Journal of Computations & Modelling, vol.3, no.4, 2013, 83-101
ISSN: 1792-7625 (print), 1792-8850 (online)
Scienpress Ltd, 2013

Reliability of Information Operations

Nicholas J. Daras[1]

Abstract

This paper provides rudimentary principles of reliability in information operations that are the same as those for mechanical systems in which the component reliabilities are replaced by the operational reliabilities. These simplified concepts allow for a better insight into different information operational scenarios to achieve a particular objective.

Keywords: Reliability of a series of information operations, reliability variation with time, information operations hazard function, support and availability of a series of information operations.

1 Introduction

Information warfare has recently become of increasing importance to the military, the intelligence community, and the business world. The term

[1] Department of Mathematics and Engineering Sciences, Hellenic Military Academy, 166 73, Vari Attikis, Greece. E-mail: darasn@sse.gr

Article Info: *Received* : July 1, 2013. *Revised* : August 30, 2013.
Published online : December 1, 2013.

information warfare is similar in meaning to cyber warfare[2] though with a more streamlined goal of achieving competitive advantage. As per *The Institute for the Advanced Study of Information Warfare* (IASIW), *"information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information* and *information systems (including information-based processes and computer-based networks) while protecting one's own. Such actions are designed to achieve advantages over military, political or business adversaries"* ([6]). Recall that *information systems are the software and hardware systems that support data-intensive applications* (*See* [3]; also [7]) Their study bridges business and computer science using theoretical foundations of information and computation to study various business models and related algorithmic processes within a computer science discipline.

Following [1], *information warfare are information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries*. For completeness, we recall that *information operations are actions taken to affect adversary information and information systems while defending one's own information and information systems*.

Remind that information operations can be divided into three separable parts:

- *kinetic warfare* that realizes in the physical dimension and it practically means the physical destruction, demolition and abuse of the components of the information infrastructures and infocommunications systems;
- *cognitive warfare*, which basically prevail in the mental dimension and it involves: *military deception*[3], *operation security*[4] and *psychological operations*[5];

---

[2] *Cyber warfare* is any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponent's system

[3] *Military deception* refers to attempts to mislead enemy forces during warfare. This is usually achieved by creating or amplifying an artificial fog of war via psychological operations, information warfare, visual deception and other methods.

• *network warfare*[6] that realizes in the information dimension and contains the following: electronic warfare and computer network operations ([2]).

As the all-source intelligence is the basic of the information operations so is the basic of cyber warfare the electronic based intelligence that is built on sensor networks. Accordingly the *network warfare* completed with the electronic based intelligence is nothing else than all the cyberspace operations, with other words: cyber warfare ([5]).

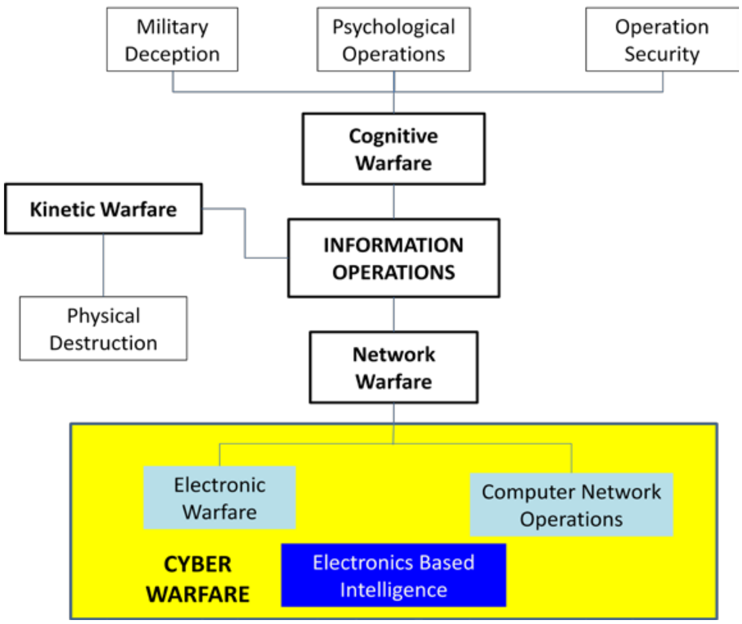


Figure 1: Connection of information operations and cyber warfare ([5])

---

[4] *Operations security* is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

[5] *Psychological operations* are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.

[6] *Network warfare* operations are the integration of the military capabilities of network attack, network defense, and network warfare support.

