SECURITY DESIGN OF VALUABLE DOCUMENTS AND PRODUCTS[1]

Rudolf L. van Renesse

TNO Institute of Applied Physics
P.O. Box 155, 2600 AD Delft, The Netherlands
phone: +31 15 2692130, fax: +31 15 2692111
e-mail renesse@tpd.tno.nl[2]

1. INTRODUCTION

Each design stems from -in the broadest sense of the word- a *problem*. The existence of a problem as such however does not suffice. The problem owner must have awareness of the problem and also must consider it of sufficient importance to justify creative action.

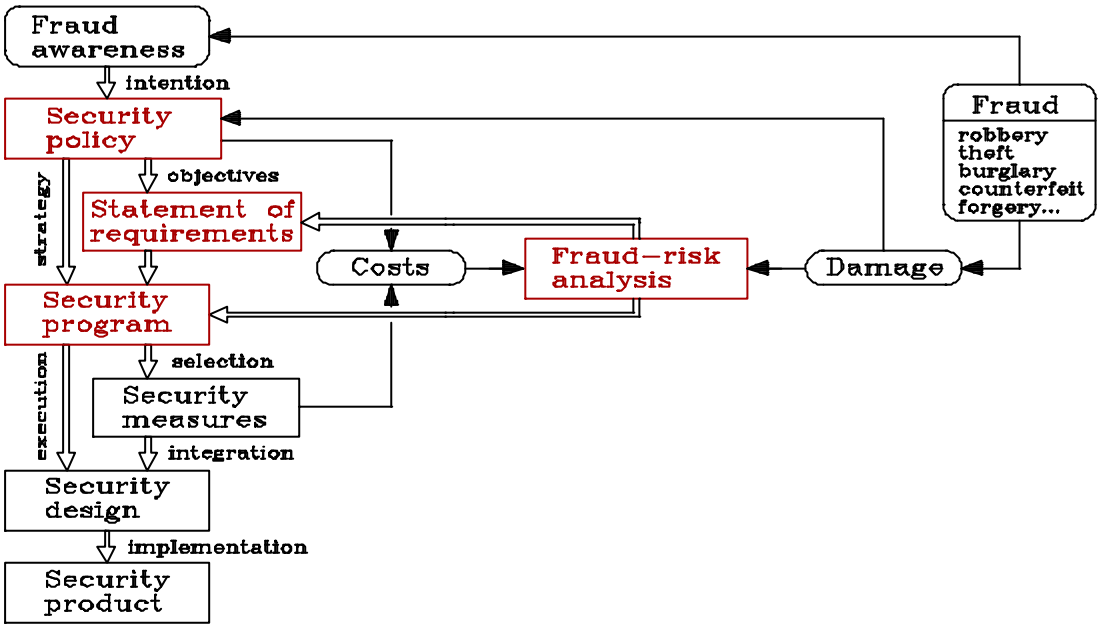

Figure 1 - The development of a security product (after Tadema Wielandt [1]).

[1] This article is a revision of: R.L. van Renesse, Security design of valuable documents and products, *SPIE vol. 2659, Conference on Optical Security and Counterfeit Deterrence Techniques*, San José, CA., 1-2 Febr. 1996, p. 10-20. This article also contains a few passages from Chapter 2 by R.L. van Renesse in the 2nd edition of the textbook *Optical Document Security*, publisher Artech House Books (Boston, London).

[2] Author's affiliation since 2002: VanRenesse Consulting, Willem de Zwijgerlaan 5, 2582 ED The Hague, The Netherlands, phone: +31 (0)70 3540333, email: ruud_van_renesse@zonnet.nl, website: www.vanrenesse-consulting.com

Ideally, the development of a security product passes, in a systematic manner, through several steps: from the awareness of a security problem (e.g. fraud awareness), via analysis of the problem and the subsequent design steps to the final product. These subsequent steps are represented schematically in figure 1 [1]. The awareness of existing or expected fraud will eventually result in the definition of a security policy, with objectives and strategies. The objectives are the basis for a statement (or program) of requirements, which, together with the drafted strategies, will result in the security program (or security scheme).

Both programs are, together with a fraud-risk analysis, the base for the selection of security measures, the security design and the final development of the security product. The various stages of this development sequence are briefly treated in this article. Attention is further paid to the iterative aspects of the design process from the standpoint of industrial design.

2. SECURITY POLICY

Awareness of a security problem and considering it of sufficient importance are prerequisites for the onset of the development of a product that will solve this problem or at least diminish its undesirable impact. A security policy is then outlined, comprising objectives and strategies.

