DE-OPPORTUNIZING DESIGN AND ITS LESSONS
FOR BUILDING SECURITY AND COUNTERTERRORISM

James A. Wise, Eco•Integrations, Inc., Richland Washington

Recent broad concerns for "Homeland Security" have renewed the field of 'hard' security design and directly resistant design strategies for buildings. However, there is an associated field of research and practice on 'soft security' design, which is equally applicable and less impacting on the general user populace. This approach works on the general principle of 'de-opportunizing', which examines the explicit control loops that a malefactor must engage with the setting in order to carry out their intentions. Then explicit interventions are designed into settings in order to disable or frustrate such needed controls. The result is enhanced security without regular users being inconvenienced or often even noticing the interventions. This paper reviews the applications of such de-opportunizing environmental design to thwart vandalism, burglaries, bank robberies and physical and sexual assaults, and extends it to counterterrorist situations using Perceptual Control Theory, which provides the theoretical basis for its use.

INTRODUCTION

While the world may end "...not with a bang, but a whimper", building security design has again been brought to the fore with the explosive collapse of the World Trade Center on September 11, 2001. Not since the late 60's social upheavals has American architecture and construction become so focused on domestic building security.

Regrettably, this new consciousness appears to be displacing another national building design and construction movement that had gone from side to mainstream in the preceding decade. This is the world trend to Green Building or Sustainable Design, which seeks exceptional energy and resource efficiency, along with occupant health, safety and well-being in the design, construction and operation of facilities. (See Wise, 2001, for an overview of Sustainable Design and Human Factors.)

For example, the City of Seattle (like many others around the country) is in the midst of a process of 'greening' new construction and tenant improvements in public and commercial buildings. All new civic construction in particular is required by city ordinance to meet a level of LEED™ Silver (a green building rating scale by the US Green Building Council), and other new Sustainability Standards are currently under development. Yet the

Puget Sound Business Journal (Kramer, 2002) has run a full-page article exclaiming that "Security, environment clash in post-Sept. 11 design." The article describes how 'Seattle may become a battlefield for green design and anti-terrorist guidelines' and opines that 'sustainable design criteria are at odds with security requirements'.

Phooey.

If there is a conflict between Sustainability and Security Design it is because neither is being done at the level of awareness and sensitivity they deserve. The sorts of security adaptations in particular being made to buildings in the immediate 9/11 aftermath are either knee-jerk 'target-hardening' responses or they are overconstrained solutions because the design or site context of a building had been already fixed. Where there is yet some design problem-solving flexibility left, one finds that Sustainable Design as well as other design goals can most always either co-exist or even converge with Security Design strategies.

'Target Hardening' vs.
"Deopportunizing' Security Design

"Target Hardening" is the term given to describe the narrow stereotypic approach to security design. It

assumes that someone takes deliberate offensive acts against a facility or its occupants, and that nothing short of built-in sheer resistance to the impact of the act itself is available as a means of self-defense. While this may have been a good biological design strategy for dinosaurs, it flies in the face of all relevant behavior-environment design research. That archive teaches us that the most effective security design is not that which narrowly focuses on direct resistance, but one which selectively removes criminal opportunities, or redirects user activities so that the possibility of crime or a security breach never occurs at all. This is sometimes called 'soft security' in order to contrast it with target hardening, but it is more often referred to as 'crime prevention through environmental design (CPTED)' or 'de-opportunizing' design.

Here are examples from actual professional practice that illustrate the difference between hard and soft approaches to security design:

Some years ago, a NW city was building a new city office building next to a park. Leading administrators became concerned that a sniper could hide in the park and shoot someone in the offices, and so directed a large wall to be built between the building and the park. This naturally upset many city office workers, who were anticipating a pleasant park view. The resulting conflict was eventually settled when the city accepted a recommendation to instead install semi-mirrored glazing on that side of the building, because any potential sniper would not be able to aim through it. There was an added benefit of reducing solar gain to the interior as this glazing was on the south side.

Another NW example stems from an inability police had to shine the spotlights on their police cars through a chain link fence to detect potential intruders near a building. A conflict arose over extending police vehicle access nearer the building on their nightly patrols. It was resolved when the chain link fence was spay painted a dark flat color so that police spotlights could shine through it without producing the interfering glare.

In both of these instances a critical behavioral control loop was affected by a deliberate design intervention. The first intervention disabled a potential control loop (aiming), while the second enabled it through removal of simultaneous brightness contrast. In neither of these cases would the design ever even be noticed as the result of a security strategy.

Security design does not need to be obvious or in any way intrusive on the desired uses of buildings if it selectively engages the behavioral control loops of potential malefactors while enabling the control loops of competing or oversight activities. Here are further examples from three different arenas of application: Design against Vandalism, Bank Robberies, and Physical Assaults against Women.