For obvious effectiveness reasons of better information operations analysis organization, it is often important to quantify and compute the reliability of information operations. Remind that, in general, *reliability* (systemic def.) *is the ability of a person or system to perform and maintain its functions in routine circumstances, as well as hostile or unexpected circumstances*. In particular, *in engineering, the (statistical) term reliability describes the ability of a system or component to perform its required functions under stated conditions for a specified period of time*. In this direction, the present paper provides the rudimentary principles of reliability in information operations that are the same as those for mechanical systems ([4]) in which the component reliabilities are replaced by the operational reliabilities. These simplified concepts allow for a better insight into different information operational scenarios to achieve a particular objective.

2 Reliability of Information Operations

Definition 1. *A series system of information operations, in a reliability sense, means that all components in the system must operate in order for the whole information operation to be successful.*

The block diagram for such an information operations system is shown in Figure 2.

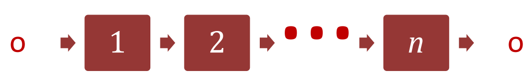


Figure 2: A series system of n component information operations

The reliability of an information operation is measured in terms of its probability of success. Thus, the probability R of success of a series of information components comprising the overall mission (operation) is the probability of success of independent events, i.e.

$$R = R_1 \, R_2 \ldots \, R_n = \prod_{i=1}^{n} R_i$$

where R_i is the probability of success (reliability) of the i^{th} information operation.

Definition 2. *A parallel system of information operations, also referred to as a redundant system, consists of two or more components. The system will fail only if all of the components will fail.*

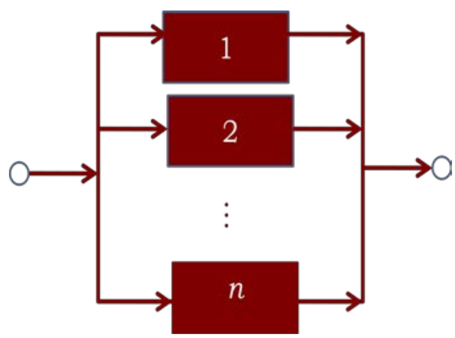


Figure 3: A parallel system of n component information operations

The overall parallel system information operation failure can be expressed as

$$P = P_1 \, P_2 \ldots \, P_n = \prod_{i=1}^{n} P_i,$$

where $P_i = 1 - R_i$ represents the probability of failure of the i^{th} information operation. Hence, the overall reliability of the parallel system information operation is

$$R = 1 - P = 1 - (1 - R_1)(1 - R_2) \ldots (1 - R_n).$$

Definition 3. Another type of parallel system of information operations is one with *standby redundancy, which means that only one component of the information operation is on-line at a time.*

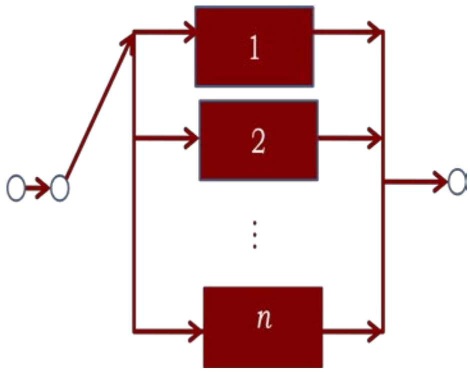


Figure 4: A parallel system of n component information operations with standby redundancy

Assuming that all standby systems are identical with constant rate of failure

$$\mu t (= constant),$$

the overall reliability for a standby system with n components is

$$R^{(n)} = \left[1 + \mu t + \frac{(\mu t)^2}{2!} + \cdots + \frac{(\mu t)^{n-1}}{(n-1)!}\right] e^{-\mu t}.$$

Example 1. For a three-component system (two standby systems backing up the first system) of information operations for which $\mu t = 0.5 = 50\%$, we have $R^{(3)} = [1 + 0.5t + 0.125]e^{-0.5} = 0.606 + 0.303 + 0.076 = 0.985$. This demonstrates that the 2nd standby system contributes only $0.076/0.985$ (or 7.7%) to the overall success of the operation. Thus, in the information operation a second backup operation would not be used.

Of course, the component information operations can be combined partly in series and partly in parallel, as shown in the Figure below.

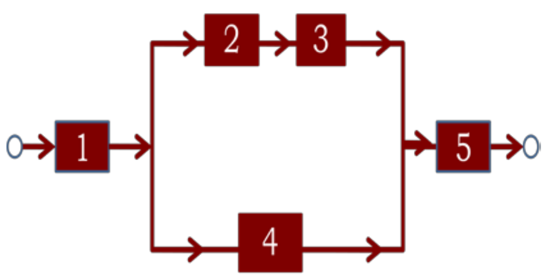


Figure 5: Combined series and parallel information operations

To obtain the overall reliability, this information system must be reduced to a system of components in series, as shown in Figure 6.