Objectives are formulated explaining what has to be achieved to halt or sufficiently diminish the problem. The experienced or expected problem may be either directly financial or may involve indirect damage to the corporate image because the fraud violates the public trust in the product. The objectives are further elaborated in the *statement of requirements*. ***Strategies*** then are drafted that explain how the formulated objectives will be achieved. Detailed solutions subsequently are the subject of the *security program*.

3. FRAUD-RISK ANALYSIS

The fraud-risk analysis involves the following five-step procedure:

1. Categorise the various methods of attack or fraud. The categories have to be sufficiently uniform. This means for instance that a single category such as "counterfeiting" can be inadequate and has to be subdivided into separate categories, for instance, "origination", "replication" and "imitation".
2. Assess the damage involved with each individual category of attack or fraud. If the categories are non-uniform a single damage figure cannot be attached to the category.
3. Assess the probability of occurrence of each individual category of attack or fraud.
4. Calculate/assess each separate risk.
5. Balance each separate risk against the expected costs of eliminating or reducing it (cost-risk analysis).

This analysis results in a report which carefully defines and/or assesses the various fraud-risk parameters, involved with the calculation of the (expected) risk. This risk equals the product of the (experienced or expected) damage and the probability of that damage to occur. The various methods of fraud are set out in a table against the damage they cause and their probability of occurrence. Each entry in the table has to be discussed and made plausible in the covering report. An exact assessment of the damage, its probability and the subsequent calculation of the risk involved, is neither always possible nor always necessary. The risk, therefore, is frequently expressed in qualitative terms. A possible and substantial damage due to an attack that adequate prevention measures have been taken against so that its probability of occurring is assessed "very small", may be considered "acceptable" as long as this is made plausible in the report. Contrary, a

small damage due for example to nuisance counterfeiting, that is very likely to be suffered, may be not worthwhile to pay any attention to and the risk being considered "negligible".

Otherwise, how will the risk be estimated of damage to the corporate image by fraud obvious to the general public, associated with recurrent publications in the media? The actual damage may be relatively small, but the corporate damage may be unacceptable on the long term. Viewed in that light, the risk of nuisance counterfeiting, after all, may not be "negligible" at all.

In the first instance the various existing patterns of fraud will have to pass in review. The future however must also be borne in mind: new technologies may lead to completely new methods of fraud. An example is de rapid development of desk-top publishing technology (flat bed scanner and ink jet printer or laser colour printer linked to a computer with advanced image processing software) by which a considerable desk-top fraud has become possible. An extended view into the near future of document fraud is given by the USA National Research Council [2].

Subject of a fraud-risk analysis may also be a discussion of the level of complexity that is involved with various methods of attack, in order to qualitatively demonstrate the expected probability of occurrence.

As figure 1 illustrates, the fraud-risk analysis is embedded in a cost-damage analysis. The assessed risk is balanced against the expected costs involved with curtailing that risk, in order to avoid 'underkill' or 'overkill'. This balance is taken into account by the drafting of the statement of requirements as well as the security program.

The fraud-risk analysis is one of the indispensable documents for the evaluator of the security design/product. It enables him to draw correct conclusions from the security system matrix that he has devised.

4. THE STATEMENT OF REQUIREMENTS

The policy, in particular the formulated objectives, as well as the fraud-risk analysis are input to the statement of requirements, which is the starting-point of the product design in a broad sense. Arranging the list of requirements is a complex and critical procedure that methodological rules and checklists have been developed for. Not only physical and chemical requirements have to be met, but also many aesthetic, semantic, ergonomic and security requirements. For example, Optically Variable Devices (OVDs) must resist peeling and wear, have an appealing, conspicuous and unique appearance. OVDs as such offer little security, they must relate to the product and integrate into the product design. Imitation and replication must be made difficult, taking the required level of security in consideration: is the valuable product a cheap gift voucher, an expensive season travel ticket or an invaluable passport?

First line inspection requires that OVDs are unambiguous, self-explanatory, easily communicated, memorized and recognized. How is this achieved? In section 7 of this article a few considerations are devoted to ergonomic aspects of OVDs as well as their resistance against counterfeiting. It will appear that requirements may be mutually exclusive in some cases, which results in a trade off between one requirement and the other. In such cases not all requirements can be fully met, unless the design is suitably adjusted.

The design of a product is, of course, adequate if it meets the criteria laid down in the statement of requirements. But what criteria must be included in the statement of requirements? In the first place a complete and valid set of requirements must be drafted. Checklists and procedures have been devised that aid in composing a suitable statement of requirements.

A useful, three-phased procedure is proposed by Roozenburg and Eekels [3]:

1 *Collection of criteria*

1.1 Identify the processes that the product has to function in and identify the persons involved.

1.2 Make an inventory of the desires, needs, demands, etc. of those involved. Use checklists and technical catalogues. Checklists have been composed by Jones [4], Hubka [5], Pahl [6] and Pugh [7].

