs to be emphasized more. Distinguishing private zone entrance from public zone entrance, e.g. the entrance door to a department store or a station building, is important. Holding a door open to an unfamiliar person coming behind is a polite and good manner for the public zone entrance but a dangerous and violating behaviour for the private zone entrance.

When a resident opens the door, It is natural and efficient to allow his/her company to pass through without any further handling of the lock. Whereas the resident should not allow any other non-residents.

(b) What the system should request the residents to judge?

The current system implicitly requests the residents to judge whether the person coming behind is a resident or not, authorized or not, and malicious or not. All these types of judgement are actually impossible, and hence the implicit requirements are not effective. So, in our solution, we have to avoid these types of judgement.

The resident can guarantee only his/her company. Thus the system should request the resident to show his own evidence (e.g. a key) and only to state the people under his/her guarantee, or more simply the number of such people.

Hence it is clear that any person, outside his/her company, who does not try to get authentication is violating the rule. The resident can recognize/judge it. However, requesting the resident for doing any defending or warning action is a different story. Defending the security and warning to the violating person are the jobs of not the (preceding) resident but the system itself.

In this manner we should eliminate the contradiction of implicitly requesting the residents to do impossible judgement and to take a risk of unwanted trouble.

4.2 Solution ideas to the problem related to the social rule.

As we have found before, we must make the social rule clear what we should do when two parties of people happen to enter the Private Zone entrance at the same time.

(a) Inconvenient rigorous rule does not work

In order to ensure the security rigorously in the present system, we should assume a rule that every party must get the authentication for themselves. But the authentication process can be performed only when the door is closed and locked. This means the second party may not enter the door opened by the first party but must wait until the door is closed and locked and then must get authentication from the system for themselves. Many people feel this rule ridiculous and want to pass through the open door without getting the authentication.

(b) Authentication need to be processed at any time

Thus our solution direction is clear. Any party should be able to get the authentication at any time without depending on the door being open or closed. This means that even when the door is open the second party should be able to make the authentication process as usual and should be allowed to pass through the open door following the first party.

In this manner, any person or party who is going to pass through the open door without trying its own authentication process can be regarded as violating the rule. Such violation can be noticed by the (preceding) resident, even though the resident should not be requested to give a warning to the violating person directly. Noticing the violation and giving warning to the violating person should be the job of the system.

(c) Our system need to be intelligent

For making such a process possible without losing the security, the new auto-locking door system must be intelligent. But at the same time we should not want it to be intelligent at the ideal (i.e., infeasible) level. At the moment we assume the authentication process uses keys, card keys, IC cards, finger prints, etc. for the residents. One step further in the intelligence of the system may be

its ability to count the number of people who have entered through the door.

With this consideration, our new system should be able to accept the number of people in the party during the authentication process and should be able to allow the entrance of such a number of people together. It should be able to either forbid, prevent, warn, or notice the entrance of people exceeding the number.

(d) The new social rule

In summary, the new social rule must simply be: 'Every party must get the authentication for themselves, regardless of the door being open or closed.' Thus, trying to enter the open door without getting authentication is a violation of the rule. We should display this rule clearly and also make it widely known as a part of our solution.

4.3 Solution ideas to the problem of long duration of open door

(a) Confirmation of the safety-first principle

As we noticed before, the current policy of door operation is: 'The large and heavy doors are moved slowly to open or close and are operated on the safety side so as to avoid any accident or injury.' This policy is applied widely now as the results of lessons from many serious accidents beforehand.

At the initial stage of the present work, we had some ideas of operating small, light parts of the doors in much quicker mode. But finally we have abandoned such a direction of solution because of possible accidents and injuries.

Another possibility of solution direction was the gate system which enforces the entrance of people one by one. Such systems are used, for example, at the entrance gates of stations, theaters, amusement parks, etc., and typically related to some tickets. We have not chosen this direction, because it seems unsuitable for apartment buildings. *Note. 1

Thus our solution direction is to accept the current type of large and heavy doors operated slowly for the safety reasons and to make the door system intelligent.

Fig. 4 shows the cards generated during the discussions of the solution ideas.