Vandalism

The application of 'de-opportunizing design' to the prevention of vandalism is now at least 20 years old (See Tausen, 1980, Wise, 1982 a,b, Wise, 1983) and in widespread use. It developed from several archival and careful observational studies on the occurrence of vandalism in a wide number of settings, from parks and campgrounds, to schools and assisted housing. Those investigations revealed recurrent patterns in types of damage attributed to vandalism and where and when these occurred. With these insights, design interventions that simply removed opportunity or disabled preparatory behaviors became readily available. These included:

- Making fire grates non-removable so that they could not be used to catapult coals onto picnic tables.
- Replacing 'lollipop' style light globes with more slender designs that did not appear to be targets for rocks and pellets.
- Slanting the tops of school lockers, or embedding them in walls so that students could not climb on top of them.
- Increasing the height or thickness of overhead beams and roof edges to prevent their being easily grasped.
- Fixing picnic tables in place, making them square instead of rectangular, and using a light colored finish that provides less contrast for carving.
- Using square wooden slats on public seating that could be rotated three times before they had to be replaced from wear.

- Opening multiple, different sightlines onto points of building entry to discourage after-hours break-ins.

Bank Robberies

While such "soft-security" approaches may seem appropriate for petty offenses like vandalism, a crime like bank robbery would seem to require a much more direct form of security design. Indeed, in Europe where bank robberies were more likely to be 'take-overs' conducted by infamous urban terrorists like the former Bader-Meinhoff gang, one sees bank lobbies take on fortress characteristics, with complete separation between tellers and patrons by bullet proof glass (called "bandit-barriers" in the US). Fortunately, these types of robberies have been in a tiny minority in the US. A major study in 1985 (Wise & Wise, 1985a,b) commissioned by the Bank Administration Institute revealed several key design features of bank lobbies that could unobtrusively yet effectively deter bank robberies or increase likelihood of the suspect's capture.

- Keeping adjacent teller's stations no more than five feet apart from each other was the single greatest deterrent to bank robberies.
- Having one public entry/exit was another significant deterrent,
- As was placing bank officers to have a clear view of the front of the teller line.

These and other strategies such as camera placement to capture **exiting** patrons, raising counter heights to disable 'jump-overs', increasing the depth of counters to disable 'reach-overs', removing tellers' last names from their station tags, and using a 'scatter-system' to feed the teller line all are effective at enhancing bank security. Yet how many of these are even noticed by regular patrons? Each of these operates by interfering with or removing a key aspect of behavioral control that an intended bank robber has to establish in order to perpetrate the crime. Yet because regular patrons behavior circuits in banks do not engage the setting in the same way, these modifications remain unobtrusive and innocuous.

Physical Assaults

Physical assaults upon people, and upon women in particular, may seem particularly difficult to prevent through indirect security design strategies, but investigations of these crimes have again shown them to be remarkably reliant on a few enabling features of settings. In his precedent setting doctoral dissertation research at the University of Washington, Frank Stoks (1982) created a CPTED model which was especially effective at revealing how human predators utilize designed settings.

Most assault crimes involve a 'position and wait' strategy on the part of the offender. Removing nearby places of concealment that allow wide oversight and predictability of user movements de-opportunizes the crime.

Most assault crimes depend on the perpetrator quickly entrapping the victim in a relatively closed setting. Making sure that small-scale urban places have multiple routes of entry and egress defeat this capability. In this regard, note how widely open are the urban bus shelters in Seattle. This is no accidental feature. Early user studies (Wise & Alden, 1978) revealed the propensity of such transit shelters to become traps for their users, and a deliberate design decision was made to decrease weather protection for increased personal security. A mid-west city that installed fully enclosed bus shelters at about the same time had to replace them all when their two small entryways enabled pairs of robbers to 'mug' an entire shelter full of riders at one time.

PERCEPTUAL CONTROL THEORY AND HUMAN FACTORS DESIGN

The above examples appear different in their respective contexts, but all have the same theoretical and strategic basis. This is to design the physical setting so as to disallow or disable the critical control loops that a protagonist needs to maintain to carry out their acts, and to strengthen the setting's support of control loops that establish alternative or conflicting use patterns. The underlying theory and analytical approach to this kind of Human Factors design is well established in Applied Psychology in the work of William T. Powers (1972) and his collaborators, and is called Perceptual Control Theory (PCT). Their focus was

(and still is) on hierarchical controls within an individual's neural organization which have an interface with the real world through the 'controlled quantity' that the loop maintains. But Wise (1988) and more recently Lulham (2002 in prep) have shown how the same theory may be extended at a control loop's interface with the environment. These explicit linkages become the strategic means to selectively engage the Human Factors of environmental design. As the perceptual 'controlled quantity' of every loop links through the physical setting, it becomes accessible to influence through pointedly explicit design of setting conditions.