2 *Analysis of criteria*
2.1 Eliminate criteria that come to the same thing.
2.2 Eliminate criteria that do not discriminate.
2.3 Identify ends-means relations between criteria of different levels. Sketch the end-means hierarchy.
2.4 Check the ends-means hierarchy for completeness and consistence. Is every criterion that is defined as a subgoal necessary to decide for the main goal? Are the combined subgoals adequate to decide for the main goal.

3 Revision of criteria
3.1 Eliminate specifications as much as possible.
3.2 Make the criteria of the lowest level operable. Describe perceptible characteristics for each criterion and define limits between acceptable and unacceptable solutions.

The statement of requirements must further be tested on six basic criteria: **completeness**, **validity**, **operability**, **accessibility**, **redundancy** and **length**. These criteria are briefly discussed in the following [3].

- **Completeness**

In order to ensure that the final product indeed meets the expectations, the statement of requirements must be as complete as possible. If essential criteria are overlooked, the final product may not perform the functions aimed at. For example, if basic ergonomic requirements are disregarded, an OVD design may become overly complex and, thus first line inspection may be hindered and the level of first line security decreased.

- **Validity**

The criteria must be valid, i.e. they must relate to the desired function. For instance if an OVD aims at raising tamper resistance, the number of yearly tamper cases cannot be a valid criterion, because this number also depends on other factors. Validity is the paramount characteristic that is required of each individual criterion in the statement of requirements.

- **Operability**

The criteria must be operable, i.e. it must be possible to establish objectively whether they are met or not. For example, simply requiring an OVD to be "appealing" or having a "harmonious radiance" will not do; it must be explained how it will be established that it indeed meets these criteria. Criteria like "reliable", "valuable", and "convenient", which are frequently mentioned as requirements are inoperable as such because they are at a too high level in the hierarchy of means end ends. Lower level entries must be added to this hierarchy, giving means to these high level ends. In some cases a panel of laymen or experienced experts may settle matters remaining immeasurable. Anyway, the procedure by which the matter will be settled must already be defined in the statement of requirements.

- **Accessibility**

The criteria must be accessible, i.e. their verification must be practically possible and the costs and time involved with this verification must remain within acceptable limits. Sometimes the problem is the time required to verify if a particular criterion is actually met. In other cases its verification is prohibitively complex and costly. For example, determining the level of counterfeit protection may be very expensive and time consuming, as this might require the procurement of additional know-h-

ow, equipment and performing extensive experiments. On the other hand, these tasks might be adequately and cost-effectively carried out by experienced independent laboratories. Such predicaments must be anticipated in the statement of requirements.

- **Redundancy**

Redundancy of different requirements must be avoided. Certain properties must not count twice or more in the valuation of the product. This situation may ensue if ends and means are not clearly distinguished, so that criteria of a different level end up as autonomous criteria in the statement of requirements. For example the list of security requirements may comprise (1) counterfeit resistance, (2) ergonomic inspection and (3) implementation of an OVD such as optically variable ink (OVI). These objectives are at three very different hierarchical levels. The OVD is a means to first line inspection which, on its turn, is a means to counterfeit resistance. Therefore these criteria do not belong in one statement of requirements as independent requirements. Their hierarchical relationships must be made clear. Moreover, the third requirement is solution-based, because it specifies what the product should *be* instead of what it should *do*.

- **Length/significance**

Finally the number of criteria and their weight must be considered. A statement of requirements containing too many product criteria becomes inoperable because a systematic evaluation becomes too awkward. Monitoring the relative significance of the criteria helps keeping the length of the statement of requirements within acceptable limits.

The statement of requirements is an indispensable help for the designer to accomplish his task in an efficient and correct manner, without wandering through endless design loops which only slowly, if at all, converge towards the desired product. The effort to create an adequate statement of requirements therefore is not a waste of time. Moreover, without this document a proper evaluation of the design or the final product is unduly laborious. And, last but not least, the formulation of the statement of requirements helps the contractor realize what he actually wants.

5. THE SECURITY PROGRAM

The composition of the statement of requirements is in fact already a part of the design process. Different designers may produce different but equally adequate statements of requirements. The statement of requirements defines the criteria that the design/product has to meet (the solution of the problem); it does not define how that shall be achieved, or anyway should not do this. The statement of requirements is a detailed elaboration of the policy objectives and it is the questionnaire that the contractor presents to the designer.

While the statement of requirements is the detailed elaboration of the policy objectives, the security program is the response to the policy strategies. Moreover, in the security program the policy strategies are elaborated, also taking into account the fraud-risk analysis, the cost-damage analysis and the statement of requirements. The security program describes how the requirements will be met; it is the framework in which all security aspects are treated in their mutual relationships. In the security program objectives and strategies assemble: it is the completed outcome of the outlined policy.