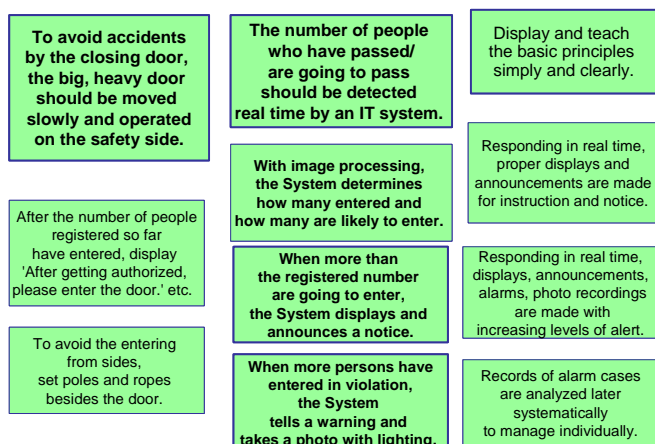|		
To avoid accidents by the closing door, the big, heavy door should be moved slowly and operated on the safety side.	**The number of people who have passed/ are going to pass should be detected real time by an IT system.**	Display and teach the basic principles simply and clearly.
After the number of people registered so far have entered, display 'After getting authorized, please enter the door.' etc.	**With image processing, the System determines how many entered and how many are likely to enter.**	Responding in real time, proper displays and announcements are made for instruction and notice.
To avoid the entering from sides, set poles and ropes besides the door.	**When more than the registered number are going to enter, the System displays and announces a notice.**	Responding in real time, displays, announcements, alarms, photo recordings are made with increasing levels of alert.
	When more persons have entered in violation, the System tells a warning and takes a photo with lighting.	Records of alarm cases are analyzed later systematically to manage individually.

Fig. 4. Solution ideas related to the door operation

(b) Alternative actions on detecting a case of violation

One of the important choices in designing the entrance door operation system is the action to take when the system recognizes a person just violating the rule. Several alternatives may be:

- Physically forbidding the violation, i.e. physically block the person by closing the door or by any other means.
- Preventing the violation, e.g. giving an alarm or warning just before the violation and stopping the person to actually entering the door.
- Alarming the violation, e.g. when a violation occurs make a large alarm sound to call for attention by the caretaker, etc.
- Warning the violation, e.g., giving a warning message/signal to the person just before or after the violation
- Recording the violation, e.g., recording the violating action with a video camera or taking a photo of the violating person with flash light
- Noticing the violation, e.g. make a notice to the violating person that the violation is detected and recorded with video or photo.

We have decided that physically forbidding the violation is not a practical goal for us to pursue and is not necessary in our case because entering the door does not give any harm yet to the residents and there are some more safety means. On the other hand, all other actions listed above are supposed to be effective and hence should be introduced in the new system.

(c) Allow a declared number of people to enter

Our main idea so far obtained in sections 4.1 and 4.2 is to allow the entrance of a party (i.e. one or more people) by the authentication of the leader while the authentication should be processed at any time. For keeping the security in this process, we need to recognize the end of the party members. A simple, feasible, and yet effective way of achieving this is to count the people who enter through the door.

Thus the system request the resident (and also the normal visitor) to declare the number of people accompanied (e.g., 1 when the resident is alone). And the system counts the number of people who enter and tries to 'close' the door when the declared number of people have entered.

Here we must be careful that closing the real door quickly is not possible mechanically, not appropriate for safety reasons, and even not necessary because we are not trying to physically forbid the entrance by an extra person. So our solution here is to introduce a logical & virtual door closed to any person who tries to enter afterward.

(d) Virtual & logical door with intelligence

We have just reached the essence of our new system. We have a logical and virtual door (over the physical and real door) which is opened to a declared number of people by the valid authentication process and is closed just after the number of people have entered the door. The open/closed status of the logical door should be displayed at the door and guide/warn the people to follow the rule.

A simple mechanism of counting the number of people who entered is a (infrared) sensor system. This assumes a narrowed entrance passage to count the people one by one by means of infrared beams from the side.

A more advanced mechanism is the use of video monitoring with intelligent software of real-time image processing to trace the movement of multiple people and to count the number of people who have entered the door. This system can be used with relatively wide, open-style doors suitable for residential building. The current state of arts in image processing certainly has the capability of implementing such a system.