Figure 6: Equivalent series information operations

Thus, the reliability of the branch 2,4 is

$$R_{2,4} = 1 - \left(1 - R_{2,3}\right)(1 - R_4).$$

Since $R_{2,3} = R_2 R_3$, it follows that the overall reliability for this information operations system is

$$R = R_1 R_{2,4}\, R_5 = R_1[1 - (1 - R_2 R_3)(1 - R_4)]R_5.$$

3 Information Operations Reliability Variation with Time

The concepts of reliability developed for systems of information operations also apply to the components of information systems. Both are also applicable to cases where the component reliabilities vary with time.

Definition 4. *The information operations reliability function $R(t)$ is the probability that no information operation failure will occur prior to time t given that the equipment is operating at time $t = 0$ and is expressed as*

$$R(t) = 1 - F(t) = \int_t^{\infty} f(s)\, ds.$$

Here, the function $F(t)$ is the information operations failure function, which is given by

$$F(t) = \int_0^t f(s)\, ds$$

which determines the probability that a failure will occur in time t, again given that the equipment is operational at time $t = 0$.

An important parameter in any reliability analysis is the *mean time to information operation failure* ($MTTIF$), which is defined here as the expected value of t for the distribution $f(t)$. Hence

$$MTTIF = E[t] = \int_0^\infty t\, f(t)\, dt.$$

The *second moment* (*variance*) of the distribution $f(t)$ about $t = MTTIF$ provides a measure of the spread of the function about its mean value. It is calculated from

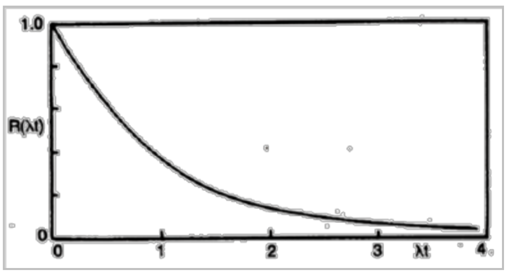
$$\begin{aligned} s^2 &= \int_0^\infty (t - MTTIF)^2\, f(t)\, dt = E[(t - MTTIF)^2] \\ &= \int_0^\infty t^2\, f(t)\, dt - 2\, MTTIF \int_0^\infty t\, f(t)\, dt + (MTTIF)^2 \int_0^\infty f(t)\, dt \\ &= \int_0^\infty t^2\, f(t)\, dt - (MTTIF)^2 = E[t^2] - (MTTIF)^2 \end{aligned}$$

Information operations reliabilities ($R(t)$) and mean times to information operation failure ($MTTIF$) corresponding to the four most commonly used distributions $f(t)$ are given in the table below.

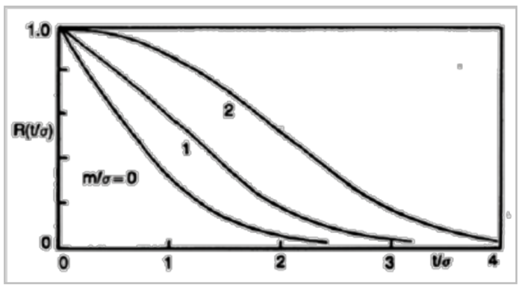
$f(t)$	$R(t)$	$MTTIF$
Exponential Distribution $\boldsymbol{f(t) = \lambda e^{-\lambda t}}$	$R(t) = e^{-\lambda t}$	$MTTIF = \frac{1}{\lambda}$
(Truncated) Normal Distribution $\boldsymbol{f(t) =}$ $\boldsymbol{\frac{\sqrt{2/\pi}}{\sigma\left[1 + erf\left(m/\sqrt{2}\sigma\right)\right]} exp\left[-\frac{(t-m)^2}{2\,\sigma^2}\right]}$ $(\boldsymbol{0 < t < \infty})$	$R(t) = \frac{2}{1 + erf\left(m/\sqrt{2}\sigma\right)}$ $\times \frac{1}{\sqrt{2\pi}} \int_{[(t-m)/\sigma]}^{\infty} e^{-\frac{1}{2}z^2}\, dz$	$MTTIF =$ $\frac{\sqrt{2/\pi}}{1 + erf\left(m/\sqrt{2}\sigma\right)}$ $\sigma\, exp\left[-\frac{m^2}{2\,\sigma^2}\right] + m$
Log-Normal Distribution $\boldsymbol{f(t) =}$ $\boldsymbol{\frac{1}{\sqrt{2\pi}\; t}\; exp\left[-\frac{1}{2}\left(ln\frac{t}{\sigma} - \frac{\mu}{\sigma}\right)^2\right]}$ ($\boldsymbol{\mu} \in\,]-\infty,\infty[$ and $\boldsymbol{\sigma} > 0$)	$R(t) =$ $\frac{1}{2}\left\{1 - erf\left[\frac{1}{\sqrt{2}}\left(ln\frac{t}{\sigma} - \frac{\mu}{\sigma}\right)\right]\right\}$	$MTTIF =$ $\sigma\, exp\left(\frac{1}{2} + \frac{\mu}{\sigma}\right)$