Technical and organizational security measures are dealt with in the security program, which may be considered as a preliminary design on a high conceptual level. Not all procedures and details are specified in detail. The security program is the base for the pursued security design. On the basis of these data the designer selects the factual operational procedures and the document/product security features. The security design finally is the starting-point for the production of the security product.

6. THE DESIGN PROCESS

6.1 The function of the product

Starting-point of each design is the desired function of the product to be developed. Not only the technical function, but also possible psychological, economical, social and cultural functions have to be considered. The designer requires at least a rough account of these functions in order to allow him to do a proper job. For example, apart from radiating the corporate image, the functions of an OVD may comprise the increase of fraud resistance, aesthetical attraction as well as market value. The product function (objective) is already defined as a part of the security policy during the product planning phase (strategy). The product function is in fact the most important input to the statement of requirements.

6.2 The basic design cycle

An existing or expected problem, when experienced as sufficiently annoying, generally results in the definition of the function of a desired product that should partly or wholly eliminate this problem. When the desired function of the product to be developed is defined, an invariable cyclic design process follows: the basic cycle of the design process. This basic cycle is an empirical cycle, a trial and error process, that involves a number of subsequent actions. As is shown in table I, each of these actions has a certain result. The *analysis* comprises the definition of the problem and the formulation of the objectives. The result is a list of criteria (the base for the final statement of requirements) that the design/product has to meet.

Problem as well as function relate to the difference between an undesirable starting point and a desirable ultimate product, a difference that has to be eliminated.

Table I - Parts of the Design Process

Action	Result of the action
Analysis	List of criteria
Synthesis	Design
Simulation	Characteristics of the design
Evaluation	Value of the design

The next phase in the basic cycle stands diametrically to the analytic phase. This is the phase of *synthesis* -the creative act- resulting in a preliminary design. Although this synthesis is the crucial step in the design cycle, it may not be inferred that other steps are less important or may be omitted. By *simulation* the characteristics of the design are subsequently established, after which an *evaluation* finally leads to an appraisal of the design. This involves assessing in how far the characteristics of the design meet the requirements delineated earlier. On the base of this evaluation it can be decided whether the accomplished design is acceptable, or if the basic cycle has to be run once more. In the latter case the analysis and/or the synthesis have to be executed once more, possibly resulting in an adjustment of the formulated requirements and/or a revised design. The actions and their results, listed in table I, lead to a repetitive, cyclic process, illustrated in figure 2.

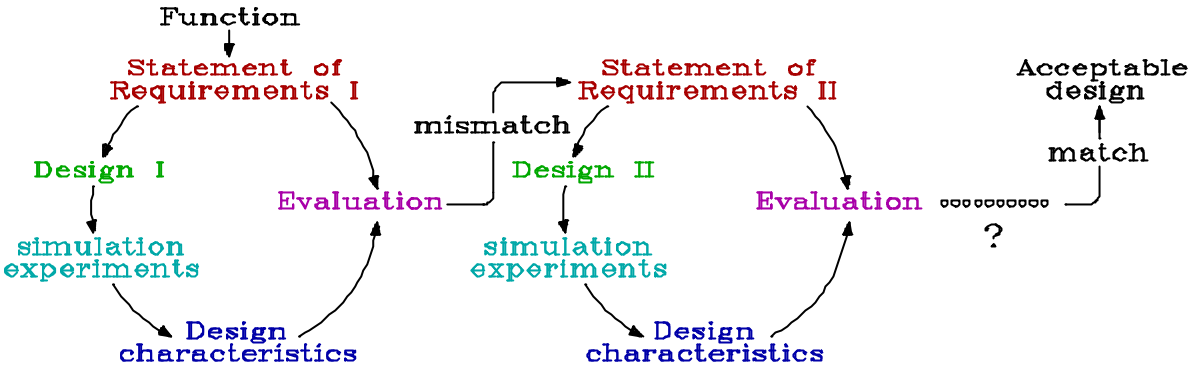

Figure 2 - The iterative structure of the design process.

Through each cycle, the design converges further towards an acceptable result. This procedure is typical for each design process, whether a design of a cheque or that of a complete security system. In fact an effective design process proceeds like this and not otherwise. This makes this design process a normative rule [3].

6.3 The characteristics of the design

From the defined functions the statement of requirements must be derived as a design base. The creative act of designing having taken place, simulation and/or experiments are required to assess the design or product characteristics.