(e) Separation of residents and visitors in space

Another idea is to separate the zones for the authentication process between the residents and the visitors. (*Note 2.) For example, the residents should operate the control panel on the left to the door while the visitors on the right to the door. Thus any person who comes in the entrance hall has to declare first whether he/she is a resident or not by its standing position. Strange movement between these two sides will become apparent to the people around and to the system.

This separation is also useful because the visitors take time to call the resident in a flat with the interphone and to get authenticated by the resident whereas the residents can get authentication quickly just by showing their evidence, e.g. keys, cards, etc. and pushing the number of accompanied members.

5. CONCEPTUAL SOLUTION OF A NEW AUTO-LOCKING DOOR SYSTEM

On the basis of the ideas generated above, we have built a consistent set of conceptual solutions addressed to the present problem. We propose here an intelligent auto-locking door system for the secured entrance of apartment buildings. The system is schematically shown in Fig. 5 and explained in the followings:
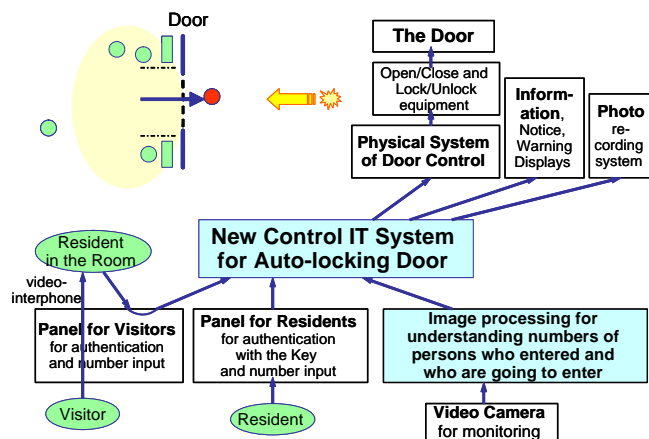

Fig. 5 An intelligent auto-locking door system for the entrance at apartment buildings.

5.1 Display the rules and guidance clearly

(1) Permanent display in front of the door

- "Private Zone Inside This Door."
- "Residents and authorized persons ONLY are allowed to enter."

(2) Permanent display in front of the door:

- "You (or your party) must get authentication for yourself. Authentication process will be accepted whenever, independent of the door Open/Closed."
- "Even while the Door is Open, you must get the authentication. Entering the Door without authentication is a violation of the rule and law."

(3) Permanent display in front of the door:

- "Residents: <== Use the panel Left to the Door."
- "Visitors: Use the panel Right to the Door. ==>"

(4) Permanent display at the Left Panel:

- "For Residents: Insert your key, Input the number of your party at moment (1 if you are alone), and turn

and remove the key. After getting the approval, you may enter through the door."

(5) Permanent display at the Right Panel:

- "For Visitors: Press the residence number you want to visit and talk with the resident via the video interphone. Get an approval by the resident, telling the number of persons of your party. After the indicator turns green, please enter the door."
- "Without turning the indicator green, YOU MUST NOT ENTER the door even if it is open."

5.2 Hardware and software components of the system

(6) Physical operation of the door and the lock:

The Door itself is operated slowly and safely, just as usual at present, by using the current mechatronic control system: It opens slowly, closes slowly, is unlocked for about 10 seconds, and re-opens in case of any obstacle for the sake of safety.

(7) An intelligent IT system controls the whole system:

The new IT system must have the real-time ability of counting the number of people who enters through the Door, and working with the panels for authentication it gives orders to the physical door control system. It is desirable to count the number of entering persons by use of an image processing method.

(8) Video monitoring and image processing:

The IT system monitors the people outside and inside the door with video camera(s) and counts in real time the accumulated number (e) of persons who have entered the door (since the door is opened this time) and the number of persons who are going to enter the door.

(9) Authentication system

The authentication system approves the keys, ID cards, etc. shown by the residents and accepts the declared number of members of the party. It also accepts the order of approval of a visitor party by the resident via dedicated lines from the residence. The authentication system tells the IT system its approval of declared number of people in real time. Thus the IT system recognizes the accumulated number (a) of approved persons (since the door is opened this time).