Weibull Distribution $\boldsymbol{f(t)} =$ $\begin{cases} \boldsymbol{0}, & \boldsymbol{0 \le t \le \gamma} \\ \dfrac{\boldsymbol{\beta}}{\boldsymbol{\eta}}\left(\dfrac{\boldsymbol{t-\gamma}}{\boldsymbol{\eta}}\right)^{\boldsymbol{\beta-1}} \boldsymbol{exp}\left[-\left(\dfrac{\boldsymbol{t-\gamma}}{\boldsymbol{\eta}}\right)^{\boldsymbol{\beta}}\right], & \boldsymbol{t > \gamma} \end{cases}$ • $\boldsymbol{t}$ *= operating time,* • $\boldsymbol{\gamma}$ *= minimum guaranteed successful operating time for which* $\boldsymbol{R(t) = 1, 0 \le t < \gamma}$*,* • $\boldsymbol{\beta}$ *= slope (shape parameter)* *(*$\boldsymbol{\beta} > 0$*) and* • $\boldsymbol{\eta}$ *= characteristic time parameter* *(*$\boldsymbol{\eta} > 0$*).*	$R(t) =$ $\begin{cases} 0, & 0 \le t \le \gamma \\ exp\left[-\left(\dfrac{t-\gamma}{\eta}\right)^{\beta}\right], & t > \gamma \end{cases}$	$MTTIF =$ $\eta \ \Gamma\left(1 + \dfrac{1}{\beta}\right) + \gamma$

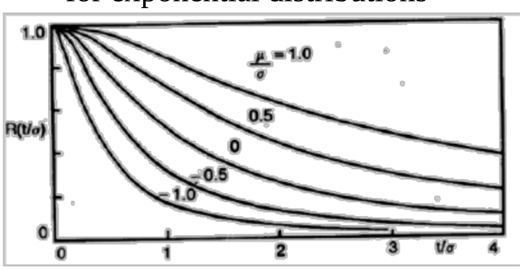
The graphical representations of the information operation reliability functions $R(t) = R(\lambda, t)$ for the above four most commonly used distributions are given just below.



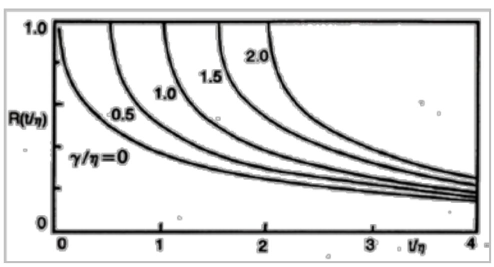
The reliability function
$R(t) = R(\lambda, t)$
for exponential distributions



The reliability function $R(t/\sigma)$
for normal distributions



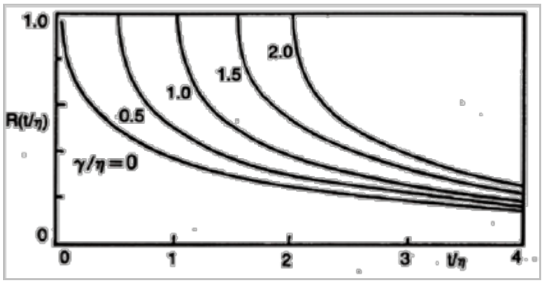
The reliability function $R(t/\sigma)$
for log-normal distributions



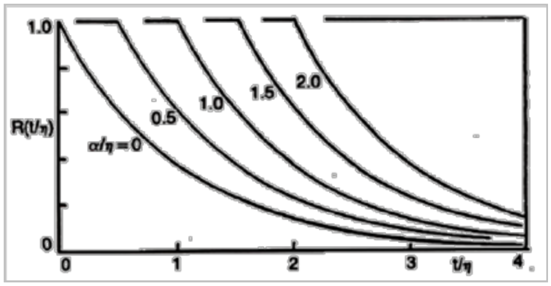
The reliability function $R(t/\eta)$
for Weibull distribution with $\beta = 0.5$

Figure 7: Information operations reliabilities for different distributions

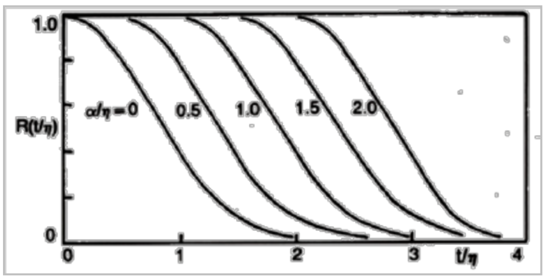
Especially, the graphical representation of the information operation reliability functions $R(t) = R(\lambda, t)$ corresponding to Weibull distributions with shape parameter $\beta = 0.5, 1.0, 2.0, 3.0$ are given below.