Table II - Simulation and Experiments		
Input	theory: knowledge reasoning, theories formulas, tables models	practice: research methods model tests laboratory research panel investigations
Output	(expected) properties of the design/product	

In table II a number of input parameters is specified. Apart from theoretical aspects, this process involves experimental aspects, in particular when it concerns a product or prototype. Once all relevant properties of the design or product are established, they can be compared with the documented criteria. This is the actual evaluation, which further may result in the establishment of weak and strong points and possible paths of attack. In case the evaluation reveals a considerable mismatch between requirements and characteristics, the design cycle must be run again and either the requirements must be adapted, the design, or both. This procedure is repeated until the remaining mismatch between requirements and design properties becomes acceptable. Experience teaches that the passing through one single cycle rarely, if at all, results in design or product characteristics that sufficiently match the documented requirements. Convergence towards an acceptable product requires almost invariably the passing through multiple design cycles.

Recognition of this fact is paramount in the stage of security policy definition, when target dates and time schedules are defined. If no adequate time is allowed for the outlined iterative process, invaluable time may be lost with last stage re-designs. Already ordered and delivered material or equipment may appear superfluous or inadequate, a product that does not (fully) match the requirements may have to be settled for, or the target date -which often is an imperative deadline- may have to be exceeded.

The evaluation of subsequent design results is normally performed by the designer. However, it is

not always easy for the designer to do this in a completely unbiased manner. There are almost inevitable subconscious tendencies to leap from the experiencing of a problem to the immediate application of countermeasures and to take the required design properties for granted without a proper analysis. This is why it is generally beneficial to have crucial stages of the design examined by an independent evaluator.

As a result of this inclination to shortcut the design cycle, a security policy may or may not be incompletely formulated, a statement of requirements may appear to be either missing or to be critically incomplete from a security point of view and the security program and fraud-risk analysis may be partly or completely missing. The desired properties of the design are taken for granted and are rarely verified methodologically. Evaluations of the design, if any, therefore fail to adequately establish its weak and strong points.

If the finished product, in its final stage, is evaluated by an independent body and its eventual inherent weaknesses are revealed, the damage may be substantial. All the more reason to have an evaluator do his job in an early stage of the process. Subject of an evaluation should not only be the designed product itself, but also

- The outlined security policy:
  Would the formulated objectives and strategies indeed thwart the threats experienced or expected?
- The fraud-risk analysis:
  Does it cover all current and expected threats involved? Does it indeed assess risks or does it just sum up threats and their (expected) damage? Are costs assessed? Do the costs satisfy the policy constraints? Are all entries explained in the report?
- The statement of requirements:
  Does it meet the security policy and the fraud-risk analysis? Is it complete, Are the requirements operable, valid, etc.?
- The security program:
  Does it realize the requirements and does it answer the security policy as well as the fraud-risk analysis?

Each of these indispensable inputs in the design cycle should be achieved through yet another design cycle. On first sight this may seem a cumbersome procedure, but it is not always realized that methodological tools are offered that help to speed it up and that at the same time this procedure makes the design process more efficient and reliable. In this process the designer and the evaluator, instead of being opponents, become partners in security.

7. SOME ERGONOMIC CONSIDERATIONS

In section 4 it was stated that inspection of an OVD requires that it is unambiguous, self-explanatory, easily communicated, memorized and recognized. This section discusses a few aspects that pertain to the resistance of OVDs to counterfeiting (remaking) and the consequences this has for first line inspection. This subject is of some importance because organised crime has devoted considerable efforts to counterfeiting OVDs, which efforts have been successful in some cases. This unfortunate development has been generally met by considerably increasing the complexity of OVD images. This approach has severe implications for the ergonomics of security design. In this context it may be illuminating to contemplate the way Donald Norman [8] treats both stages of the interaction between the user and the product: the execution of a strategy and the evaluation of the result. An adaptation of his 'action cycle' is presented in figure 3.

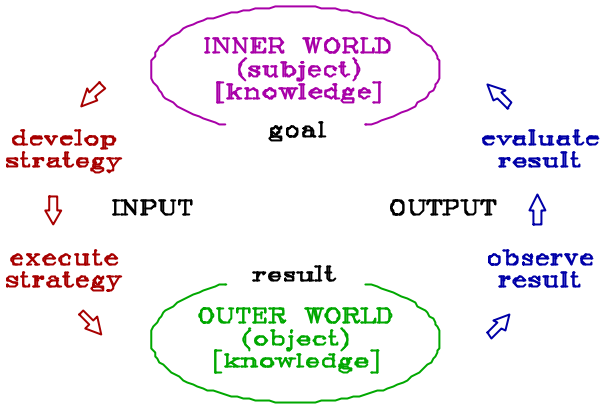

Figure 3 - The interaction between subject and object.