5.3 Software control of the virtual and real doors

(10) Main control parameter: $p = a - e$

The main parameter for controlling the door operations and displays is defined by $p = a - e$. This is 'accumulated number of authenticated persons' (a) minus 'accumulated number of persons entered the door' (e); thus it means the number of persons left to enter with authentication. This parameter is known in real time in the IT system.

(11) While $p > 0$, Open-Door.

While $p > 0$, the IT system gives the Open-Door direction to the mechatronic door control system and displays 'Please enter' at the top of the Door.

(12) While $p = 0$, Close-Door, Normal state.

While $p = 0$, the System gives the Close-Door direction and displays 'Please get authentication on the panel, right (for residents) or left (for visitors) for entering the door'.

This is a normal state. If the Door is open, it will start the closing motion. When the Door is closed and locked, the variables $a, e,$ and p are reset to be 0.

(13) While $p = 0$, detecting a possible case of violation:

If the IT system detects any person is going to enter the Door, while p = 0 and the Door is unlocked, the system

recognizes it as a possible case of violation. Then the system flashes the display (12) and make an announcement for notice.

(14) When p becomes negative, warning against violation:

When p turns to negative (and also when p increases its absolute value while $p < 0$), the IT system has detected a case of violation of the rule. Then it flashes a light and takes a photo from front of the person who has just entered the Door. And it displays and announces as 'Since more persons than those being authenticated have been detected to enter, a photo was taken for the security reasons. To avoid this inconvenience, please enter the Door after getting authentications.'

(15) Resetting p and Close-Door.

If nobody has entered for a certain period of time (say, 10 seconds) while $p \neq 0$, the IT system gives the Close-Door direction. When the Door gets closed and locked, the variables $a, e,$ and p are reset to 0.

5.4 Human management of the security

(16) Utilizing the operation records and photos:

The records of operations, especially the photos taken in the cases of violation, are analyzed every day by the managers/caretakers for the purpose of making appropriate means both individually and generally for enhancing the security of the building. Warning to any relevant party and reporting to police in serious cases may be among such actions.

6. DISCUSSION

After writing this paper, I tried to think the structure of the present problem again. For doing this, I first tried a tabular form of 'problem - root cause/root contradiction - solution'. But the logic behind is much more closely related among the rows of such a table. Thus I finally chose the diagrammatic representation, as shown in Fig. 6.

The boxes in the second column are the main sequence of root causes. The arrows show the logical or cause-effect relationships among the facts in the present system itself. Boxes in the first (i.e. left) column shows various effects or problem phenomena. Boxes in the third and forth columns are the basic ideas of solutions and their further design decisions.

The safety of door operation is the fundamental requirement (or constraint) in this problem. Thus, the door need to be closed slowly. Trials to close the door quickly violate the safety principle. The most basic solution concept in the present paper is the introduction of the virtual & logical door, which can be opened/closed quickly and intelligently under the software control.