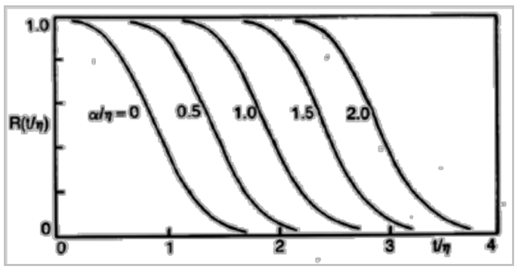
The reliability function $R(t/\eta)$
for Weibull distribution with $\beta = 0.5$



The reliability function $R(t/\eta)$
for Weibull distribution with $\beta = 1.0$



The reliability function $R(t/\eta)$
for Weibull distribution with $\beta = 2.0$



The reliability function $R(t/\eta)$
for Weibull distribution with $\beta = 3.0$

Figure 8: Information operations reliabilities $R(t/\eta)$ for Weibull distributions

4 Derivation of Information Operations Reliability from Probabilistic Considerations

Let

- N_0 *=number of information operation components at* $t = 0$*,*
- N_t *=number of functioning information operation components at* t*,*
- $N_{t+\Delta t}$ *=number of functioning information operation components at* $t + \Delta t$*,*
- Δt *= time increment under consideration.*

Then, the following result is easily proved.

Proposition 1.

i. *The information operation failure rate is*

$$\lambda(t) = lim_{\Delta t \to 0} \frac{N_t - N_{t+\Delta t}}{N_t \ \Delta t} = -lim_{\Delta t \to 0} \frac{R(t+\Delta t) - R(t)}{R(t)\Delta t} = -\frac{1}{R(t)} \frac{dR(t)}{dt}.$$

ii. *The information operation reliability $R(t)$ represents the theoretical probability that a component will operate for t units of time without failure:*

$$R(t) = exp\left[-\int_0^t \lambda(t)\, dt\right].$$

iii. *The information operation reliability $R(t)$ can be approximated by the fraction of survivors at time t:*

$$R(t) \cong N_t / N_0.$$

iv. *If $\lambda(t) = \lambda = constant$, then*

$\lambda \cong -\frac{1}{t}\ ln\ \frac{N_t}{N_0}, \frac{N_t}{N_0} \cong e^{-\lambda\, t}$ *and* $R(t) = e^{-\lambda\, t}$.

5 The Information Operations Hazard Function

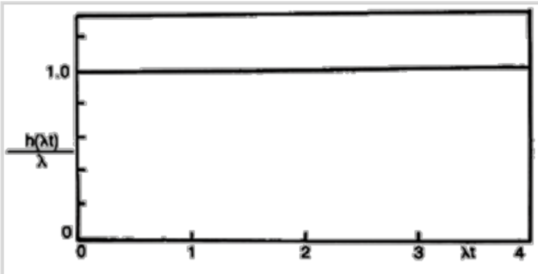
Definition 5. *The instantaneous rate of information operation (failure defined as the fraction of components failing per unit time is the hazard function $h(t)$.*

Proposition 2. $h(t) = \lambda(t) = -\frac{1}{R(t)}\frac{dR(t)}{dt}$ and $h(t) = \frac{f(t)}{R(t)}\left(\Leftarrow \frac{dR(t)}{dt} = f(t)\right)$.

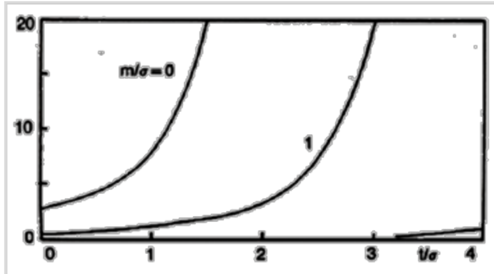
The hazard functions corresponding to the commonly used distributions are given below.