Because would-be perpetrators of criminal acts have very different use intentions of settings than regular occupants, their 'controlled quantities' which maintain the information loops in their particular environmental behaviors are also very different, or at least held in a different range. Security design that selectively disengages these does so without the need to inconvenience or impede the normal setting user. Although PCT has seen successful application in other areas of Human Factors, it is time to bring its application to the foreground of environmental design.

DE-OPPORTUNIZING TERRORISM THROUGH ENVIRONMENTAL DESIGN

The events of September 11, 2001 have been particularly engraved on the hearts and minds of architects who design tall buildings (Johnson, 2002). A recent exhibition at the National Building Museum in Washington DC ("A New World Trade Center", April 6-June 10) demonstrated a very wide range of responses to the tragedy and what it foreshadows for future mega-structures.

One lesson evident in this exhibition is that no entrant felt that a hard security design approach to highly visible or important buildings is called for. Like the replacement for the destroyed (in 1995) Murrah Building in Oklahoma City demonstrates, it is possible to fulfil both security goals and human use and aesthetic ones through selectively sensitive design. Human Factors has a significant role to play in this process, just as it has in prior CPTED applications. The vast depth and planning of terrorist activities that necessarily occurs prior to an actual strike -- and even that sequence of events

itself -- opens terrorist perpetrators to countless opportunities to be observed or disabled in their plans, because the designed environments they utilize simply don't allow things to be done in certain ways. Indeed, new building HVAC strategies and controls actually decrease the ability for terrorists to introduce biological agents into buildings. And these new strategies were introduced for energy saving or IAQ improvements, not counter-terrorism. Yes, it is a changed world. But we still have the understanding and the tools to do the right things for it.

REFERENCES

Johnson, Reed (2002) Architects search souls after Sept. 11. *Eugene Register-Guard.* Tuesday, January 22, 3-4D.

Kramer, Ari (2002). Security, environment clash in post-Sept. 11 design. *Puget Sound Business Journal.* April 5-11, 27. Seattle, WA.

Lulham, Rohan, (2002). *Investigation of the interrelationships between the Goals of staff and detainees, and the physical environment in a number of Juvenile Justice Centres.* Doctoral Dissertation in preparation. Dept. of Architecture, University of Sydney, Sydney, Australia.

Powers, William T. (1972). *Behavior: The Control of Perception.* Chicago, Aldine.

Stoks, Francis G. (1982) *Assessing Urban Public Space Environments for Danger of Violent Crime-Especially Rape.* Doctoral Dissertation, University of Washington, Seattle, WA.

Tausen, M. (Ed.) (1980). *Creating Safe Schools.* Office of the Superintendent of Public Instruction, Olympia, Washington, April.

Wise, J.A. & Alden, R. (1978). Spatial Behavior and Perceived Qualities of Urban Bus Shelters. *Proceedings of the Human Factors Society*, 22nd Annual Meeting. (pp. 64-68) Santa Monica, CA. HFES.

Wise, J.A. (1982a) A Gentle Deterrent to Vandalism. *Psychology Today.* September, 31-38.

Wise, J.A. (1982b) Workshop Abstract: "De-Opportunizing Design: A Comprehensive Strategy for Deterring Vandalism." *EDRA 13 Proceedings.* Washington, D.C., 283-284.

Wise, J.A. (1983). Designing Against Vandalism: A Threefold Way. *The Recreation Reporter,* January-February, 8-10.

Wise, J.A. & Wise, B.K. (1985a). *Bank Interiors and Bank Robberies: A Design Approach to Environmental Security.* Bank Administration Institute, Rolling Meadows, Illinois:.

Wise, J.A. & Wise, B.K. (1985b). The Interior Design of Banks and the Psychological Deterrence of Bank Robberies. *Proceedings of the International Conference on Building Use and Safety Technology.* (pp. 24-28) Los Angeles, CA.

Wise, James A. (1988) Control is Beautiful: Measuring Facility Performance as if People (and Buildings) Really Mattered. ASTM Symposium on Overall Facility Performance: Use, Operation and Cost, October 13-14, published in STP 1029--*Performance of Buildings and Serviceability of Buildings,* G. Davis & F. Ventre, Eds., (pp. 121-143) ASTM, Philadelphia. PA.

Wise, J.A. (1997). How Nature Nurtures: Buildings as Habitats and their Benefits for People. *HPAC Magazine*, February, pp. 48-51, 78.

Wise, James A. (1997) Measuring the Occupant Benefits of Green Buildings. *Proceedings of the 41st Meeting of the Human Factors and Ergonomics Society.* (pp. 495-499) Santa Monica, CA HFES.

Wise, J.A. & Hazzard, Tracy L. "Green Building Benefits and Bionomic Design", *Archi*Tech.* Jan 2000, PP 24-30.

Wise, J.A. (2001) Human Factors & the Sustainable Design of Built Environments. *Proceedings of the 45th Meeting of the Human Factors and Ergonomics Society.* (pp. 808-812) Santa Monica, CA, HFES.