In handling a product, the user will develop and execute a strategy in order to adequately put the object to use. Subsequently the result of the action will be evaluated on the basis of what is observed. In order to properly handle the product, the user must have adequate knowledge (information) about the way it functions or else make either errors in handling or judgement. In the worst case the particular product function may not be used at all, because of lack of adequate information. From the action cycle in figure 3 it follows that the required knowledge is basically twofold: (1) knowledge about the action to be taken (input) and (2) knowledge about the result of that action (output). This twofold information may either be present in the world, that means provided by the product itself (not by a manual or a brochure!), or it may be in the user's head. In the latter case it has to be provided orally, by manuals, brochures or other information sources apart from the product and subsequently memorised. Norman presents amusing as well as terrifying examples of what may (and frequently will) go wrong if it is insisted that the information is in the users head.

Most unfortunately, the user of security products is made almost entirely dependent on knowledge in the head in order to inspect these products. The issuers of security products like banknotes, cheques, credit cards, etc., sometimes go to great lengths to educate the potential user about the security measures present on the product and the way to verify them. To this end they issue detailed brochures and posters or even broadcast TV spots. In spite of all painstaking efforts, the users remain oblivious and largely unaware of the information they are supposed to store in their heads. No wonder, given the considerable variety of different security products and the sometimes inept way in which the information is presented. It may be safely concluded that such efforts are largely ineffective and are likely to remain so.

For many designers, the starting point is the aesthetics of the design and the security features, somehow, are experienced, more or less, as impediments that have to be "integrated" in order not to interfere with the aesthetics. As a result of such "integration", none of the security features may be self-explanatory, easily communicated, memorised or recognised. No wonder the instructions given do not settle in the heads of the users. Norman's action cycle (figure 3) raises a few questions about the usability of security devices:

How easily can the user:	
determine and understand the function of the device?	
tell what actions are possible?	compare the observed results with the expected results?
execute the actions?	observe the results?

7.1 Image complexity

It is generally accepted that counterfeit resistance of diffractive OVDs is an increasing function of their image complexity. In fact several hologram manufacturing companies explicitly propagate the high image complexity of their products as an advantageous property that thwarts counterfeiting. In other cases the number of proposed optical and graphic effects and their combinations appears next to bewildering. And indeed, in practice, security OVDs are produced that are so complicated that the unambiguous communication of their image properties as well as their recollection becomes virtually impossible. To the opinion of this author, this must be considered a major violation of sound security design rules. Mindful of Norman's action cycle, the following guidelines may be taken into account in designing first line security features [9]:

Function
- The security feature must convey a message relevant to the product.
- It must obviously belong where it is and relate to the product. On related products, the security features must also mutually relate.
- The function of the feature must be obvious and intelligible.
- A feature that remains a riddle for the user does not function. It must be obvious what the device is meant for apart from embellishing the product.
- The functions must be standardised.
- The function of security designs that are very diverse and/or periodically change layout will not likely become understood.

Execution
- It must be evident what too look for and how to inspect it, preferably even without a preceding verbal or written communication.
- The information on the "what" and "how" of the feature should preferably be in the world.
- If not in the world, the "what" and "how" of executing the inspection must be easy to communicate and easy to memorise. Standardization is an effective means to this end.
- It should be possible to carry out the inspection in a casual and unobtrusive manner.
- Even a slightly complicated inspection will be considered annoying. The obviousness of the act may further be considered embarrassing and offensive. For these reasons, the inspection will not likely be performed.

Evaluation
- The effects to be observed must be self-evident; the information will preferably be in the world.
- If not in the world, the information on the effects to be observed must be easy to communicate and easy to memorise. The description must uniquely and unambiguously relate to the specific effects, while the briefness of the description must not result in vagueness.
- The observed effects must unambiguously relate to the expected effects.
- Indistinct signals will cause uncertainty.
- The security feature must unambiguously relate to the overall design.
- The feature must be "in its place". Inconsistent "add on's" present inadequate or even confusing information.
- The security features must not have existing competitors, which may serve as successful imitations.

Contrary, the pursued complexity of image content of OVDs is regarded as equivalent to advancement and sophistication by their originators. This image- or visual complexity is associated with the number of reconstructed first order channels, the number and intricacy of image elements and the number and intricacy of possible kinematic- and colour effects. It may be noted that such

OVD parameters are completely brought about by diffraction elements, characterized by practically uniform orientation and frequency and diffraction grooves with practically sinusoidal cross sections. Alternatives to these properties are discussed in the next section.

Figure 4 schematically illustrates the view that counterfeit resistance increases with image complexity. On the low end we find simple images that, consequently, can be easily counterfeited. Such images tend to be self explanatory, and easily communicated, remembered and recognized. Therefore, their first line inspection is easy, but, understandably, our confidence in their authenticity remains relatively low. On the high end of the graph in figure 4 we find very complex images that are expectedly difficult to counterfeit. Although we may have a high confidence in their authenticity, such complex images are not likely self-explanatory and they tend to be difficult to communicate, remember and recognize. Therefore, their first line inspection is considerably more demanding.