The main design decision in the current system is found in the second box of the second column, i.e. "To authenticate a person when the door is closed". This design has two main limitations; a group of people are (implicitly) allowed to enter with one authentication and this authentication process can not be performed during
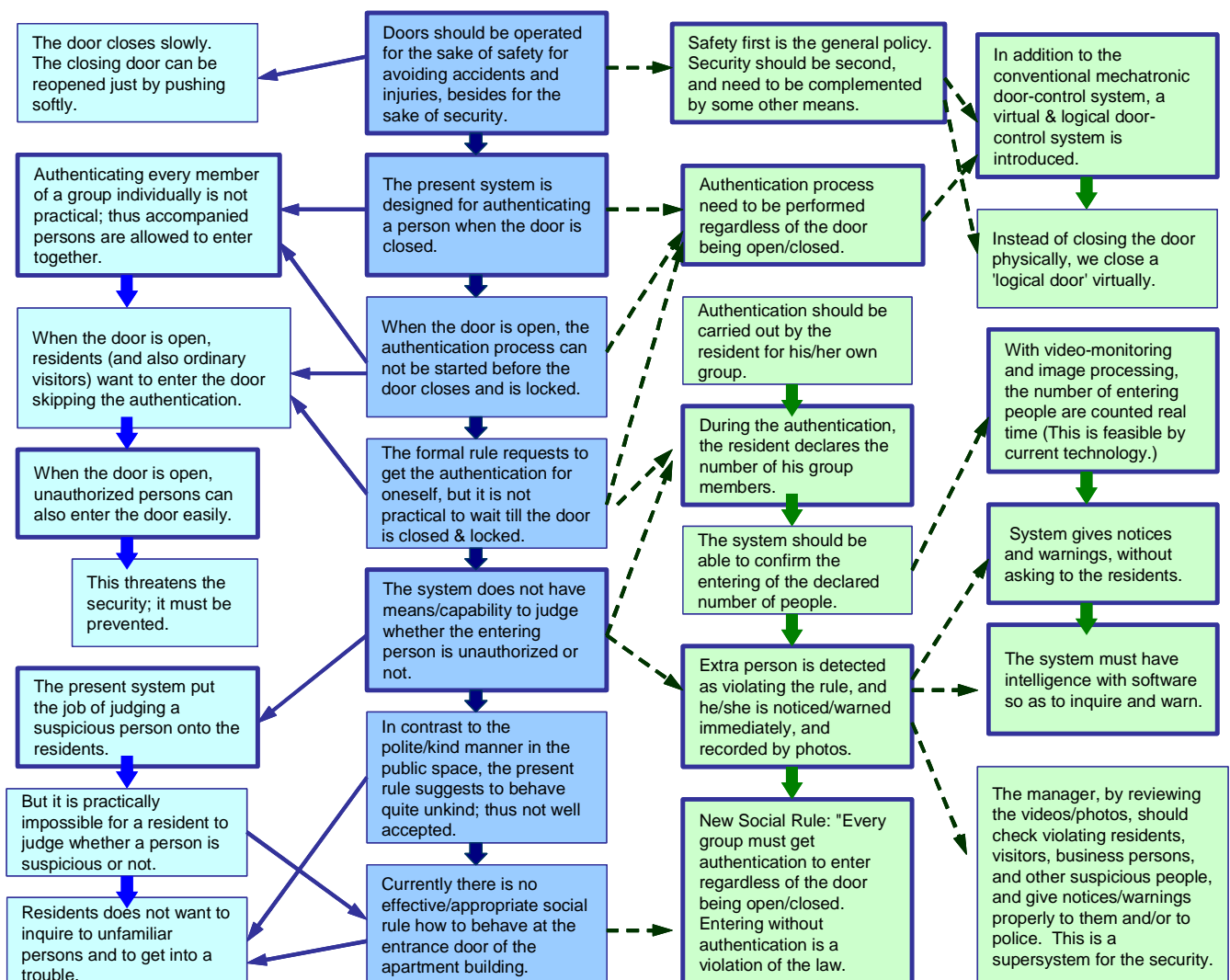

Fig. 6 Structure of the whole problem and solution of the present study

the door open or unlocked. Since people cannot wait until the door closed, residents and good visitors often want to enter the already open door without waiting. This gives criminals the chance of entering the door by pretending to be ordinary residents.

The system does not have any means to distinguish residents and unauthorised people, thus it implicitly request the residents to make such distinction and to prevent the unauthorized persons from entering. However, this is a request of impossible tasks. Residents can not do and does not like to do such a job,. Thus, we have a security hall here as we all know well.

After understanding all these situations, our decision choice is clear. We make the authentication process available at any time regardless of the door being closed/open. And we try to clarify the group of people whom the system gives an authentication. The resident, leader of the group, is requested to declare the number of members of his/her group.

Hence we prepare a system which can count the number of people who have entered the door. This will be technically achieved by the video monitoring and the image processing. Extra persons who entered the door exceeding the authenticated number of people are regarded as violating the rule. Thus the system gives a warning and takes a photo of the person. For doing all these functions the system must be intelligent and operated in software.

With this new system, the social rule is now clear: "Every group must get authentication to enter the door regardless of the door being open/closed. Entering without authentication is a violation of the law." This social rule specifies only what one should do without mentioning on other persons behaviour. Thus this social rule can be followed smoothly by good residents and visitors.