Distribution	*Hazard Function*	*Parameter Range*
Exponential Distribution $\boldsymbol{f(t) = \lambda e^{-\lambda t}}$	$h(t) = \lambda$	$\lambda > 0$
(Truncated) Normal Distribution $\boldsymbol{f(t) =}$ $\boldsymbol{\frac{\sqrt{2/\pi}}{\sigma\,[1+erf(m/\sqrt{2}\sigma)]}\, exp\left[-\frac{(t-m)^2}{2\,\sigma^2}\right]}$ $\boldsymbol{(0 < t < \infty)}$	$h(t) =$ $\frac{exp\left[-\frac{(t-m)^2}{2\sigma^2}\right]}{\sigma\int_{([t-m]/\sigma)}^{\infty} e^{-\frac{1}{2}z^2}dz}$	$\sigma > 0$ $m \geq 0$
Log-Normal Distribution $\boldsymbol{f(t) = \frac{1}{\sqrt{2\pi}\;t}\; exp\left[-\frac{1}{2}\;\left(ln\frac{t}{\sigma} - \frac{\mu}{\sigma}\right)^2\right]}$ ($\boldsymbol{\mu} \in\,]-\infty, \infty[$ and $\boldsymbol{\sigma} > 0$)	$h(t) =$ $\frac{\left(\sqrt{2/\pi}\right)\left(exp\left[-\frac{1}{2}\left(ln\frac{t}{\sigma}-\frac{\mu}{\sigma}\right)^2\right]\right)}{t\left(1-erf\left[\frac{1}{\sqrt{2}}\left(ln\frac{t}{\sigma}-\frac{\mu}{\sigma}\right)\right]\right)}$	$\sigma > 0$ $-\infty < \mu < \infty$
Weibull Distribution $\boldsymbol{f(t) =}$ $\boldsymbol{\begin{cases} 0\,, & 0 \leq t \leq \gamma \\ \frac{\beta}{\eta}\left(\frac{t-\gamma}{\eta}\right)^{\beta-1} exp\left[-\left(\frac{t-\gamma}{\eta}\right)^{\beta}\right], & t > \gamma \end{cases}}$ • $\boldsymbol{t}$ = *operating time,* • $\boldsymbol{\gamma}$ = *minimum guaranteed successful operating time for which* $\boldsymbol{R(t) = 1}$ *and* $\boldsymbol{0 \leq t < \gamma}$*,* • $\boldsymbol{\beta}$ = *slope (shape parameter)* *(*$\boldsymbol{\beta} > 0$*),* • $\boldsymbol{\eta}$ = *characteristic time parameter (*$\boldsymbol{\eta} > 0$*).*	$h(t) =$ $\begin{cases} 0, & 0 \leq t \leq \gamma \\ \frac{\beta}{\eta}\left(\frac{t-\gamma}{\eta}\right)^{\beta-1}, & t > \gamma \end{cases}$	$\eta > 0$ $\beta > 0$ $\gamma \geq 0$

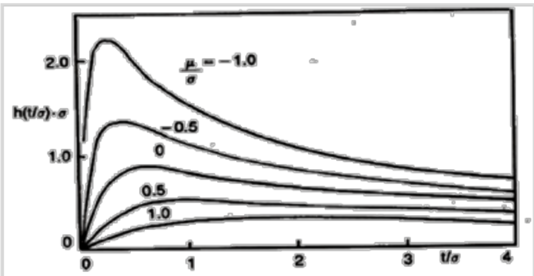
The graphical representations of the information operation hazard function $h(t)$ for the above four most commonly used distributions are given just below.



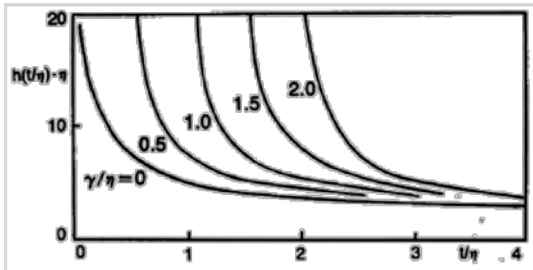
The hazard function $h(t) = h(\lambda, t)$
for exponential distributions



The hazard function $h(t/\sigma)$
for normal distributions



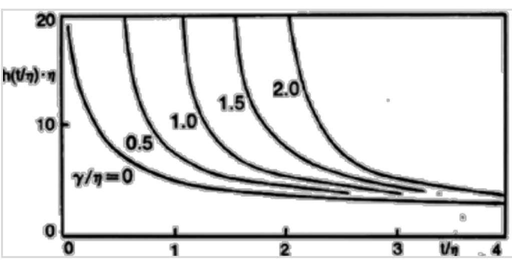
The hazard function $h(t/\sigma)$
for log-normal distributions



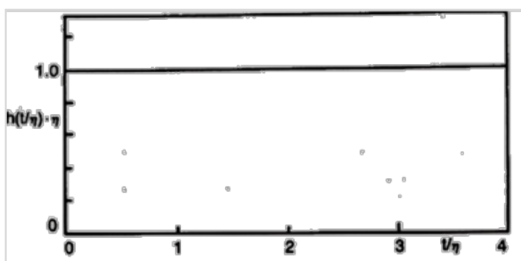
The hazard function $h(t/\eta)$
for Weibull distribution with $\beta = 0.5$