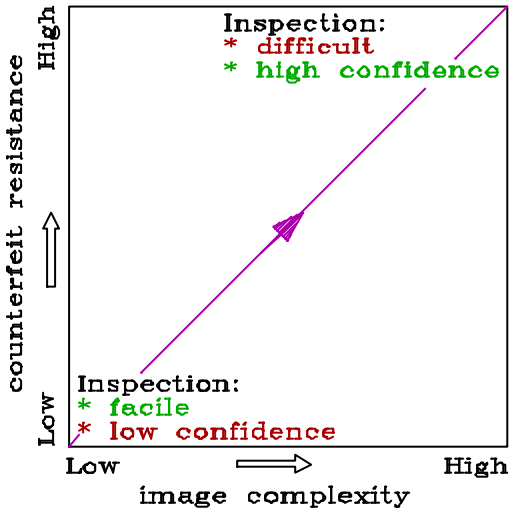

Figure 4 - Counterfeit resistance is an increasing function of image complexity. (No complex structures involved).

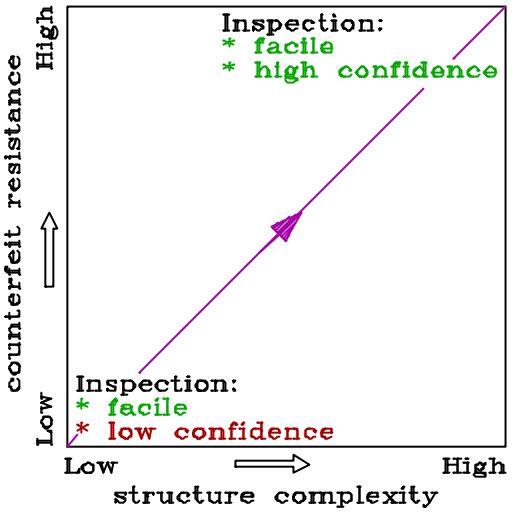

Figure 5 - Counterfeit resistance is an increasing function of structure complexity. (No complex images involved).

A brief discussion of existing opinions on the practicality of OVDs for security, expressed on the preceding Intergraf conference in Lisbon (1995), may be in place here. One event put forward was that of an inspector that reacted in surprise on the deliberate replacement of a genuine and simple OVD (e.g. of a dove) by a fake one (e.g. of a rabbit) with words like "*Oh look, they changed the hologram!*". This reaction was presented as a demonstration of the uselessness of OVDs. This is most unfortunate, because such an occurrence actually proves that the recognition of the deviation was immediate, once it was looked for. The naive conclusion, drawn by the inspector, that the original OVD was legitimately substituted by another, does not prove anything about the potential of OVDs. It only proves that training and information of the inspector was lacking.

And again, the frequently expressed, nonchalant and rejective pronouncement that "*if it's shiny, they'll accept it*" does not prove the uselessness of OVDs, but rather proves the impossibility of adequate inspection due to design complexity, the lack of adequate public information, or both. Such information and training may become more efficacious if the above rules for security design are taken into account. The required knowledge should be in the world (i.e on the device), not in the head!

Obviously, the introduction of complex images will impede the adequate training of the public as well as professional inspectors like bank tellers. In general we may expect a tendency to omit an

adequate first line inspection of complex OVDs, and indeed, a tendency of taking them for granted as long as they are shiny! Evidently, in this case, a trade off exists between the ease of inspection in first line and the confidence that we have in authenticity of the security feature. The conclusion is, that increasing the complexity of OVDs, in order to considerably raise their counterfeit resistance, leads to dangerously overshooting the mark.

7.2 Structure complexity

An antithesis is, that counterfeit resistance is an increasing function of structure complexity. This antithesis is schematically illustrated in figure 5. This subject has been addressed extensively in an earlier paper [10]. Structure complexity is associated with the amount of fineness and complexity of the structures that generate the relevant optical effects. This fine structural order may be brought about by non-uniformities in diffraction structures, asymmetric cross-sections of diffraction grooves, sub-wavelength 3D detail of diffraction grooves, combined gratings [11], interference structures, and order on a molecular level. Table III presents an overview.

Techniques to achieve structure complexity are interferometry and holography combined with chemical differential etching or ion beam etching, laser beam lithography, electron beam lithography, electron beam modulation techniques, thin film vacuum technology, liquid crystal- and liquid crystal photopolymer technology. On rotation or tilting of the security feature, such structural order may result in positive-negative image swaps (pixelgram), reverse in contrast between first diffraction orders (kinegram), and well defined colour conversions (DID, thin film composites, OVI and liquid crystals). These optical effects are unusual, conspicuous and well-defined, and therefore tend to sustain easy communication, recollection and recognition, which in their turn allow efficient inspection in first line. At the same time these optical effects are hard to counterfeit, so that their first line inspection may provide a high confidence in authenticity as well. The image content may remain very simple while the optical effects are based on complex structures. Obviously in this case a combination is achieved of easy inspection in first line and a high confidence in authenticity of the security feature.