One interesting findings: During most of the time of this work, this problem was thought to be related not only to technical but also, or even with more weight, to psychological and social aspects. However, Fig. 6 revealed that everything came from the design choice in the present system. The design "to authenticate a person when the door is closed" has caused various effects in the technical system and various reactions to the people. Thus, the basic solution to the present problem is to choose a different decision in this basic point. I.e., "to authenticate a group of people at any time." This was made effective by the introduction of virtual & logical door controlled intelligently in real time by the software.

7. CONCLUSION

This paper has applied the TRIZ/USIT methodology to the security problem of auto-locking door system for the entrance of apartment buildings and has proposed a consistent set of conceptual solutions which is supposed to be practical and effective.

The analysis of this problem has revealed that a simple technical approach is not suitable at all but rather psychological and social approaches are necessary and more important. Thus the problem was analyzed from multiple aspects, including the psychology of resident to judge an unfamiliar person and the social manner in case of two parties meeting by chance at the entrance door. We have used different methods including TRIZ, USIT, RCA+ diagram, the KJ method (or the Affinity Diagram method) in the analysis.

We have revealed a number of root causes and corresponding contradictions and have solved them one by one to find basic directions for a new solution system.

The process for proceeding to the solution is described in Section 4. Then on fragments of such ideas, a consistent conceptual solution was built as shown in Section 5. The final discussion in Section 6 has revealed a much clearer view of the whole problem and solution of the present study. Psychological and social aspects related to the present problem are understood as the effects or reactions to the basic choice in the technical system. Thus, on the basis of this overall view, the new basic choice in the technical aspect is expected to have solved most of the problems.

REFERENCES

[1] Arata Fujita: 'Case Study of Creative Problem Solving: How to Prevent Unauthorized Persons from Entering the Auto-locking Door of Apartment Building', Thesis, Osaka Gakuin University, Jan. 2007. (J)

[2] Toru Nakagawa and Arata Fujita: 'How to Prevent Unauthorized Persons from Entering the Auto-locking Door of Apartment Building: Applying TRIZ/USIT to A Social & Technical Problem', Third TRIZ Symposium in Japan, Held at Toshiba Kenshu Center, Yokohama, on Aug. 30-Sept. 1, 2007; TRIZ Home Page in Japan, Sept. 2007 (J & E).

[3] Ed Sickafus: "Unified Structured Inventive Thinking: How to Invent", Ntelleck, LLC, Grosse Isle, MI, USA (1997).

[4] Jiro Kawakita: "Hasso Hou" (Idea Generation Method), Chuo-Kouron, 1967 (in Japanese); "Zoku Hasso Hou" (Idea Generation Method, Continued), Chuo-Kouron, 1970 (in Japanese). The KJ Method is also called 'Affinity Diagram' in the New Seven QC Tools for Management.

[5] Valeri Souchkov, Rudy Hoeboer and Mathijs Van Zutphen: "TRIZ in Business: Application of RCA+ to Identify and Solve Conflicts Related to Business Problems", ETRIA TFC 2006, Held at Kortrijk, Belgium, on Oct. 9 - 11, 2006.

CONTACT

Toru Nakagawa

Osaka Gakuin University,

2-36-1 Kishibe-minami, Suita, Osaka, 564-8511 Japan

E-mail: nakagawa@ogu.ac.jp

http://www.osaka-gu.ac.jp/php/nakagawa/TRIZ/eTRIZ/

* Note 1. Usage of RFID seems to make this direction easier and more flexible for the residents. However, among the people having no proper RFID, the system need to distinguish the visitors to be approved from those not. For this purpose, the authentication process by the resident for his/her accompanying visitors at the gate and also by the resident in the flat via interphone system for his/her visitors coming at the entrance are necessary. Thus the procedures which are very similar to the one discussed later in sections 5 and 6 are also necessary in case of the gate system using RFID.

* Note 2. We owe this idea to the WG members of MPUF USIT/TRIZ Study Group. We thank Kunio Fukatsu, Takuo Maeda, and Fumiko Kikuchi for this idea.