Figure 9: Information operations hazard functions for different distributions

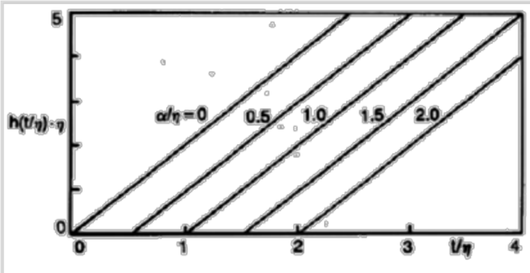
Especially, the graphical representation of the information operation hazard function $h(t)$ corresponding to Weibull distributions with shape parameter $\beta = 0.5, 1.0, 2.0, 3.0$ are given below.



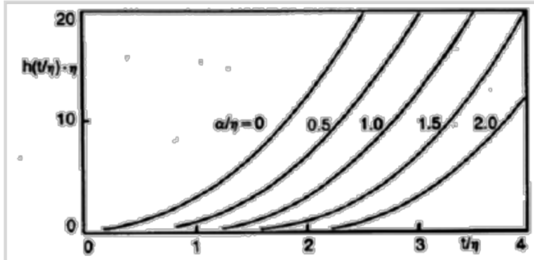
The hazard function $h(t/\eta)$
for Weibull distribution with $\beta = 0.5$



The hazard function $h(t/\eta)$
for Weibull distribution with $\beta = 1.0$



The hazard function $h(t/\eta)$
for Weibull distribution with $\beta = 2.0$



The hazard function $h(t/\eta)$
for Weibull distribution with $\beta = 3.0$

Figure 10: Information operations hazard functions $h(t/\eta)$ for Weibull distributions

6 Computation of Information Operations Series Reliability Functions from Experiment

Once the defective information operations components have been weeded out through control and simulation testing, some ingredient components will fail *randomly* in time. Thus, the reliability function $R(t)$ for such a series of information operations will take the general form represented by the exponential probability distribution.

To illustrate this case, a set of data for a sample of $N_0 = 120$ information operation components will be considered. The simulation test data for a total of 3000 $seconds$ are shown in Table 1 below.

Computing the average value of λ over a $3000 - minutes$ simulation test period, it is found that its average value is 0.0003240 $(1/seconds)$. Because the data approximate to a straight line on a semilog scale, it can be concluded from an exponential distribution. In this case the function $R(t) = N_t/N_0$ at time $t = MTTIF$ is given by

$$R(MTTIF\ ) = e^{-\lambda t} = e^{-1} = 0.367879.$$

Table 1: Datta

Time t (in *seconds*)	Number of Failures	N_t	$R(t) = N_t/N_0$	$\lambda = -[lnR(t)]/t$ (in $1/seconds$)
$0-200$	8	112	0.9333	0.0003450
$200-400$	7	105	0.8750	0.0003338
$400-600$	7	98	0.8167	0.0003375
$600-800$	6	92	0.7667	0.0003321
$800-1000$	6	86	0.7167	0.0003331
$1000-1200$	5	81	0.6750	0.0003275
$1200-1400$	5	76	0.6333	0.0003263
$1400-1600$	5	71	0.5916	0.0003280
$1600-1800$	4	67	0.5583	0.0003238
$1800-2000$	4	63	0.5250	0.0003222
$2000-2200$	3	60	0.5000	0.0003151
$2200-2400$	4	56	0.4667	0.0003176
$2400-2600$	3	53	0.4417	0.0003143
$2600-2800$	2	51	0.4250	0.0003056
$2800-3000$	2	49	0.4083	0.0002986

Approximating the mean time to the failure of a series of information operations

Therefore $MTTIF$ is approximately equal to 3100 $seconds$:

$$MTTIF \approx 3100\ seconds.$$

This also agrees with the $MTTIF$ computed from the average value of λ, i.e.

$$MTTIF = \frac{1}{\lambda} = \frac{1}{0.0003240} = 3086.$$

7 Support and Operational Availability of a Series of Information Operations

The standard of information operations may be designed with *redundancy* of components in order to improve their overall reliability. However, the improved reliability is not the only factor that contributes to the effectiveness. If the series of information operations fails and has to be promptly corrected, then the *time to redesign* is also an important factor in operational effectiveness.