Table III - overview of complex security structures based on diffraction and interference

device type	structure characteristics	examples
Exelgram (pixelgram)	Non-uniform distribution of azimuth and pitch of diffraction grooves	Australian "Opal stamp", Vietnam Bank Cheque Amex travellers cheques
Kinegram	Asymmetric cross-sections of diffraction grooves, combined gratings [11]	Netherlands Postcheque "Einstein", Swiss ID-card
Zero order devices (ZODs)	Submicron three-dimensional high refractive index diffraction structures embedded in low index matrix	Diffractive Identification Device (DID), commercial applications currently being developed
Thin film interference coatings	Multilayer composite interference structures	Canadian banknotes, Optically Variable Ink (OVI) on many banknotes
Polymerized liquid crystals	Helical molecular organisation of interference layers in cholesteric liquid crystal phase	Advantage seal and Identiseal on many valuable documents

7.3 Discussion: nano-technology versus ergonomics

Considering both cases, that of image- and structure complexity, and their apparent consequences for security design, a gradual shift from complex OVD images towards simple OVD images with complex structures, can be foreseen. This is only a logical continuation of the ongoing progress of nano-technology, which has lifted security features to their current advanced state. Mankind is beginning to learn how to sculpture matter with nanometer precision, so that matter is becoming a virtually unlimited recording medium that is only at the onset of revealing its seemingly magic potential. One of the results of this technological development is, that matter can be shaped into extremely precise diffractive and interference elements, rendering unexpected and highly uncommon optical effects that are extremely difficult to counterfeit, can be easily verified and yet can be economically mass produced. Moreover, intricate machine readable codes can be incorporated in security devices, thus rendering them additional and powerful second line security potential (with the use of tools, like a magnifier, an ultraviolet source, an inspection machine, etc). It would seem that, on the long run, these remarkable advancements of nano-technology will enable us to largely eliminate document fraud and product piracy.

There is a "but" though, associated with this seemingly bright view on the future. Nano-technology security features, however powerful, are useless if they are not adequately inspected. And adequate inspection in first line becomes only possible if security design follows at least some basic ergonomic rules. Here we enter a field that has scarcely been set foot on until now, and this field seems to be as bare as the field of nano-technology is becoming profuse. It appears paramount therefore that fundamental and practical research on ergonomic security design is carried out in the near and remote future.

Although the examples given in this paper mostly relate to optically variable devices (OVDs), this does not imply that the discussion on security design is limited to OVDs. The systematic approach of security design discussed is generally valid for security design of documents, products and systems.

References

[1] R. Tadema Wielandt, "The evaluation of document fraud resistance", *Optical Document Security*, R.L. van Renesse (ed), chapter 2, Artech House, Boston/London 1993.

[2] National Materials Advisory Board, Commission on Engineering and Technical Systems, National Research Council, *Counterfeit Deterrent Features for the Next-Generation Currency Design*, Publication NMAB-472, National Academy Press (1993).

[3] N.F.M. Roozenburg and J. Eekels, Produktontwerpen, structuur en methoden, Lemma, Utrecht, The Netherlands (1991).

[4] J.C. Jones, *Design methods; seeds of human futures*, 9th edition, John Wiley & Sons, Chichester (1982).

[5] V. Hubka and W.E. Eder, *Theory of technical systems; a total concept theory for engineering design*, Springer, Berlin (1988).

[6] G. Pahl and W. Beitz, *Konstruktionslehre; Handbuch für Studium und Praxis*, 2nd revised edition, Springer, Berlin (1986).

[7] S. Pugh, *Total design; integrated methods for successful product engineering*, Addison Wesley, Wokingham (1990).

[8] Donald A. Norman, *The psychology of everyday things*, Basic Books, New York (1988).

[9] For security design considerations see also:
J.-F Moser, "Document protection by Optically Variable Graphics (Kinegram)", *Optical Document Security*, R.L. van Renesse (ed), chapter 9, Artech House, Boston/London 1993.

[10] R.L. van Renesse, "Ordering the order - a survey of optical document security features", *SPIE vol. 2406, Conference on Practical Holography IX*, San José, Ca., 5-10 February 1995, p. 268 - 275.

[11] R. Staub, W.R. Tompkin, J.-F. Moser, Combined gratings, *SPIE vol. 2689*, p. 292-299.