For example, in Figure 11 below, two series of information operations are compared: the series of information operations A has higher reliability (higher $MTTIF$) and a longer downtime to redesign, whereas the series of information operation B has a lower reliability and a shorter downtime (shorter mean downtime (MDT)). Clearly, if the operational availability of a series of information operations, measured as the operation readiness per unit time, is more important than its reliability, then the series of information operations B is superior to the series of information operations A, despite the fact that it has a lower reliability.

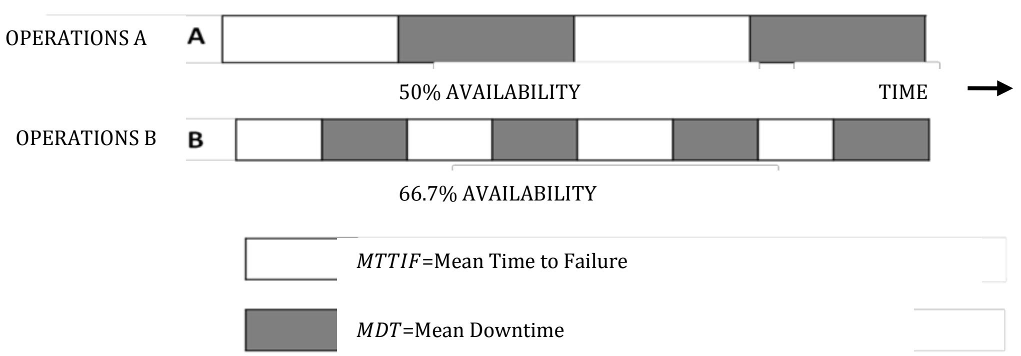


Figure11: Comparison of operational availability of two series of information operations

Definition 6. *Suppose given a series of information operations.*

i. *The support function $S(t)$ describing the probability that a component of the series, either a subseries or the whole series itself, will be redesigned to operational status within a specified period of time $[0, t]$ is defined as*

$$S(t) = \int_0^t g(s)\, ds$$

where $g(s)$ is the time-to-redesign probability density function.

ii. *The mean time to redesign $MTTRD$ is defined as*

$$MTTRD = E[t] = \int_0^t s\, g(s)\, ds$$

where $g(s)$ is (as before) the time-to-redesign density function.

In particular, we obtain immediately the following result.

Proposition 3. *If the redesign rate is constant and equal to λ_R, then the following hold.*

i. *$g(t)$ represents an exponential distribution for which*

$$g(t) = \lambda_R\, e^{-\lambda_R t}.$$

ii. *The support function takes the form*

$$S(t) = 1 - e^{-\lambda_R t}$$

where $e^{-\lambda_R t}$ is the probability that a redesign will not be completed in time t.

iii. *The mean time to redesign is given by*

$$MTTRD = 1/\lambda_R.$$

Definition 7. *Given a series of information operations, its operational availability A_0 is defined as the probability that a component, either a subseries or the whole series itself, will operate successfully at a given time*

$$A_0 = \frac{MTBS}{MTBS+MDT} = \frac{1}{1+(MDT/MTBS)},$$

where

- *$MTBS$ is the mean time between support*

- *MDT is the mean downtime, which includes the active support downtime and mean delay times caused by lack of logistics and / or administrative support.*

In this direction, we can also consider the following two concepts of availability.

i. *The inherent availability A_I is defined as the ratio*

$$A_I = \frac{MTTIF}{MTTIF+MTTRD} = \frac{1}{1+(MTTRD/MTTIF)}.$$

ii. *The achieved availability A_A is defined as the ratio*

$$A_A = \frac{MTBS}{MTBS+MASD} = \frac{1}{1+(MASD/MTBS)}.$$

Here

- *$MTTIF$ is the mean time to failure,*
- *$MTTRD$ is the mean time to redesign and*
- *$MASD$ is the mean active support downtime, resulting from both preventative and corrective support actions.*

References

[1] L.D. Alford, Jr., Cyber Attack: Protecting Military Systems, *Acquisition Review Quarterly*, **7**(2), (2000), 105.

[2] J. Bourque, The Language of Engagement and the Influence Objective, *The Journal of Electronic Defense*, **30**(1), (2007), 30–35, ISSN 192429X.

[3] Definition of Application Landscape, Software Engineering for Business Information Systems, Jan 21, 2009, retrieved January 14, 2011.

[4] B.S. Dhillon, *Mechanical Reliability: Theory, Models, and Applications*, AIAA Education Series, AIAA, Washington, DC, 1989.

[5] Z. Haig, Connections between cyber warfare and information operations, AARMS, **8**(2), (2009), 329–337.

[6] Institute for the Advanced Study of Information Warfare (IASIW), http://www.psycom.net/iwar.1.html

[7] L.M. Jessup and J.S. Valacich, *Information Systems Today*, 3rd ed., Pearson Publishing, 2008.